قرارگاه پدافند سایبری کشور

سازمان پدافند غیرعامل کشور

تهدیدات نوین سایبری
و روش های مصون سازی
زیرساخت های سایبری و وابسته به سایبر

هادی کریمی نیسیانی

معاونت فنی قرارگاه پدافند سایبری کشور

خرداد ۱۴۰۰

بسم الله الرحمن الرحیم

اگر مدیران کشور اهمیت این مسئله را درک نکنند و پدافند غیرعامل به طور شایسته توسعه پیدا نکند، کشور در معرض تهدیدهای بعضاً غیرقابل جبران قرار خواهد گرفت، بنابراین مسئولان بخش‌های مختلف کشور چه بخشهای نظامی و چه بخشهای غیرنظامی، باید با پدافند غیرعامل همکاری کامل و لازم انجام دهند.

بیانات رهبر معظم انقلاب اسلامی

در دیدار رئیس و مسئولان سازمان پدافند غیرعامل کشور

پدافند غیرعامل

- مجموعه‌ی اقدامات غیرمسلحانه که موجب بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیتهای ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات خصمانه می‌شود.
- بنابراین پدافندغیرعامل یعنی کاهش آسیب پذیری ها در مقابل تهدیدات کشور

تعاریف مراکز

- مراکز حیاتی

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تاثیرگذاری در سراسر کشور گردد.

- مراکز حساس

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تاثیر گذاری منطقه‌ای در کشور گردد.

- مراکز مهم

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز آسیب و صدمات محدود در نظام سیاسی، اجتماعی، دفاعی با سطح تاثیر گذاری محلی در کشور گردد.

مقدمه

- ابعاد و ویژگی های فضای سایبری کشور جمهوری اسلامی ایران و جذابیت هدف برای کشور های متخاصم
- تسلط و اشراف نسبی دشمنان کشور بر فضای سایبری و توان استفاده از آسیب پذیری های موجود درزیرساختهای حیاتی و حساس کشور

برآورد تهدیدات سایبری دشمنان جمهوری اسلامی ایران
(آمریکا، رژیم صهیونیستی و اذناب منطقه ای آنها)

- سازمان دهی یگان های عملیاتی تهاجمی و تدافعی در ساختار ارتش امریکا(تنها در فرماندهی سایبری، ۱۳۳ تیم به استعداد ۶۲۰۰ رزمنده سایبری به توانمندی عملیاتی رسیده اند.)
- سرمایه‌گذاری قابل ملاحظه آمریکا در ساخت تسلیحات سایبری به ویژه در NSA
- علاقه‌مندی به فعالیت در این فضا به دلیل برتری نسبی آمریکا در فضای سایبری
- وجود بسترهای لازم برای راه‌اندازی جنگ در فضای سایبری مانند:
  - شبکه اینترنت، تجهیزات کنترل صنعتی غیربومی در زیرساخت‌های حیاتی (مورد ونزوئلا)
- آسیب‌پذیری قابل توجه آمریکا در حوزه فیزیکی
  - قرارگیری پایگاه‌های هوایی امریکا در تیررس موشکی ایران انگیزه مضاعفی به آمریکا برای بهره‌گیری از تهدیدهای فضای سایبری می‌دهد.
- رویکرد امریکا به جنگ هیبریدی و تهدیدات ترکیبی (سایبری-نظامی، سایبری-فیزیکی، سایبری-شناختی، سایبری-اطلاعاتی)

شواهد و قرائن آرایش جنگی دشمن در فضای سایبری

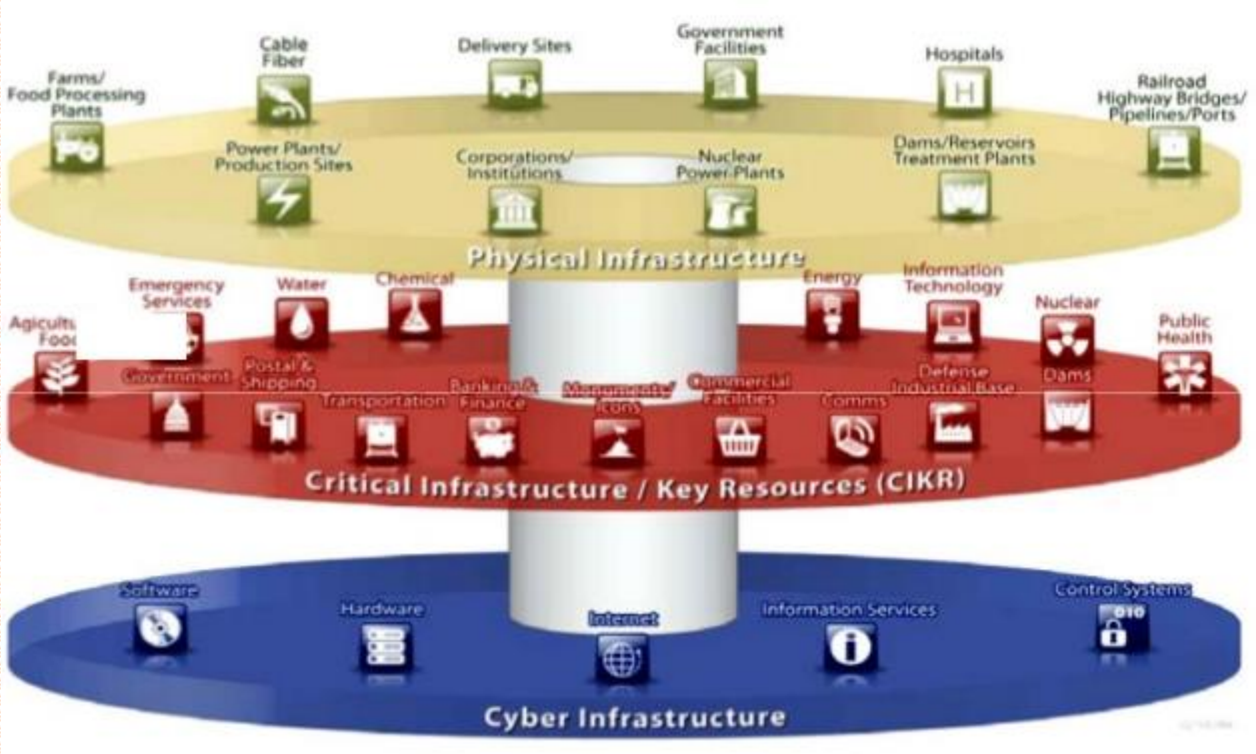
- سرمایه‌گذاری قابل ملاحظه دشمن در ساخت تسلیحات سایبری و علاقه‌مندی به فعالیت در این فضا به دلیل حفظ برتری نسبی آمریکا در فضای سایبری
- وجود بسترهای آماده برای راه‌اندازی جنگ در فضای سایبری مانند شبکه اینترنت، تجهیزات کنترل صنعتی غیربومی آسیب پذیر در زیرساخت‌های حیاتی
- تقویت شدید توان سایبری نیروهای نظامی آمریکا و هم پیمانان آن در منطقه
- رویکرد آفندی آمریکا در اسناد راهبردی سایبری جدید آن کشور
- افشای زرادخانه سلاحهای سایبری آژانس امنیت ملی آمریکا
- اذعان امریکایی ها به کاشت ایمپلنت های بدافزاری در زیرساخت های کشور در عملیات نیترو زئوس (شبکه دفاع هوایی، شبکه برق، شبکه ارتباطات، شبکه حمل و نقل)

مقدمه

نیاز به انجام اقدامات پیشگیرانه و پیش‌کنش‌گرانه جهت پایش و رصد تهدیدات و خنثی سازی آنها و کاهش و/ یا حذف آسیب پذیری ها با هدف مصون سازی زیرساخت های سایبری و وابسته به سایبر

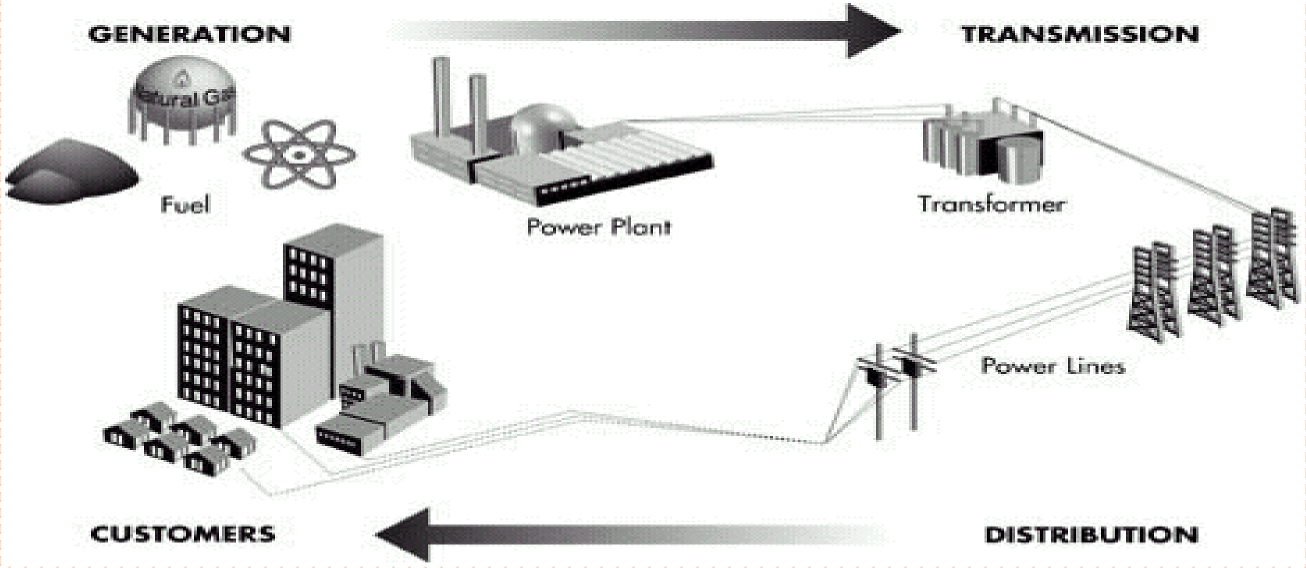
تعریف فضای سایبری

شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده (جاگذاری شده)، کنترل کننده های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات.



سرمایه ملی سایبری

سرمایه ملی سایبری، عبارت است از اطلاعات، فضای سایبری (محیط مجازی) که تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات در آن انجام می گیرد و اثر متقابل این محیط با انسان که نقش حیاتی در امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و باورهای دینی، ملی و قومی داشته باشد.



طیف تهدیدکنندگان سایبری

- دولت ها : ارتش های سایبری
- مزدوران سایبری (گروه های سازمان یافته پنهان دولتی)
- جاسوسان سایبری
- تروریست های سایبری
- مجرمین سازمان یافته سایبری
- هکرهای دارای انگیزه سیاسی

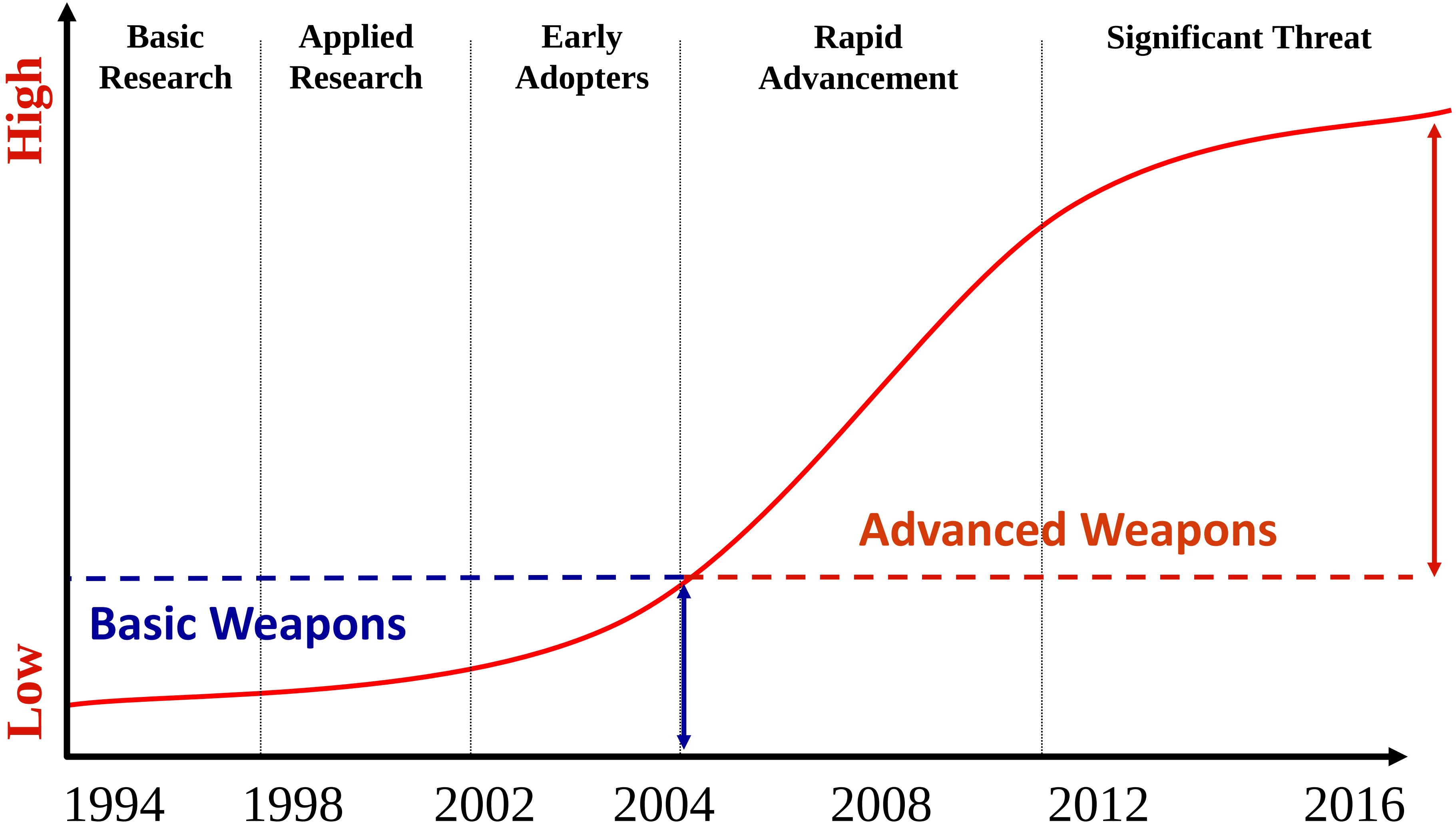
تهاجم سایبری

- به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات سرمایه سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می‌گردد.
- استفاده عمدی از یک سلاح سایبری (یا سامانه‌ای که بتواند به عنوان سلاح سایبری استفاده شود)، بر علیه یک سامانه اطلاعاتی، به شکلی که موجب بروز یک حادثه سایبری شود.

تسلیحات سایبری

- نرم‌افزار، میان‌افزار یا سخت‌افزاری است که برای ایجاد صدمه از طریق قلمرو سایبری، طراحی‌شده یا اعمال‌شده است.
- تفاوت اصلی یک سلاح سایبری با سایر انواع نرم‌افزار، میان‌افزار و سخت‌افزار، در بزرگ‌بودن (زیادبودن تعداد عناصر تشکیل‌دهنده)، پیچیدگی و وابستگی‌های متقابل زیاد بین عناصر تشکیل‌دهنده یک سلاح سایبری است.
- یک سلاح سایبری نیز باید بتواند در فضای سایبر دشمن که آلوده به انواع سازوکارهای تشخیصی و مختل‌کننده است، به‌سوی هدف سایبری خود پیش برود و اقدام به اعمال ممانعت (تنزّل، مختل یا منهدم) و یا دستکاری هدف نماید.

سیر تکاملی سلاح سایبری



اقتصاد اسلحه های جدید

هزینه یک فروند بمب افکن Stealth: $1.5 to $2 billion

هزینه یک فروند جنگنده Stealth: $80 to $120 million

هزینه یک فروند موشک Cruise: $1 to $2 million

هزینه یک سلاح سایبری: **$300 to $50,000**

تقسیم بندی انواع تسلیحات سایبری

توسعه دهندگان	شیوه انتشار و استقرار	روش انتشار خودکار داخلی (آلوده سازی)	ریخت شناسی	شیوه کاشت	شیوه کنترل	نوع هدف مورد هجمه	نحوه آسیب-رسانی

مفاهیم پایه و بنیادین در حفاظت از

زیرساخت های حیاتی سایبری

زیرساخت حیاتی (Critical Infrastructure)

زیرساخت‌های حیاتی و سرمایه‌های کلیدی، شامل زیرساخت‌ها و دارایی‌های است که برای امنیت، حاکمیت، بهداشت عمومی و ایمنی، اقتصاد و اعتماد عمومی حیاتی است.

زيرساخت حياتي سايبري
(Critical Cyber Infrastructure)

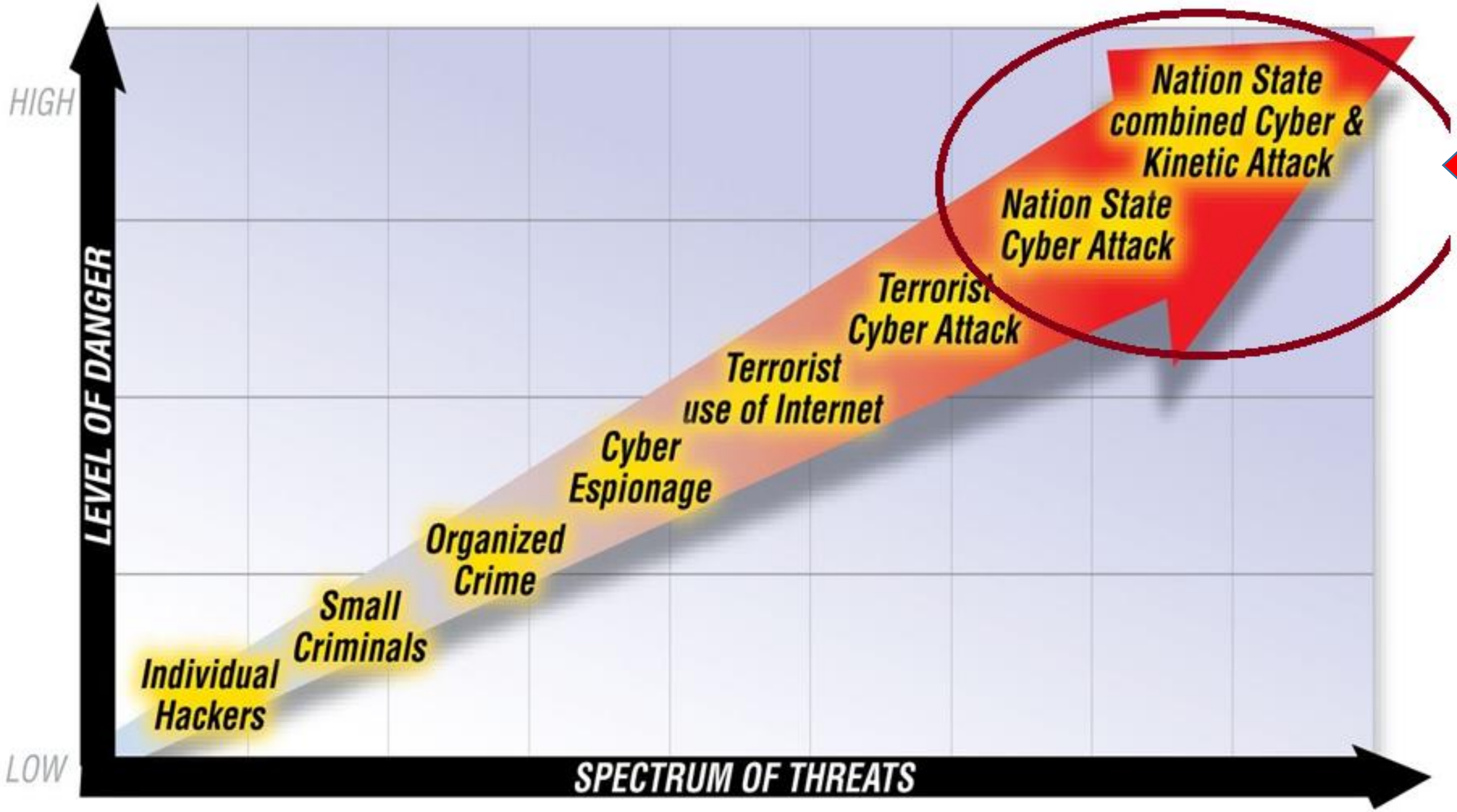
به زیرساخت‌های حیاتی و سرمایه‌های کلیدی سایبری یا زیرساخت سایبری زیرساخت‌های حیاتی و سرمایه‌های کلیدی غیرسایبری اطلاق می‌شود که برای امنیت، حاکمیت، بهداشت عمومی و ایمنی، اقتصاد و اعتماد عمومی حیاتی هستند.

زیرساخت‌های سایبری که برای ارائه خدمات حیاتی از منظر ایمنی عمومی، ثبات اقتصادی، امنیت ملی، ثبات بین‌المللی و برای پایداری و بازسازی فضای سایبر حیاتی ضروری هستند.

تهدید سایبری

- یک عامل خوف‌ناک که می‌تواند از یکی از طرق برقراری ارتباط یا احساس، از یک آسیب‌پذیری سایبری، بهره‌برداری کند.
- انواع تهدید سایبری که نظام دفاع سایبری کشورها با آن مواجه می‌باشند:
  - تهدید دولت یک کشور
  - تهدید غیردولتی
  - اشخاص حقیقی یا گروه‌های کوچک
  - حوادث و خطرات طبیعی

طیف کلی تهدیدات سایبری



طیف تهدیداتی که در حوزه موضوعات دفاع و پدافند سایبری تعلق دارد.

حفاظت از زیرساختهای حیاتی

زیرساخت های حیاتی را می توان به عنوان یک سیستم عصبی مرکزی در جامعه مدرن قلمداد کرد. خدمات این زیرساختها نه تنها نیازهای اساسی بلکه امنیت ملی و توسعه اقتصادی را نیز در بر می گیرد که از طریق حفاظت از زیرساخت های حیاتی به شهروندان آن ارائه می شود.

- حفاظت از زیرساخت های حیاتی اطمینان از عملکرد زیرساخت ها در هر شرایطی می باشد چرا که در مواقع اضطراری گستردگی شبکه زیرساختی باعث می گردد تعداد زیادی از مردم و مناطق قابل توجهی با روندی رو به رشد، تحت تأثیر قرار گیرند.

محافظت از زیرساخت حیاتي سایبری
(Cyber Critical Infrastructure Protection)

- **محافظت از زیرساخت حیاتی سایبری، مجموعه‌ای از اقداماتی است که برای جلوگیری، ترمیم یا درمان مخاطرات ناشی از آسیب‌پذیری دارایی‌های زیرساختی حیاتی انجام می‌شوند. بسته به مخاطره، این اقدامات می‌توانند شامل تغییرات در تاکتیک‌ها، تکنیک‌ها یا فرآیندها باشد. اضافه‌کردن افزونگی، انتخاب دارایی دیگر، ایزوله‌کردن و استحکام‌بخشی، نمونه‌هایی از اقدام‌های محافظتی است.**
- **محافظت از زیرساخت حیاتی و سرمایه کلیدی سایبری، متکی به تجزیه‌وتحلیل، هشدار، به‌اشتراک‌گذاری اطلاعات، مدیریت مخاطره، شناسایی آسیب‌پذیری و کاهش آن و کمک به تلاش‌های بازیابی ملی است.**

(Cyber Resilience) تاب آوری سایبری

- تاب‌آوری، توانایی تداوم یا بازگشت به عملیات عادی در صورت وقوع برخی از اختلال‌ها، اعم از طبیعی یا انسانی، و عمدی یا غیرعمدی است.
- برای تاب‌آوری سامانه‌های سایبری، باید برنامه‌های سامانه جایگزین، فرآیندهای اضطراری پشتیبان‌گیری و گزینه‌های پیکربندی جایگزین/راه‌اندازی مجدد وجود داشته باشد.

بازدارندگي سايبري (Cyber Deterrence)

- بازدارندگی، پیش‌گیری از اقدام غیرقابل پذیرش توسط یک تهدید موثّق و/یا باور به این نکته است که هزینه‌ی اقدام، بیش از مزایای قابل‌دریافت است.
- گزینه‌های بازدارنده، یک دوره اقدام است که براساس بهترین قضاوت‌های اقتصادی، دیپلماتیک و نظامی، به‌منظور دلسردکردن (منصرف‌کردن) یک دشمن از یک دوره اقدام جاری یا عملیات موردنظر (فکرشده)، طراحی‌شده است.

جنگ سایبری

- يك حمله سایبری است که توسط بازیگران دولتی علیه زیرساخت‌های سایبری، در ارتباط با یک اردوکشي دولتی انجام مي‌شود. جنگ (Warfare)، به اقدام‌ها یا تکنیک‌های انجام شده توسط یک یا هردو طرف تخاصم اشاره دارد.

شاخص های جنگ سایبری

تاثیر بر امنیت ملی	سلاح های مورد استفاده	شدت حمله	زیرساخت های مورد حمله	منشأ حمله

انواع جنک سایبری

- جنگ سایبری - ترکیبی
- جنگ سایبری- نظامی
- جنگ سایبری مردم محور مبتنی بر شبکه های اجتماعی
- جنگ سایبری – الکترونیک (رباتیک)

انواع جنگ سایبری

جنگ سایبری – ترکیبی

- استفاده از فضای سایبری به عنوان پیش مقدمه حملات نظامی به علت وجود وابستگی های زیاد زیرساخت ها به این فضا آن
- انجام عملیات روانی با از کارانداختن شبکه های اطلاع رسانی کشور هدف و راه اندازی شبکه های اجتماعی و رسانه های اطلاع رسانی توسط دشمن

انواع جنگ سایبری

جنگ سایبری- نظامی

- در این جنگ ها نه تنها نیاز چندانی به مهمات جنگی نیست بلکه تجهیزات و ادوات جنگی متعارف نیز متاثر از این فناوری است
- می توان جنگهایی را بدون شلیک حتی یک گلوله شکل داد و پیروز یا اینکه در کمک به سایر قوای نظامی متعارف تاثیر زیادی در پیروزی نیروهای عملیاتی عمل کننده داشت

انواع جنگ سایبری

جنگ سایبری مردم محور مبتنی بر شبکه های اجتماعی

- تهدیدات نرم یا تهدیدات و حملاتی که متوجه انسان های مرتبط با حوزه سایبر بویژه کاربران است؛ تغییر و تاثیر بر اذهان، ادراک، باورها، ارزش ها، حافظه و سیستم تصمیم گیری انسان هـا، از قبیـل مهندسـی اجتماعی(سوءاستفاده از اعتماد کاربر)، جنگ روانی و ...

- استفاده از مردم به عنوان پیاده نظام و هدایت و مدیریت افکار عمومی برای مواجه با حکومت

- سازماندهی و جریان سازی مردم در بستر شبکه های اجتماعی

- جایگزینی و تغییر انگاره های سنتی و دینی مردم با تزریق اطلاعات غلط و جعلی

انواع جنک سایبری

جنگ سایبری – الکترونیک (رباتیک)

- فصل مشترک اقدامات نظامی سایبری(کارکردی و عملیاتی) با طیف الکترومغناطیس و جنگ الکترونیک که امریکایی ها از آن بعنوان ابعاد سایبر الکترونیک نام می برند.
- استفاده از ربات های هوشمند برای اختلال و یا انهدام تجهیزات
- استفاده از امواج الکترومغناطیسی برای ارسال داده بر روی تجهیزات هدف که به صورت ایزوله و فاقد ارتباط با شبکه عمومی است.

جنگهای هیبریدی

استفاده از جنگ سایبری به عنوان مقدمه ای برای جنگ نظامی

- شروع حملات با حمله سایبری
- بهره گیری از فضای سایبری برای تاثیرگذاری بیشتر حملات در حوزه های سنتی
- ایجاد آشوب، بحران، ناامنی و اغتشاش با از کار انداختن زیرساخت های اساسی
- انجام عملیات روانی با از کارانداختن شبکه های اطلاع رسانی کشور هدف و راه اندازی شبکه های اجتماعی و رسانه های اطلاع رسانی توسط دشمن

نمونه های اخیر جنگ سایبری علیه زیرساخت های کشورها

نمونه ۴

تخریب سانتریفیوژهای سایت غنی سازی شهید احمدی روشن (نطنز) به وسیله بدافزار استاکس نت

نمونه ۳

فلج سازی سراسری دولت در کشور گرجستان با حمله سایبری قبل از شروع تهاجم نظامی

نمونه ۲

قطع سراسری برق در کشور اوکراین با حمله سایبری

نمونه ۱

قطع سراسری برق در کشور ونزوئلا با حمله سایبری

سناریوهای محتمل جنگ سایبری دشمن علیه ج.ا.ایران

- جنگ سایبری به صورت یک سناریوی منفرد
- جنگ سایبری به عنوان مقدمه جنگ نظامی
- جنگ رسانه های اجتماعی در قالب جنگ نوین
- جنگ شناختی (عملیات روانی + شبکه سازی در حوزه مردم)
- جنگ ترکیبی : تلفیقی از ابزارهای جنگ متعارف و غیرمتعارف شامل (جنگ منظم، جنگ نامنظم، جنگ اطلاعات، جنگ سایبری، جنگ اقتصادی، دیپلماسی، حمایت از ناآرامی های محلی و عملیات ویژه)

۱۶ بخش اصلی زیرساختهای حیاتی
در هر کشور

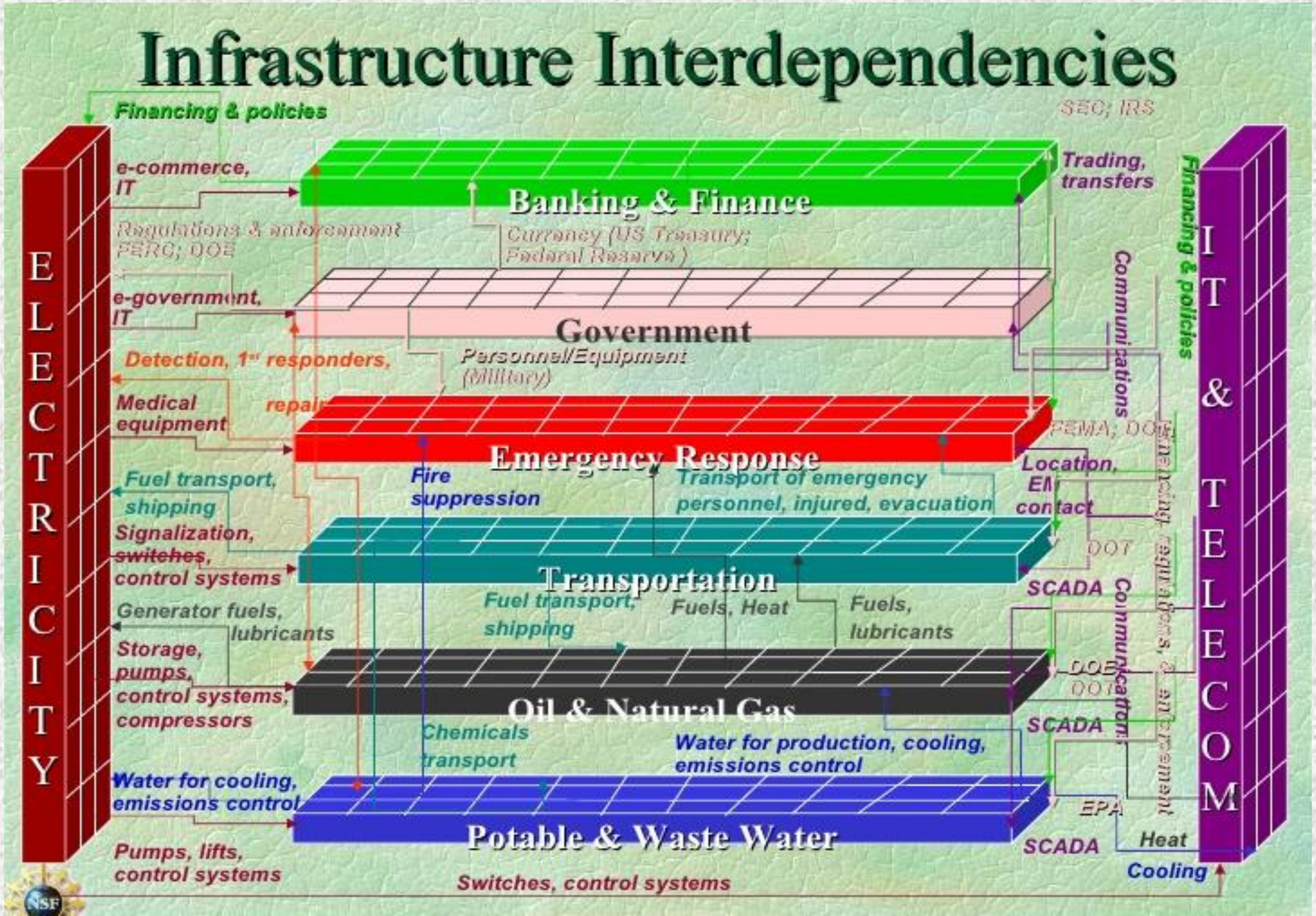
وابستگی متقابل زیرساخت ها

Infrastructure Interdependencies

وابستگی متقابل زیرساخت ها به رابطه‌ای میان زیرساختها گفته می‌شود که در آن یک زیرساخت نسبت به زیرساختی دیگر وابستگی دارد (وابستگی یک طرفه یا دوطرفه) و درصورت بروز حادثه ای برای زیرساخت مادر، سایر زیرساخت ها دچار وقفه و یا از کار افتادگی خواهند شد. مانند زیرساخت مخابرات که برای ادامه فعالیت به زیرساخت برق وابسته است.

وابستگی متقابل زیرساخت ها

Infrastructure Interdependencies



پدافند سایبری

پدافند سایبری، بهره‌گیری از کلیه امکانات سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به فضای سایبری و سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری،اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم، گروه‌های تحت حمایت پنهان دولت‌های متخاصم، جاسوسان سایبری، تروریسم‌های سایبری، مجرمین سازمان‌یافته سایبری، هکرهای دارای انگیزه سیاسی و سایر منشاءهای تهدید مطرح شده و رسیدگی فوری و موثر به منشاء و کلیه پیامدهای ناشی از تهاجم سایبری اعم از حوادث سایبری، آسیب‌پذیری‌ها، سلاح‌های سایبری و اقدام قانونی علیه منشاء تهاجم سایبری می‌باشد به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین، سلب نماید.

اقدامات پدافند سایبری سایر کشورها

- تشکیل فرماندهی سایبری توسط امریکا با هدف انجام عملیات آفندی و پدافنــدی در ارتــش امریکا و در سطح کلیه نیروهای ارتش
- تشکیل یگان های تخصصی عملیات سایبری در امریکا جهت انجام عملیات تخصصیِ سایبری متشـــــــــکل از تخصـــــــــص ســــــــــایبر و حـــــــــوزه تخصصـــــــــی مربوطـــــــــه (نیروگاه ها، پالایشگاه ها، تاسیسات هسته ای، ارتباطی، بانکی و ....)
- تشکیل یگان های سایبر در اکثر کشورها بویژه : ناتو، انگلیس، ترکیه، رژیم صهیونیستی
- اجرای مانورهای مختلف سایبری در مقاطع مختلف

Reactive Defense

Proactive Defense

Predictive Defense

انواع دفاع در فضای سایبر

Reactive (Past)	Proactive (Present)	Predictive (Future)
Respond to Incidents and accidents that have already happened	***Actively seek identification of hazardous conditions through analysis of organization's processes***	***Analyze system processes and environment to identify potential future problems***

قرارگاه پدافند سایبری کشور

از سال ۱۳۹۰ به منظور مقابله با تهدیدات سایبری دشمن و امن سازی زیرساخت های سایبری کشور، قرارگاه پدافند سایبری کشور توسط سازمان پدافند غیر عامل کشور و با هدف راهبری و هدایت دستگاه های اجرایی کشور جهت این امر مهم تشکیل گردید.

قرارگاه پدافند سایبری کشور

براساس ابلاغیه قرارگاه پدافند سایبری، کلیه دستگاه های اجرایی کشـــور، پس از تعیین سطح اهمیت سرمایه های سایبری خود، موظف به امن سازی زیرساخت های حیاتی، حساس و مهم ســـایبری خـــود بـــوده و بـــه منظـــور آمادگی جهت مقابله با حملات سایبری دشـــمن، نســـبت بـــه ایجـــاد مراکـــز پدافند سایبری در سطح وزارتخانه ها، سازمان ها، استان ها و مناطق ویـــژه اقدام نمایند.

کارکردهای اصلی پدافند سایبری

- کاهش آسیب پذیری زیرساختهای سایبری
- افزایش پایداری و تولید قدرت در حوزه سایبری
- تداوم فعالیتهای ضروری سایبری کشور
- ارتقاء پایداری ملی زیرساختهای سایبری کشور
- گسترش تولید داخلی و بومی سازی سامانه های مبتنی بر حوزه سایبر
- تسهیل مدیریت بحران در زیرساختهای سایبری کشور

چرخه پدافند سایبری

تهدیدات نوین سایبری علیه

زیرساخت های

حیاتی و حساس

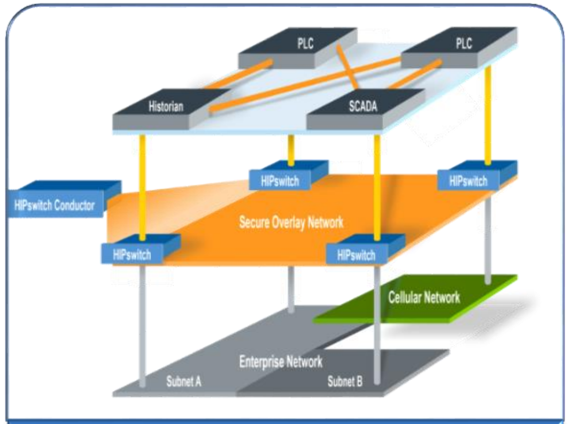
تعاریف

مخاطره سایبری
(Risk)

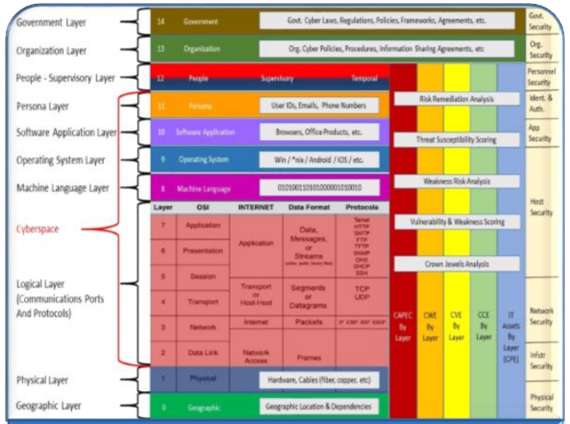
تهدید سایبری
(Threat)

آسیب پذیری
سایبری
(Vulnerability)

زیرساختهای حیاتی و فضای سایبر



کاربرد ارتباطات و فناوری اطلاعات در زیرساختهای حیاتی



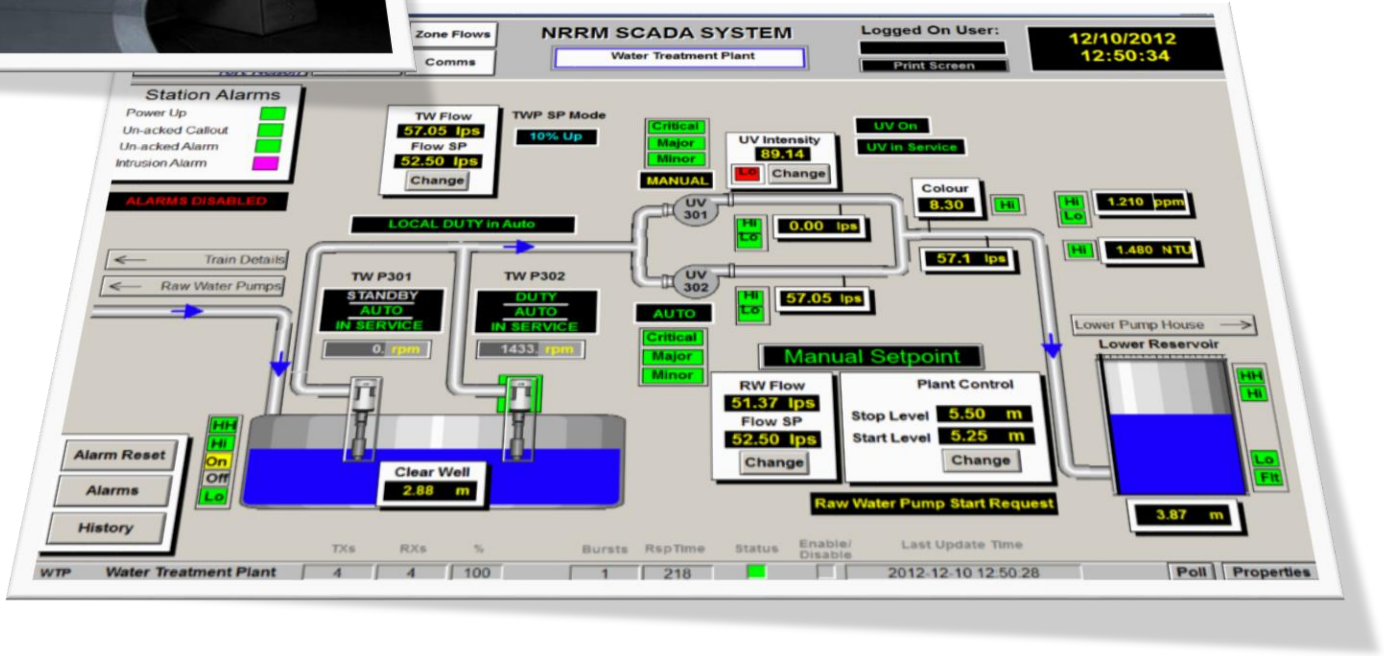
فضای سایبر در زیرساختهای حیاتی

رشد و گسترش روز افزون ICT در زندگی امروز

- رشد و گسترش ارتباطات و فناوری اطلاعات
- بکارگیری زیرساختهای نرم افزاری و نرم افزارهای کاربردی
- استفاده از تکنولوژیهای شبکه ای و تبادل داده ها
- سامانه های کنترل متمرکز و جمع آوری داده ها
- سامانه های مرتبط با فناوری محاسبات ابری
- نرم افزارهای کاربردی با قابلیت کار با داده های حجیم

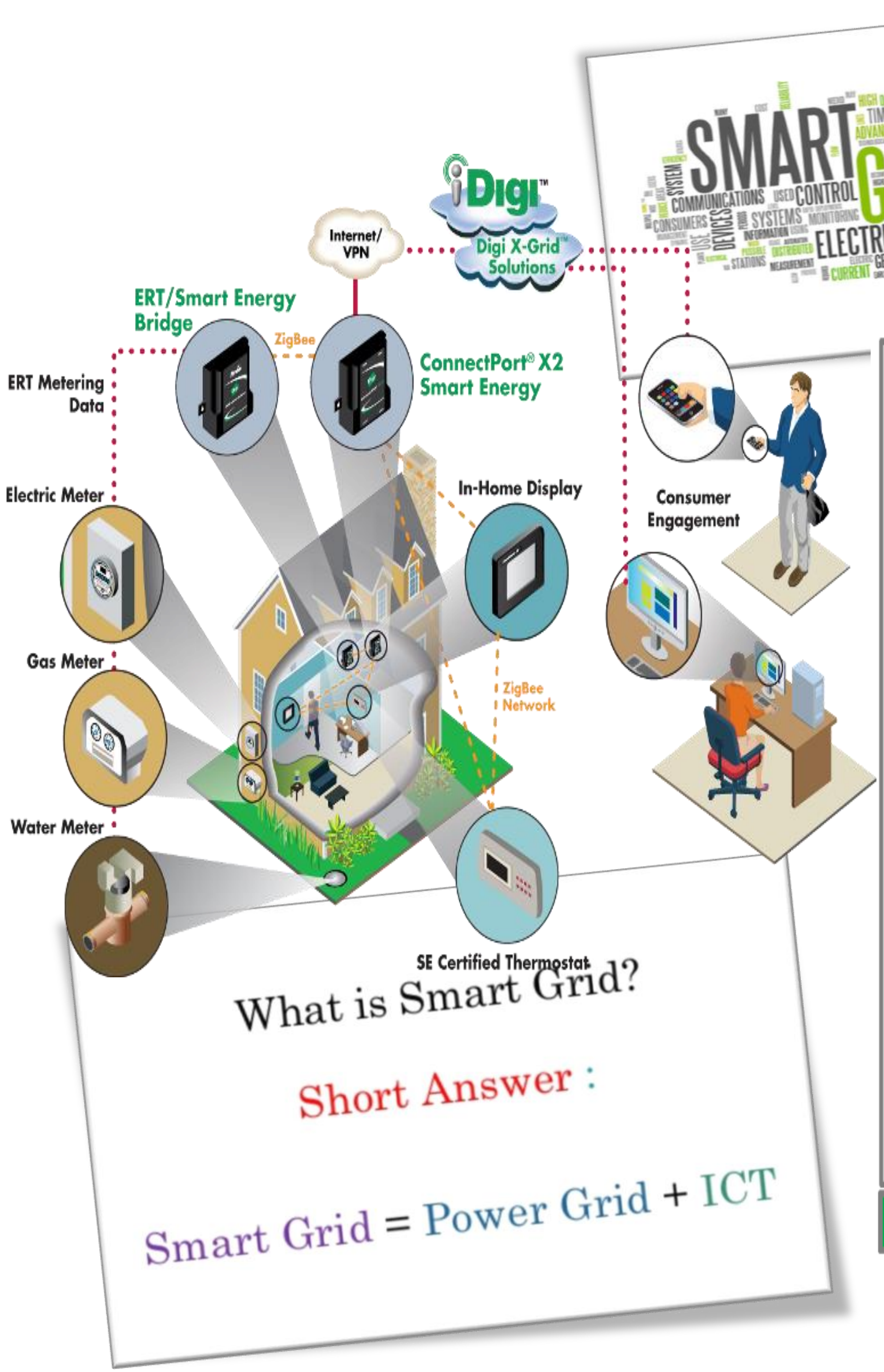
مثال ۱:

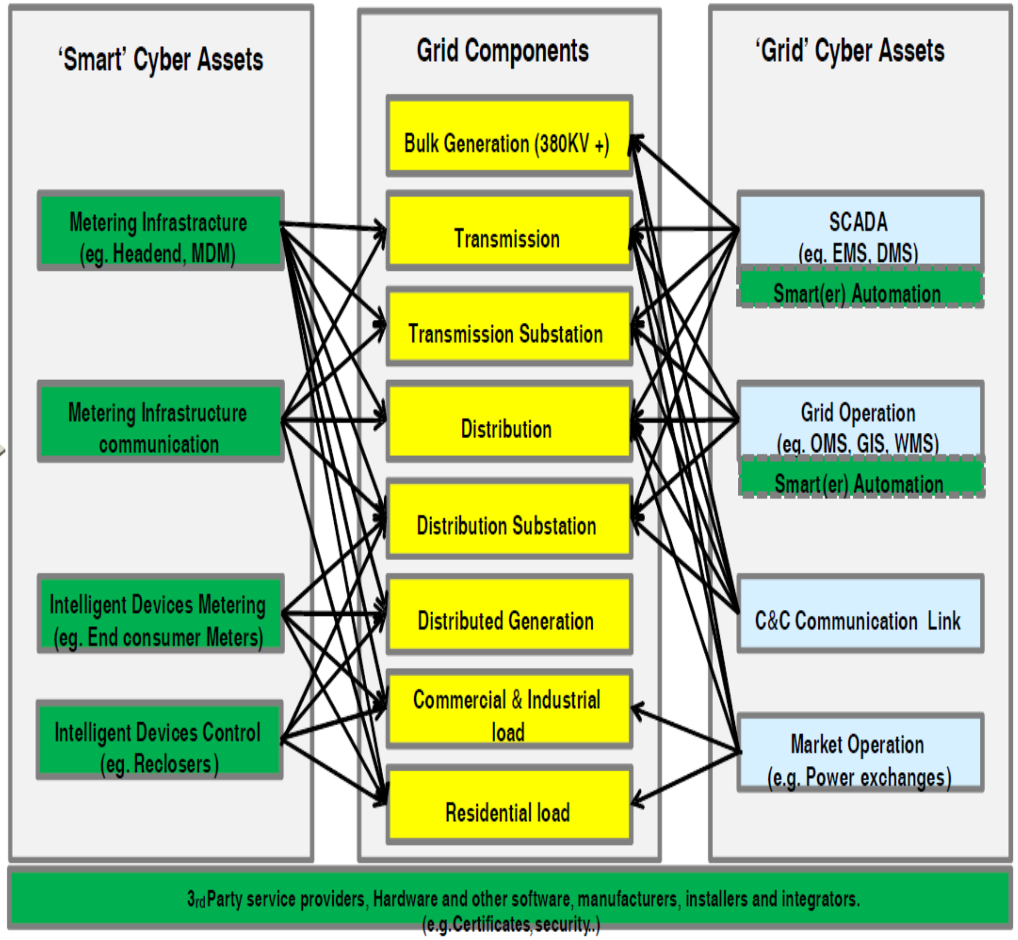
سامانه های کنترل متمرکز و جمع آوری داده ها



مثال ۲ :

شبکه های هوشمند برق
SMART GRID

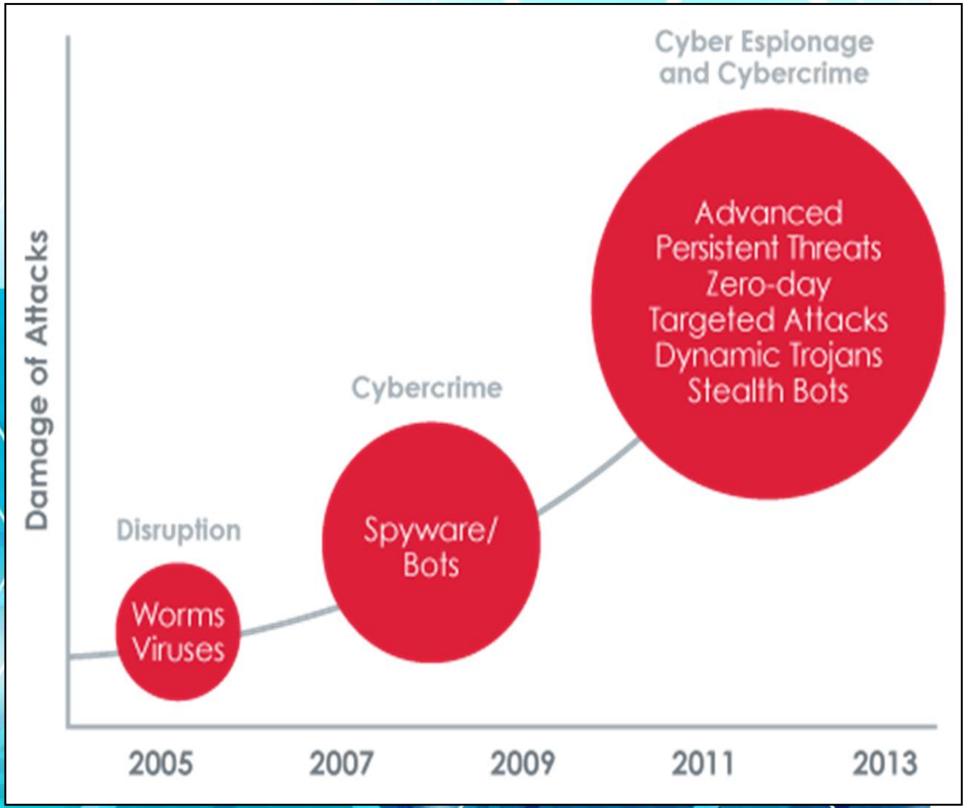




▪ تغییر نوع و ماهیت ... مان

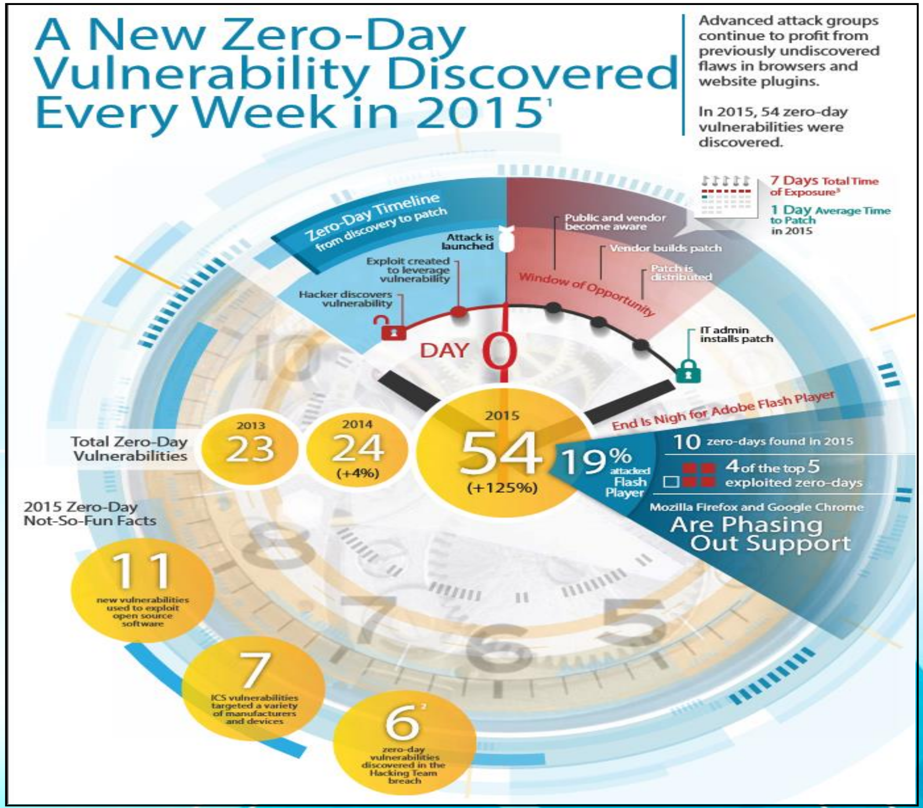
دسته بندی انواع حملات سایبری جدید

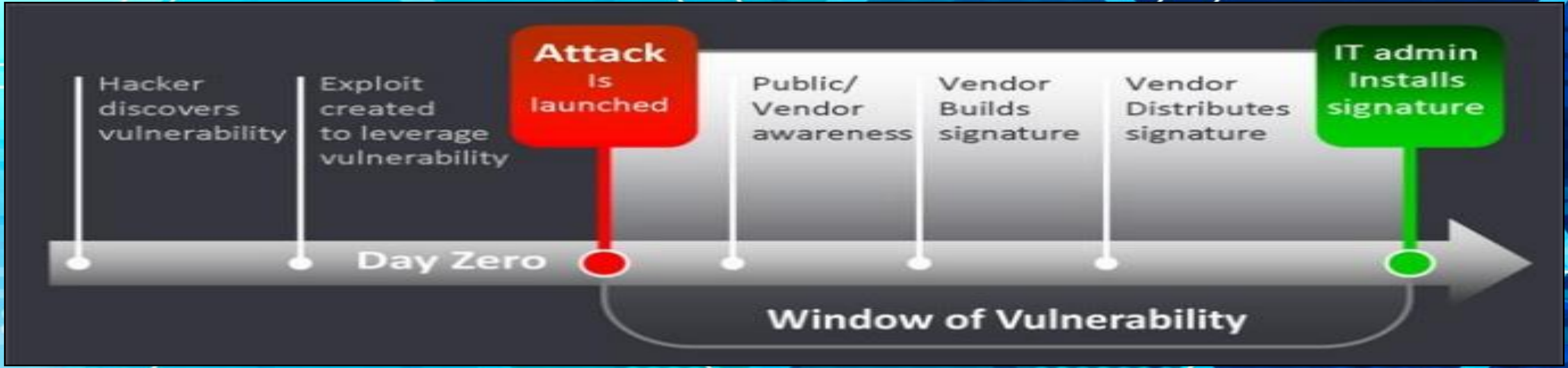
- Zero-day Attacks
- Botnet (zombie army)
- AET (Advanced Evasion Technique)
- APT (Advanced Persistent Threat)



Zero-day Attacks

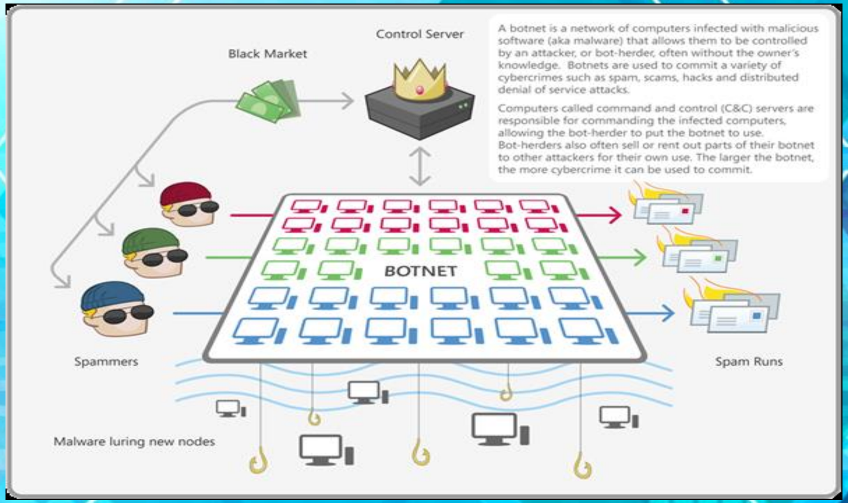
حملات ناشناخته (آسیب پذیری ناشناخته)
عدم شناسایی توسط آنتی ویروسها
نحوه انتشار
phishing
drive-by (dropper)
USB, etc.

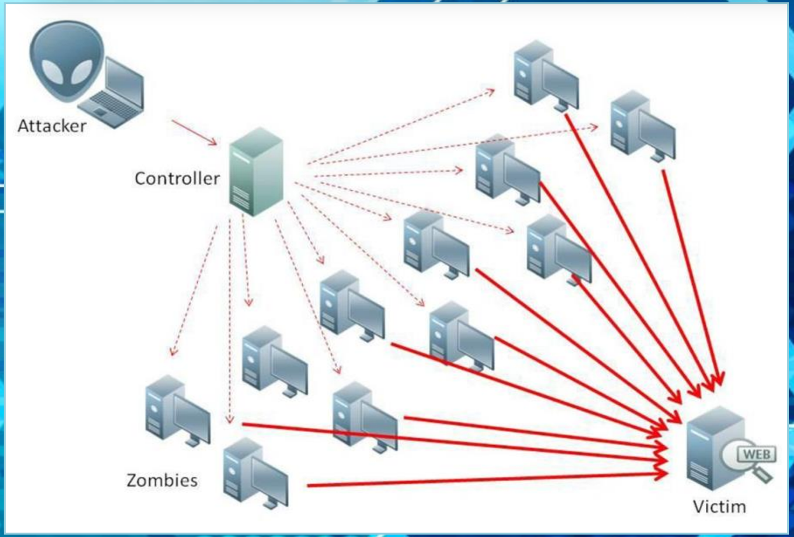


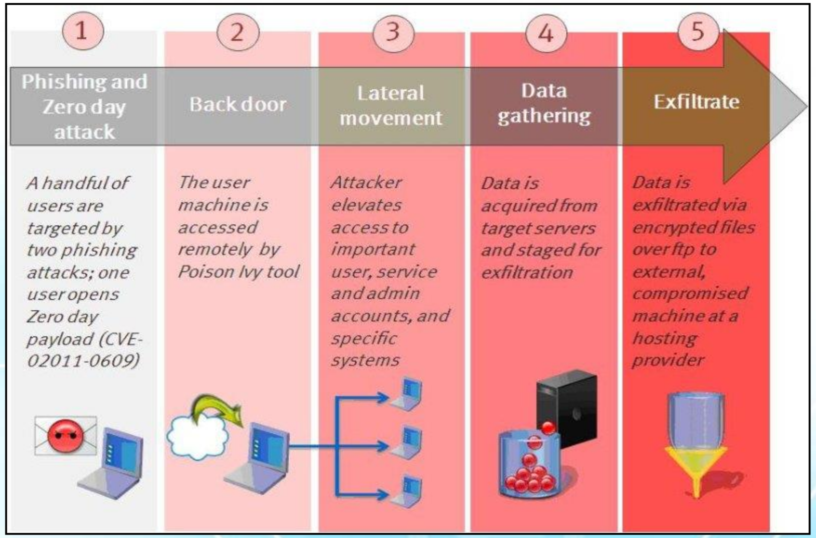


Botnet (zombie army)

- شبکه ای از کامپیوترهای هک شده
- بصورت روبات عمل می کنند
- کنترل باتها از طریق IRC/http
- کنترل مرکزی توسط C&C
- آلودگی توسط اسبهای تروا/rootkitها







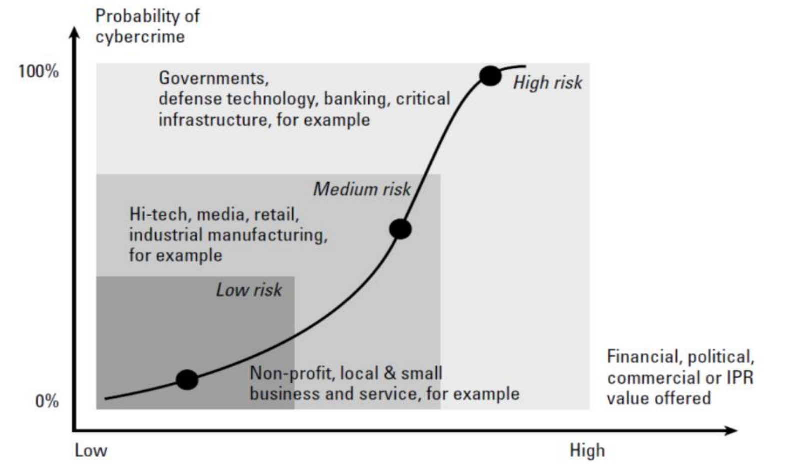


Figure 3-1: How the onslaught of advanced threats affects different industries.

APT (Advanced Persistent Threat)

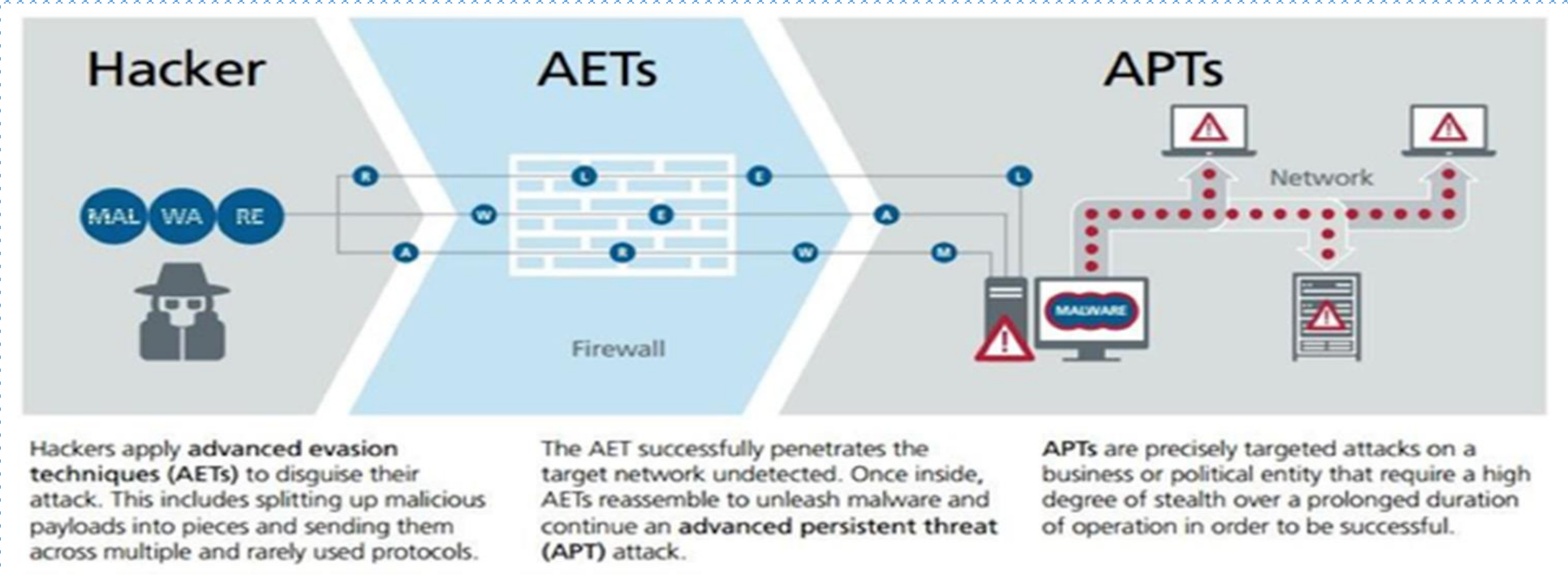
Advanced : بهره گیری از تکنولوژیهای بسیار پیشرفته و استفاده از آسیب پذیریهای شناخته و ناشناخته

Persistent: مداوم و مرتب در حال تغییر هستند (Polymorphic)، پویا، گریز از دفاع نوع Signature (AV, IDS, …)

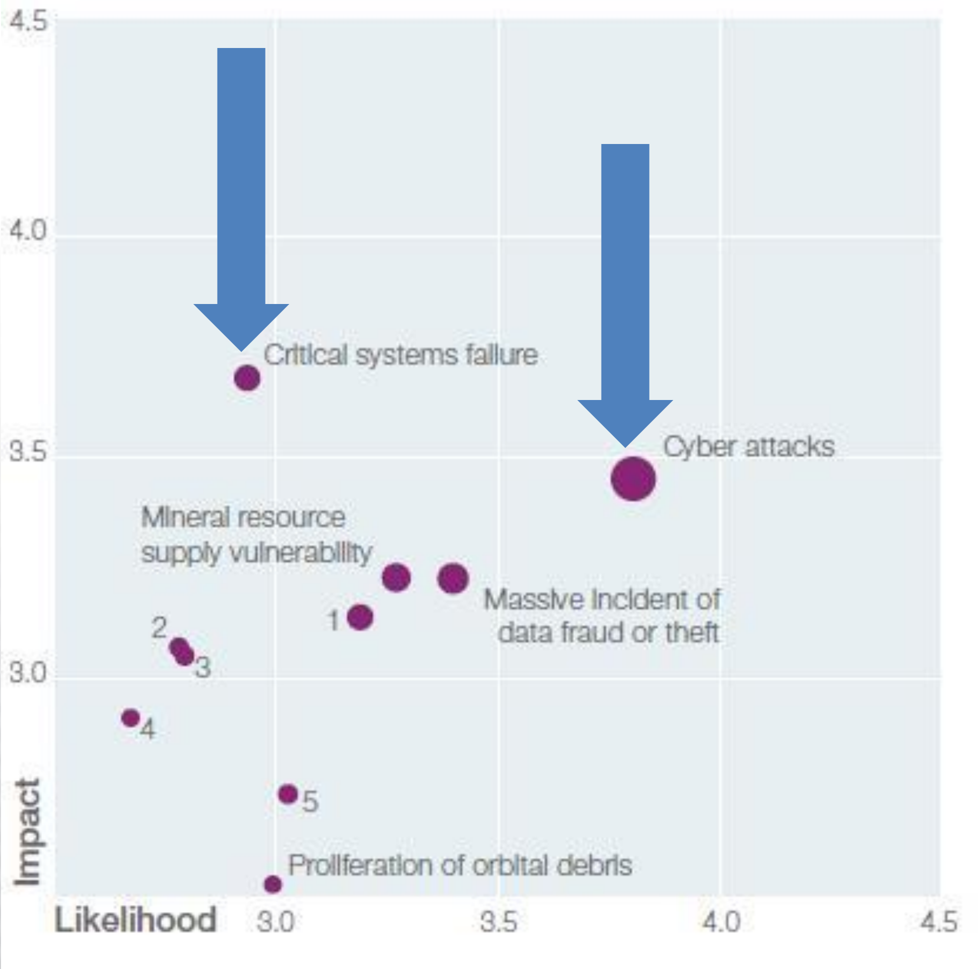
Threats: دنبال هدف خاصی هستند، فرصت طلب نیستند!

AET (Advanced Evasion Technique)

- مبتنی بر ترکیب تکنیک ها و روشهای متعدد حمله جهت خلق یک روش جدید و منحصر به فرد حمله سایبری جهت گریز از لایه های متنوع دفاعی
- کدهای AET به خودی خود ممکن است تهدید جدی تلقی نشوند ولی برای یک حمله همه جانبه طرح ریزی شده باشند
- روش مورد استفاده حمله کنندگان بسیار حرفه ای در تهاجمات وسیع
- بسیار پویا و غیر قابل تشخیص توسط لایه های متعدد امنیتی
- به عبارت دیگر کدهای AET می تواند به عنوان بی اثر کننده لایه های متعدد امنیتی یک سازمان به کار رود

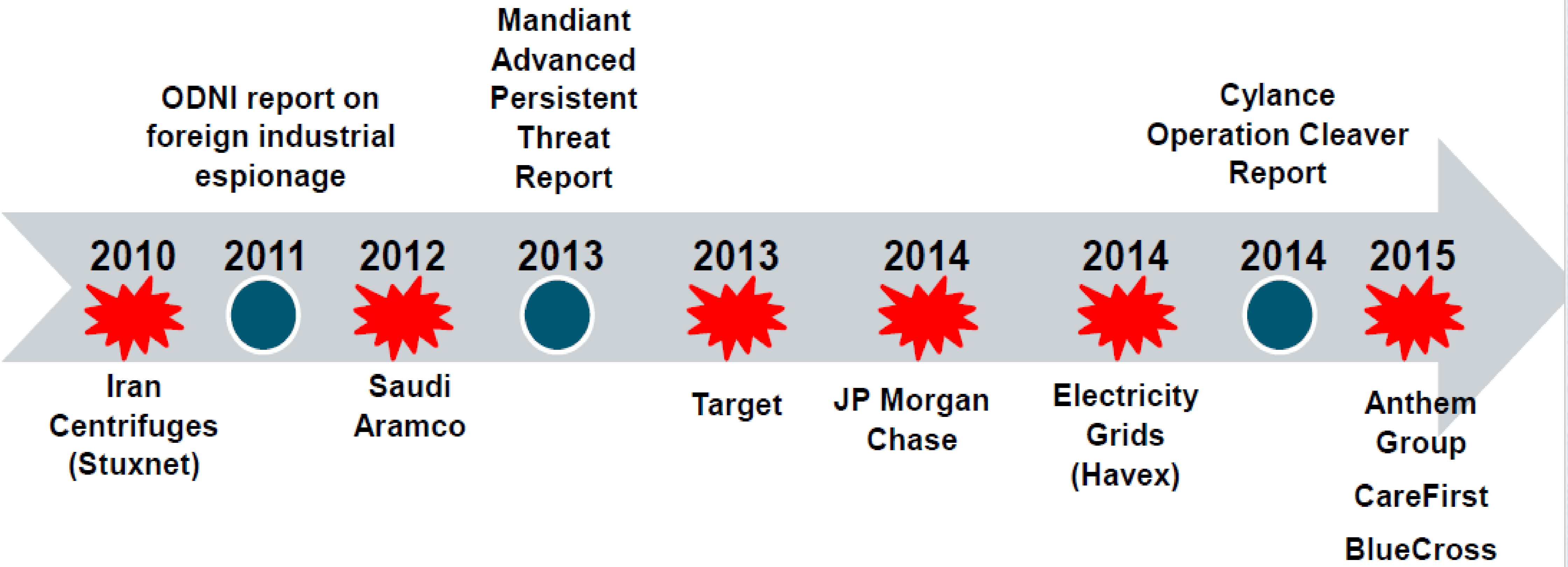


احتمال وقوع حملات سایبری نوین چقدر است؟



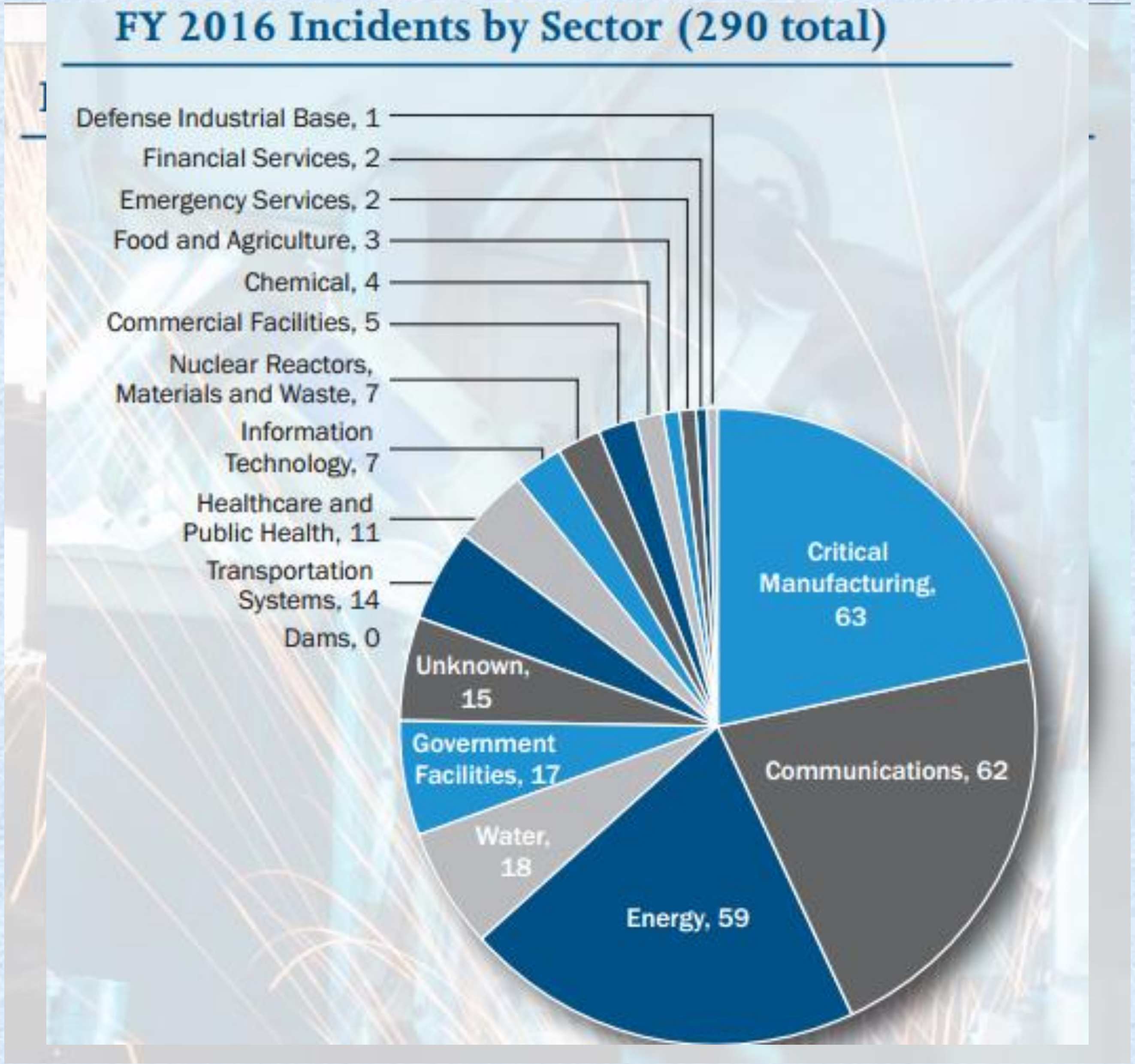
چشم انداز خطرات فناوری های جهانی و تاثیر بالقوه ی آن ها در ۱۰ سال آینده نشان می دهد که خطرات ناشی از توقف ارایه خدمات حیاتی بیشترین اثر و حملات سایبری بیشترین احتمال وقوع را دارند.

Everyone is a target, including energy companies



ICS-CERT

Industrial Control Systems Cyber Emergency Response Team



	Country*	% of systems attacked
1	Vietnam	71.0
2	Algeria	67.1
3	Morocco	65.4
4	Indonesia	58.7
5	China	57.1
6	India	56.0
7	Iran	55.3
8	Saudi Arabia	51.8
9	Egypt	51.6
10	Peru	50.8
11	Thailand	47.8
12	Malaysia	47.2
13	Ukraine	46.3
14	Portugal	46.1
15	Kazakhstan	45.9

Kaspersky-2017

TOP 10 countries by share of users attacked by mobile malware:

	Country*	%**
1	Bangladesh	31.17
2	China	31.07
3	Iran	30.87
4	Nepal	30.74
5	Nigeria	25.66
6	India	25.04
7	Indonesia	24.05
8	Ivory Coast	23.67
9	Pakistan	23.49
10	Tanzania	22.38

securelist.com - 2018

برخی از مهمترین حملات سایبری بر روی سامانه های کنترل صنعتی

- حمله سایبری رخ داده علیه نیروگاه برق هسته ای **Gundermmingen**آلمان (آپریل ۲۰۱۶)
- حمله سایبری به شبکه برق اکراین (ژانویه ۲۰۱۶)
- حمله سایبری علیه تاسیسات برق رژیم غاصب صهیونیستی (ژانویه ۲۰۱۶)
- حمله سایبری به صنعت فولاد آلمان (اکتبر ۲۰۱۴)
- حمله سایبری به سدی در آمریکا (۲۰۱۳)
- حمله سایبری به تاسیسات هسته ای ایران (۲۰۱۰)

برخی از مهمترین بد افزارهای منتج به حمله سایبری در دنیا

- استاکس نت
- Havex
- BlackEnergy
- PLC-Blaster
- Irongate

مفاهیم اساسی بدافزار

Basic Concepts Of Malware

بدافزار چیست؟

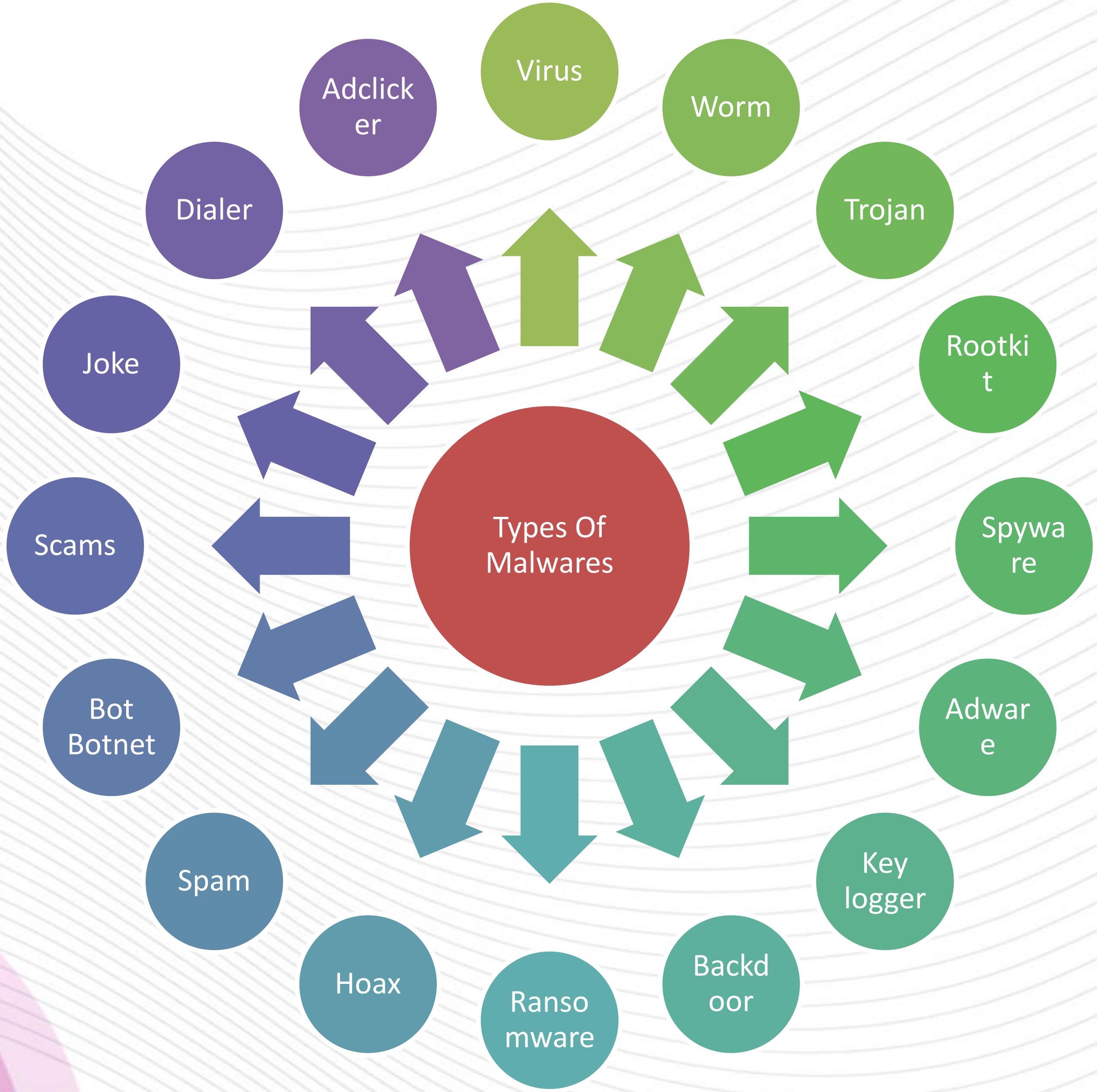
- بـدافــزار یک اصطلاح فراگیر و جامع است که به هر برنامه نرم افزاری اطلاق می شود که عمداً برای انجام اعمال غیرمجاز و گاهاً مضر ایجاد شده است

Malicious + Software = Malware

انواع بدافزار

TYPES OF MALWARES

انواع بدافزار
ویروس
کرم
تروجان
Rootkit
جاسوس افزار
ابزارهای تبلیغاتی
Key logger
درب پشتی
باج افزار
کلک
هرزنامه
Bot Botnet
فریب
جوک
شماره گیر
کلیک کننده

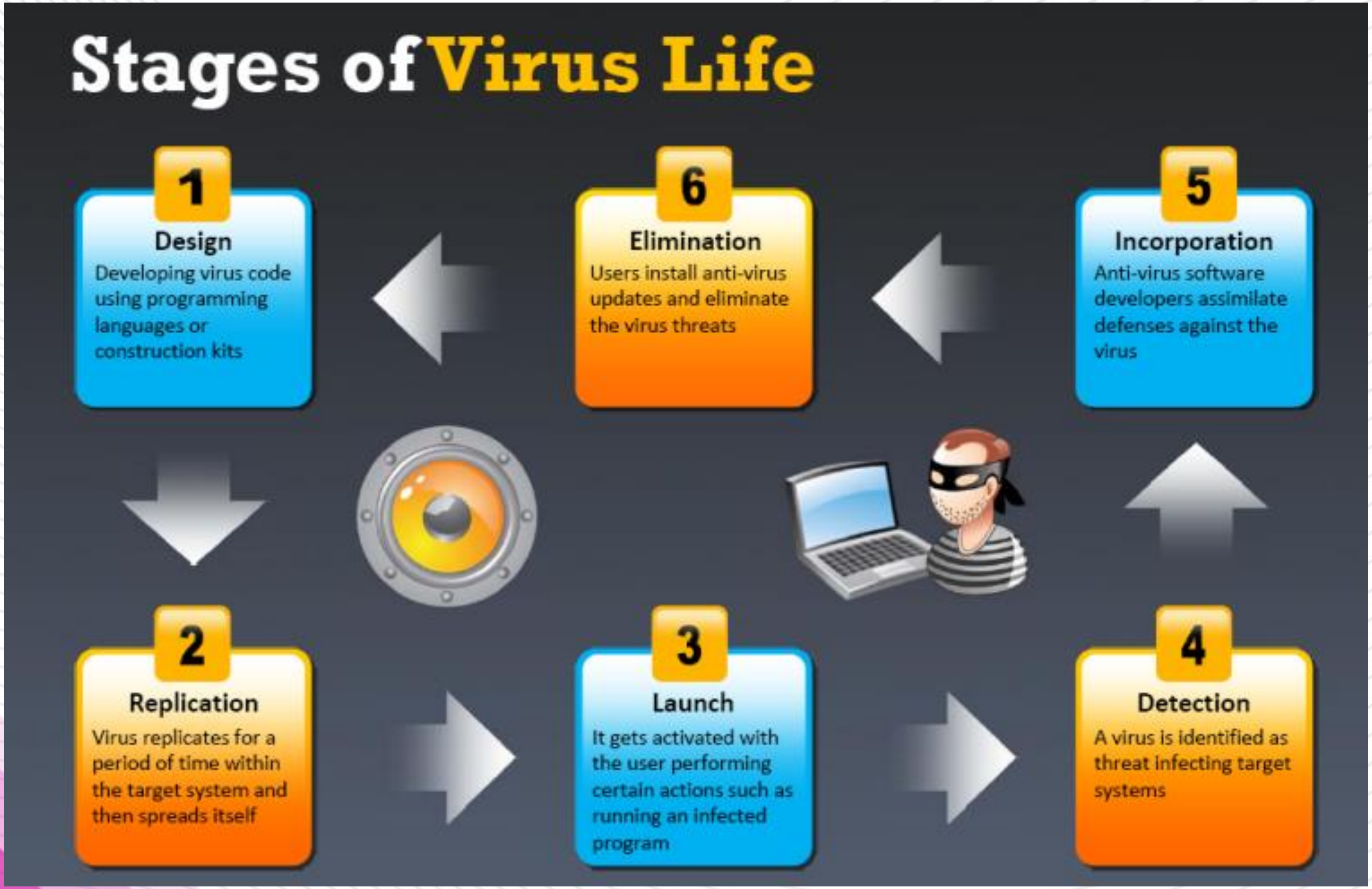

Types Of Malwares
Virus
Worm
Trojan
Rootki t
Spywa re
Adwar e
Key logger
Backd oor
Ranso mware
Hoax
Spam
Bot Botnet
Scams
Joke
Dialer
Adclick er

آشنایی بیشتر با بدافزارها

ویروس

- قطعه کدی است که برای تکثیر خودکار
- انتشار از طریق اتصال به یک برنامه میزبان
- زمانی که برنامه میزبان اجرا می شود، برنامه ویروس نیز اجرا می شود و برنامه های دیگری را نیز آلوده کرده و به عنوان میزبانهای جدید از آنها استفاده می کند
- ویروس مستقل نبوده و نیازمند میزبانی است که با استفاده از آن دست به عمل زند

ویژگی های ویروس



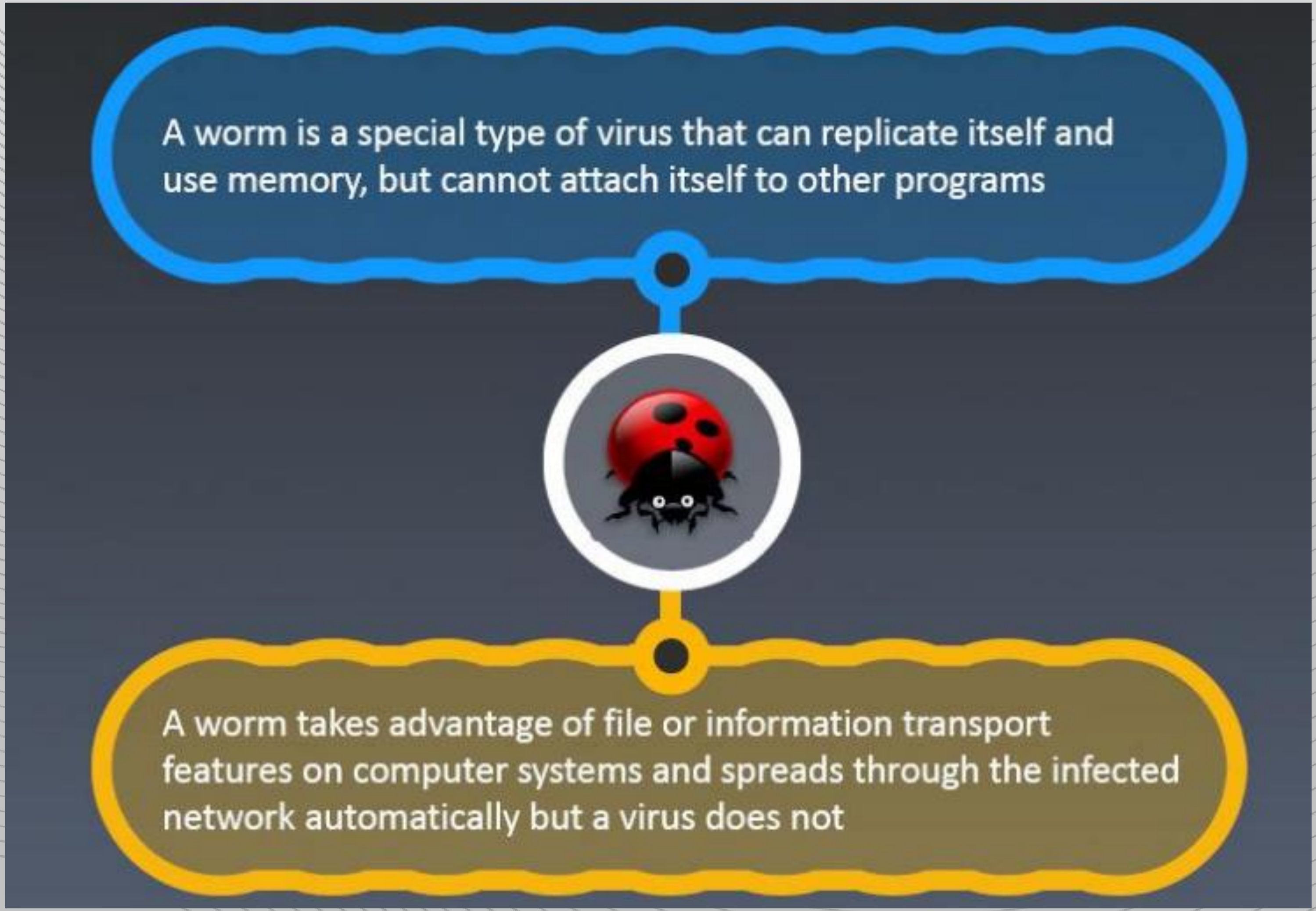
Stages of Virus Life
1
Design
Developing virus code using programming languages or construction kits
6
Elimination
Users install anti-virus updates and eliminate the virus threats
5
Incorporation
Anti-virus software developers assimilate defenses against the virus
2
Replication
Virus replicates for a period of time within the target system and then spreads itself
3
Launch
It gets activated with the user performing certain actions such as running an infected program
4
Detection
A virus is identified as threat infecting target systems

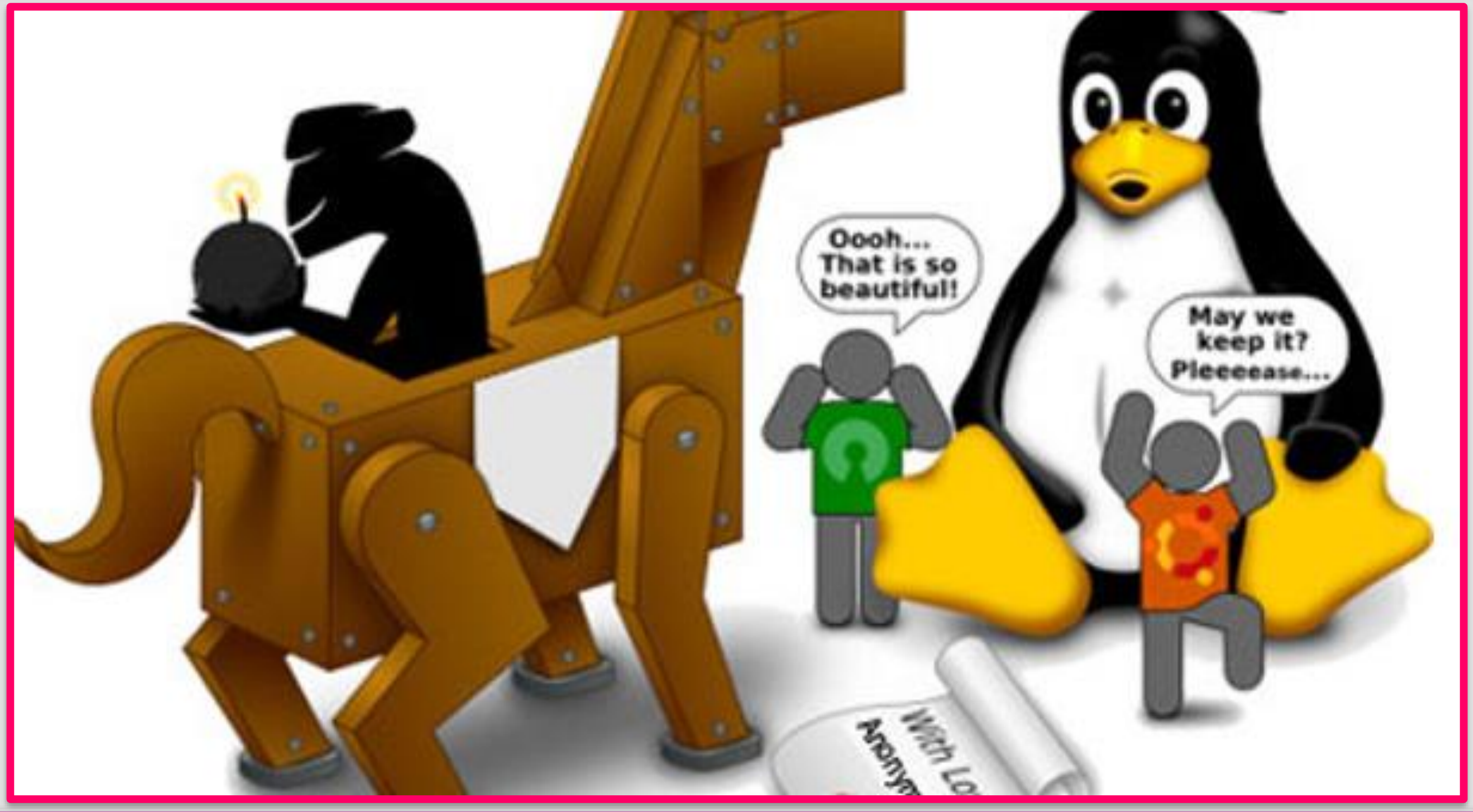
کرم

- یک کرم برنامه‌ی مستقلی است که معمولاً خود را با کپی کردن از یک رایانه به رایانه‌ی دیگر بر روی یک شبکه <u>تکثیر</u> می‌کند.
- کرم رایانه‌ای <u>استقلال خود را حفظ کرده</u> و نیازی به میزبان ندارد.
- برخی از کرمها می توانند بدون مداخله کاربر اجرا شده و گسترش پیدا کنند

یک کرم، کد خرابکاری است که خود را انتشار می دهد و قادر است به صورت خودکار در شبکه ها گسترش پیدا کند

تفاوت ویروس و کرم



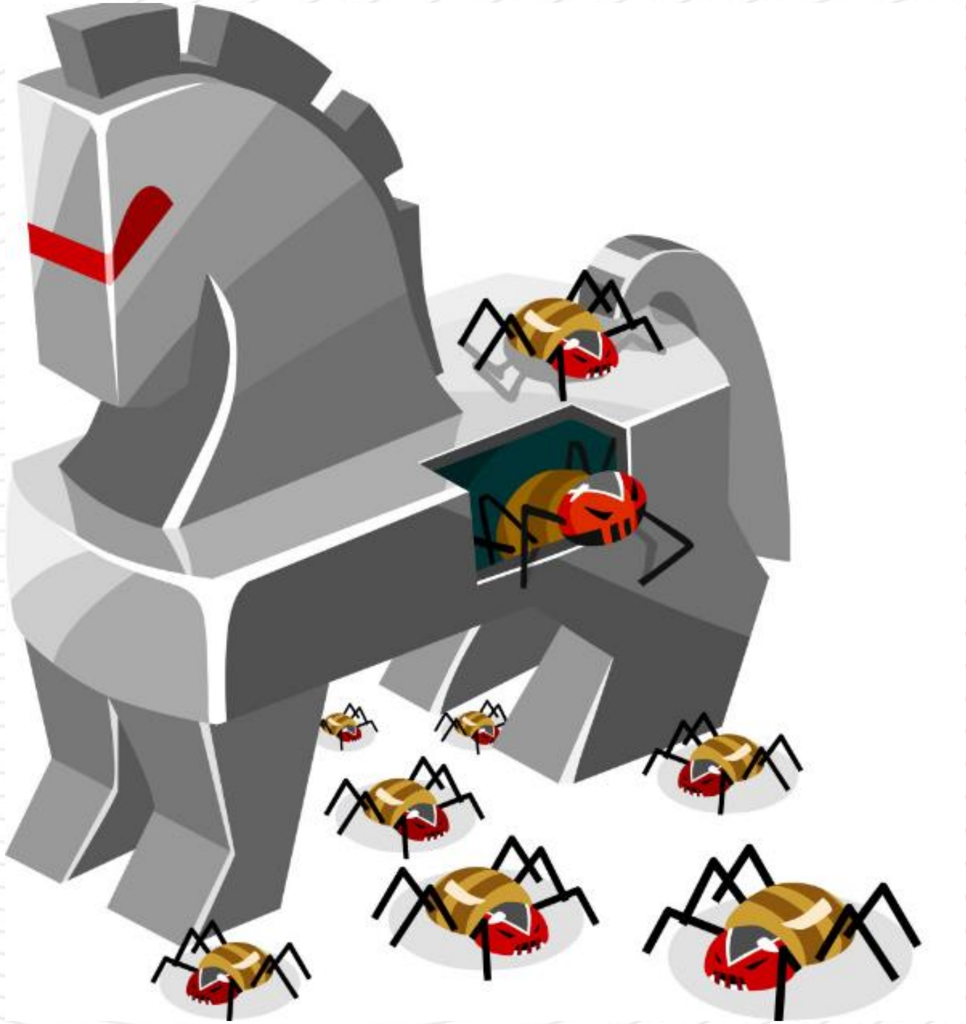


تروجان

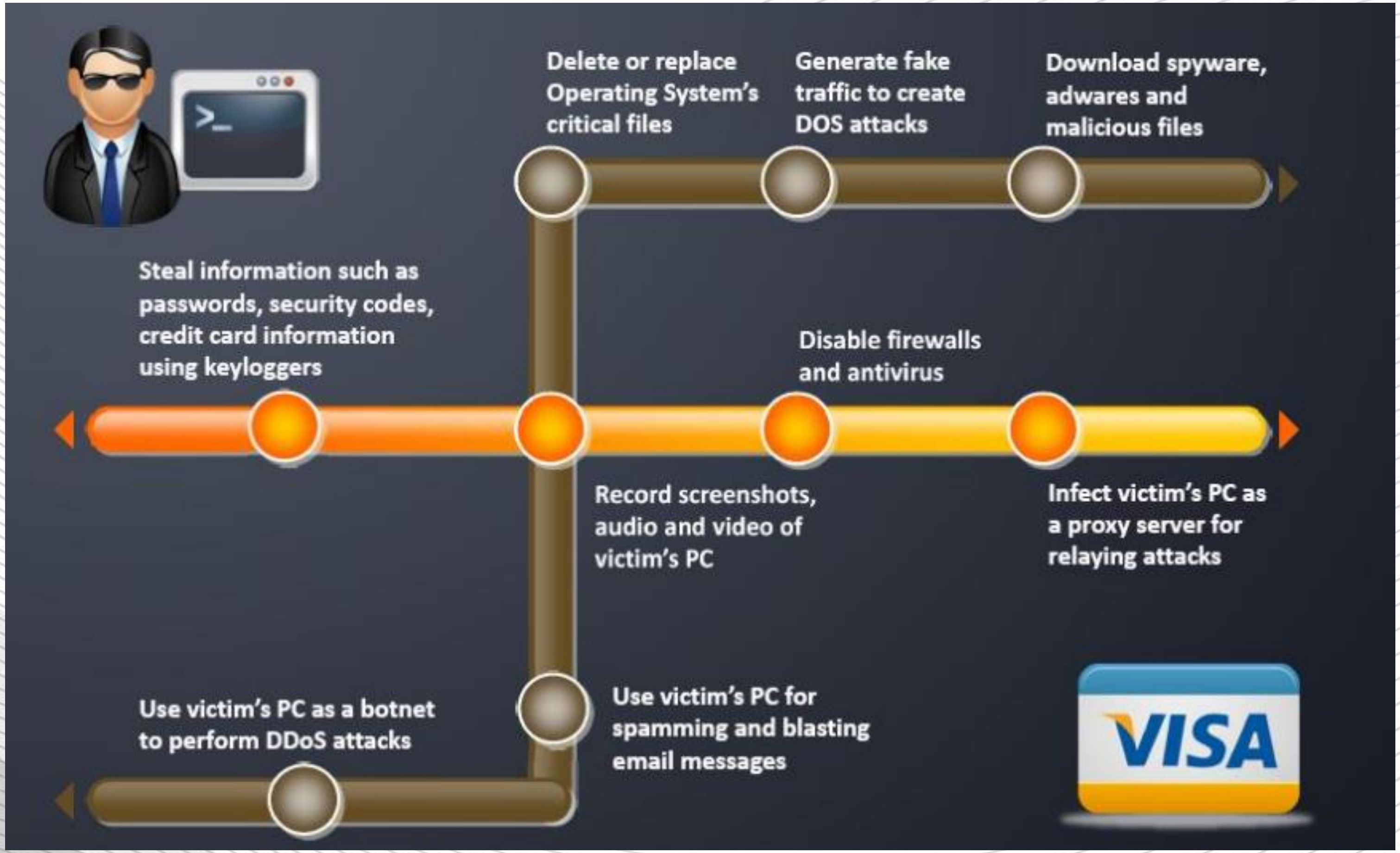
- برنامه ای است که ظاهراً مفید یا بی خطر به نظر می رسد ولی شامل کدهای پنهانی است که برای سوءاستفاده یا صدمه زدن به سیستمی که بر روی آن اجرا می شود، به کار می رود

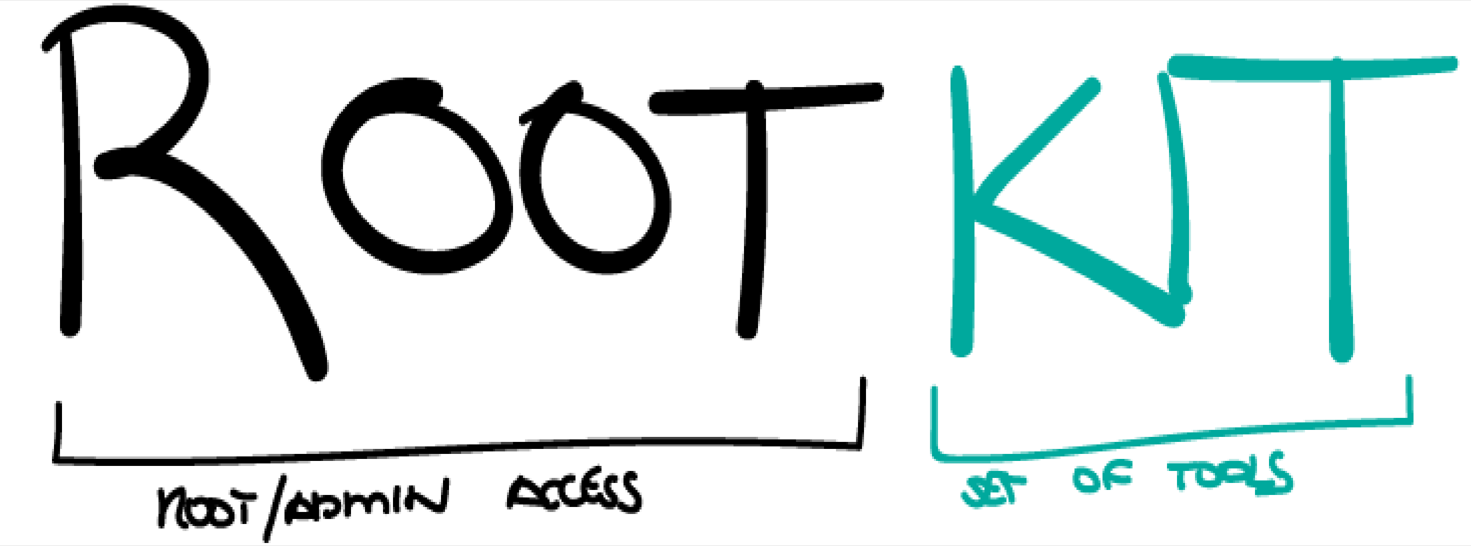
- تروجان تکه برنامه‌ای است که درون برنامه‌ی دیگری مخفی شده و عملیاتی را تحت پوشش برنامه‌ی مذکور انجام می‌دهد

در اسطوره های قدیمی، اسب تروا یک اسب توخالی ساخته شده از چوب است که توسط ادیسیوس، سردار سپاه یونان در جنگ با امپراطوری تروا مورد استفاده قرار گرفت. سربازان یونانی در این اسب مخفی شدند و زمانی که سربازان تروا آن را به داخل شهر آوردند، از آن خارج شده و دروازه‌های شهر را برای سربازان یونانی باز کردند و به این ترتیب در جنگ پیروز شدند



اهداف استفاده از تروجان

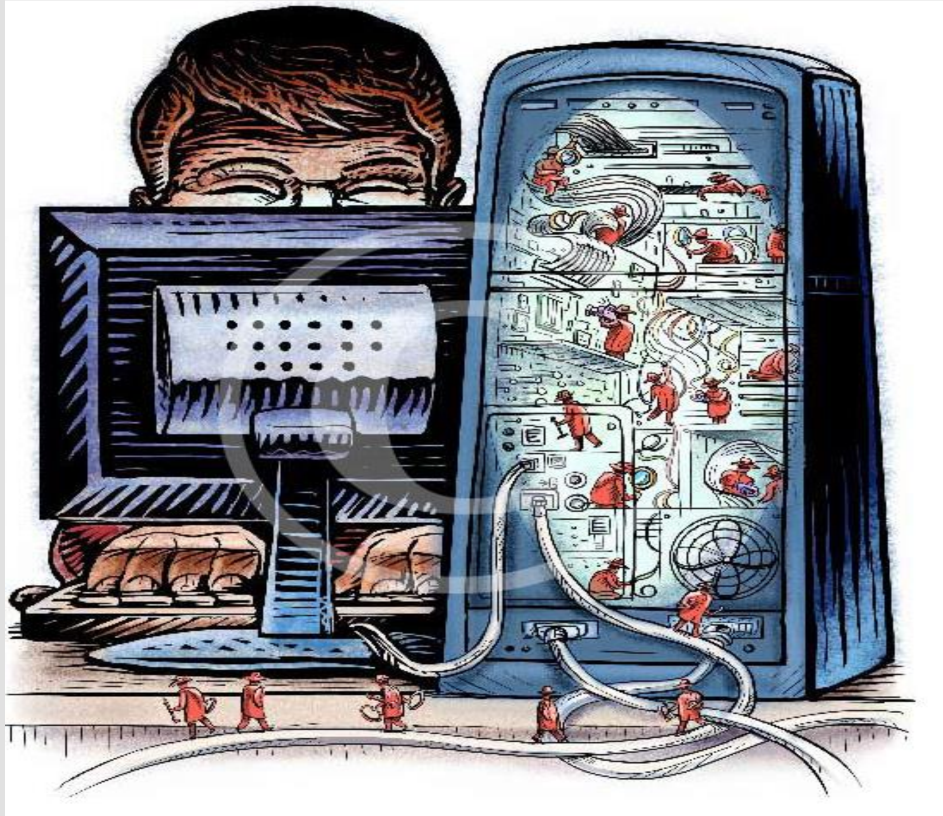




Rootkit

- این نرم افزار برای پنهان کردن این واقعیت که سیستم مورد سوء استفاده قرار گرفته است طراحی شده است
- استفاده از Rootkit برای جایگزین کردن فایلهای اجرایی حیاتی سیستم با فایلهای مورد نظر
- Rootkitها با گول زدن و فریب دادن بخش امنیتی سیستم عامل و مکانیزمهای امنیتی مانند آنتی ویروسها و ابزارهای ضد جاسوسی، وجود خود را انکار می‌کنند
- در اغلب موارد اینRootkit ها تروجان نیز هستند و با فریب کاربر، وی را قانع می‌کنند که در حال اجرای برنامه امن و قابل اعتمادی است

Rootkitها برای انواع مختلف سیستم عاملها مانند ویندوز، لینوکس، Mac OS و Solaris تولید می‌شوند. این برنامه های خرابکار اغلب بخشهایی از سیستم عامل را تغییر داده یا خود را به عنوان درایور و یا ماژولهای هسته ای نصب می‌کنند.

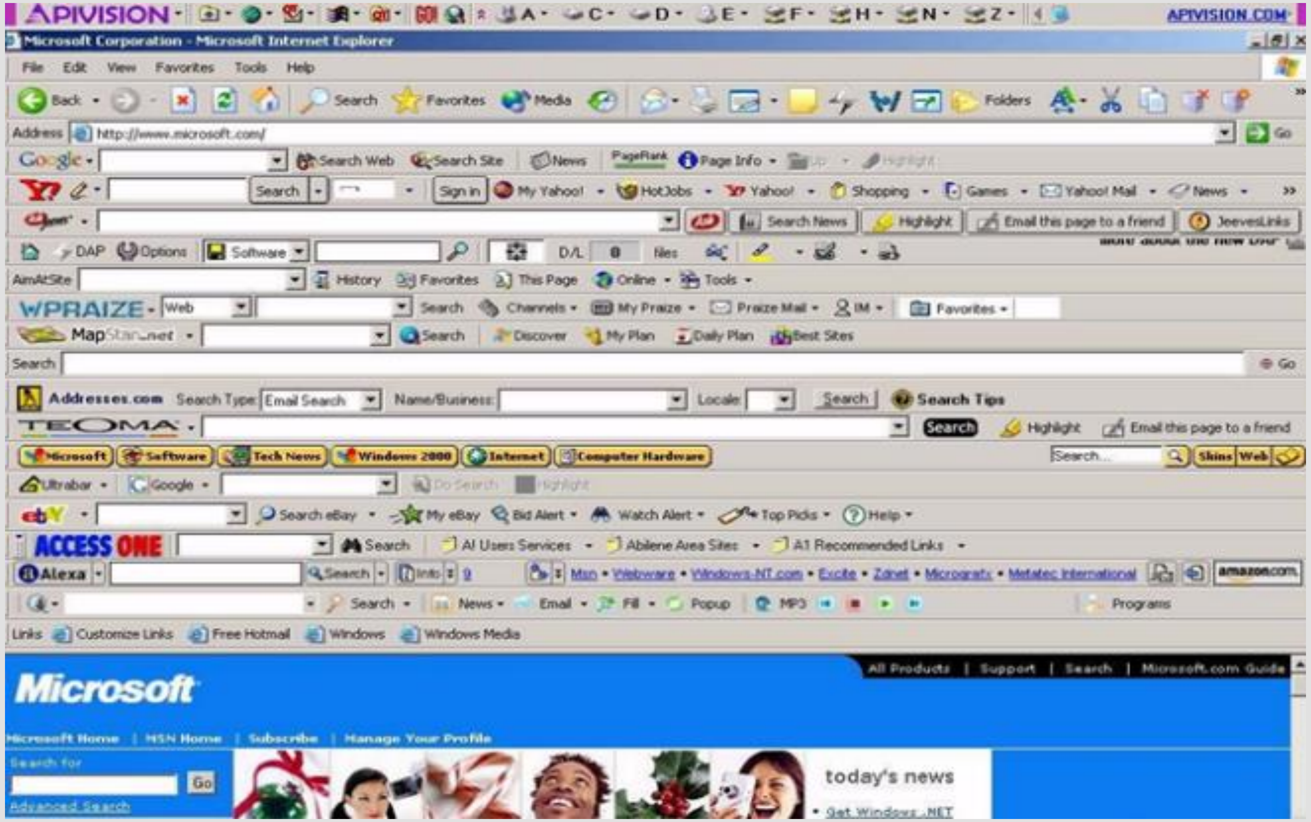


جاسوس افزار

جاسوس افزار

- اهداف جاسوسی و سرقت اطلاعات شخصی و سازمانی
- اطلاعات مورد نیاز در خصوص فعالیت های کاربر بر روی سیستم و یا هرگونه اطلاعات مورد نیاز را جمع آوری و در زمان مناسب برای شخص دیگری ارسال می کنند

- به این نوع از نرم افزارها گاهی اوقات روبات جاسوسی یا نرم افزار دنبال کننده نیز گفته می شود
- وب سایتهایی که ابزار جاسوسی منتشر می کنند از ترفندهای متنوعی برای فریب دادن کاربران و ترغیب آنها به دریافت و نصب اینگونه نرم افزارها استفاده می کنند



ابزارهای تبلیغاتی

- هر نرم افزاری یا برنامه ای که از وجود تبلیغات در کنارش استفاده کند به عنوان تبلیغ افزار یا Adware شناخته می شود
- ابزارهای تبلیغاتی غالباً با یک برنامه کاربردی میزبان ترکیب می شوند به طوری که برنامه میزبان تا زمانی که کاربر دریافت ابزارهای تبلیغاتی را قبول می کند، به صورت رایگان به وی خدمات می دهد ← موضوع فریب کاربران در میان نیست

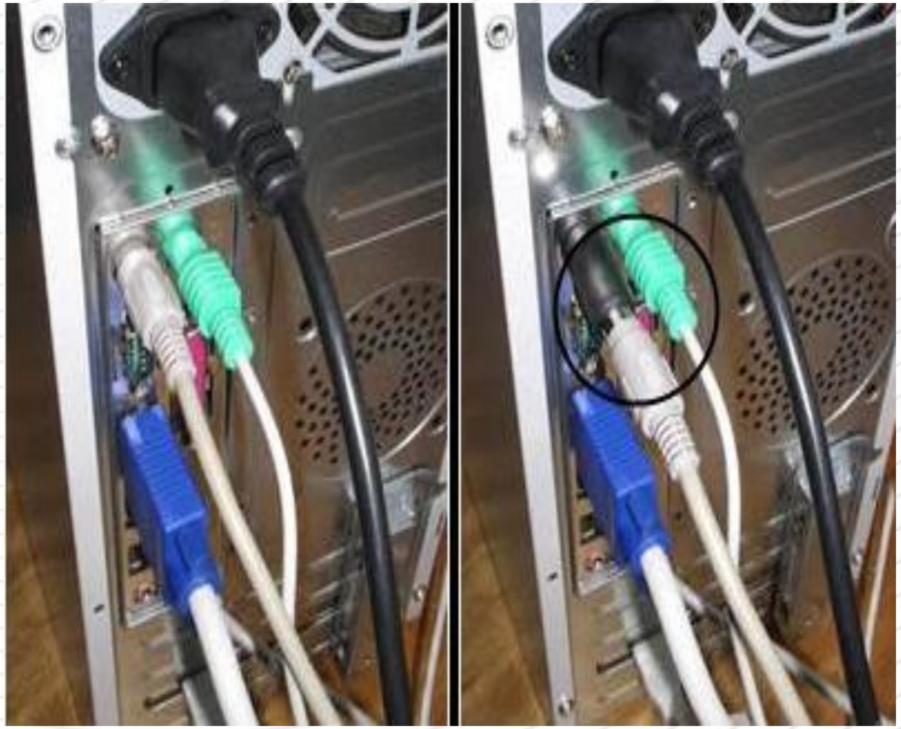
تفاوت بین Spywareو Adware

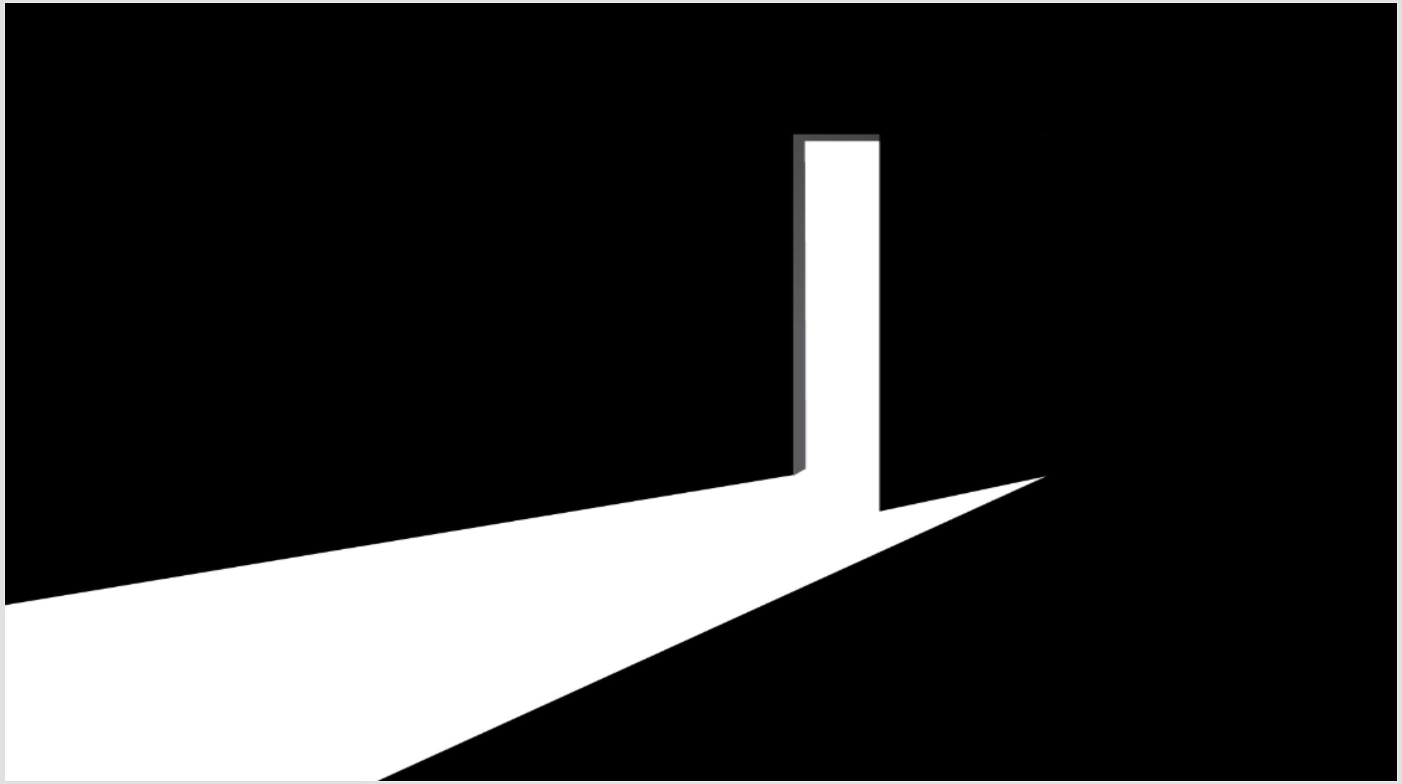
- Adwareاهداف تبلیغاتی دارد و Spyware اهداف جاسوسی دارد
- Adwareها بصورت مشهود قابل مشاهده هستند و Spyware ها مخفی و غیرقابل مشاهده هستند
- Adwareها معمولا به عنوان یک تهدید در کامپیوتر دیده نمی شوند اما Spyware ها به عنوان کد مخرب و آسیب زننده شناخته می شوند

Key Logger

- کلیه کلید هایی که کاربر بر روی کیبورد خود فشار می دهد را در قالب یک فایل ذخیره می کند

- اطلاعات قابل استفاده و مفیدی از جمله رمزهای عبور ، اطلاعات و شماره های کارت های اعتباری ، اطلاعات شخصی





درب پشتی

درب پشتی

- درهای پشتی ممکن است از قبل در سامانه وجود داشته باشند یا اینکه فرد نفوذگر با فریب کاربر، او را نسبت به نصب در پشتی ترغیب کند

انواع درب پشتی

فعال

- آغازگر ارتباط با میزبان‌های دیگر هستند

غیرفعال

- منتظر رسیدن دستورات ازطریق درگاهها می‌شوند

حمله بنیان

- با استفاده از حمله‌ای مبتنی بر یک اکسپلویت و با روش‌هایی مانند سر ریز بافر به دسترسی‌های لازم در میزبان هدف دست می‌یابند

باج افزار

- دسترسی به سیستم را محدود می‌کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کنند
- برخی از انواع آنها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می‌خواهد مبالغی را واریز کنند
- تنها راه مقابله با این بدافزارها پیشگیری و آلوده نشدن به آنهاست

بررسی حملات باج افزارها

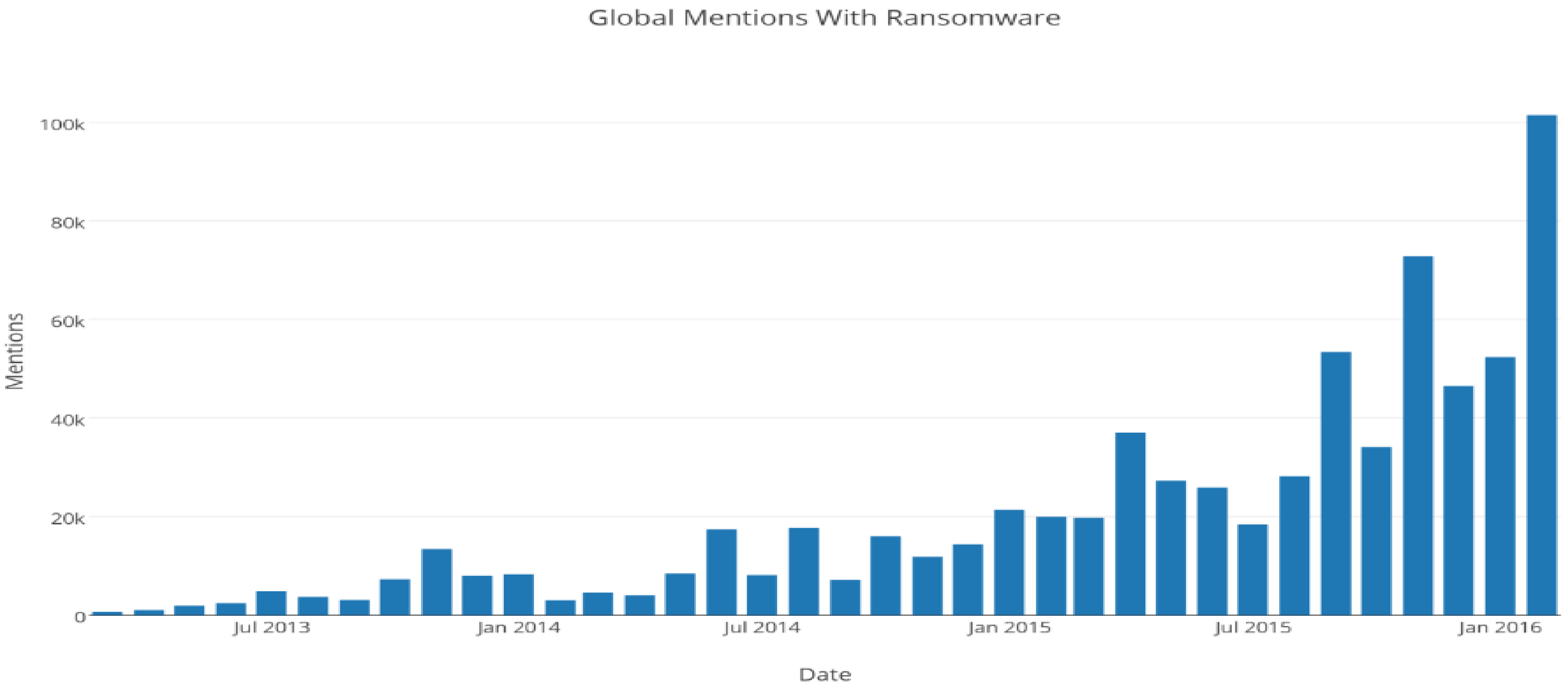
- Ransomware یا باج افزار نوعی از بدافزار است که به محض اینکه دستگاهی را آلوده کند ، مانع دسترسی به آن دستگاه یا اطلاعات ذخیره شده آن میگردد.

انواع باج افزار

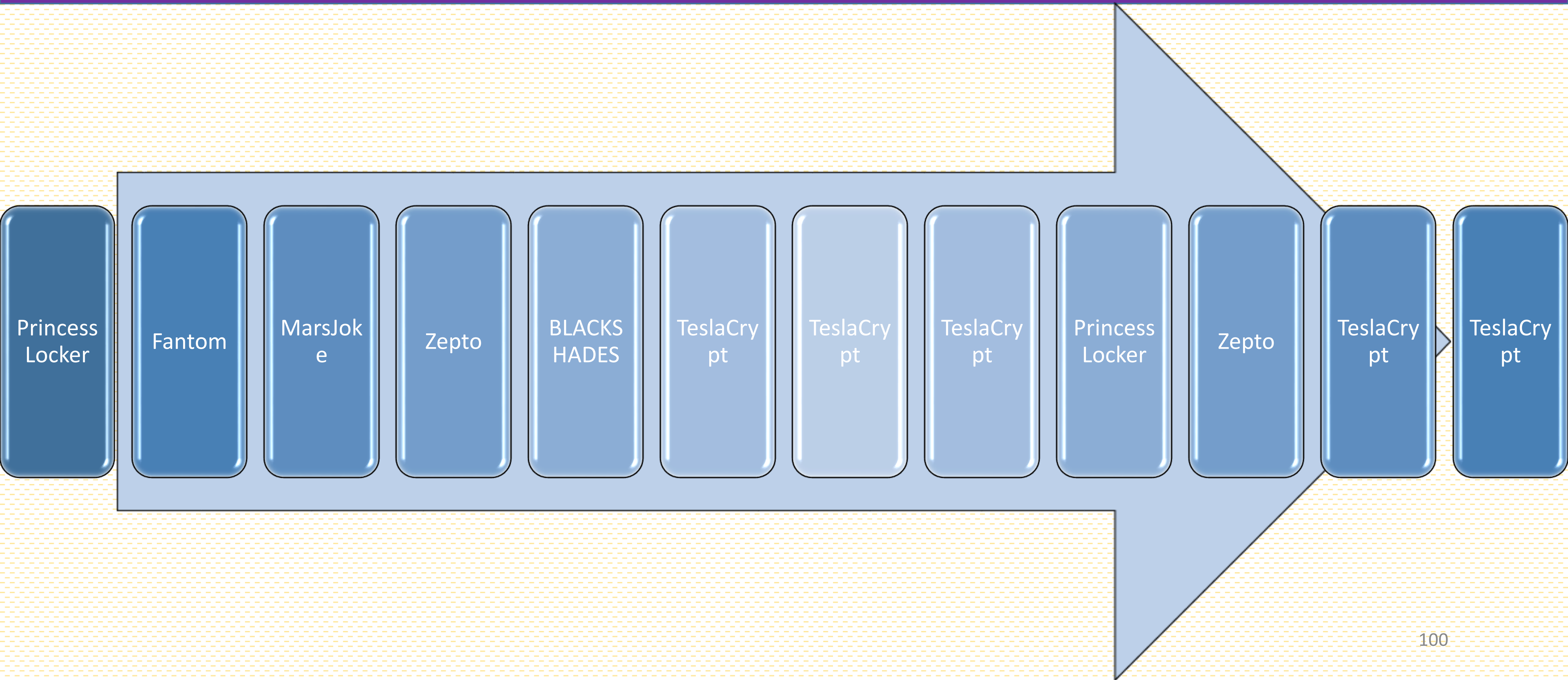
❖**باج افزارهای از نوع مسدودکننده دسترسی به سیستم عامل**

❖**باج افزارهای از نوع رمزگذار**

بررسی حملات باج افزارها



بررسی حملات باج افزارها

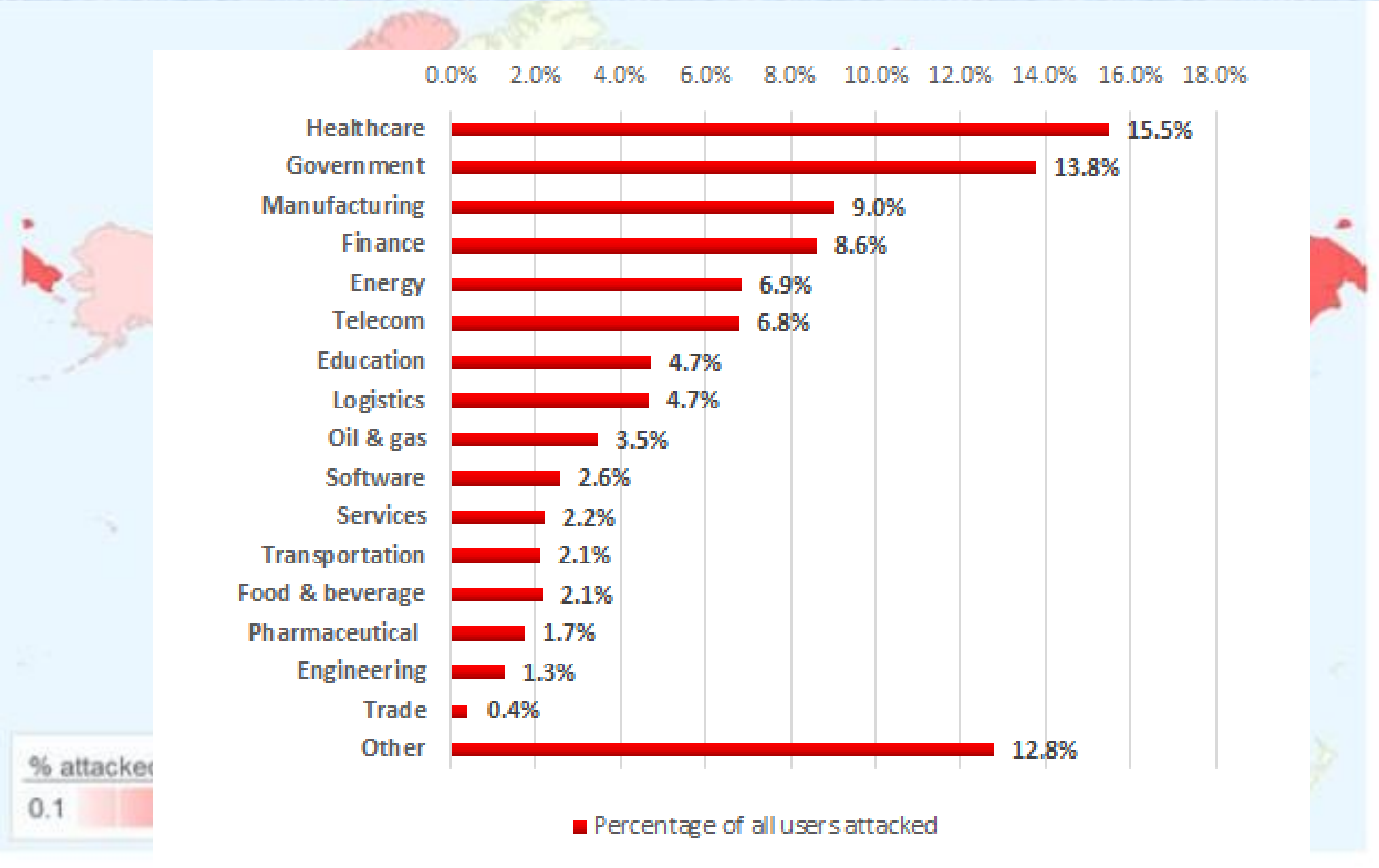


بررسی حملات باج افزارها

کشور	درصد کاربران مورد حمله با باج‌افزار رمزگذاری 2014-2015	درصد کاربران مورد حمله با باج‌افزار رمزگذاری 2015-2016
Russian Federation	6.09%	20.43%
India	3.34%	6.93%
United States	14.27%	39.79 %
Germany	4.64%	94.41%
Vietnam	2.32%	22.87 %
Ukraine	1.34%	28.86%
Kazakhstan	1.14%	25.59%
Algeria	1.18%	13.48 %
Italy	8.93%	89.7%
Brazil	2.56%	31.83%
Other	41.16%	46.3%

Source : Kaspersky

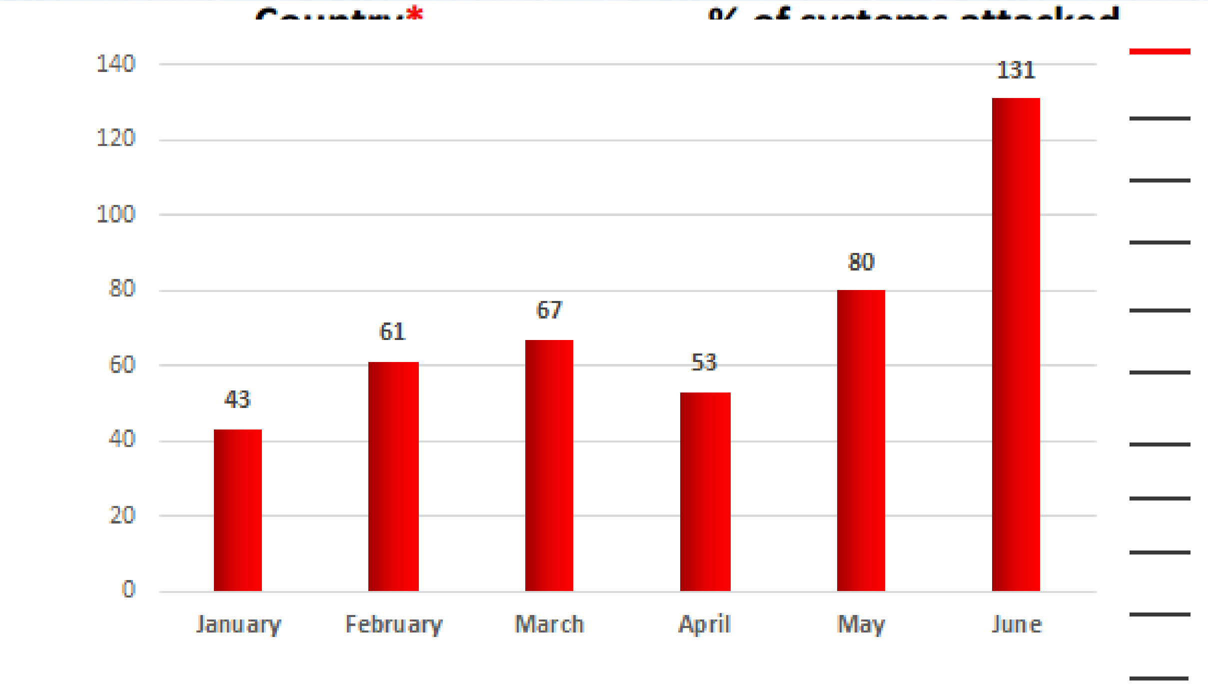
Top 10 countries based on the percentage of ICS computers attacked by encryption malware <u>Kaspersky-2017</u>



Geogra*p* *Distribution of companies attacked by WannaCry by industry, May – June 2017* *ns*

(percentage of ICS computers attacked in each country)

Top 10 countries based on the percentage of ICS computers attacked by encryption malware Kaspersky-2017



Number of unique ICS computers attacked by encryption Trojans, H1 2017

بررسی باج افزار Wannacry

- باجافزار WannaCry از دو روش NSA که براساس پروتکل SMB بود، استفاده می نماید
- باج افزار WannaCry با استفاده از حفره های امنیتی که در ویندوز وجود دارد، فایل های کاربران را رمزگذاری کرده و برای جلوگیری از حذف داده ها، ۳۰۰ دلار به صورت بیت کوین طلب می کند
- هکرها از حفره EternalBlue که در ویندوز وجود داشته استفاده کرده اند(حفره ای که سازمان NSAپیشتر از آن برای دور زدن امنیت ویندوز بهره گرفته بود).

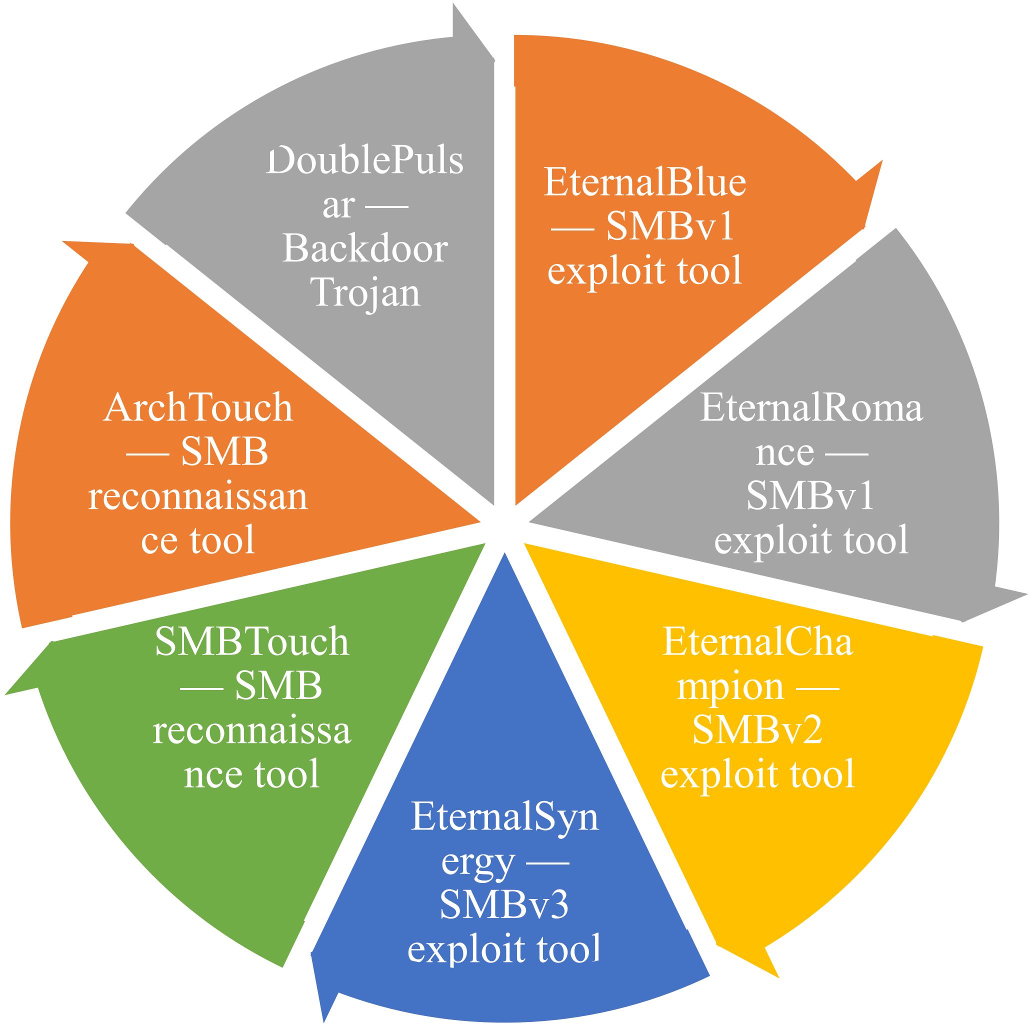
باج افزارهای خطرناک تر از Wannacry

EternalRocks

- باج‌افزار واناکرای WannaCry فقط از دو روش NSA که براساس پروتکل SMB بود، استفاده می‌کرد، اما بدافزار اترنال راکس از تمامی هفت روش استفاده می‌نماید
- این بدافزار جدید از ابزارهای EternalBlue و DoublePulsar که متعلق به آژانس امنیت ملی آمریکا بوده، استفاده کرده است

باج افزارهای خطرناک تر از Wannacry

ابزارهای مورد استفاده NSA




facebook
Search for people, places and things
Sean Doyle
Home
HOAX
Privacy Shortcuts
Where do you work?
Which high school did you go to?
Which city do you live in?
See More Settings

کلک

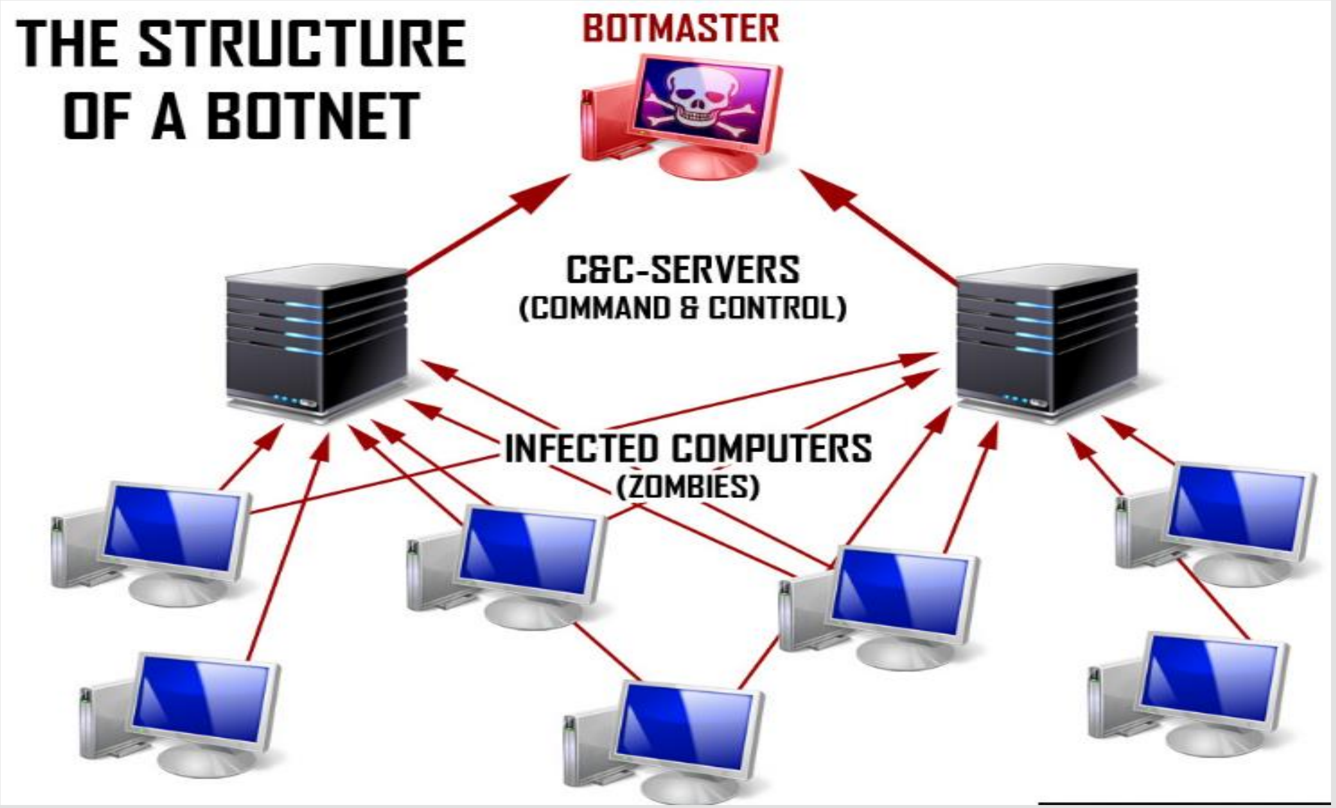
Hoax

- با سوء استفاده از کم بودن اطلاعات تخصصی کاربران، آنها را فریب داده و با دستورات و توصیه‌های اشتباه باعث می‌شوند که کاربر شخصاً کاری تخریبی بر روی سیستم خود انجام دهد
- Hoaxها نیز مانند برخی انواع بدافزارها از تکنیک های مهندسی اجتماعی برای گول زدن کاربران و ترغیب آنها به انجام برخی کارها استفاده می کنند

هرزنامه

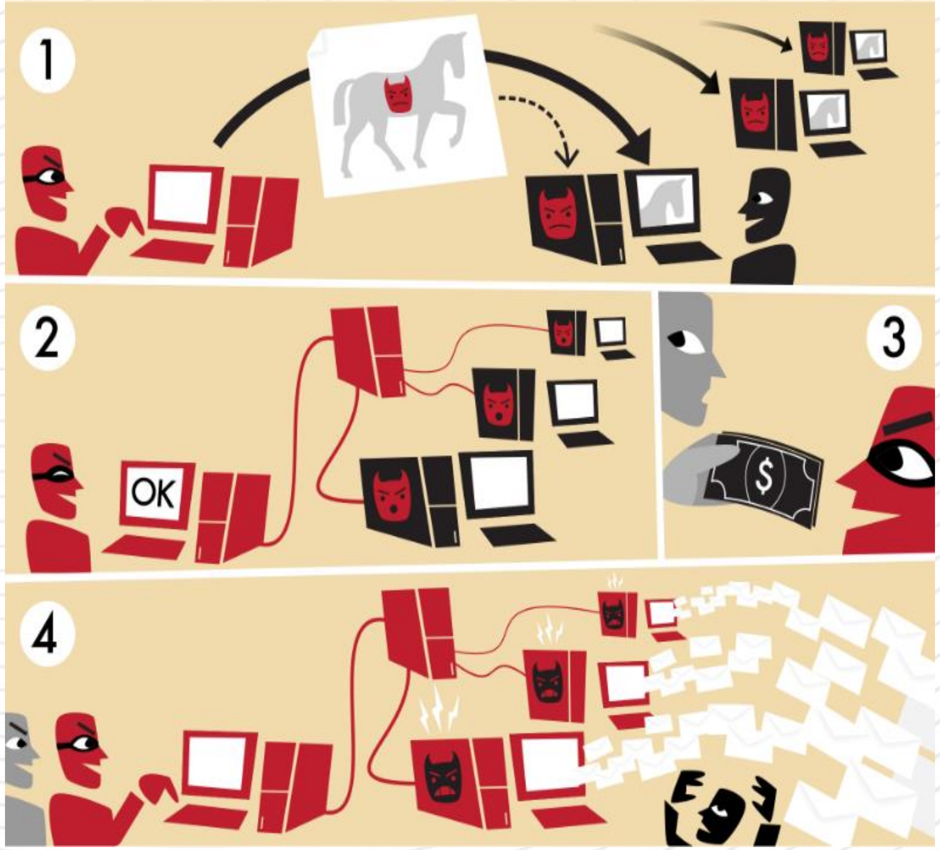
هرزنامه

- هرزنامه، ایمیل ناخواسته‌ای است که برای تبلیغ یک سرویس یا محصول تولید می شوند.
- هرزنامه ها سلامت فضای تبادل ایمیل را در سراسر جهان مورد تهدید قرار می دهند


THE STRUCTURE
OF A BOTNET
BOTMASTER
C&C-SERVERS
(COMMAND & CONTROL)
INFECTED COMPUTERS
(ZOMBIES)

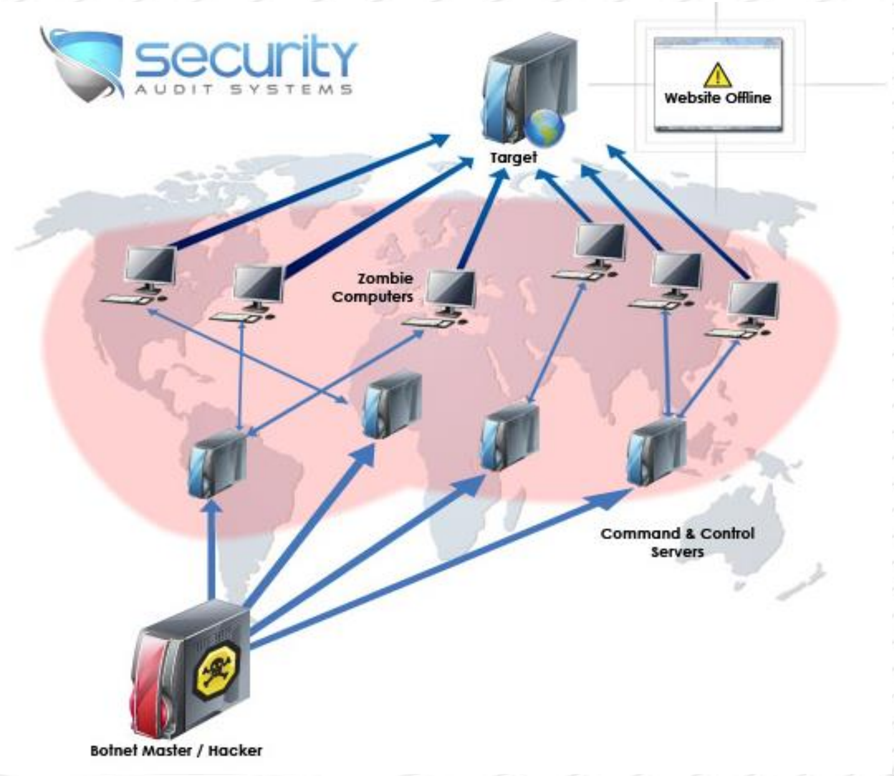
Bot/Botnet

- Botnetها شبکه هایی از کامپیوترهای آلوده هستند.
- این کامپیوترها تحت کنترل یک مجموعه دستورات هستند که از طریق نرم افزاری که تعمدا و یا نا آگاهانه نصب شده است، مدیریت شده و تغییر می‌کنند.
- این نرم افزار توسط یک کامپیوتر خرابکار کنترل می‌گردد.
- اندازه یک botnet به پیچیدگی و تعداد کامپیوترهای استخدام شده در این Botnet بستگی دارد.

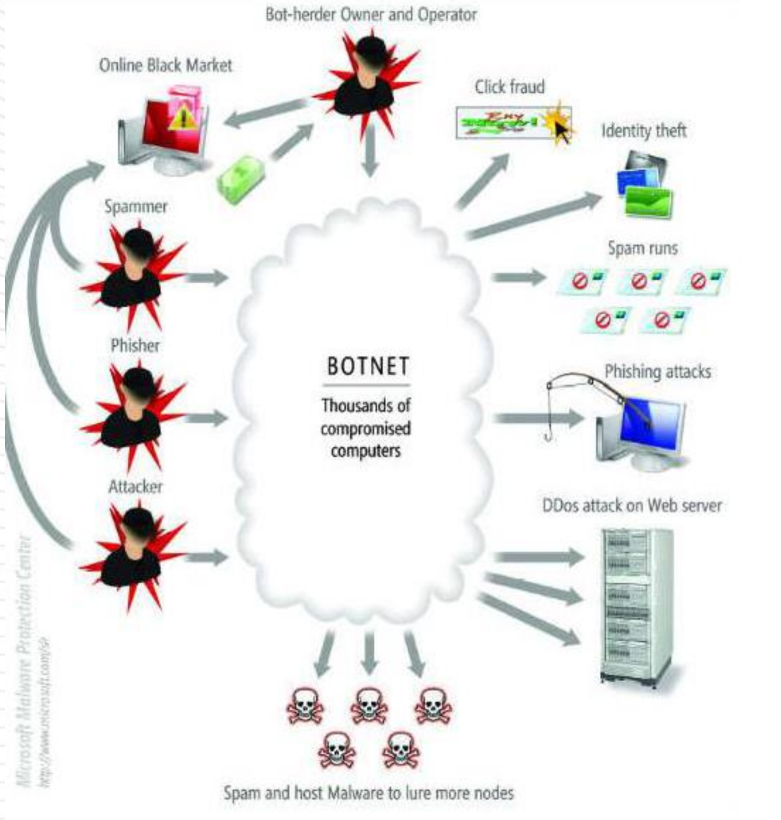


کاربردهای Botnet

حملات انکار سرویس توزیع شده (DDOS)



ابزار جاسوسی و بدافزار



فریب (Scam)

- ایمیلهایی که کاربران را برای فاش ساختن اطلاعات شخصیشان (مانند اطلاعات حساب بانکی) فریب می دهند تا از آنها در موارد غیرقانونی استفاده کنند، از نمونه های رایج فریب هستند

- جعل هویت یا phishing

عملیات بازیهای المپیک

جنگ تمام عیار سایبری بر علیه ایران

استاکس نت دوکیو فلیم و ...

Stuxnet

- اولین سلاح سایبری بکارگیری شده
- این اولین بدافزار رایانه ای است که با هدف ایجاد تغییرات فیزیکی در جهان واقعی ساخته شده است
- استاکس‌نت به عنوان بزرگترین حمله سایبری تاریخ بر علیه تاسیسات کنترل صنعتی تلقی می‌شود
- این بدافزار به عنوان نخستین بدافزار از سلسله عملیاتی با عنوان بازی‌های المپیک بوده است
- این کرم برای این منظور طراحی شد تا سانتریفیوژهای ویژه غنی سازی اورانیوم در سایت هسته ای نطنز را مختل کند
- این بدافزار از هفت روش حمله مختلف و از چهار آسیب‌پذیری مختلف به منظور انتشار خود استفاده می نمود

کشورهای آلوده شده توسط بدافزار استاکس نت

Iran	Indonesia	India	Pakistan	Uzbekistan	Russia	Kazakhstan	Belarus
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Kyrgyzstan	**Azerbaijan**	**United States**	**Cuba**	**Tajikistan**	**Afghanistan**	**Rest of the world**	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

Stuxnet

- این بدافزار پس از آلوده کردن یک سیستم به دنبال سیستم‌های Siemens Simatic WINCC وSTEP 7 SCADA می گردد
- استاکس‌نت در مهمترین بخش از حمله به سیستم های کنترل صنعتی، یک فایل کتابخانه ای حساس مربوط به نرم افزار Step7 را با فایل کتابخانه‌ای بدافزار جایگزین می‌کند
- استراتژی حمله در استاکس‌نت تلاش برای کنترل مخفی سیستم به جای تخریب آن است
- در استاکس‌نت؛ حمله به شکل دایره ای انجام می گیرد. به عبارت دیگر؛ حمله در استاکس‌نت بارها و در چندین مرحله انجام می گیرد
- کد استاکس نت از هشت بخش مجزا تشکیل شده است که حمله بدافزار از بخش ۲ تا ۶ انجام می گیرد.

Stuxnet

مراحل عملکردی استاکس نت

- مرحله صفر با مقدار دهی اولیه شروع می‌شود و یک پروسه مانیتورینگ صرف است. در این مرحله؛ دو شرط با هدف آغاز حمله بررسی می‌شود. اطلاعاتی که بر مبنای آنها این دو شرط بررسی می شوند، از قطعه کد FC 6064 دریافت می شوند.
- مرحله یک، تصویر فرآیند (Inter-proceess image) به مدت ۲۱ ثانیه ثبت می‌شود. این اطلاعات به منظور فریب نرم افزار کنترل در زمان اجرای حمله به کار می رود
- در مرحله ۲ حمله واقعی آغاز می‌شود. در این مرحله سعی می‌شود تا خروجی ها به شکل ماهرانه ای دستکاری شود. این عمل در مراحل ۲ تا ۶ انجام می گیرد. عمل تغییر در خروجی ها و فریب نرم افزار کنترلی به صورت پشت سر هم و به دفعات مختلف انجام می گیرد. (به طور همزمان تصویر عملکرد معمول سیستم به نرم افزار مانیتورینگ ارسال می‌شود. در چنین شرایطی نرم افزار کنترلی و کاربر انسانی قادر به تشخیص عملکردهای تخریبی بدافزار در موتورهای تابع PLCها نخواهد بود)
- در مرحله هفتم دوباره مقداردهی اولیه انجام می‌گیرد

Stuxnet

- آسیب‌پذیری‌های 0-day مورداستفاده در ویروس stuxnet عبارت‌اند از:
- MS08-067 RPC Exploit (http://www.microsoft.com/technet/security/bulletin/ms10-067.mspx)
- MS10-046 LNK Exploit (http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx)
- MS10-061 Spool Server Exploit (http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx)

Two privilege escalation (or Elevation of Privilege) vulnerabilities:

- MS10-073 Win32k.sys Exploit (http://www.microsoft.com/technet/security/bulletin/ms10-073.mspx)
- MS10-092 Task Scheduler Exploit (http://www.microsoft.com/technet/security/bulletin/ms10-092.mspx)

مصون سازی زیرساخت های

سایبری و وابسته به سایبر

گام های اساسی جهت مصون سازی زیرساخت های سایبری و وابسته به سایبر

- شناسایی دارایی ها، مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- تعیین سطح اهمیت دارایی‌ها، مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر به سطوح ویژه حیاتی، حساس و مهم، فاقد طبقه بندی
- احصای تهدیدات سایبری مترتب در مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر و ترسیم بردار تهدیدات
- تدوین سناریوی تهدید پایه و سناریوهای تهدیدات محتمل

گام های اساسی جهت مصون سازی زیرساخت های سایبری و وابسته به سایبر

- شناسایی آسیب پذیری های سایبری مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- دسته بندی تهدیدات مترتب به مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- دسته بندی آسیب پذیری های مترتب به مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- ترسیم ماتریس تهدید-آسیب پذیری برای بررسی برهم کنش تهدیدات و آسیب پذیریها و تحلیل برهم کنش تهدیدات-آسیب پذیری ها

گام های اساسی جهت مصون سازی زیرساخت های سایبری و وابسته به سایبر

- تعیین مخاطرات سایبری در صورت اعمال تهدیدات بر آسیب پذیری ها
- پیامدسنجی مخاطرات و وزن دهی به هر یک
- محاسبه ریسک و تعیین ریسک قابل قبول
- تدوین راهکارهای پدافند سایبری جهت امن سازی/ مصون سازی مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر مطابق با معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق
- تدوین راهکارهای مقابله با حملات سایبری (تهیه دستورالعمل های مدیریتی امنیت و پدافند سایبری، تعریف فرایندهای کاری قبل، حین و پس از حادثه، تشکیل تیم CSIRT و ...)

گام های اساسی جهت مصون سازی زیرساخت های سایبری و وابسته به سایبر

- تدوین طرح تداوم خدمات و فعالیت های ضروری (BCP) در صورت بروز بحران سایبری
- نظارت مستمر، ارزیابی امنیتی-پدافندی و کنترل اقدامات در مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- برگزاری تست نفوذ های سایبری و رزمایش های سایبری
- ایجاد آمادگی کامل جهت رصد، پایش و تشخیص تهدیدات و آسیب پذیری ها و تحلیل تهدیدات و آسیب پذیری های جدید به همراه محاسبه میزان اثرگذاری و پیامدسنجی آنها و ارائه گزارشات دوره ای
- به روز رسانی راه کارهای پدافند سایبری با توجه به تهدیدات و آسیب پذیری های جدید
- برگزاری آموزش های ارتقاء توانمندی های سایبری و پدافند سایبری بصورت برگزاری دوره های طولی و عرضی برای کارشناسان و مدیران زیرساختهای سایبری و وابسته به سایبر در سطوح مختلف

مدلسازی تهدیدات سایبری

روش مدلسازی تهدیدات مطابق

با متدولوژی STRIDE

مقدمه

- متدولوژی STRIDE توسط مایکروسافت، توسعه داده شده است و بر پایه تهدیدات امنیتی سایبری اقدام مینماید.
- STRIDE بین این شش خصوصیت نگاشت انجام می دهد و برآیند آنها را به عنوان تهدیدات و موارد مهمی که بایستی درنظر گرفته شود، لحاظ می گرداند.
- شناسایی تهدیدات از دیدگاه مهاجمین

STRIDE

Spoofing	**Tampering**	**Repudiation**	**Information Disclosure**	**Denial of Service**	**Elevation of Privilege**

STRIDE

Threat	Property Violated	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be any of Bill Gates, Paypal.com or ntdll.dll
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the network
Repudiation	Non-repudiation	Claiming to have not performed an action.	“I didn’t send that email,” “I didn’t modify that file,” “I *certainly* didn’t visit that web site, dear!”
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP.

Spoofing Over a Network

مثال

Threat Example	What the Attacker Does	Notes/Examples
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	
	DNS compromise	Can be at the TLD, registrar or DNS server
	IP redirection	
Spoofing a person	Take over account	“Stranded in London”
	Set the display name	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account, setting up a domain/website, other “verifiers”

Tampering with Memory

مثال

Threat Example	What the Attacker Does	Notes/Examples
Modifying code	Changes your code to suit themselves	Hard to defend against if the attacker is running code inside the trust boundaries
Modifying data they've supplied	Supplies data to a pass by reference API, then changes it	Works because of TOCTOU issues
	Supplies data into a shared memory segment, then changes it	

روش تعیین سطح اهمیت

تهدیدات مطابق با متدولوژی

CARVER+Shock

مقدمه

- مدل CARVER توسط نیروهای ویژه ارتش ایالات متحده در طول جنگ ویتنام توسعه داده شد.
- این مدل تشکیل یک ماتریس از عناصر شکل دهنده مدل CARVER را می دهند و بر نقاط ضعف در اهداف دوست و دشمن تمرکز دارد.
- از این مدل می توان برای ارزیابی تهدیدات بر زیرساخت ها، بهره برد.

Criticality

- در این مقیاس سطح اهمیت هدف و یا به نوعی ارزش هدف برای کشور مورد حمله قرارگرفته، مطرح می گردد. بنابراین مقیاس، آسیب رساندن به هدفی که سطح اهمیت بالایی داشته باشد تاثیر قابل توجهی بر عملیات نظامب، سیاسی، اقتصادی و ... بر کشور قربانی خواهد داشت.

Accessibility

- در این مرحله، نحوه نفوذ از محل شروع تا هدف، حرکت از نقطه ورود تا مرکز و عمق هدف، رسیدن به نقطه کانونی هدف و همینطور نحوه خروج تاحد امکان بی صدا از هدف مورد بحث قرار می گیرد

Recuperability

- در این مرحله آمادگی قربانی، برای جایگزین نمودن زیرساخت هایی که مورد حمله قرار گرفته اند، بررسی می شود. معیار مهم در این مرحله، زمان می باشد که در چه مدت زمانی امکان تعمیر و یا جایگزینی زیرساخت مورد حمله، میسر است

Vulnerability

- آسیب پذیری وابسته به عوامل متعددی از قبیل طبیعت، ماهیت و ساختار هدف و میزان آسیبی که نیاز است تا هدف متلاشی شود، می باشد

Effect

- در این مرحله میزان تاثیرگذاری حمله بر روی هدف و دستاوردهای حمله تمرکز می گردد

Recognizability

- در این مرحله میزان توانایی حمله کننده در شناخت کامل از قربانی، قابلیتهایی که برای شناخت کامل نیاز است و ... بررسی می گردد.

نمونه سوالات CARVER برای یک زیرساخت فرضی

جدول تعیین سطح اهمیت سرمایه های ملی بر اساس تهدیدات سایبری

	پرسش ها	مقیاس اندازه گیری				
		۹-۱۰	۷-۸	۵-۶	۳-۴	۱-۲
۱	با توجه به موارد زیر، آیا نابودی، اختلال یا آسیب رساندن به این سرمایه ها، تاثیر قابل توجهی به عملکرد و عملیات زیرساخت/ سرمایه وارد می کند؟	قطعا	بسیار زیاد	زیاد	کم	خیلی کم
۲	میزان دسترس پذیری نقاط کلیدی سایبری به چه میزان است؟	بسیار راحت	راحت	نسبتا دشوار	دشوار	بسیار دشوار
...	با توجه به فاکتورهای موثر مندرج در پیوست، جایگزینی، تعمیر یا رفع اشکال سامانه /	یک ماه یا بیشتر	یک هفته تا یک ماه	۷۲ ساعت تا یک هفته	۲۴ ساعت تا ۷۲ ساعت	زیر ۲۴ ساعت

نمونه ماتریس CARVER برای یک زیرساخت فرضی

BULK ELECTRIC POWER SUPPLY							
POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
FUEL TANKS	8	9	3	8	5	6	41
FUEL PUMPS	8	6	2	10	5	3	34
BOILERS	6	2	10	4	5	4	31
TURBINES	8	6	10	7	5	9	45
GENERATORS	4	6	10	7	5	9	41
CONDENSERS	8	8	5	2	5	4	34
FEED PUMPS	3	8	5	8	5	6	33
CIR. WATER PUMPS	3	8	5	8	5	4	33
GENERATOR STEP UP TRANSFORMER	10	10	10	9	5	9	53

بررسی آسیب پذیری های

زیرساخت های سایبری و وابسته

به سایبر

ارزیابی آسیب پذیری های زیرساخت های حیاتی و حساس و مهم

بررسی آسیب پذیری های مرتبط با فضای سایبر

- آسیب پذیری های عمومی ناشی از بهره برداری از فناوریهای سایبری (ناشی از ماهیت، ضعف ساختاری و یا نحوه بهره برداری از فناوریهای اطلاعاتی ارتباطی)

- آسیب پذیری های ناشی از چگونگی عملکرد و ترکیب اجزای سازمانهای بهره بردار از فناوریهای اطلاعاتی/ارتباطی و برهمکنش این اجزاء با یکدیگر.

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

- آسیب پذیریها و تهدیدات بر روی **Web Server**

- آسیب پذیریها و تهدیدات بر روی **Web Application**

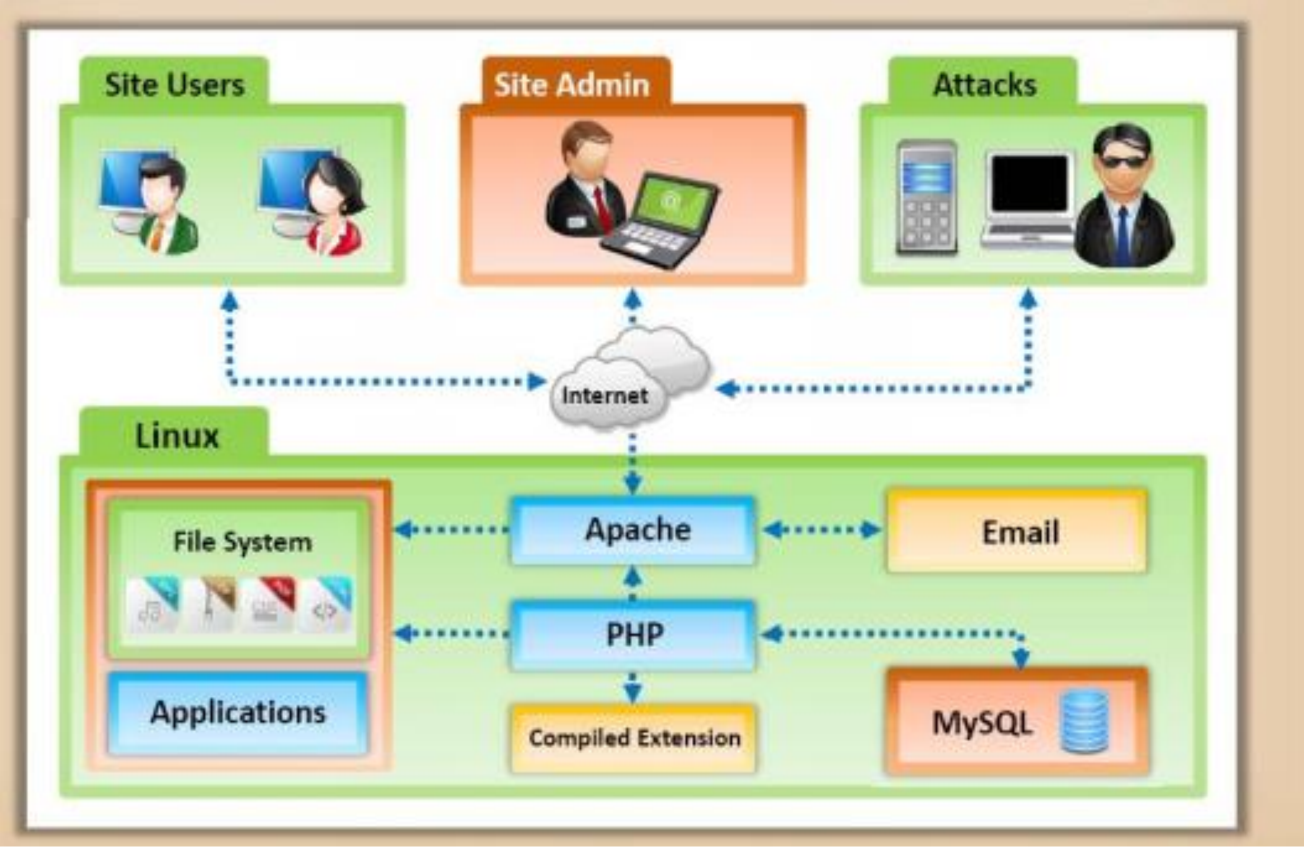
آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

الف. آسیب پذیریها و تهدیدات بر

روی Web Server

درصد استفاده از انواع مختلف Web Server تا پایان سال ۲۰۱۷

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

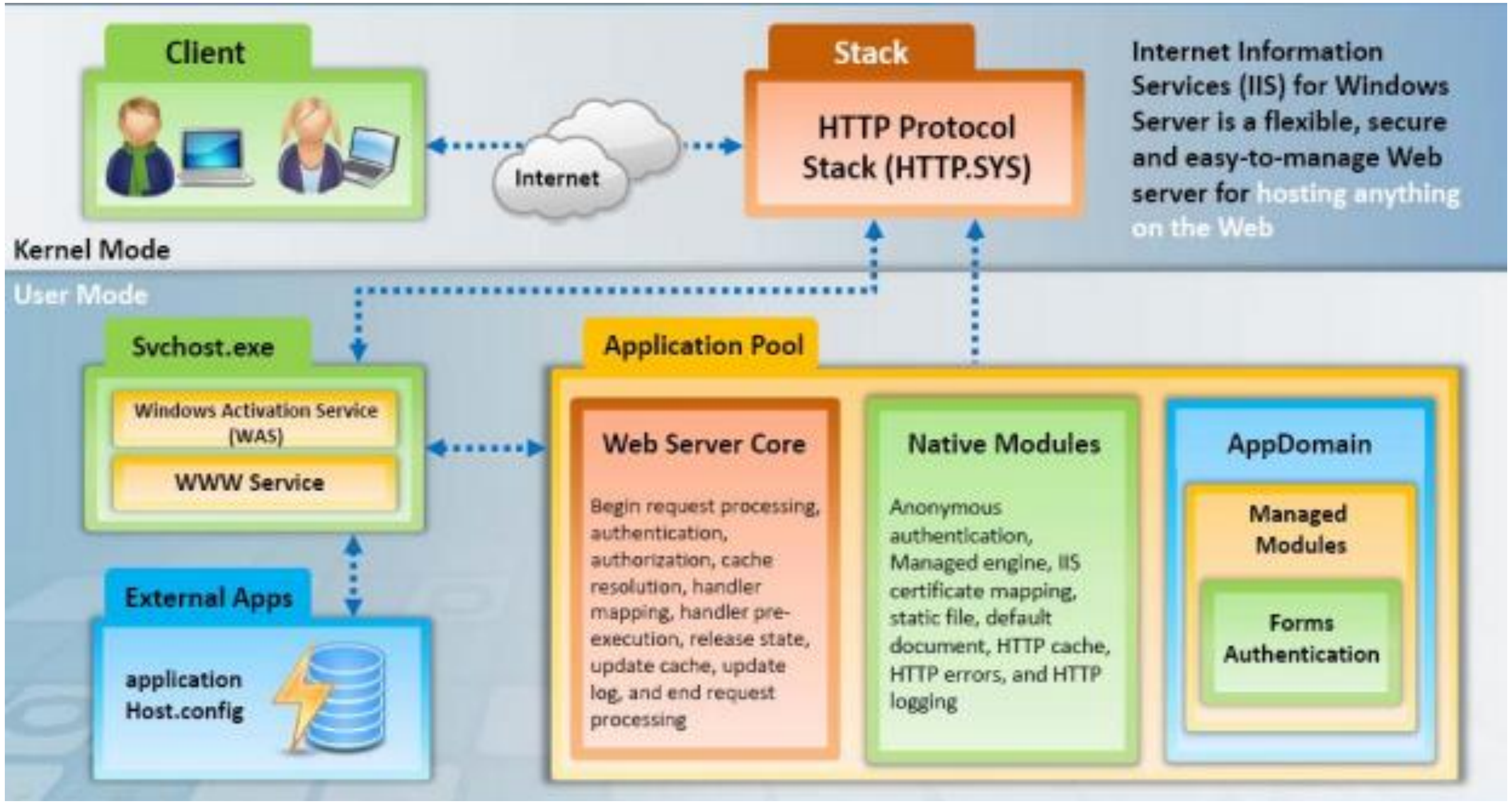


<u>الف. آسیب پذیریها و تهدیدات بر روی</u>

<u>**Web Server**</u>

معماری رایج وب سرورهای متن باز

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها



الف. آسیب پذیریها و تهدیدات بر روی **Web Server**

معماری رایج وب سرورهای ویندوزی

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

الف. آسیب پذیریها و تهدیدات بر روی Web Server

- پیکربندی اشتباه نرم افزار وب سرور
- باگ های برنامه نویسی در کد سیستم عامل یا اپلیکیشن های وب
- آسیب پذیری نصب پیش فرض
- عدم وجود سیاست های امنیتی صحیح
- مشکلات سیستم عامل یا نرم افزارها یا خطا در کد برنامه

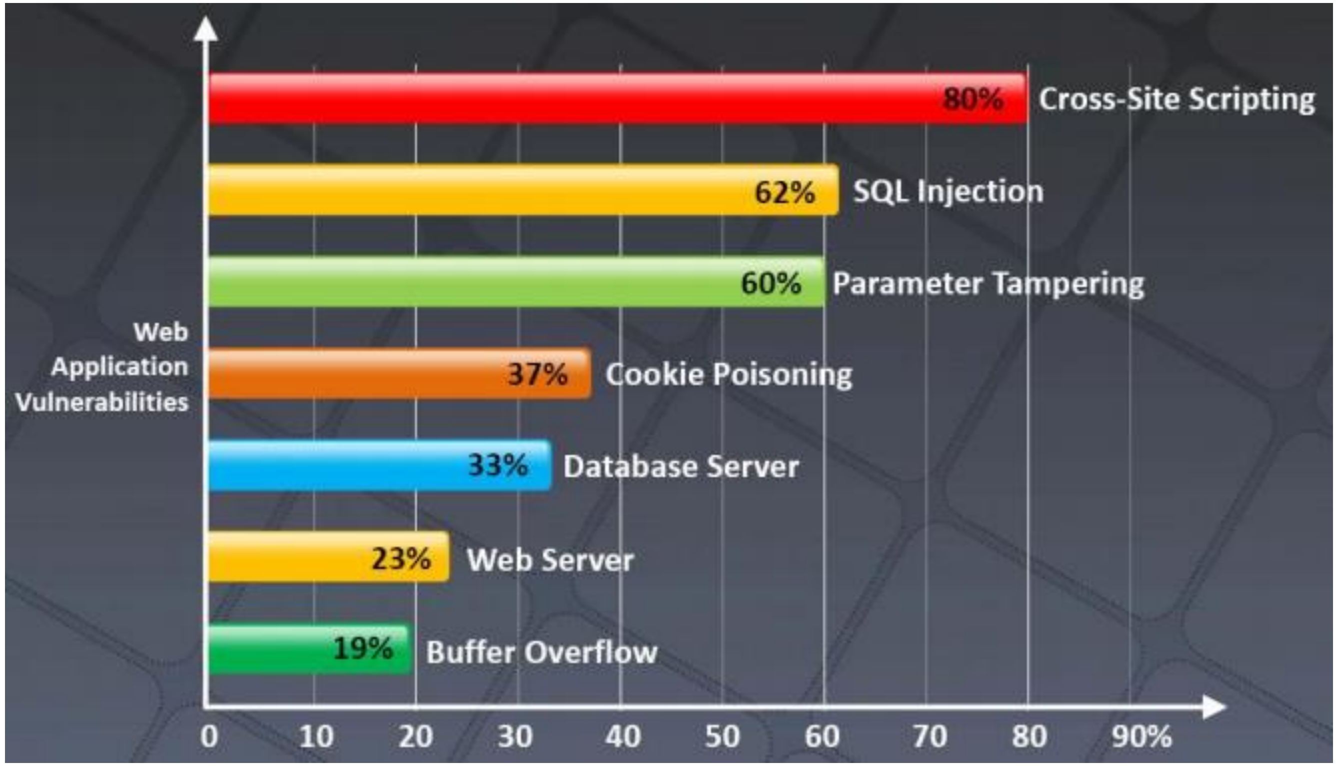
آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

روشهای امن سازی Web Server

- تغییر نام اکانت administratorو استفاده از پسورد پیچیده
- حذف برنامه های بدون استفاده از سرور از قبیل WebDAV
- غیر فعال کردن directory browsingمشاهده دایرکتوری(در تنظیمات وب سرور)
- اضافه کردن یک هشدار قانونی در سایت برای آگاه ساختن هکرها از تاثیرات هک سایت
- نصب patchها و سرویس پکهای جدید برای سیستم عامل و نرمافزار وب سرور
- بررسی ورودیهای کاربر در فرم وب برای جلوگیری از حملات buffer overflowو...
- غیر فعال ساختن مدیریت از راه دور
- استفاده از اسکریپتی برای نگاشت فایلهای غیر لازم به یک پیام خطا از قبیل ("File not found" 404)
- فعال کردن auditing و logging
- استفاده از فایروال بین وب سرور و اینترنت و باز کردن تنها پورتهای لازم از قبیل ۸۰یا ۴۴۳
- جایگزینی روش GET با روش POST

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

ب. آسیب پذیریها و تهدیدات بر روی **Web Application**



- SQL Injection
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Header Injection
- Session Hijacking
- Remote file inclusion(RFI)
- Session fixation
- Cookie Poisoning and Snooping
- Buffer Overflow
- Directory Traversal

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

ب. آسیب پذیریها و تهدیدات بر روی Web Application

SQL Injection

- SQL Injection یک نوع حمله با استفاده از ارسال یک رشته(String) حاوی کد مخرب به SQL Server Instance می باشد
- فرم اولیه این نوع حمله شامل درج یک دستور SQL در مقادیری است که توسط برنامه از کاربر دریافت می شود
- Blind SQL Injection
- Time-Based SQL Injection
- Error-Based SQL Injection

آسیب پذیری ها و تهدیدات رایج بر روی وب سایت ها

ب. آسیب پذیریها و تهدیدات بر روی Web Application

XSS

- Scripting یکی از روش های حمله هکرها به سایت ها است و یک نقص امنیتی محسوب می شود. البته در این حمله کدهای سمت کلاینت از قبیل جاوا اسکریپت به سایت تزریق می شوند و هدف اصلی هکرها کاربرانی هستند که به سایت مراجعه کرده اند. در حقیقت هکرها در این نوع از حمله اطلاعات کاربران یک سایت را بدون اینکه خودشان آگاهی داشته باشند، به سرقت می برند.
- Reflected
- Stored
- Dom-Based

ارزیابی آسیب پذیری های زیرساخت های
حیاتی و حساس و مهم صنعتی

مقدمه

- سیستم‌های کنترل صنعتی در بخش‌های اساسی و زیرساختی هر کشوری نقش بسیار مهمی بازی می‌کنند که در صورت بروز مشکل در این سیستم‌ها آسیب‌های حیاتی و گاه جبران‌ناپذیری به کل کشور وارد می‌شود
- این تهدیدات در سطوح مختلف طرح و عملیاتی می‌شوند (حملات سایبری دولتی توسط کشورهای متخاصم گرفته تا اشتباهات و بی‌احتیاطی مدیران و کارمندان داخلی)

دلایل مهم حملات بر روی سامانه‌های کنترل صنعتی

- سیستم‌های کنترل صنعتی امن هستند چون به‌صورت ایزوله کار می‌کنند و ارتباطی با شبکه‌های خارجی ازجمله اینترنت ندارند
- سیستم‌های کنترل صنعتی امن هستند چون نفوذگران خارجی اطلاعات فنی لازم را در مورد این سامانه‌ها ندارند

تفاوت بین امنیت فناوری اطلاعات با امنیت سیستمهای کنترل صنعتی

شبکه ها و کامپیوترهای فناوری اطلاعات	سیستم های کنترل صنعتی
درصورت از دست دادن داده و یا بروز وقفه های ناخواسته ، می توان سیستم را با راه اندازی مجدد و یا برگرداندن فایل های پشتیبان به حالت اولیه برگرداند.	از دست دادن داده و یا بروز وقفه قابل تحمل نیست و ممکن است نتایج مهلکی را به دنبال داشته باشد
با تاخیر ناخواسته می توان کنار آمد	تاخیر زیاد قابل تحمل نیست
درصورت بروز مشکلات حاد برای سیستم با راه اندازی مجدد آن می توان مشکل ناخواسته را به نوعی حل کرد!	کارکرد سیستم می بایست همواره عاری از خطاء باشد . از کار افتادن سیستم حتی برای لحظاتی اندک می تواند فاجعه آمیز باشد
از نرم افزارهای آنتی ویروس استفاده زیاد می شود	بکارگیری نرم افزارهای آنتی ویروس در اکثر موارد مشکل است ، چراکه تاخیر قابل تحمل نمی باشد .
ارایه دوره های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی بسیار متداول است	ارایه دوره های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی کم است
از رمزنگاری استفاده می شود	تعداد بسیار زیادی از سیستم های کنترل صنعتی داده و پیام های کنترلی را به صورت غیر رمز شده ارسال می نمایند.
تست نفوذ به صورت ادواری انجام می شود	تست نفوذ به صورت ادواری در شبکه کنترلی انجام نمی شود و زمانی هم که این کار انجام می شود می بایست این کار با دقت صورت پذیرد تا باعث بروز اختلال نگردد .
پیاده سازی **patch** نرم افزارها به صورت ادواری انجام می شود	پیاده سازی **patch** نرم افزاری می بایست با دقت صورت پذیرد و معمولا" مستلزم هماهنگی با شرکت فروشنده تجهیزات کنترل صنعتی می باشد
ممیزی امنیت اطلاعات لازم است و معمولا" به صورت ادواری انجام می شود	ممیزی امنیت اطلاعات بطور ادواری انجام نمی شود
تجهیزات معمولا" هر سه تا پنج سال جایگزین و یا ارتقاء می یابند	تجهیزات استفاده شده برای مدتی طولانی و بدون جایگزینی استفاده می گردند .

تفاوت بین امنیت فناوری اطلاعات با امنیت سیستمهای کنترل صنعتی

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is a serious concern
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime is not acceptable Major risk impact is regulatory non-compliance, loss of life, equipment, or production

تفاوت بین امنیت فناوری اطلاعات با امنیت سیستمهای کنترل صنعتی

Category	Information Technology System	Industrial Control System
Communications	Standard communications protocols Primarily wired networks with some localized wireless capabilities Typical IT networking practices	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite) Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. PCS outages often must be planned and scheduled days/weeks in advance
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Access to Components	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

آسیب‌پذیری‌های پروتکل‌های Siemens

- پارامترها، سرویس‌ها و مکانیزم‌های امنیتی در پروتکل‌های Siemens وجود ندارد.
- به علت بهره‌گیری از قاعده لایه‌بندی در طراحی پروتکل‌های Siemens، حتی در صورت ایجاد یک کانال ارتباطی رمزنگاری شده میان سرور و کلاینت پروتکل، همچنان امکان طراحی و اجرای حملات MITM وجود دارد.
- هیچ‌گونه تغییر و به‌روزسانی در خصوص پروتکل از اواخر دهه ۸۰ میلادی صورت نپذیرفته است.

برخی از مهمترین آسیب پذیریهای تجهیزات کنترل صنعتی

آسیب پذیریها بر روی اجزای سیستمهای کنترل صنعتی

آسیب پذیریهای موجود بر روی اجزای سیستمهای کنترل صنعتی

بررسی آسیب‌پذیری‌های RTU و PLC

- آسیب‌پذیری اعتبارسنجی نامناسب ورودی‌ها
- آسیب‌پذیری Directory Traversal
- آسیب‌پذیری شناسه‌های TCP قابل پیش‌بینی
- سوءاستفاده از گواهی‌های Hard Coded
- احراز هویت ضعیف (ارسال پیام‌های مخرب)
- احراز هویت ضعیف (آپلود Firmware)
- آسیب‌پذیری CROSS-SITE REQUEST FORGERY
- کنترل دسترسی نامناسب
- افشای اطلاعات
- آسیب‌پذیری سرریز بافر
- عدم وجود رمزنگاری در پروتکل ارتباطی
- حمله Reply (دور زدن مکانیسم احراز هویت)
- آسیب‌پذیری Cross Site Scripting
- آسیب‌پذیری NULL Pointer
- آسیب‌پذیری حلقه بی‌انتها

آسیب پذیریهای موجود بر روی اجزای سیستمهای کنترل صنعتی

بررسی آسیب‌پذیری‌های OPC COM و OPC DCOM

- کنترل دسترسی نامناسب
- آسیب‌پذیری سرریز بافر مبتنی بر **Stack**
- آسیب‌پذیری سرریز بافر مبتنی بر **Heap**
- آسیب‌پذیری حلقه بی‌انتها
- آسیب‌پذیری **Directory Traversal**
- مکانیسم احراز هویت ضعیف
- آسیب‌پذیری عدم کنترل صحیح خطا و استثنا
- آسیب‌پذیری سرریز عدد صحیح

آسیب پذیریهای موجود بر روی اجزای سیستمهای کنترل صنعتی

بررسی آسیب‌پذیری‌های HMI

- مکانیسم احراز هویت ضعیف
- استفاده از گذرواژه‌های پیش‌فرض
- استفاده از گذرواژه‌های HardCoded
- آسیب‌پذیری در برابر حمله Man In The Middle
- اعتبارسنجی ضعیف ورودی‌ها
- آسیب‌پذیری Cross Site Scripting
- آسیب‌پذیری CROSS-SITE REQUEST FORGERY

- آسیب‌پذیری از طریق TELNET
- سرریز بافر
- آسیب‌پذیری Directory Traversal
- دزدیدن نشست
- تزریق کد
- آسیب‌پذیری تزریق SQL

آسیب پذیریهای موجود بر روی اجزای سیستمهای کنترل صنعتی

بررسی آسیب‌پذیری‌های Historian

- اعتبارسنجی نامناسب ورودی‌ها
- آسیب‌پذیری سرریز بافر
- آسیب‌پذیری Cross Site Scripting
- آسیب‌پذیری Directory traversal
- عدم کنترل صحیح خطاها و استثناها
- آسیب‌پذیری SQL Injection

آسیب پذیریهای موجود بر روی اجزای سیستمهای کنترل صنعتی

بررسی آسیب‌پذیری‌های پروتکلهای ارتباطی

- اعتبارسنجی نامناسب ورودی‌ها
- آسیب‌پذیری سرریز بافر
- حمله Man In The Middle

آسیب پذیریها به دلیل مشکلاتی در طراحی شبکه و عدم استفاده از عناصر و سیاست‌های مناسب در کل شبکه

آسیب پذیریها به دلیل مشکلاتی در طراحی شبکه و عدم استفاده از عناصر و سیاست‌های مناسب در کل شبکه

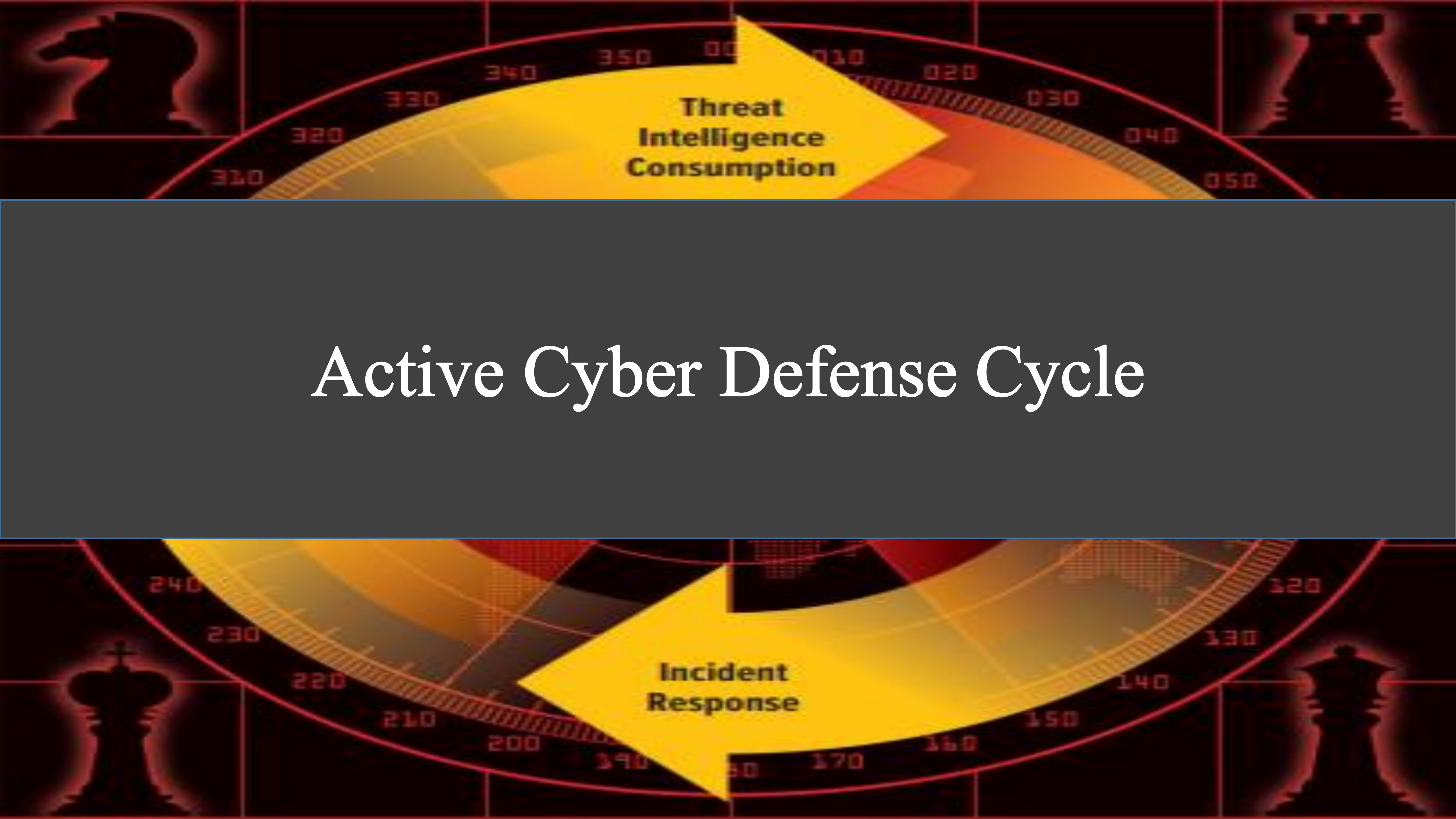
- عدم تعریف ناحیه بندی مناسب در شبکه
- عدم استفاده از فایروال‌های مناسب با پیکربندی صحیح
- عدم استفاده از سامانه تشخیص نفوذ (IDS)
- عدم استفاده از سامانه مدیریت اطلاعات و رخدادهای امنیتی (SIEM)
- کنترل دسترسی نامناسب فیزیکی
- دسترسی‌های حفاظت نشده برنامه نویسان
- ارتباطات ناامن Wireless

آسیب پذیریها به دلیل مشکلاتی در طراحی شبکه و عدم استفاده از عناصر و سیاست‌های مناسب در کل شبکه

- ارتباطات ناامن از طریق VSATها
- عدم وجود سیستم‌های پشتیبان
- عدم تعریف سیاست‌های مناسب برای به‌روزرسانی سیستم‌ها
- عدم استفاده از مکانیسم‌های رمزنگاری
- به اشتراک‌گذاری فایلها
- پیکربندی ناامن پایگاه داده

Active Cyber Defense

Active Cyber Defense Cycle



Threat Intelligence

Threat Intelligence

- Intelligence اطلاعات و دانشی راجع به یک عامل مخرب است که از طریق مشاهده، بررسی، تحلیل و درک به‌دست می‌آید.
- نکته اول، Intelligence اطللاعات یا داده تنها نیست بلکه اطلاعاتی است که تحلیل شده است، یعنی از نتیجه یک تحلیل و بررسی به دست آمده است.
- نکته دوم، Intelligence باید عملیاتی (قابل به‌کارگیری) باشد. در غیر این صورت داشتن آن مزیتی نخواهد داشت.

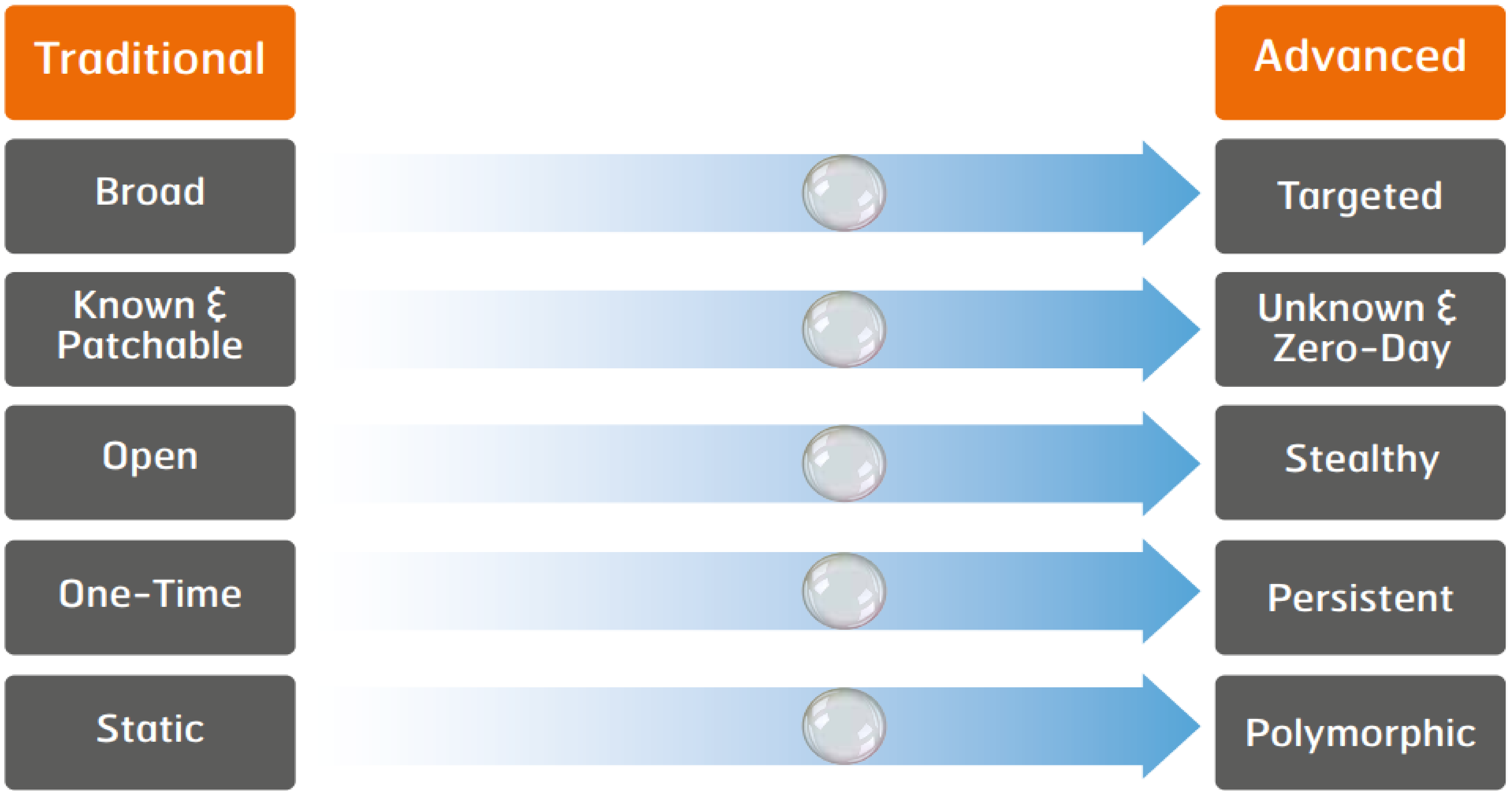
Threat Intelligence

- Threat Intelligenceیک دانش مبتنی بر ادله (شواهد) شامل محتوای زمینه ای، ساز و کارها، نشانگرها، پیامدها و توصیه های عملی پیرامون یک تهدید موجود یا در حال وقوع علیه دارایی های سازمان است. این دانش می تواند برای کمک به تصمیم گیری درباره چگونگی پاسخگویی و مواجعه با آن تهدید یا مخاطره مورد استفاده قرار گیرد. (گارتنر، ۱۶ می ۲۰۱۳)

Threat Intelligence ، اطلاعاتی است که به ما در شناسایی مهاجم و دستیابی به پاسخگویی سریع و موثر کمک می کند

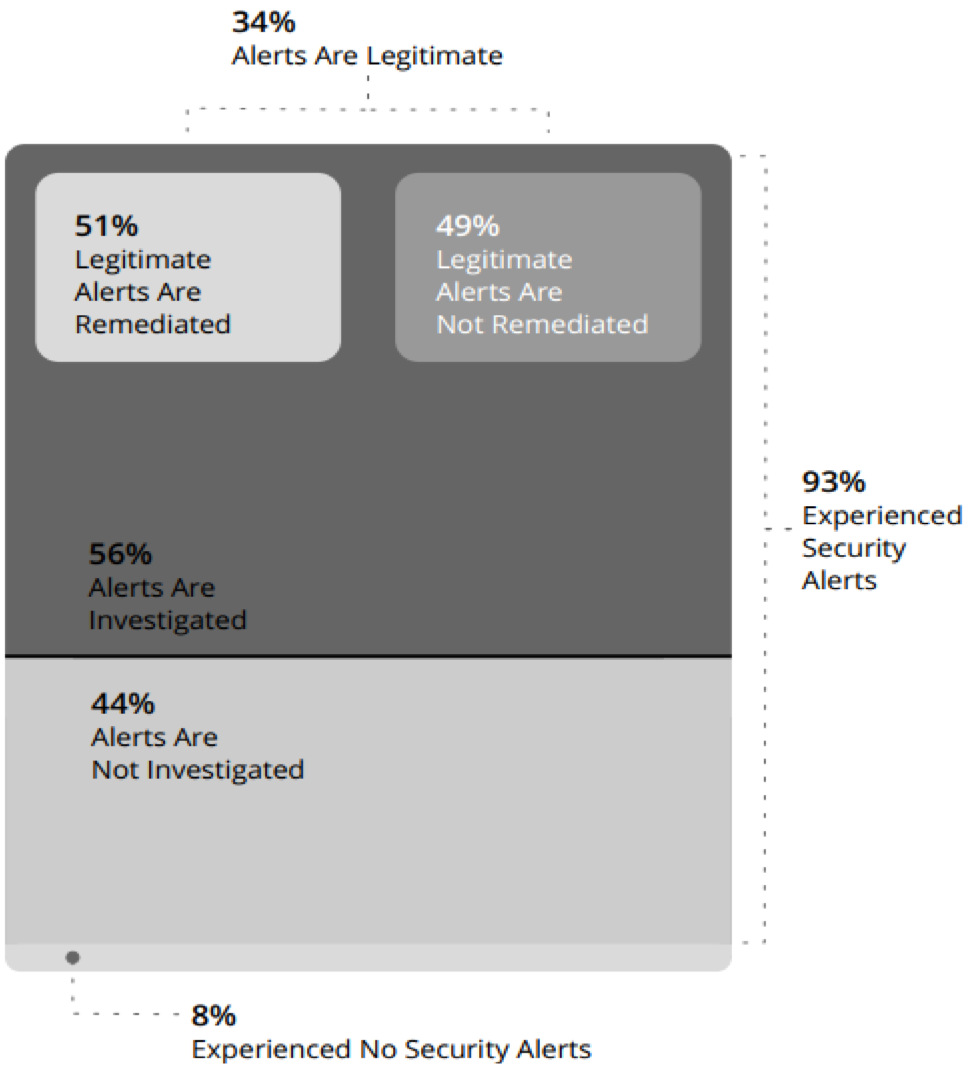
Threat Intelligence

The characteristics and nature of the transformation in the malware threat



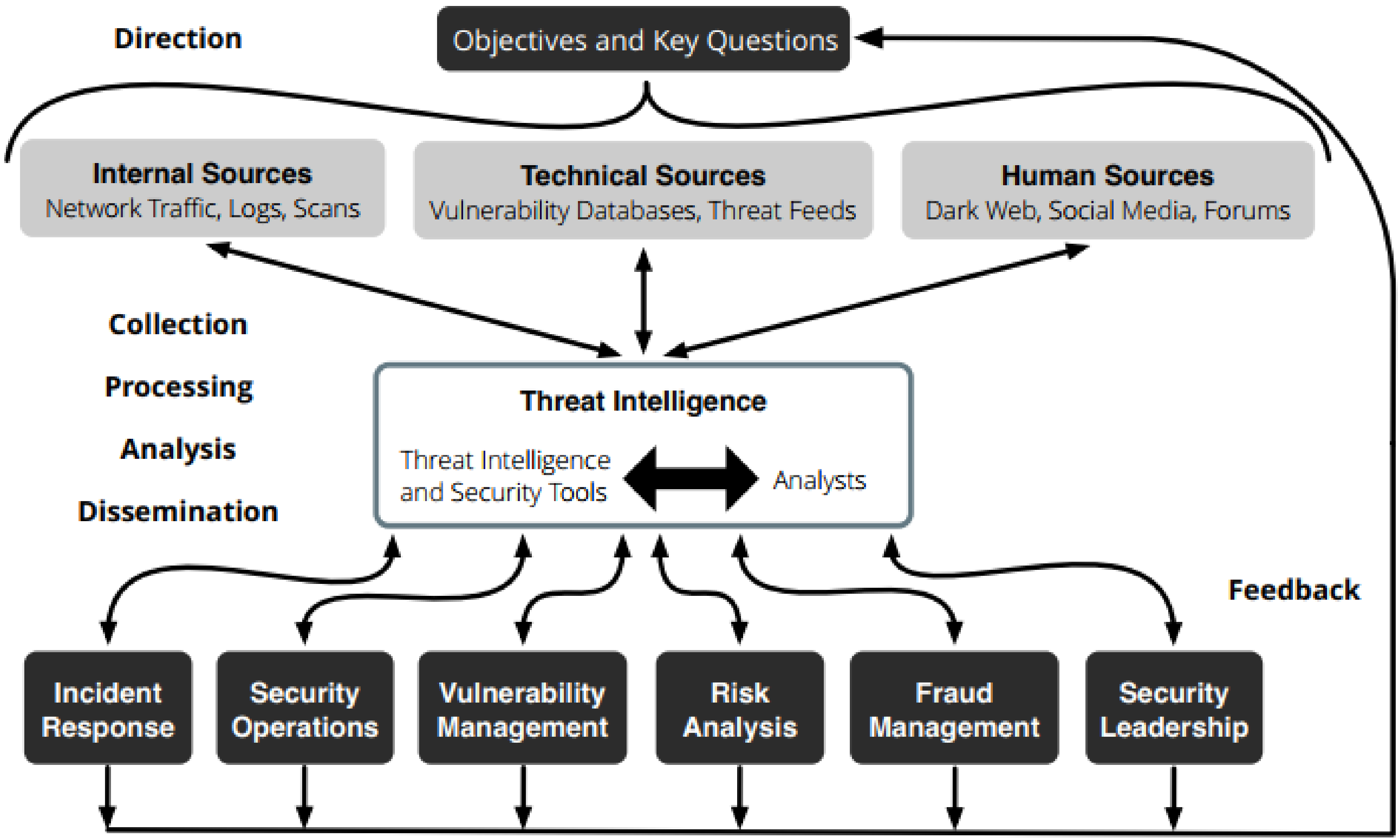
Threat Intelligence

Many threat alerts are not investigated or remediated. (Source: Cisco)



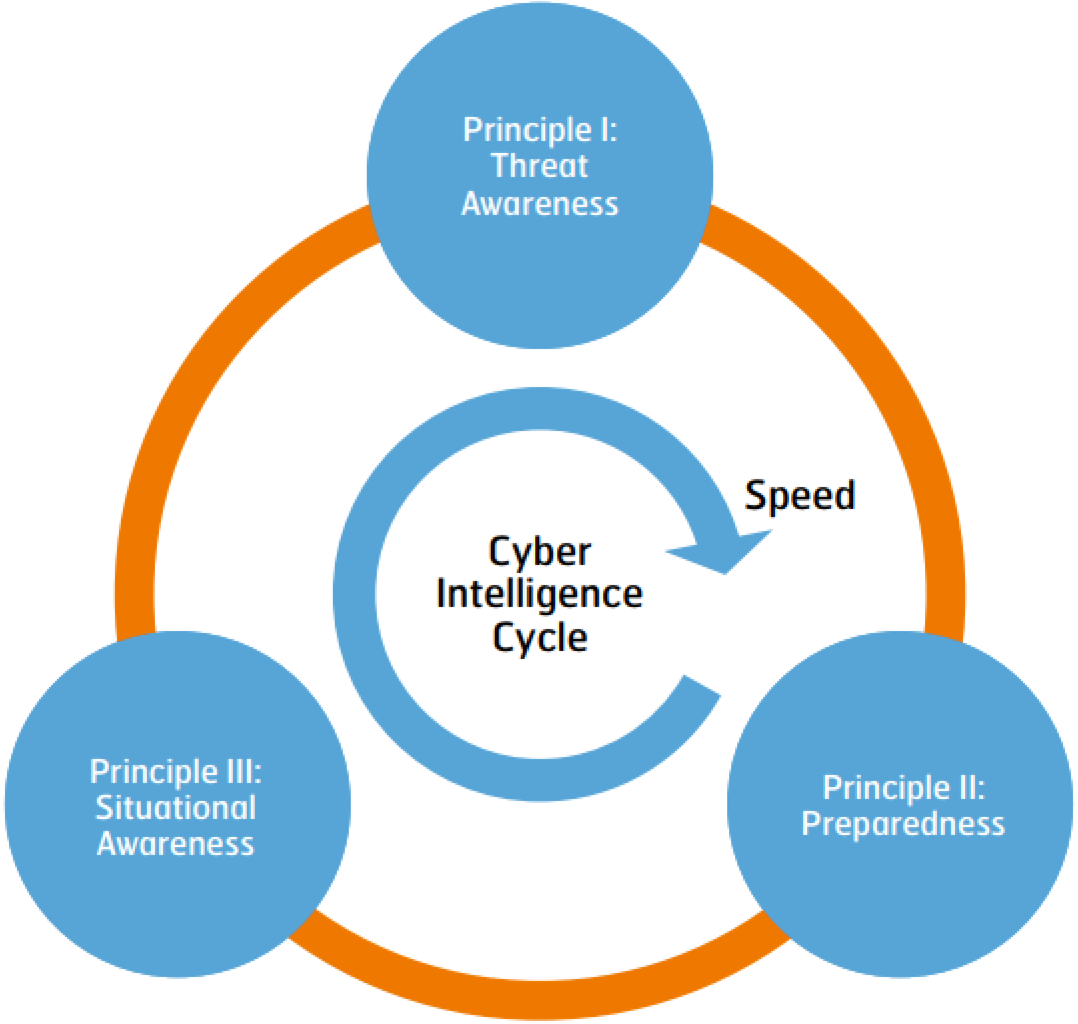
Threat Intelligence

Threat intelligence and the six phases of the intelligence lifecycle

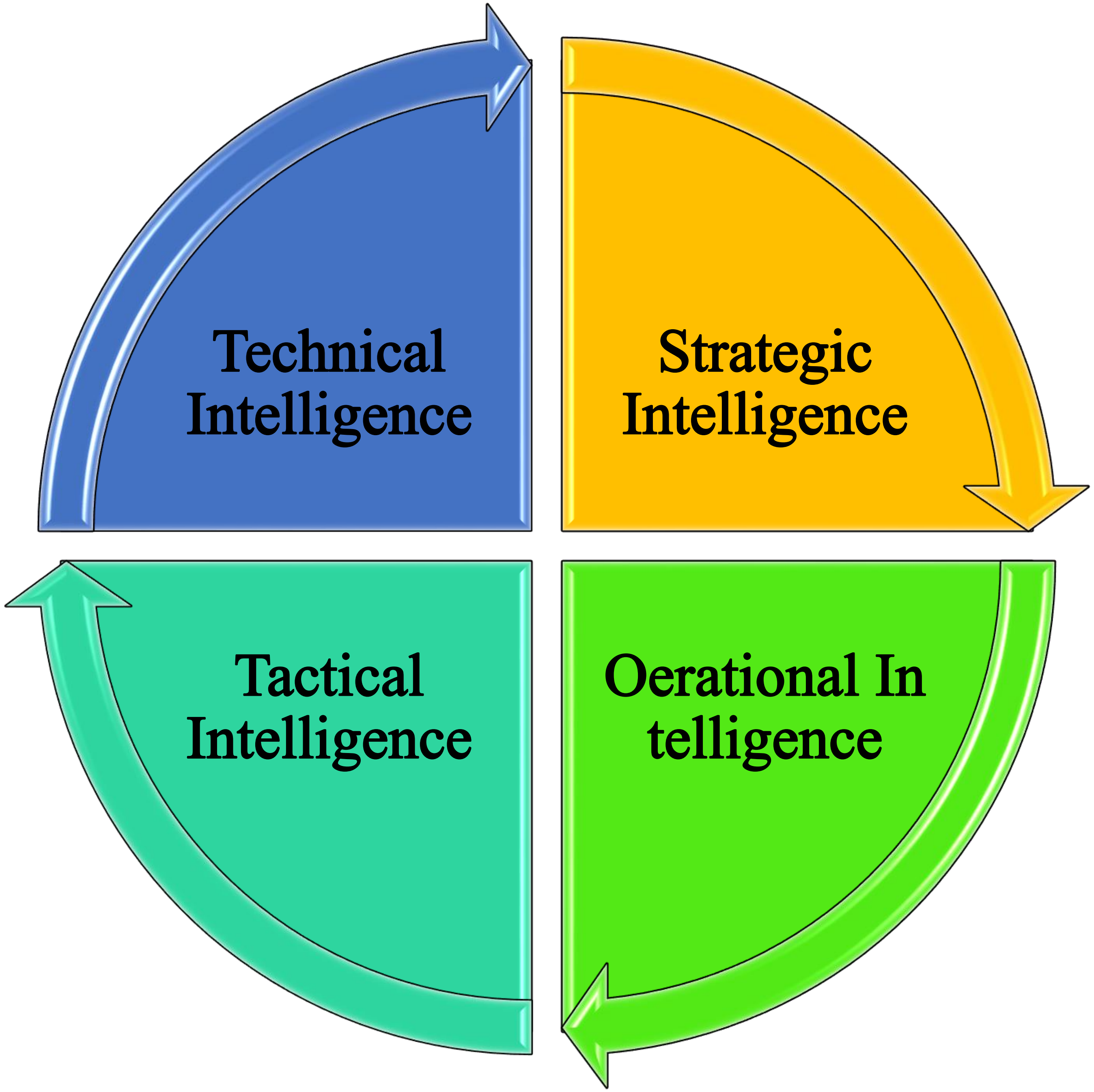


Threat Intelligence

3 principles for Cyber Threat Intelligence



Threat Intelligence



Threat Intelligence

Subtypes of threat intelligence

Threat Intelligence

Strategic Intelligence

- اطلاعات سطح بالایی که توسط هیئت رئیسه/سهامداران یا دیگر تصمیم گران اصلی یک سازمان مورد استفاده قرار می گیرند.
- موارد مرتبط با تاثیر مالی رخداد سایبری، روندهای حملات آتی، حوزه های مستعد برای حمله مهاجمان و حوزه اثرگذار بر تصمیمات کلان و سطح بالای تجاری سازمان
- چنین اطلاعاتی به شرکت ها در تعیین اقدامات، ظرفیت ها و بودجه لازم را برای مقابله و کاهش خطر حملات احتمالی کمک می کند

Threat Intelligence

Oerational Intelligence

- اطلاعات مربوط به حملات خاص در شرف وقوع علیه سازمان
- این اطلاعات توسط کارمندان امنیتی سطح بالای سازمان (مدیریت لایه میانی) نظیر مدیران امنیت اطلاعات یا سرپرستان واحد پاسخگویی به رخداد مورد استفاده قرار می گیرند.

Threat Intelligence

Tactical Intelligence

شیوه ها
Tactics

فنون
Techniques

رویه ها
Procedures

Threat Intelligence

Technical Intelligence

- اطلاعاتی که برای مصارف فنی مورد استفاده قرار می گیرند.
- **Indicator of Compromise**
  - IOCها یکی از عملیاتی‌ترین نوع CTIها است که شامل مواردی نظیر آدرس IP، نام دامنه، URL و هش فایل است.
- رایج ترین استفاده کنندگان از هوش اطلاعاتی فنی افراد تیم پاسخگویی به رخداد و مرکز عملیات امنیت هستند.
- محدوده زمانی استفاده از این اطلاعات می تواند چند ساعت تا چند ماه را شامل شود.

Threat Intelligence

Threat Intelligence Sources

Threat Intelligence Sources

Technical sources (e.g., threat feeds) — Available in huge quantities, often for free. Technical sources are easy to integrate with existing security technologies but often contain a high proportion of false positives and outdated results.

Media (e.g., security websites, vendor research) — These sources often provide useful information about emerging threats but are hard to connect with technical indicators in order to measure risk.

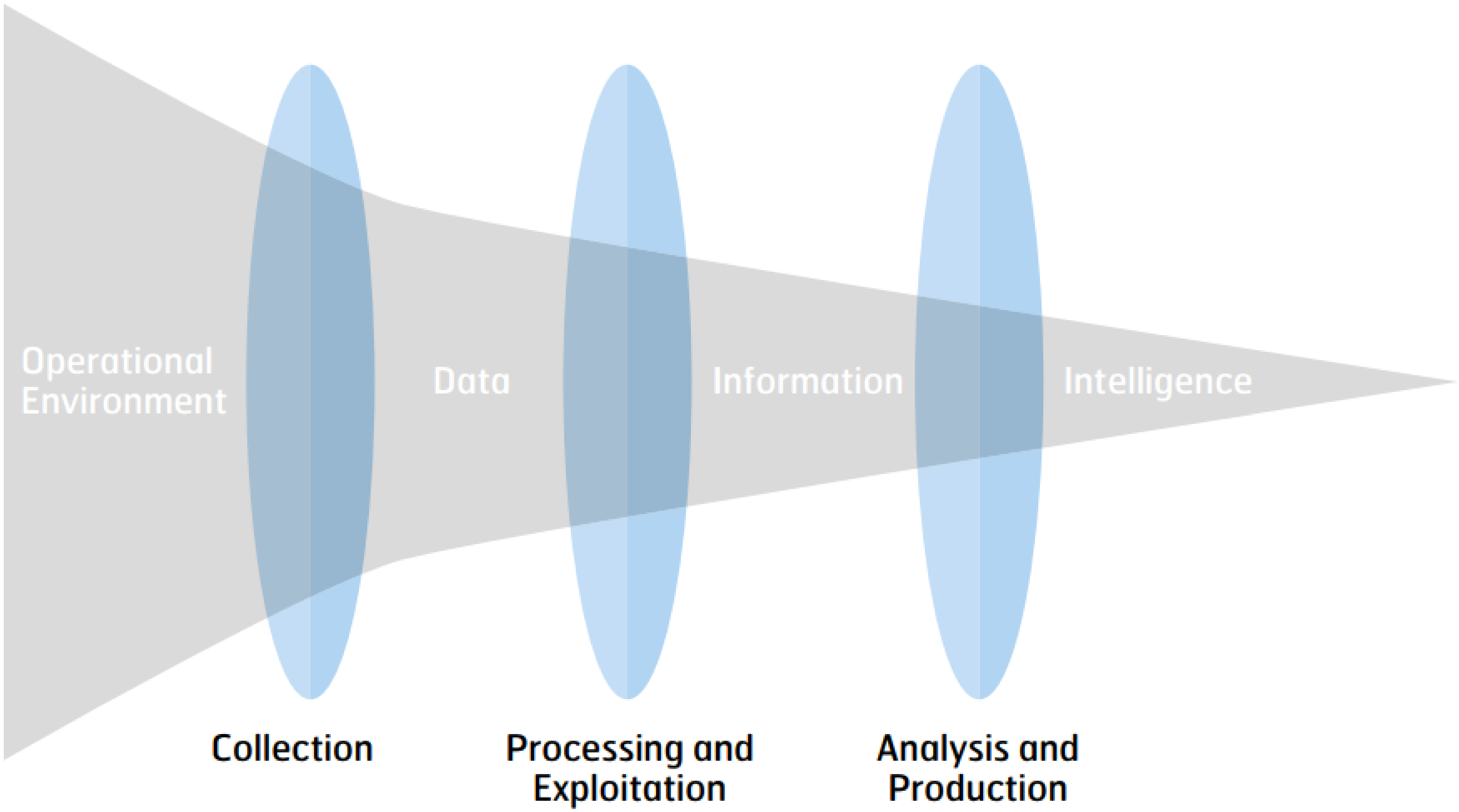
Social media — Social channels offer huge amounts of valuable data, but it comes at a price. False positives and misinformation are rampant, so determining which insights are usable requires a tremendous amount of cross-referencing with other sources.

Threat actor forums — Specifically designed to host relevant discussions, forums offer some of the most helpful insights available anywhere. Once again, though, analysis and cross-referencing are essential to determine what is truly valuable.

The dark web (including markets and forums) — While often the birthplace of hugely valuable intelligence, dark web sources can be extremely hard to access, particularly those that play host to serious criminal communities.

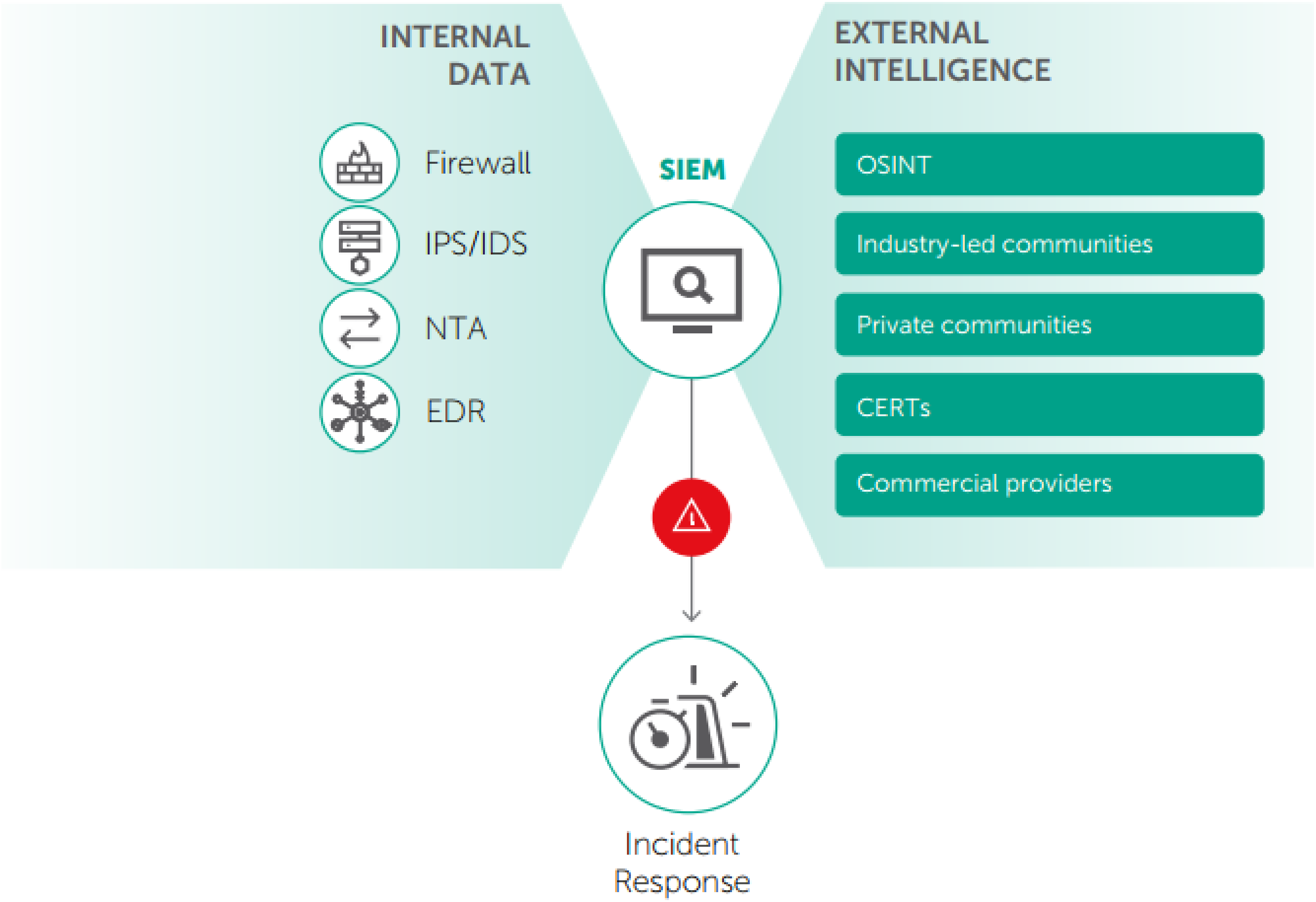
Threat Intelligence

Relationship between data, information and intelligence



Threat Intelligence

Operationalizing External Threat Intelligence



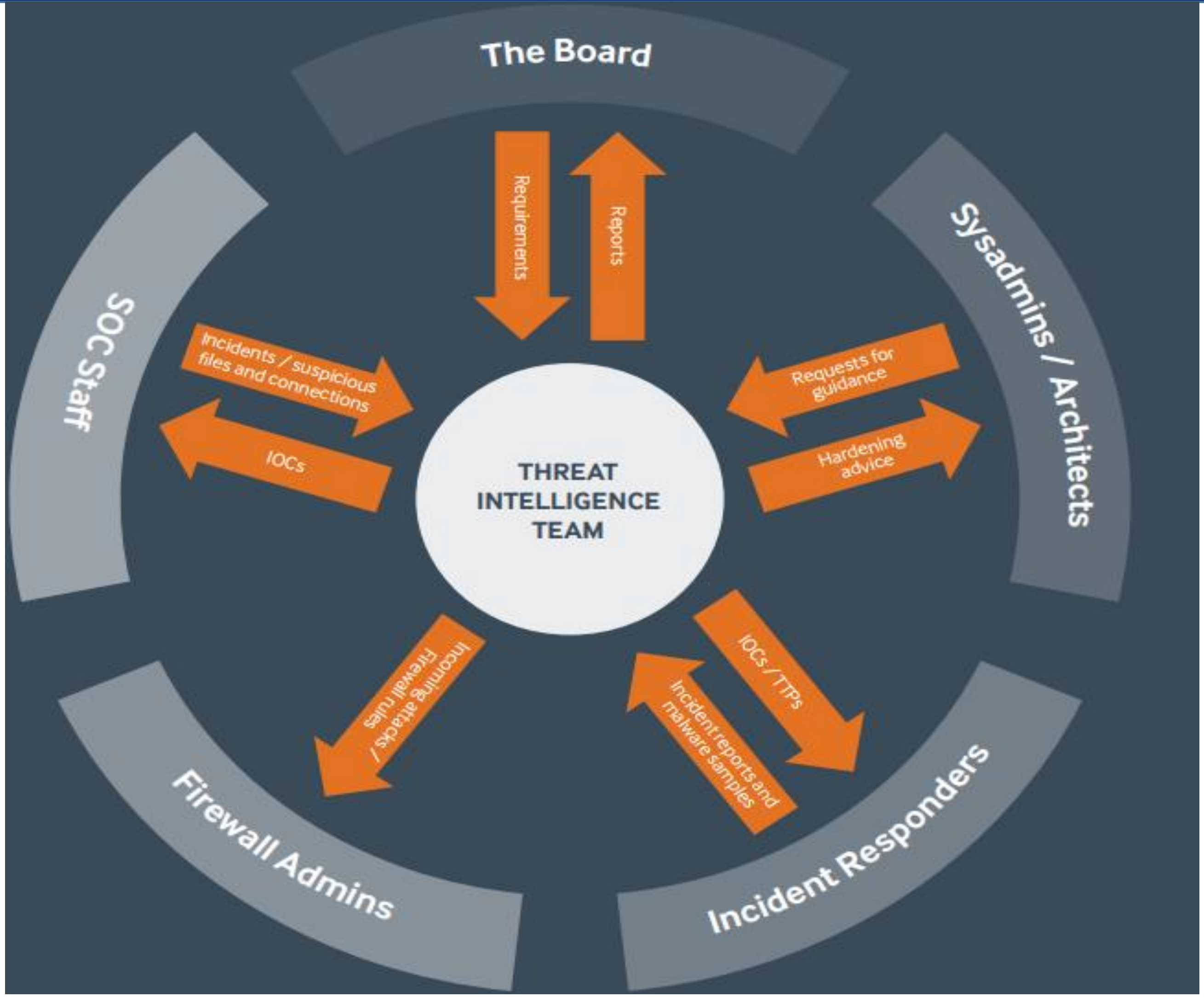
Threat Intelligence

The Data Feeds for TI

- IP Reputation Feed
- Malicious and Phishing URL Feed
- Botnet C&C URL Feed
- Mobile Botnet C&C URL Feed
- Ransomware URL Feed
- Vulnerability Data Feed
- Whitelisting Data Feed
- APT IoC Feeds
- IoT URL Feed
- Malicious Hash Feed

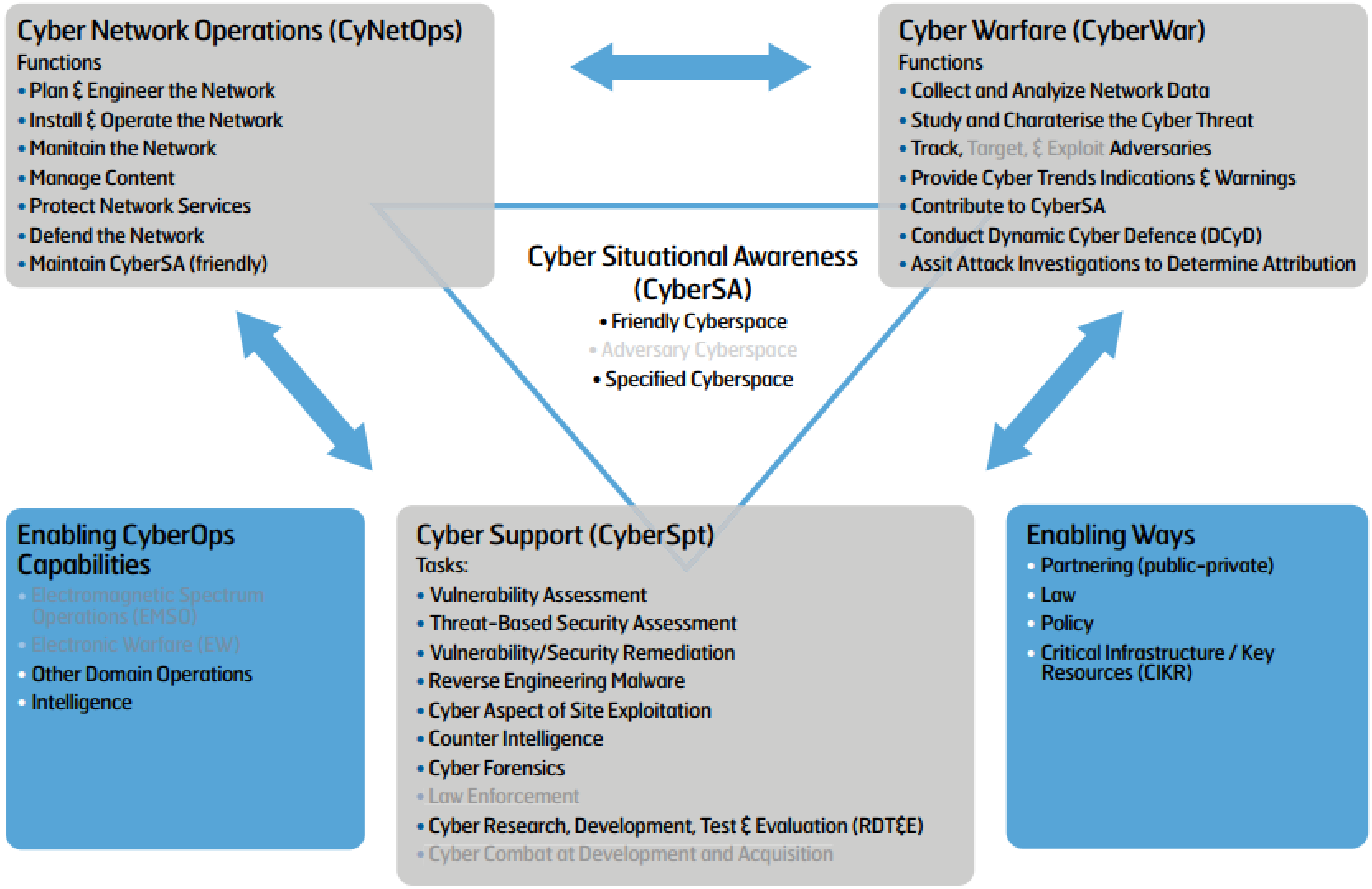
Threat Intelligence

Functions of a Threat Intelligence Team



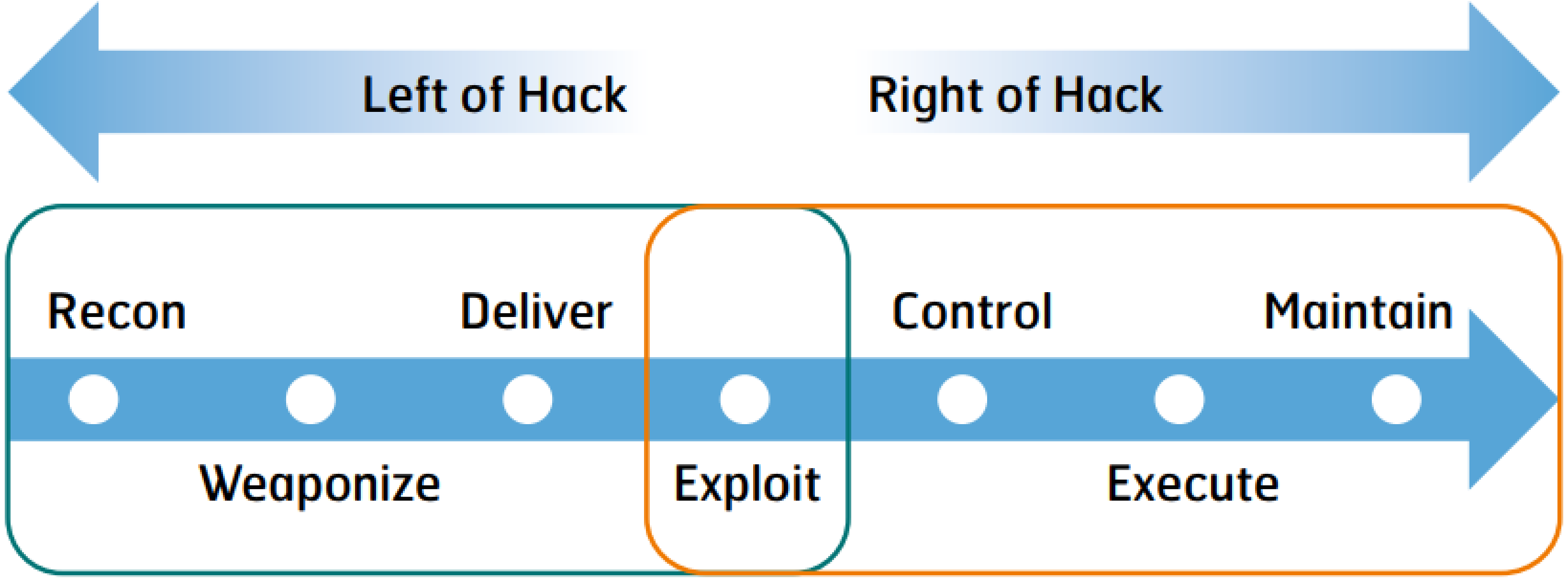
Threat Intelligence

US TRADOC Cyber Operations Model



Threat Intelligence

Cyber Kill Chain

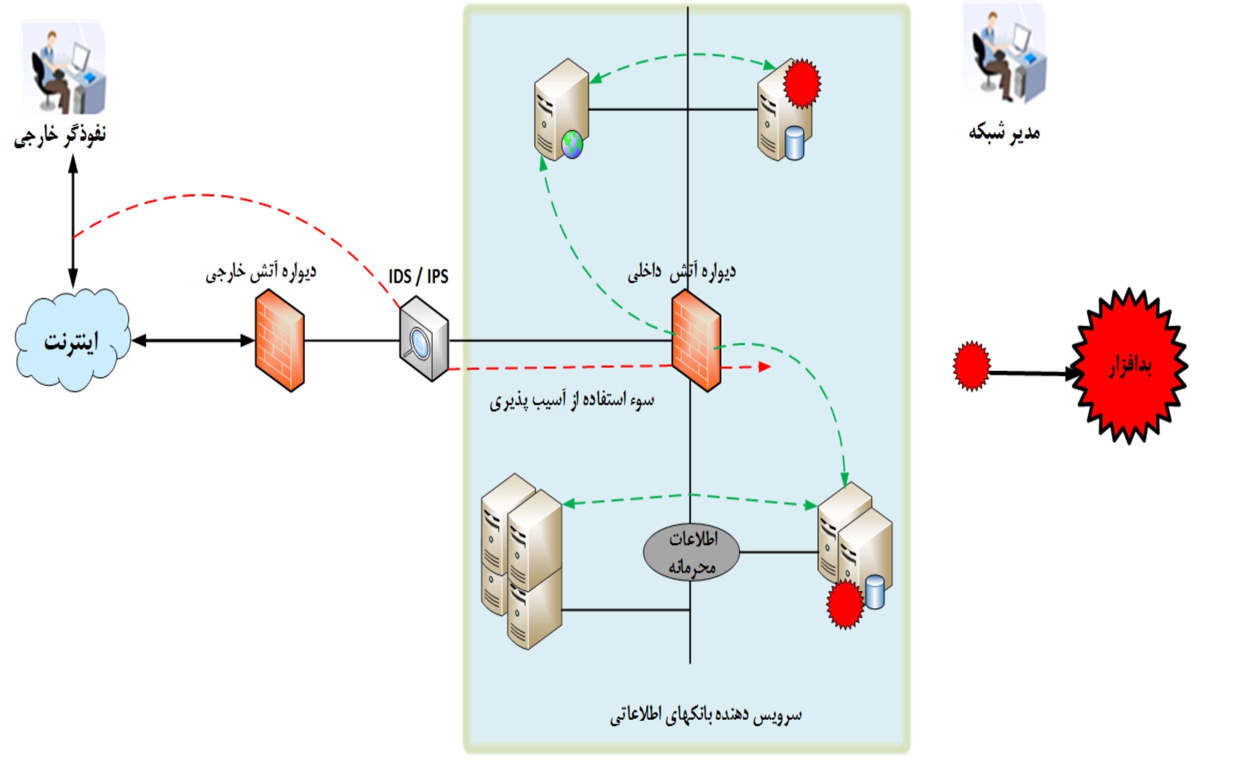


Threat Intelligence &

Security Operation Center (SOC)

چرا مراکز عملیات امنیت پیاده سازی میشوند؟

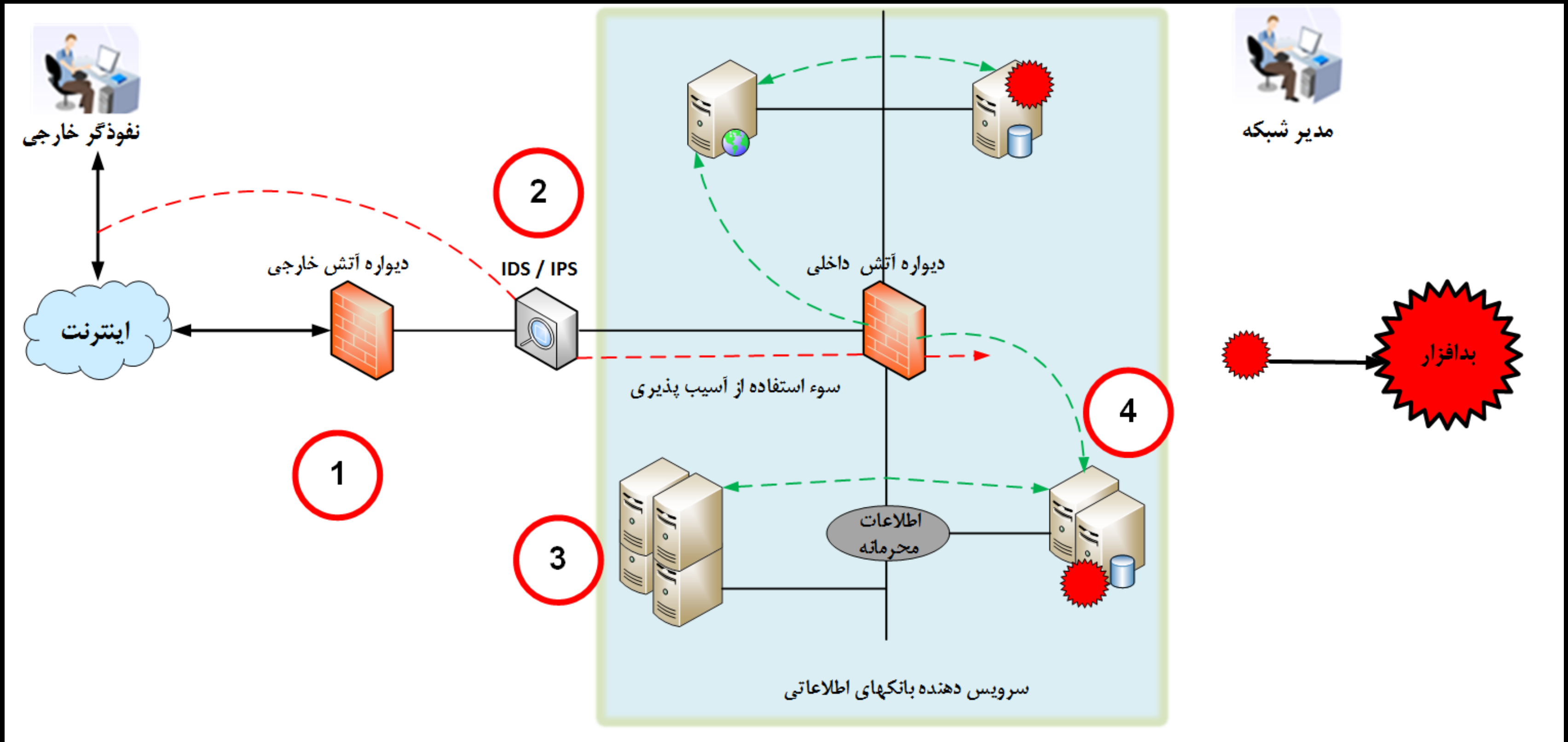
کالبدشکافی یک نفوذ ساده



- نفوذ گر با پایش لایه دفاعی بیرونی، در جستجوی یک شکاف امنیتی در شبکه است.
- با عبور سامانه دفاعی و با استفاده از یک نقطه آسیب پذیر به سرویس دهنده وب نفوذ میکند.
- از سرویس دهنده وب به سمت سرویس دهنده های بانک اطلاعاتی که حاوی اطلاعات محرمانه است پیشروی میکند.
- با نصب نرم افزارهای مخرب که باعث گشودن یک درب پشت امکان دسترسی و سرقت اطلاعات را می یابد.

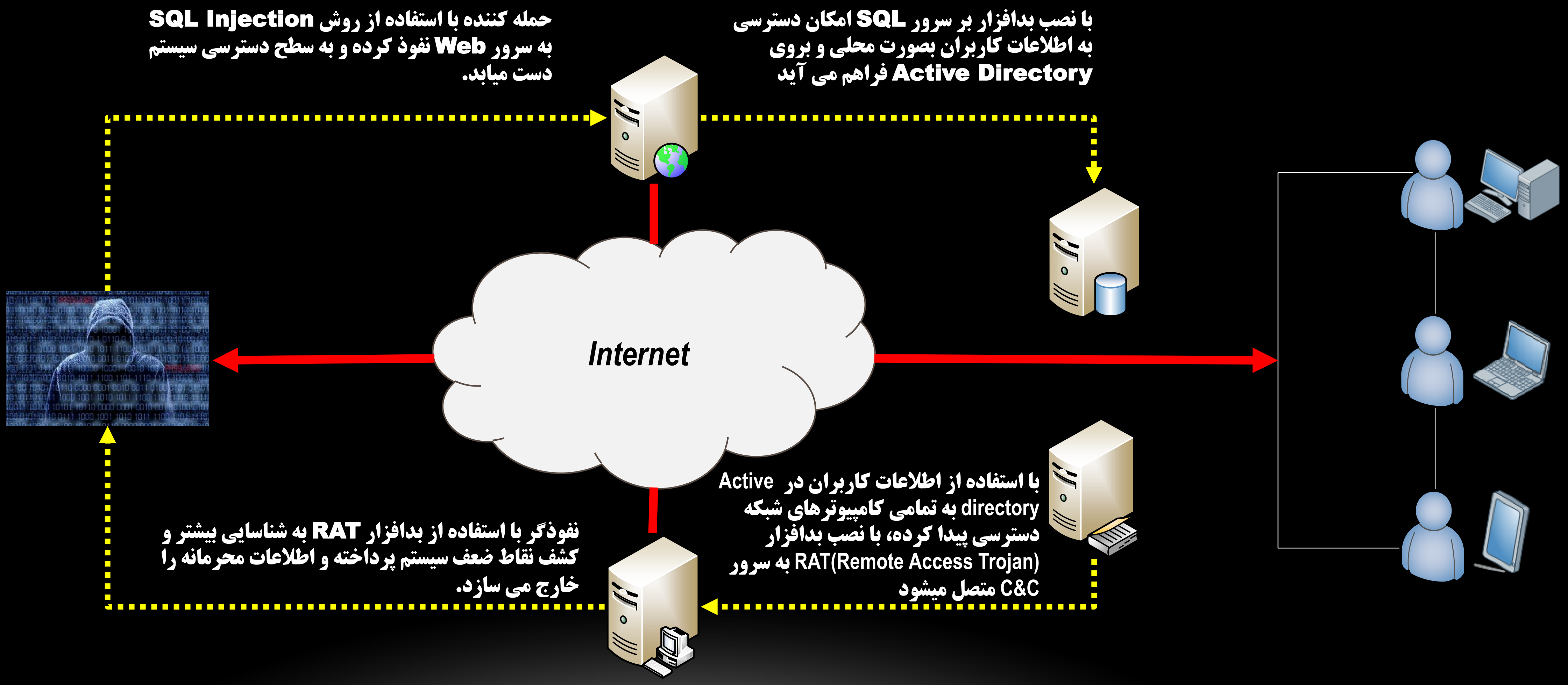
چگونه می توان از این نفوذ آگاه شد؟

1. وقایع ثبت شده دیواره های آتش (رخدادهای شناسایی، پایش و...).
2. وقایع ثبت شده سامانه های IDS/IPS (رفتار غیرعادی).
3. وقایع ثبت شده دز سرویس دهنده های وب/برنامه های کاربردی (ترافیک ورودی/خروجی، دسترسی ها)
4. وقایع بانکهای اطلاعاتی



با وجود SOC امکان ردیابی سریع و دفع نفوذ وجود دارد.

چگونگی انجام حملات

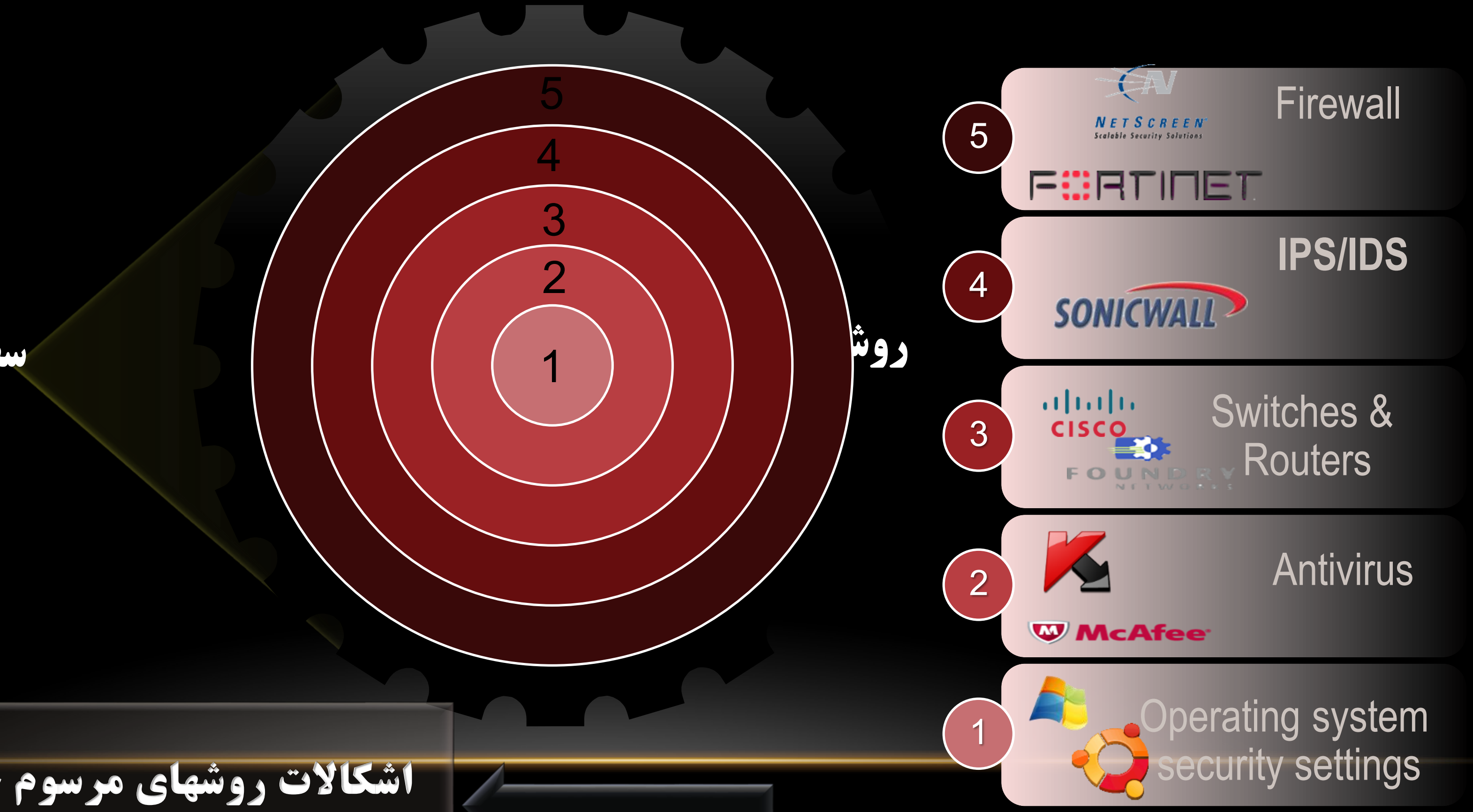


مرکز عملیات امنیت
SOC

دفاع درعمق

امنیت در سازمانهای امروزه

سطوح امنیت در یک سازمان



اشکالات روشهای مرسوم چیست؟

نواقص راه حلهای سنتی

- نواقص ذاتی
  - ❄ هنجارسازی (Normalization)
  - ❄ تجمیع (Aggregation)
  - ❄ ارتباط یابی (Correlation)
- برخورداری از تیمهای پشتیبانی جداگانه
- پایش و مدیریت شبکه با تجهیزات متنوع و گوناگون
- زمان بر بودن شناسایی و تجزیه و تحلیل تهدیدات

امنیت سازمانی

نقایص راه حل های مرسوم

- امکانپذیر نبودن تحلیل حجم های بالای وقایع ثبت شده (Log) توسط نیروی انسانی
- عدم امکان مرتبط سازی وقایع ثبت شده و کشف حملات پیچیده توسط نیروی انسانی
- مشکل یکپارچه سازی وقایع ثبت شده
- گروه های پشتیبانی مجزا
- زمان بر بودن تحلیل وقایع ثبت شده
- مشکل تحلیل بلادرنگ نفوذ
- پایش امنیتی توسط تجهیزات مختلف و گروه های متفاوت

مرکز عملیات امنیت
SOC

مرکز عملیات امنیت

نیروی انسانی

فناوری

فرآیندها

SOC

ساختار یکپارچه برای ایمن سازی سازمانها

وجود ساختار یکپارچه باعث ایجاد هم افزایی در سازمان خواهد گردید.

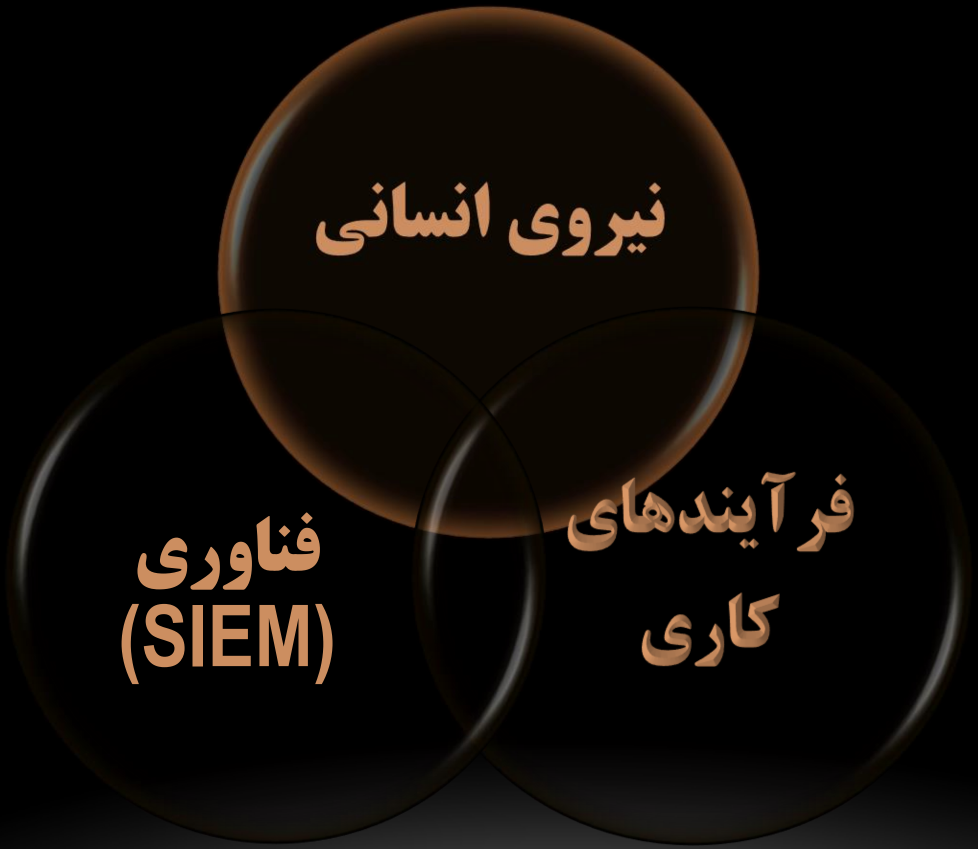
امنیت هوشمند

مزایای مرکز عملیات امنیت برای سازمان ها

- پشتیبانی از امنیت شبکه در قبال تهدیدات داخلی و خارجی
- پایش آنی رخدادها و تهدیدات سایبری
- پایش تجهیزات و شبکه به صورت ۲۴ x ۳۶۵
- طبقه بندی رخدادهای معنا دار
- کاهش زمان جمع آوری و تحلیل رخدادها
- کشف ارتباطات بین رخدادها و حوادث مختلف
- هماهنگ سازی رخدادها و سیاستهای امنیتی سازمان
- جمع آوری و تحلیل ترافیک شبکه
- دریافت منظم اطلاعات و آگاه سازی سازمان

- شناسایی آسیب پذیری های شبکه و سامانه های در معرض خطر
- سیاستهای پیشگیرانه در قبال آسیب پذیری ها
- اطلاع رسانی هماهنگ رخدادها و حوادث امنیتی
- ایجاد روال های منظم پیگیری رخدادها در محدوده سامانه
- بررسی حادثه امنیتی توسط گروه حرفه ای
- اجتناب از عملیات اضافی در رسیدگی به حادثه امنیتی
- تولید گزارشهای مختلف برای مدیران و متخصصان فنی
- کشف شواهد قانونی برای پیگیری یک حادثه امنیتی

اجزای مرکز عملیات امنیت



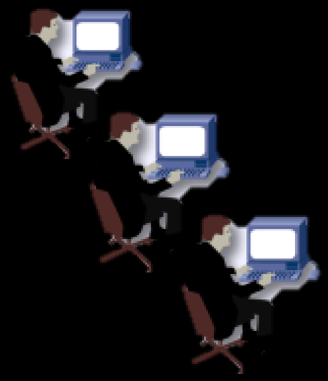
نیروی انسانی

لایه های مرکز عملیات امنیت

لایه اول: اپراتورهای امنیتی

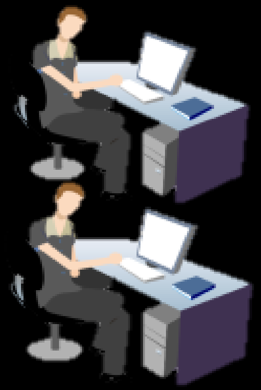
- پایش
- اطلاع رسانی
- گزارش دهی
- مستندسازی

لایه دوم: تحلیل گران امنیتی



- تحلیل و تحقیق
- مدیریت آسیب پذیری
- مدیریت تجهیزات و پیکربندی

لایه سوم: مدیران حوادث امنیتی



- پژوهش در تهدیدات
- تحلیل و پژوهش پیشرفته

جریان رویه های
مرکز عملیات امنیت

فرآیندها

ساختار مرکز عملیات امنیت سایبری (فرایندهای کاری-۱)

فرایند های SOC

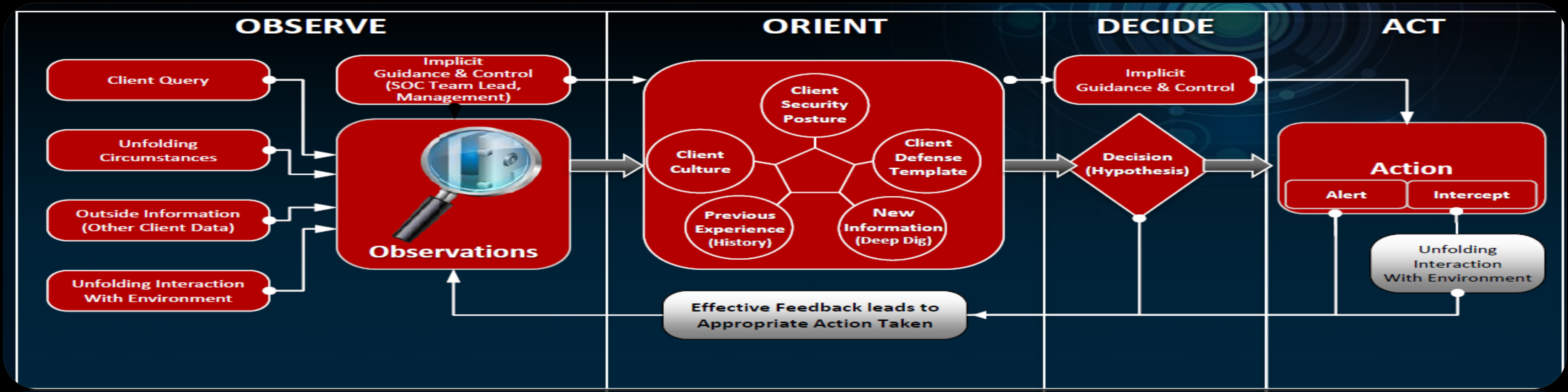
چرخه OODA
آموزش
زمانبندی
تعیین صلاحیت تهدید ها
کاهش خطر تهدید ها
طبقه بندی حوادث
هشدار دهی
مدیریت حوادث

ثبت تیکت
اشتراک گذاری دانش
آموخته ها وسازماندهی آن
هماهنگی باNOC

ساختار مرکز عملیات امنیت سایبری (فرایندهای کاری-۲)

1

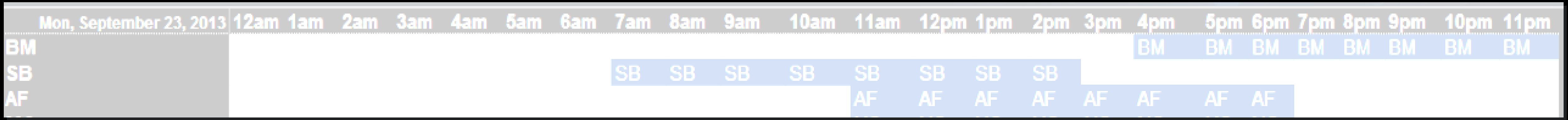
کلیه فرایند های مرکز عملیات امنیت در ٤ قسمت که جریان کاری آنها به صورت یک حلقه بیان می شود قابل مشاهده است :



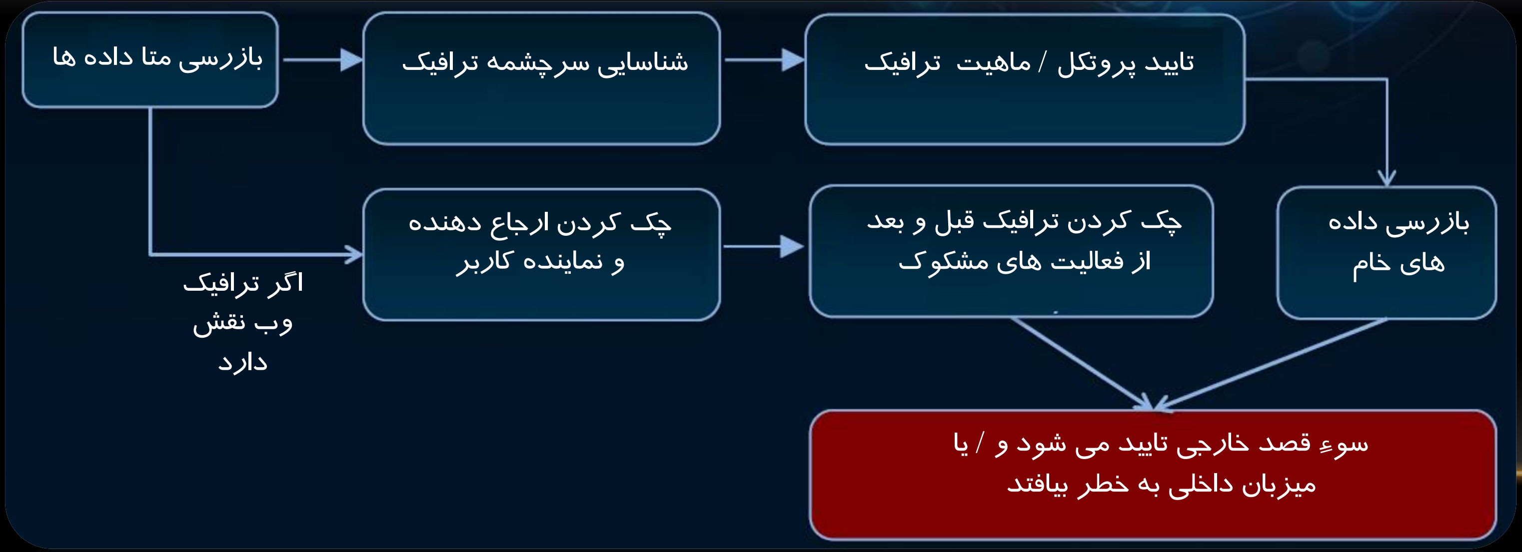
ساختار مرکز عملیات امنیت سایبری (فرایندهای کاری)

2

3



4



ساختار مرکز عملیات امنیت سایبری (فرایندهای کاری-۳)

5

Traffic blocked by FW/NGFW

No

Traffic blocked by IDS

No

IP/domain blacklisted

No

Manual TCP kills

کاهش خطرات تایید شده

تأییدیه اسپم : Live TCP dump on port 25

رد کردن میل سرور در پاسخ به اسپم

اگر SPAMINGموردتاییداست پورت ۲۵ برای آن دستگاه خاموش می شود

هشدار و درخواس جدا کردن ماشین از شبکه

برداشتن مانع از روی پورت ۲۵ بعد از اینکه دستگاه پاکسازی شد

قرار دادن یک " دیده بان " در آن دستگاه به مدت ۲۴ ساعت دیگر

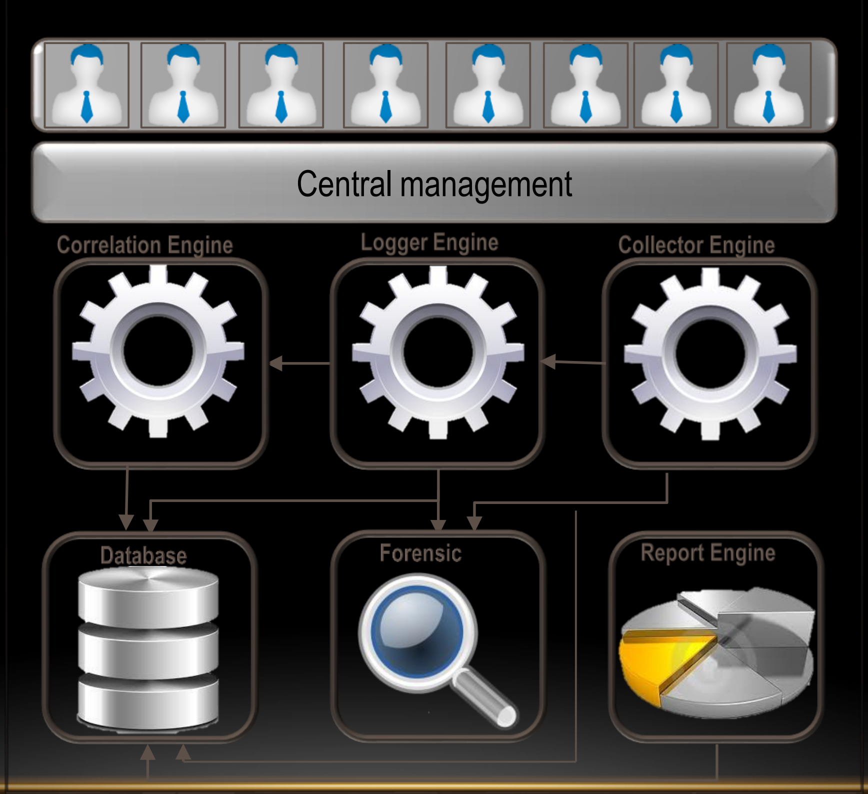
کاوش در عمق به منظور شناسایی دلیل مشکل
از روی ترافیک وب /پهنای باند و...
Back channles

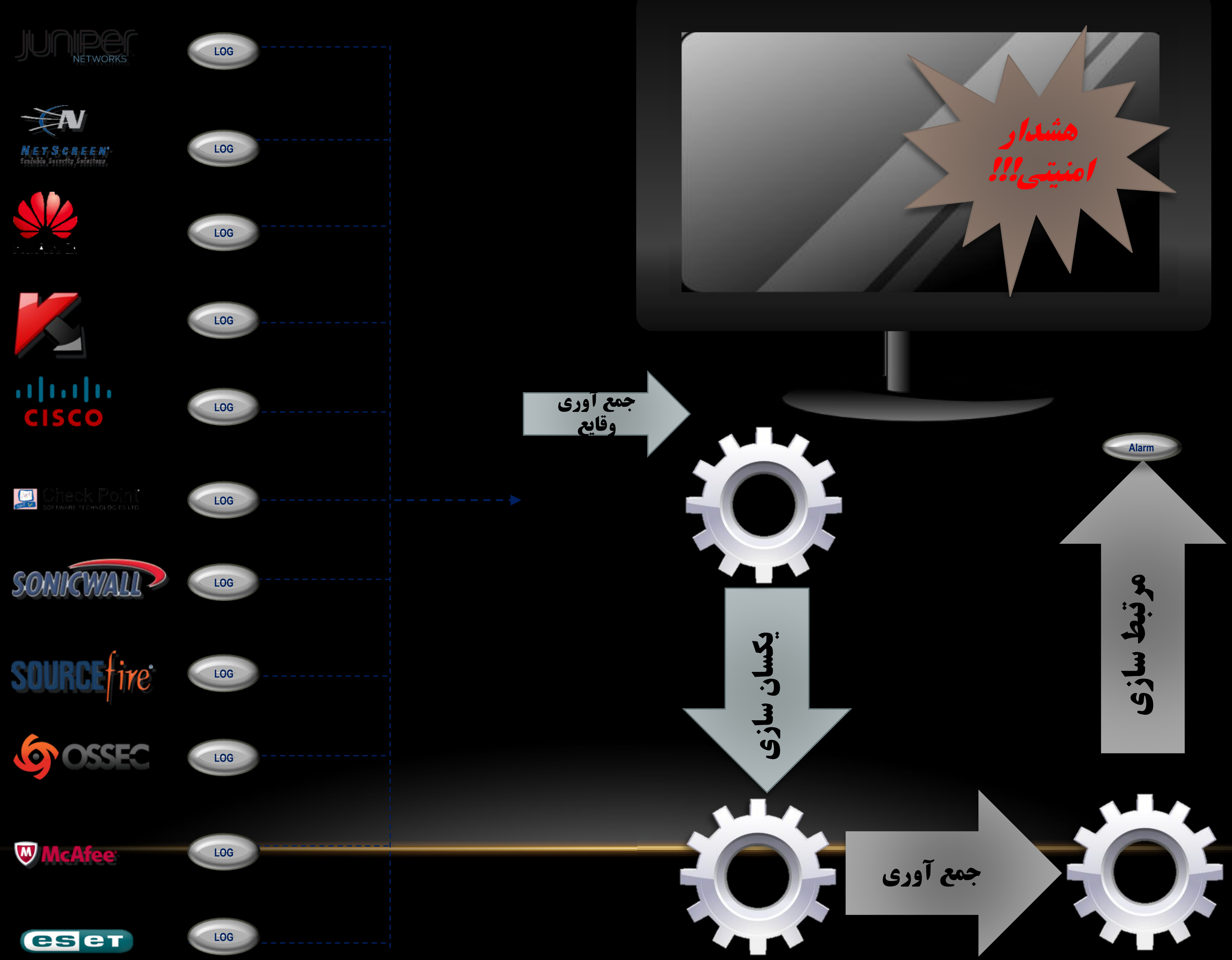
از بین بردن کانال (ها)
Back Channle(s)

مدیریت اطلاعات و رخدادهای امنیتی
SIEM

فناوری

هسته مرکزی مرکز عملیات امنیت، سامانه مدیریت اطلاعات و رخدادهای امنیتی (SIEM) است.




LOG
هشدار
امنیتی!!!
جمع آوری
وقایع
یکسان سازی
جمع آوری
مرتبط سازی
Alarm

نیاز به استفاده از فناوری بومی

- عدم اطمینان به سامانه های خارجی
- اطلاعات حساس به عنوان دارایی های سازمان ها
- بستر غیرقابل اطمینان با توجه به تحریم های مختلف
- عدم دسترسی به شرکت تولید کننده در صورت نیاز
- عدم پشتیبانی فنی
- سازگاری فناوری بومی بر مبنای نیازهای خاص سازمان ها

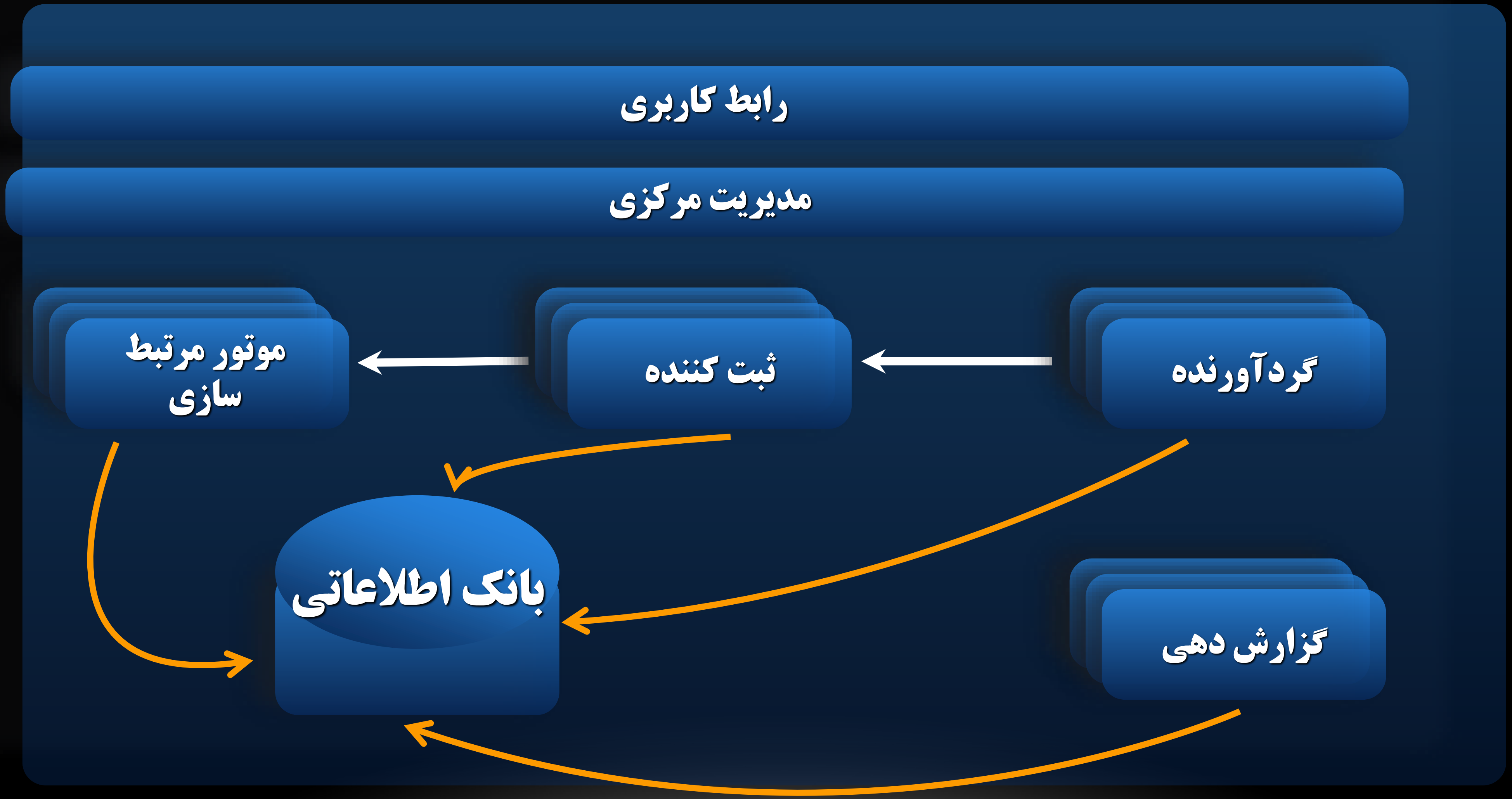
کارکردهای اصلی SIEM

- جمع آوری داده های شبکه
- پیاده سازی سیاستها و قوانین امنیتی
- تحلیل و مرتبط سازی رخدادها
- تعیین سطح تهدید بر مبنای هشدارها
- گزارش های مدیریتی و فنی
- مدیریت، ذخیره سازی و کشف شواهد قانونی وقایع ثبت شده و رویدادها

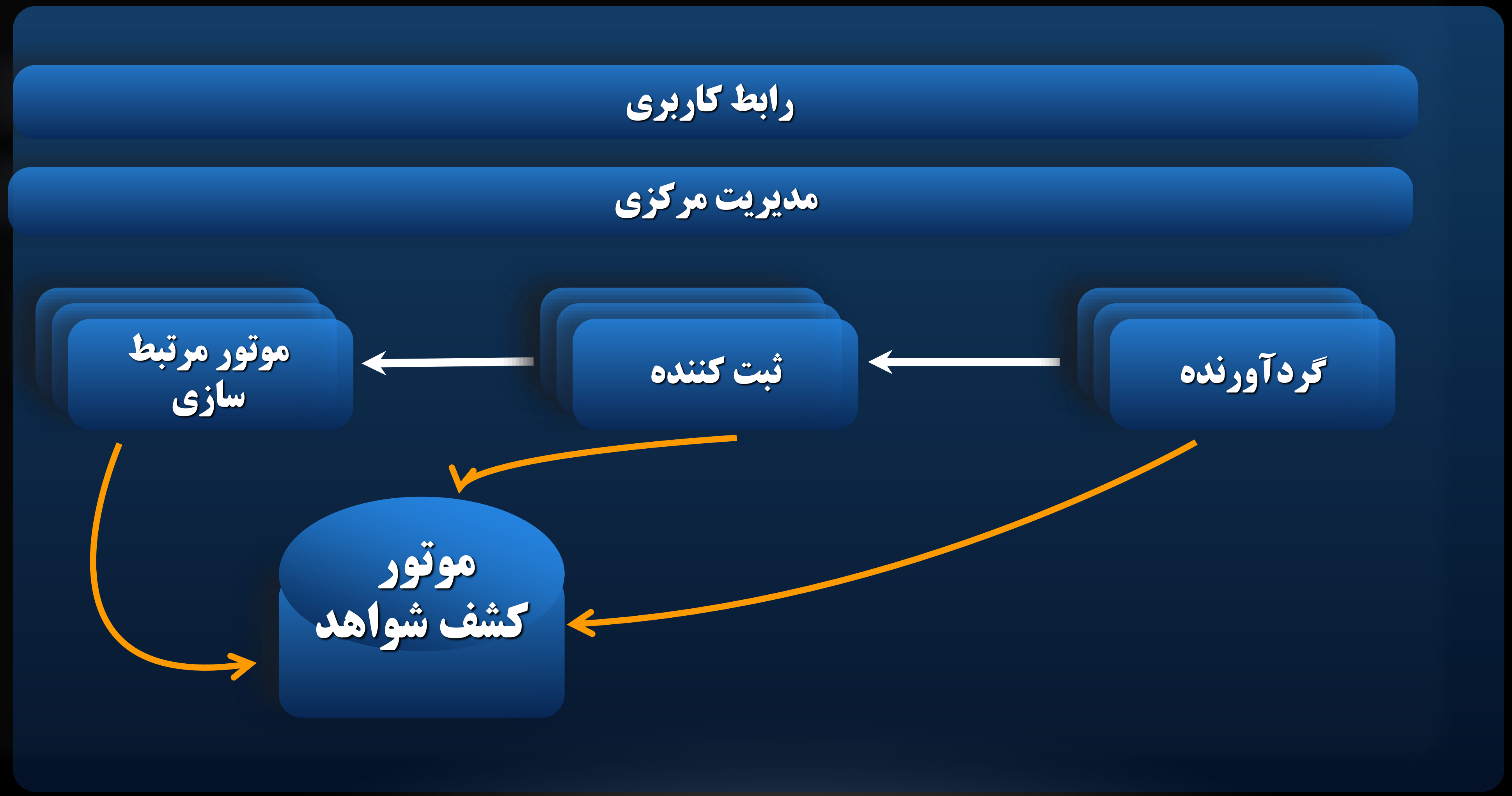
معماری SIEM


SIEM
مدیریت حوادث امنیتی
گزارش دهی
ارزیابی ریسک
مرتبط سازی
طبقه بندی
بانک اطلاعاتی
Forensic
ذخیره سازی با حجم بالا
جستجوی پیشرفته وقایع
امضای دیجیتال
NAS & SAN
Collector
گردآوری
یکسان سازی
پالایش
IDS
HIDS
Vulnerability Scanner
Network Discovery
سرورها
تجهیزات امنیت صنعتی
بانکهای اطلاعاتی
تجهیزات امنیت شبکه
تجهیزات شبکه
برنامه های کاربردی
ضد ویروسها
دیگر تجهیزات امنیتی

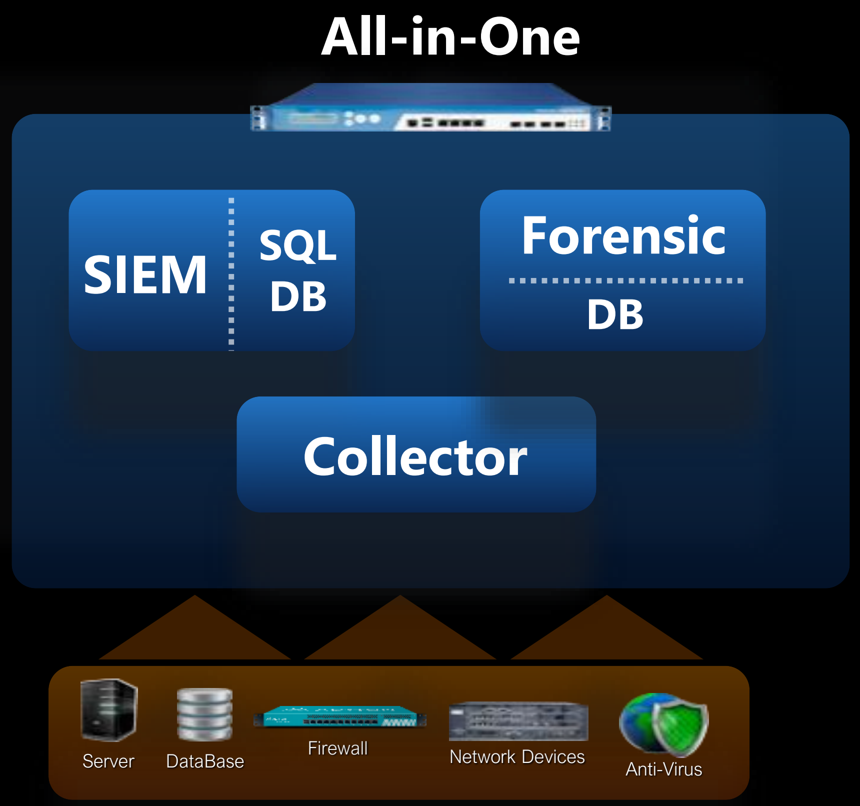
موتور سامانه مدیریت اطلاعات و رخدادهای امنیتی



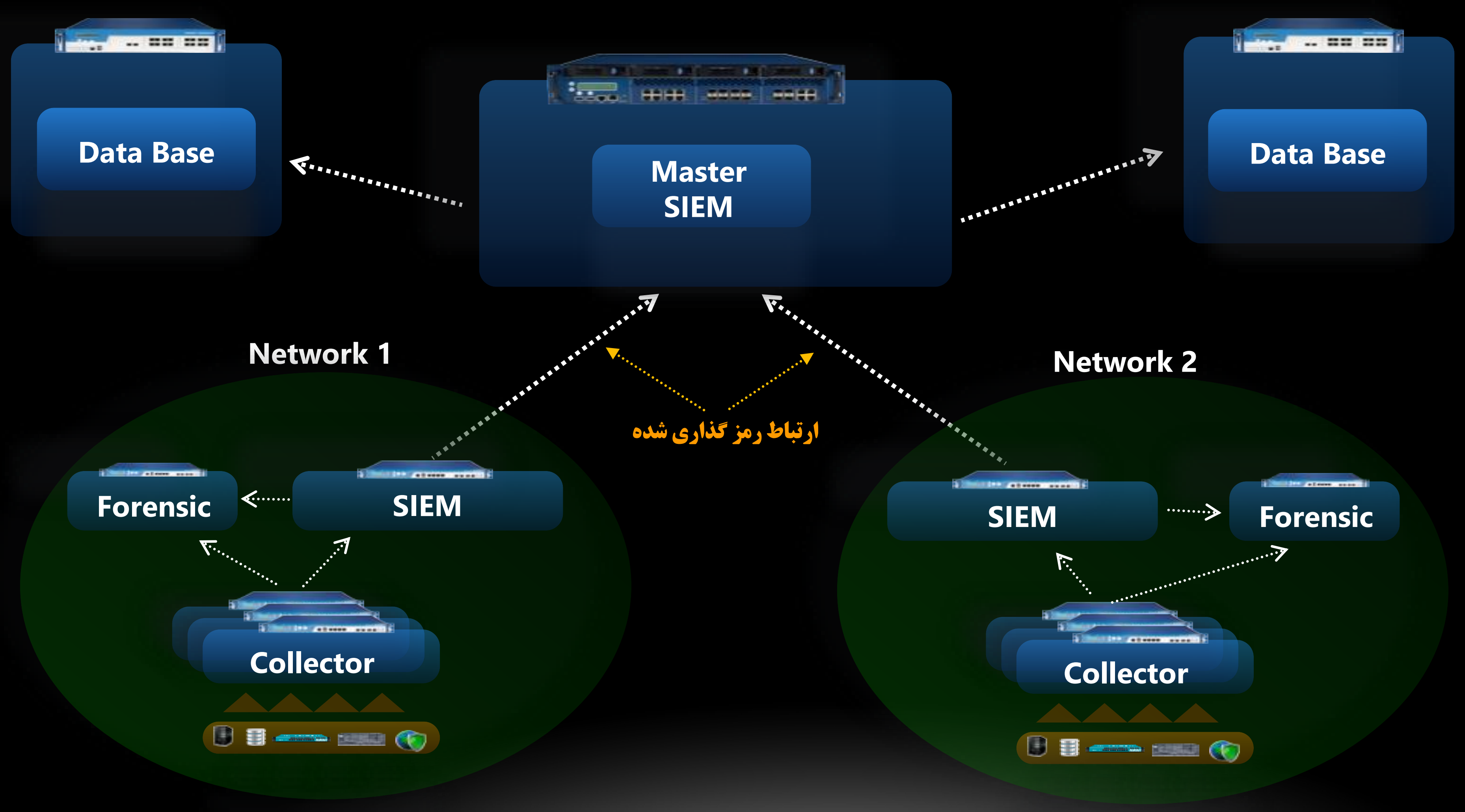
موتور سامانه مدیریت اطلاعات و رخدادهای امنیتی



مدلهای پیاده سازی SIEM



مدل توزیع شده



ارزیابی ریسک

- فرآیند ارزیابی ریسک و تشخیص اهمیت یا عدم اهمیت رویداد
- مساعدت در فرآیند تصمیم گیری
- محاسبه بر مبنای سه پارامتر:
  - ارزش دارایی Asset Value
  - تقدم Priority
  - اعتبار Reliability

رخداد

0 - 5 | 0 - 5 | 0 - 10

(ارزش دارایی x تقدم x اعتبار)/25 ⩾1 = هشدار امنیتی

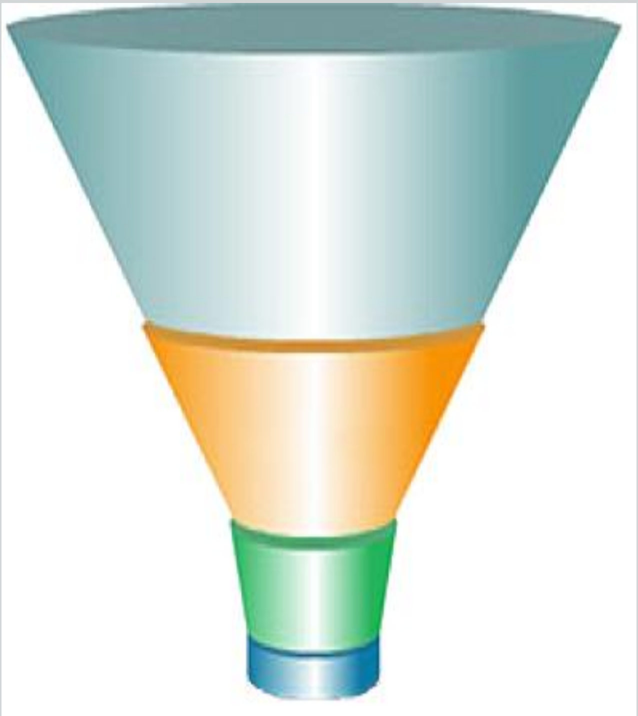
مرتبط سازی

موتور مرتبط سازی SIEM:

- دارای دستور از پیش تعریف شده برای مرتبط سازی مبتنی بر دستور
- مرتبط سازی مبتنی بر آسیب پذیری
- قابلیت تعریف دستور جدید

سامانه مدیریت اطلاعات و رخدادهای امنیتی

(اعداد به عنوان مثال آورده شده است و معیار تصمیم گیری نمی باشد)



Raw Events	۱۰۰ میلیون
رخدادهای تجمیع هنجارسازی شده	۱۰ میلیون
رخدادهای مرتبط سازی شده	۲۵۰۰۰
رخدادهای قابل بررسی بیشتر	۷۵۰
باز نمودن تیکت	۵۰
موارد خطرناک	۲۰

قادر نیست SIEM

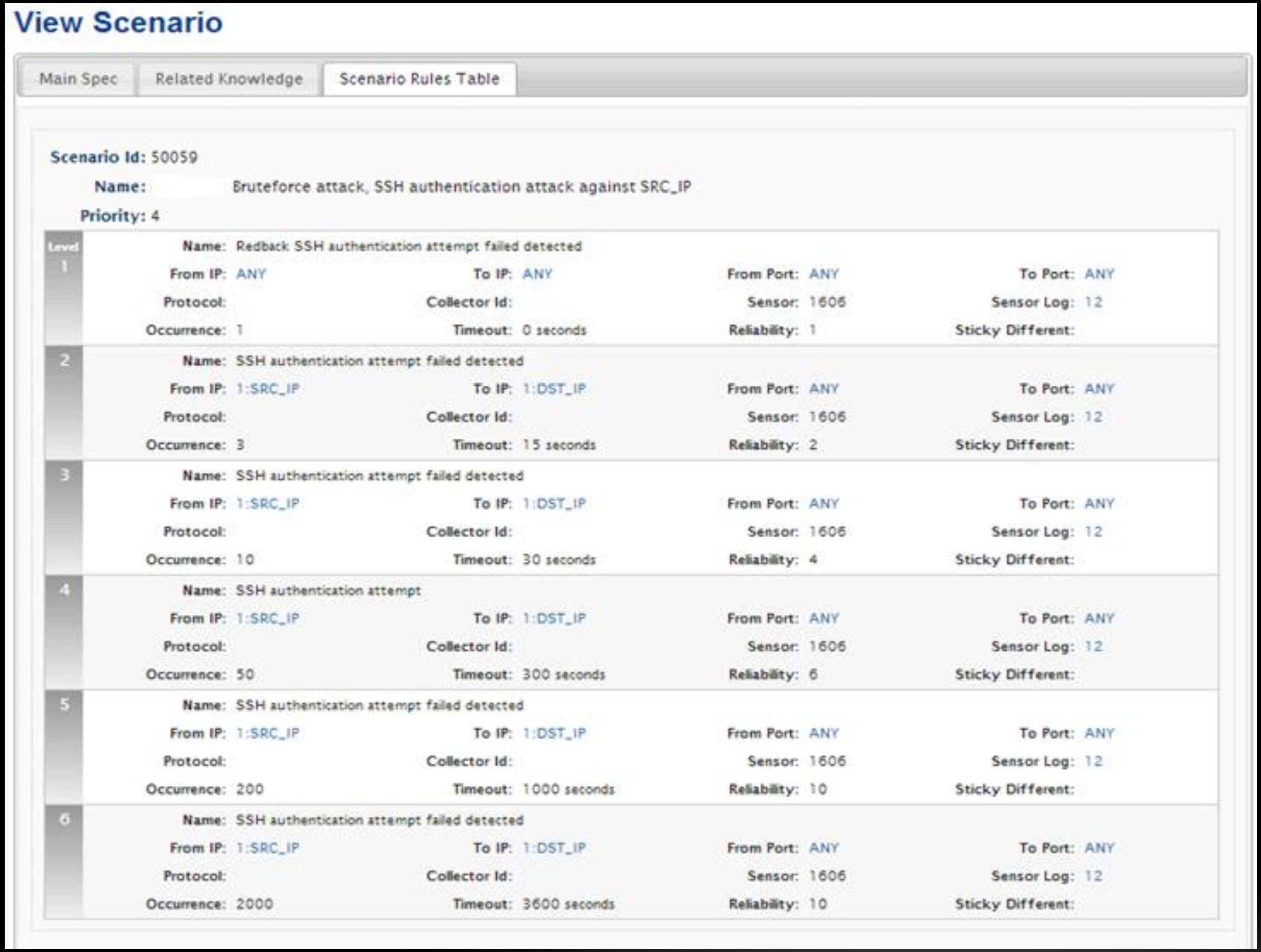
- ✓ SIEMنیاز به دیگر سیستم‌های امنیت فناوری اطلاعات را از بین نمی‌برد، بلکه ارزش هرکدام از آن ابزارها را افزایش می‌دهد
- ✓ SIEM مستقیماً از سوء استفاده‌ها جلوگیری نمی‌کند، بلکه در شناسایی محدوده‌هایی که سطح مخاطرات آنها افزایش یافته است و کاهش هزینه و زمان واکنش به رخداد کمک می‌کند.
- ✓ SIEM نقش مدیران و پرسنل عملیاتی امنیت را حذف نمی‌کند، بلکه ارزش چنین کارمندانی را مشخص می‌کند

SIEM قادر است

- ✓ مدیریت لاگ‌ها جهت تسهیل همبستگی سنجی، هشداردهی و گزارش دهی رویدادهای امنیتی
- ✓ تسهیل فرآیندهای مدیریت مخاطرات، پاسخ به رخداد و انطباق سنجی
- ✓ فراهم کردن بستری برای مقایسه سطح تهدیدات و فعالیت‌های امنیتی
- ✓ افزایش بهره وری و اثر بخشی عملکرد مدیران سیستم و امنیت، ممیزان داخلی و خارجی و مدیران ارشد درگیر در مدیریت مخاطرات
- ✓ اتخاذ روش بهبود مدیریت مخاطرات و اولویت‌بندی رسیدگی به آسیب پذیری‌ها

سناریو

- مرتبط سازی مبتنی بر قوانین



View Scenario

Main Spec | Related Knowledge | Scenario Rules Table

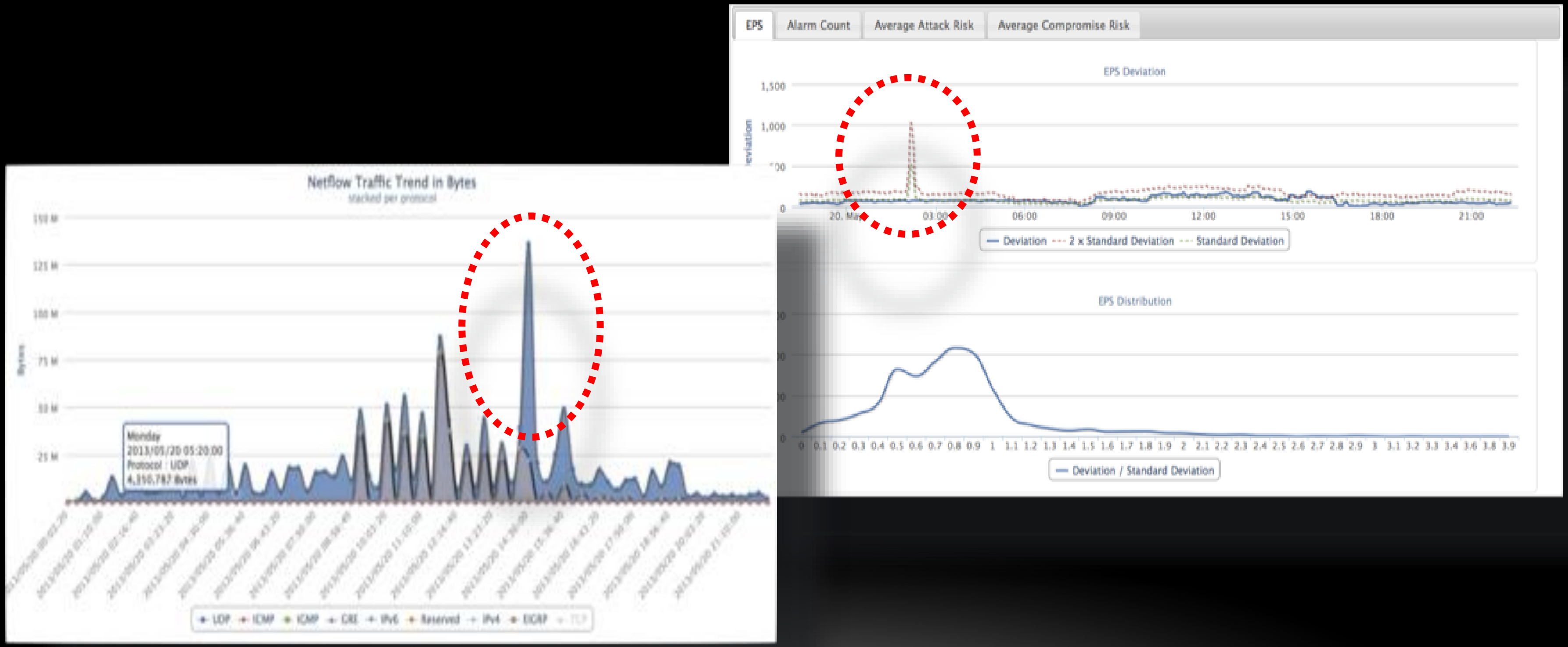
Scenario Id: 50059
Name: Bruteforce attack, SSH authentication attack against SRC_IP
Priority: 4

Level				
1	Name: Redback SSH authentication attempt failed detected			
	From IP: ANY	To IP: ANY	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 1	Timeout: 0 seconds	Reliability: 1	Sticky Different:
2	Name: SSH authentication attempt failed detected			
	From IP: 1:SRC_IP	To IP: 1:DST_IP	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 3	Timeout: 15 seconds	Reliability: 2	Sticky Different:
3	Name: SSH authentication attempt failed detected			
	From IP: 1:SRC_IP	To IP: 1:DST_IP	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 10	Timeout: 30 seconds	Reliability: 4	Sticky Different:
4	Name: SSH authentication attempt			
	From IP: 1:SRC_IP	To IP: 1:DST_IP	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 50	Timeout: 300 seconds	Reliability: 6	Sticky Different:
5	Name: SSH authentication attempt failed detected			
	From IP: 1:SRC_IP	To IP: 1:DST_IP	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 200	Timeout: 1000 seconds	Reliability: 10	Sticky Different:
6	Name: SSH authentication attempt failed detected			
	From IP: 1:SRC_IP	To IP: 1:DST_IP	From Port: ANY	To Port: ANY
	Protocol:	Collector Id:	Sensor: 1606	Sensor Log: 12
	Occurrence: 2000	Timeout: 3600 seconds	Reliability: 10	Sticky Different:

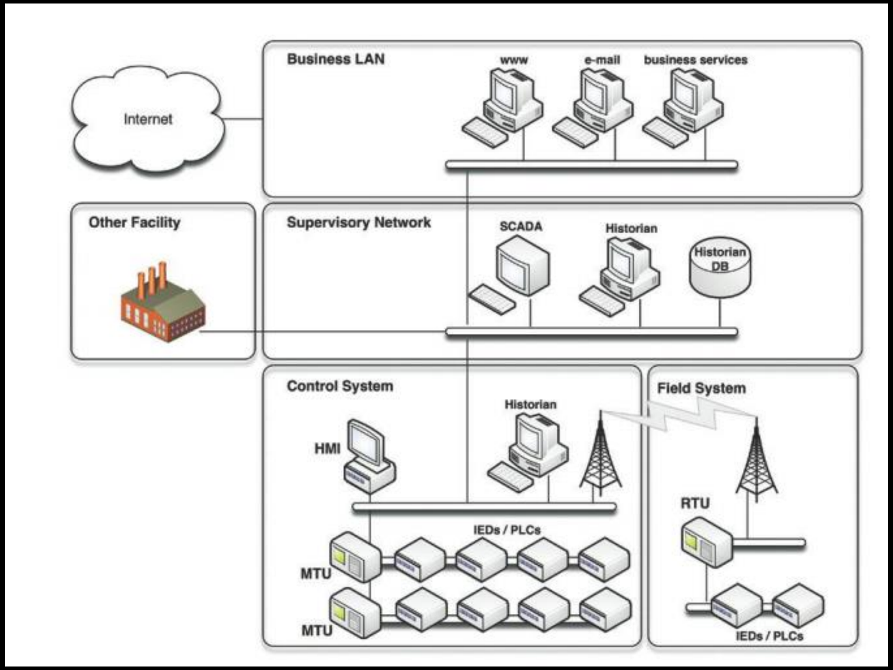
تشخیص ناهنجاری

قابلیت پایش رفتاری SIEM، پایه ای را برای فعالیتهای طبیعی شبکه شناسایی می کند.

فقط ظرف چند ساعت قادر به شناسایی الگوهای ناهنجاری که شاید علامت مشکلی عملیاتی یا حادثه بالقوه امنیتی است خواهید بود.



مرکز عملیات امنیت صنعتی



- یکپارچه سازی رخدادهای IT و OT
- پشتیبانی از پروتکل های صنعتی مانند:

  Modbus,DNP3,OPC,...
- قابلیت دریافت وقایع ثبت شده حس گرهای صنعتی مانند:

  RTU, PLC, IED,HMI,...

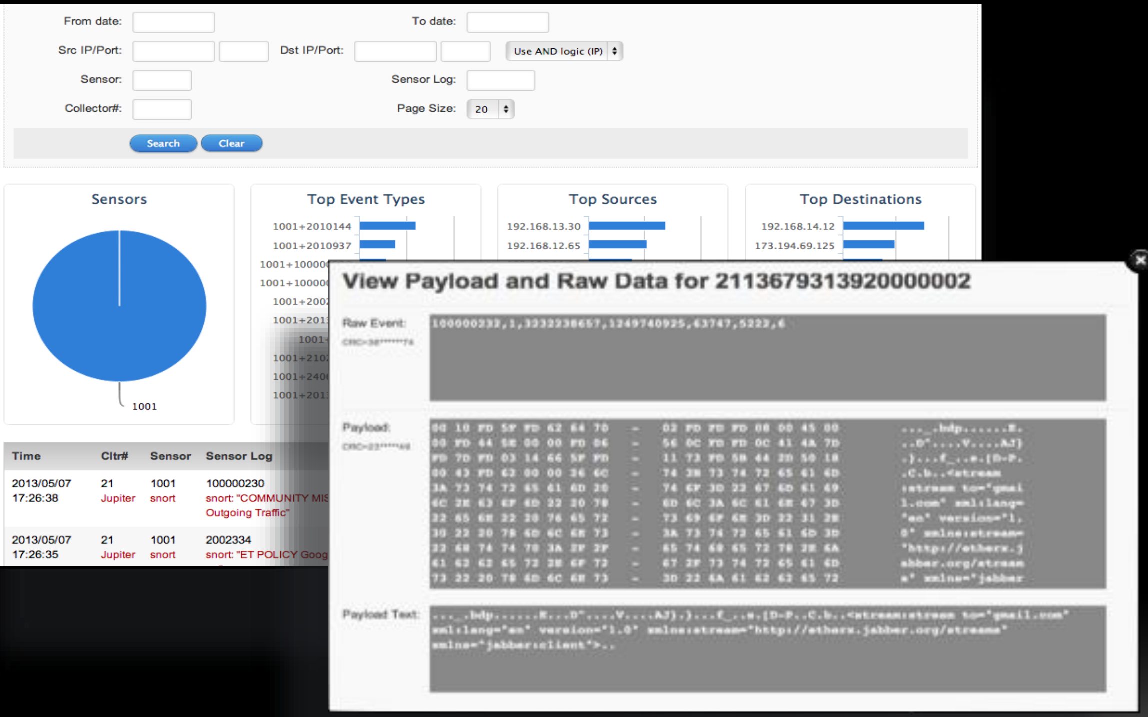
آگاهی از هویت کاربر

از آنجائیکه تمامی اطلاعات امنیتی در ارتباط با کاربران مشخص می باشد، SIEM، قادر به کلیه فعالیتهای کاربر با جزئیات مورد نیاز است.

- **قابلیت یکپارچه سازی با سرویس هایی مانند** Active Directory

کشف شواهد

SIEM، تمامی اطلاعات بدست آمده از جمله داده های خام را برای زمانی طولانی در یک یا چند پایگاه اطلاعاتی برای تحلیل یا گزارشهای مدیریتی بایگانی می کند. داده های حجیم ایندکس گذاری می شوند و هنگام نیاز میتوان آنها را با فیلترهای متنوع با سرعت جستجو کرد.



- رمز گذاری شده و با امضای دیجیتال
- فشرده سازی با نسبت مناسب
- جستجوی یکپارچه
- ایندکس گذاری تمامی اطلاعات ذخیره شده
- استفاده بانکهای اطلاعاتی NoSQL در حجم های بزرگ داده

Threat Intelligence &

Incident Response

Incident Response Plan

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned

ISAC & ISAS

مرکز اشتراک و تحلیل اطلاعات (ISAC & ISAS)

- بر هم کنش، وابستگیها و تعاملات بین زیر ساختهای حیاتی حائز اهمیت فراوانی است به گونه ای که بدون اتخاذ یک نگاه سیستمی و یکپارچه، امکان ملاحظه تمام ابعاد عملکردی یک زیر ساخت وجود ندارد و عدم توجه به این ارتباطات می تواند منجر به افزایش تهدیدات و بحرانهای ملی گردد.
- در راستای کاهش آسیب پذیریهای زیر ساختهای حیاتی، مراکز اشتراک و تحلیل اطلاعات، با ایجاد بستر امن و مطمئن جهت تبادل اطلاعات مربوط به حملات و آسیب پذیریهای این حوزه، امکان پیشگیری ، تشخیص به موقع و مقابله با بحرانهای ملی را فراهم می سازد

مرکز اشتراک و تحلیل اطلاعات (ISAC & ISAS)

- به اشتراک گذاری اطلاعات، یک ابزار کلیدی برای ایجاد آگاهی موقعیتی و پاسخ موثر به واقعه است.
- مرکز اشتراک گذاری و تحلیل اطلاعات، یک موجودیت عملیاتی است که عملیات گردآوری، تحلیل، نگهداری مناسب و انتشار اطلاعات وابسته به زیرساخت‌های حیاتی، قابلیت هشدار تهدیدات و گزارش‌دهی حوادث را فراهم می‌کند. این مرکز توانایی کافی برای اشتراک‌گذاری اطلاعات درون قلمرو زیرساختی، بین قلمروها، با حاکمیت و نیز ذینفعان حوزه خصوصی را دارد.

مرکز اشتراک و تحلیل اطلاعات (ISAC & ISAS)

اهداف ISAC & ISAS

۱- گردآوری یا تحلیل اطلاعات زیرساخت های حیاتی برای بهبود درک مسایل امنیتی و وابستگی‌های مرتبط با زیرساخت‌های حیاتی و سیستم‌های حفاظت شده، برای اطمینان از سه رکن مهم در زیرساخت‌های حیاتی دسترسی‌پذیری، یکپارچگی و قابلیت اطمینان.

۲- تبادل و انتشار اطلاعات زیرساخت‌های حیاتی برای کمک به جلوگیری، آشکارسازی، کاهش و بازیابی از آثار یک تداخل یا به‌خطر افتادن زیرساخت‌ها و سیستم‌های حفاظت شده.

۳- انتشار داوطلبانه اطلاعات زیرساخت‌های حیاتی

مرکز اشتراک و تحلیل اطلاعات (ISAC & ISAS)

جایگاه اشتراک اطلاعات در چرخه حوادث امنیت سایبری

مرکز اشتراک و تحلیل اطلاعات (ISAC & ISAS)

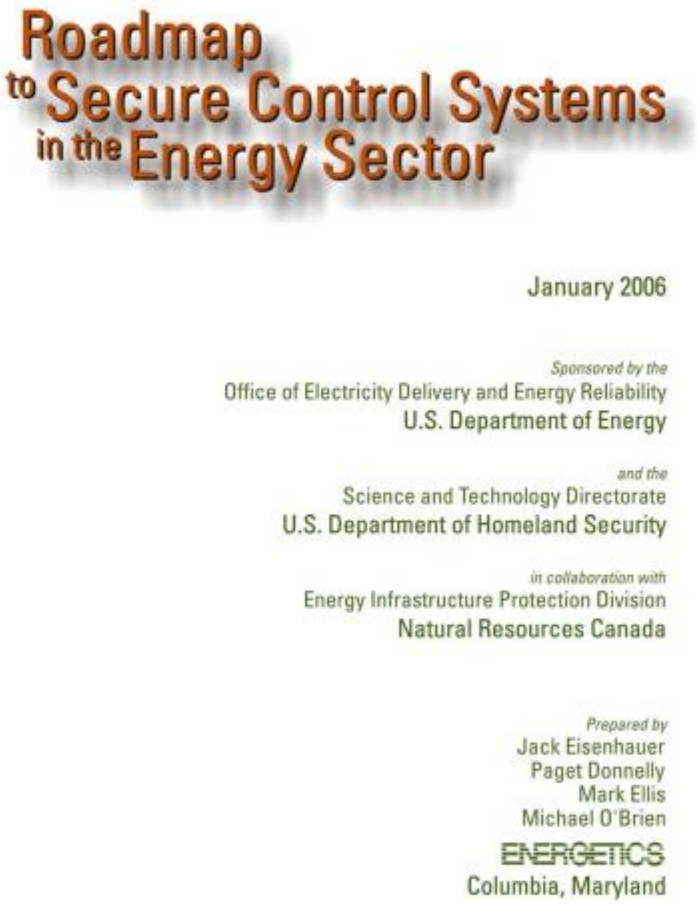
Telecom ISAC

- Telecom ISACمرکز به اشتراک گذاری و تحلیل اطلاعات در حوزه زیر ساخت حیاتی شبکه ارتباطات می‌باشد.
- این مرکز تسهیل کنندهٔ تبادل اطلاعات آسیب پذیری ها، تهدیدات، و نفوذهای موثر بر زیرساخت های ارتباطاتی می باشد.
- اطلاعات دریافت شده از اعضای صنعت ارتباطات، دولت، و منابع دیگر را برای جلوگیری و یا کاهش اثرات بحران‌های مؤثر بر زیرساخت های ارتباطات راه دور تجزیه و تحلیل می‌نماید و نتایج را به اشتراک می‌گذارد.

معماری بومی پدافند سایبری مبتنی بر

متدولوژی دفاع در عمق

برخی از اقدامات کشورها در خصوص امن سازی زیرساخت های حیاتی و حساس حوزه انرژی



Roadmap to Secure Control Systems in the Energy Sector

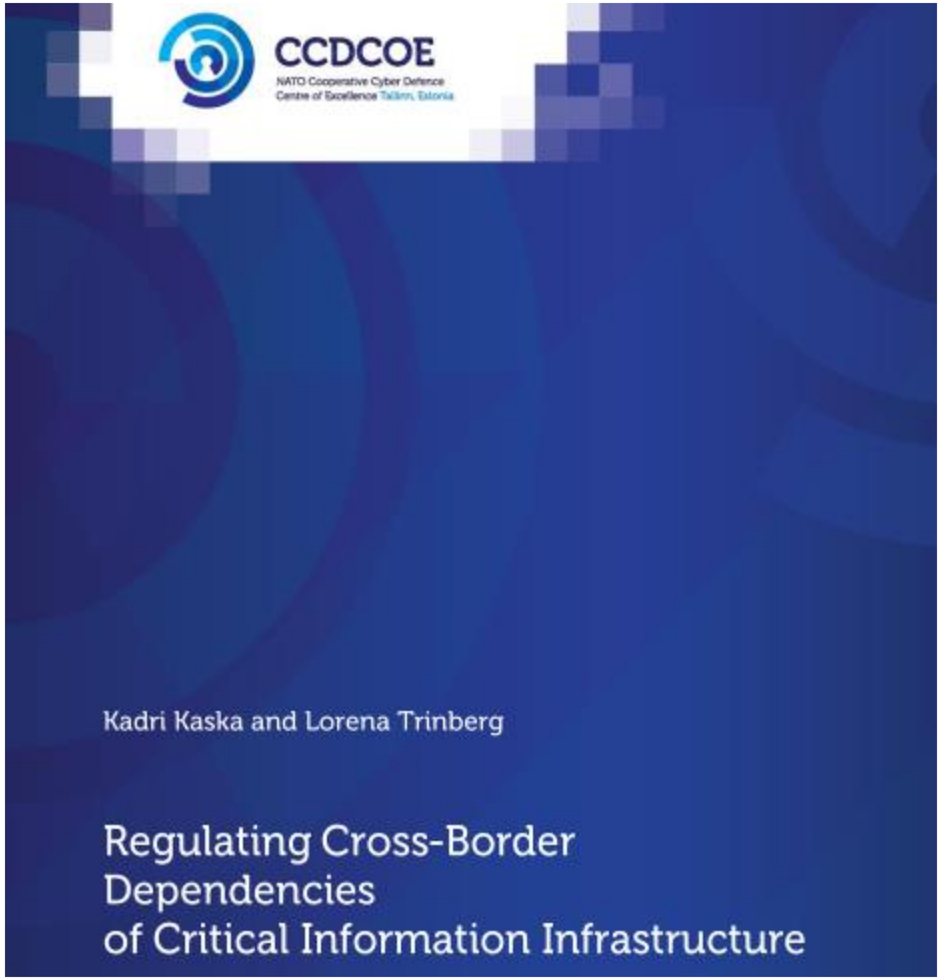
January 2006

Sponsored by the
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy

and the
Science and Technology Directorate
U.S. Department of Homeland Security

in collaboration with
Energy Infrastructure Protection Division
Natural Resources Canada

Prepared by
Jack Eisenhauer
Paget Donnelly
Mark Ellis
Michael O'Brien
ENERGETICS
Columbia, Maryland

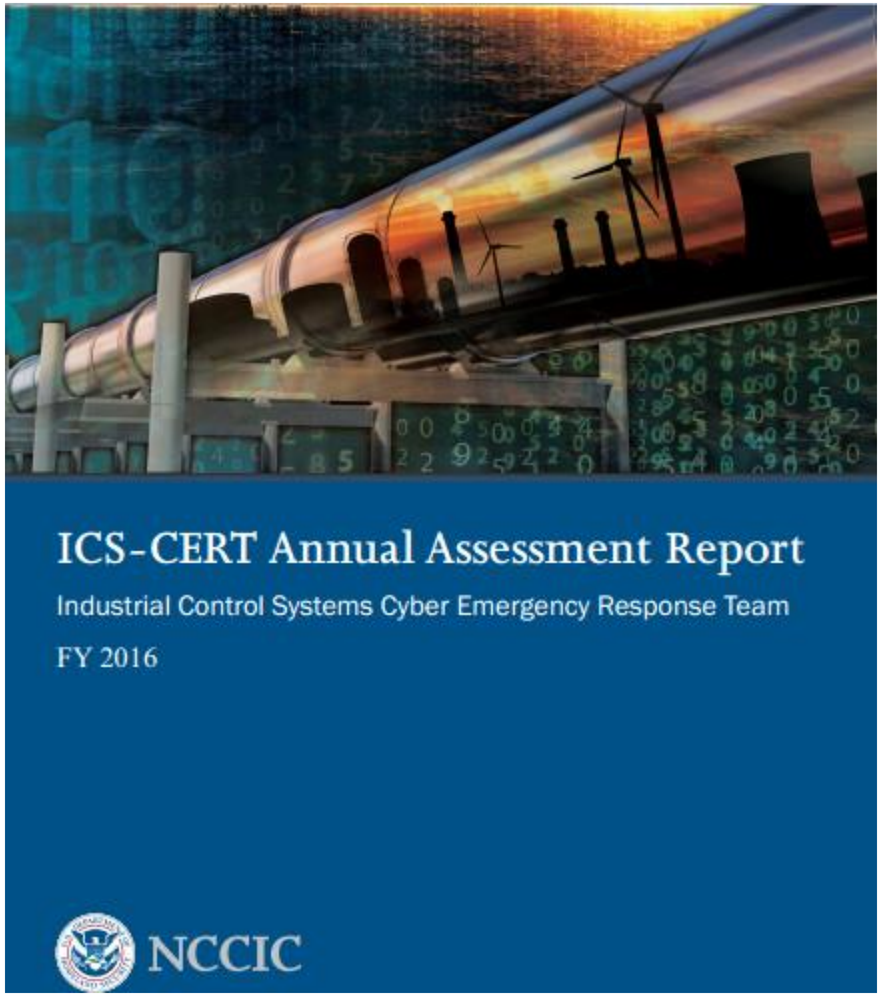


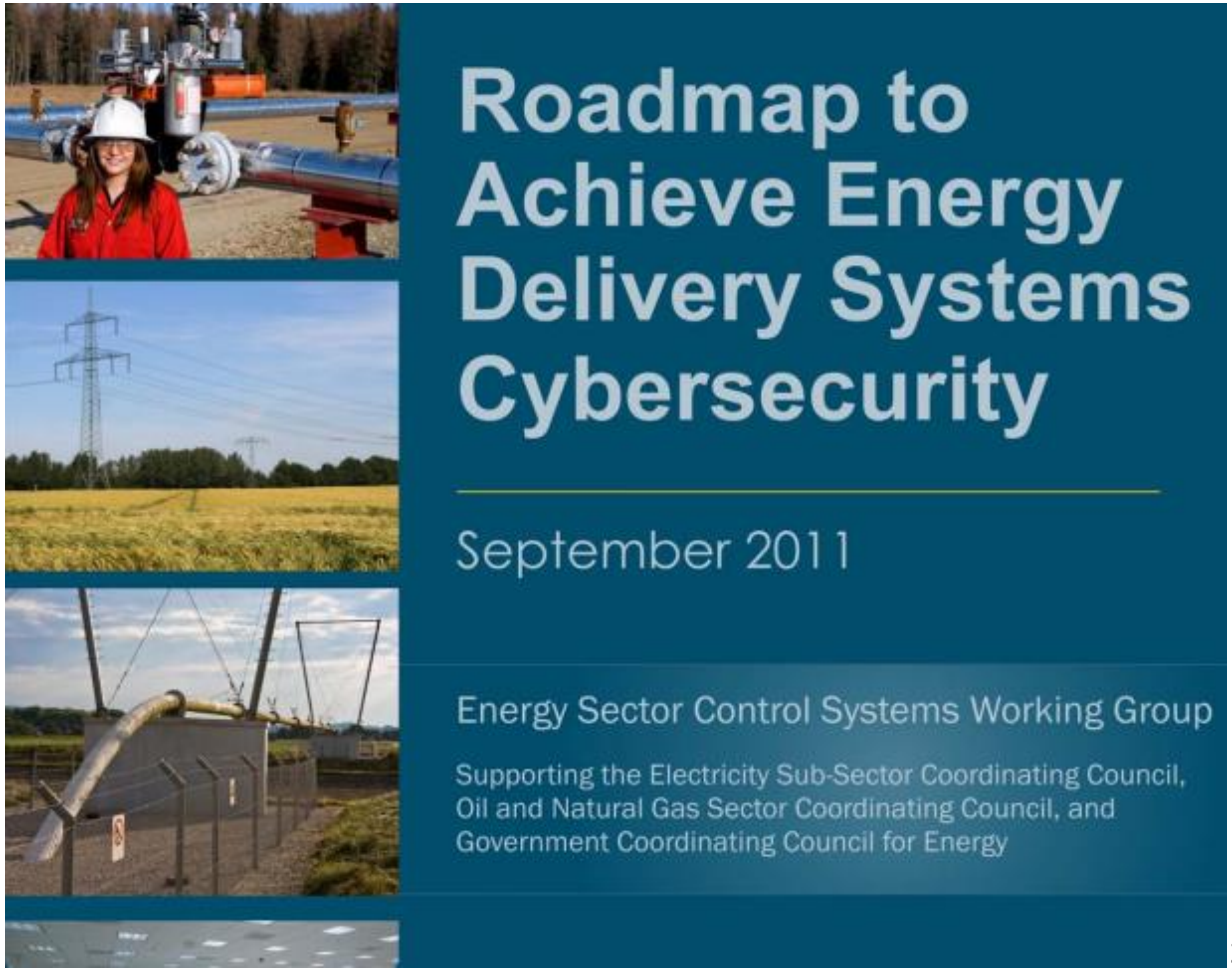
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Kadri Kaska and Lorena Trinberg

Regulating Cross-Border Dependencies of Critical Information Infrastructure

برخی از اقدامات کشورها در خصوص امن سازی زیرساخت های حیاتی و حساس حوزه انرژی





برخی از اقدامات کشورها در خصوص امن سازی زیرساخت های حیاتی و حساس حوزه انرژی

U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

September 15, 2011

The Department of Energy Releases New Roadmap to Guide Public-Private Cybersecurity Initiatives

New Roadmap Outlines Strategy for Improving Energy Sector Cyber security; Latest Protective Measures Aim to Reduce Risk, Protect Consumers and Businesses

WASHINGTON, DC – As part of the Obama Administration's goals to enhance the security and reliability of the nation's energy infrastructure, the U.S. Department of Energy today released the 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. Developed as an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*, today's report outlines a strategic framework over the next decade among industry, vendors, academia and government stakeholders to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions.

"Increased insight from private-public collaborations will allow us to better protect the nation's energy delivery systems that keep our lights on and the power flowing," said U.S Energy Secretary Steven Chu. "The 2011 Roadmap takes the necessary steps to strengthen the security and reliability of our country's electric grid, in a climate of increasingly sophisticated cyber incidents."

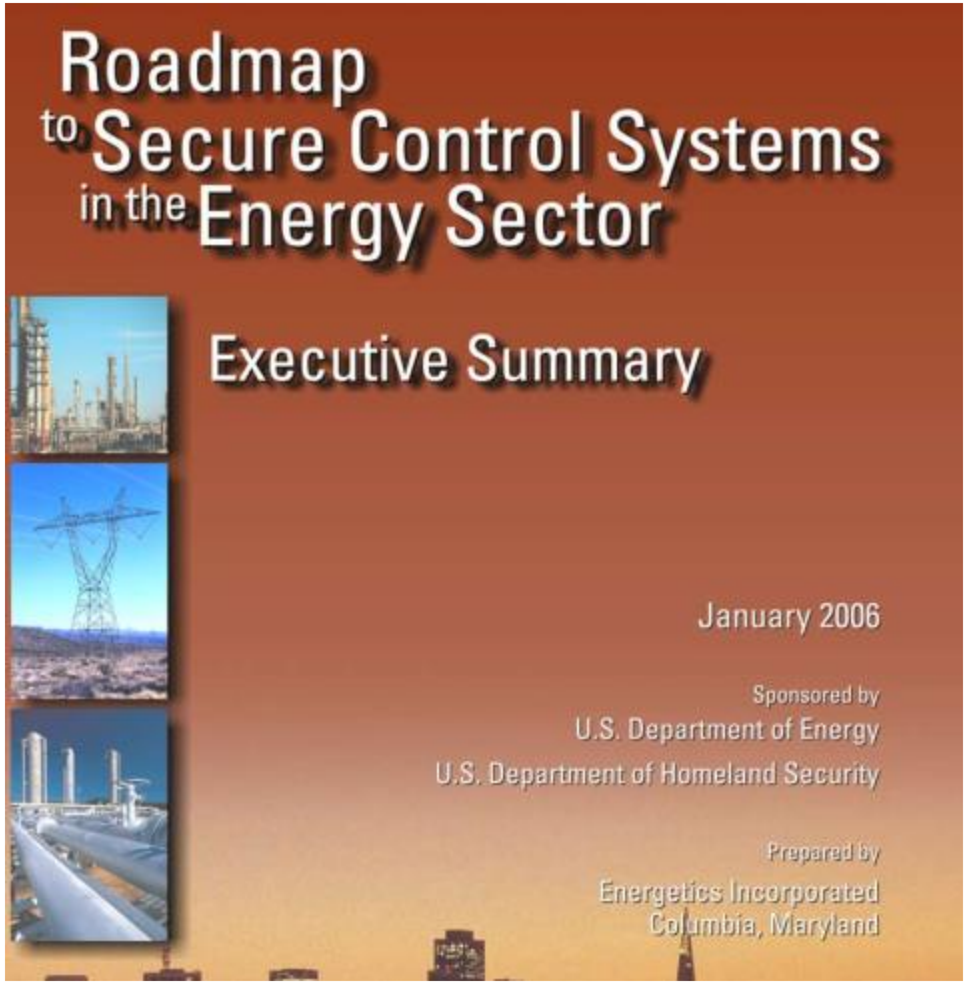
Cybersecurity for Energy Delivery Systems (CEDS) R&D

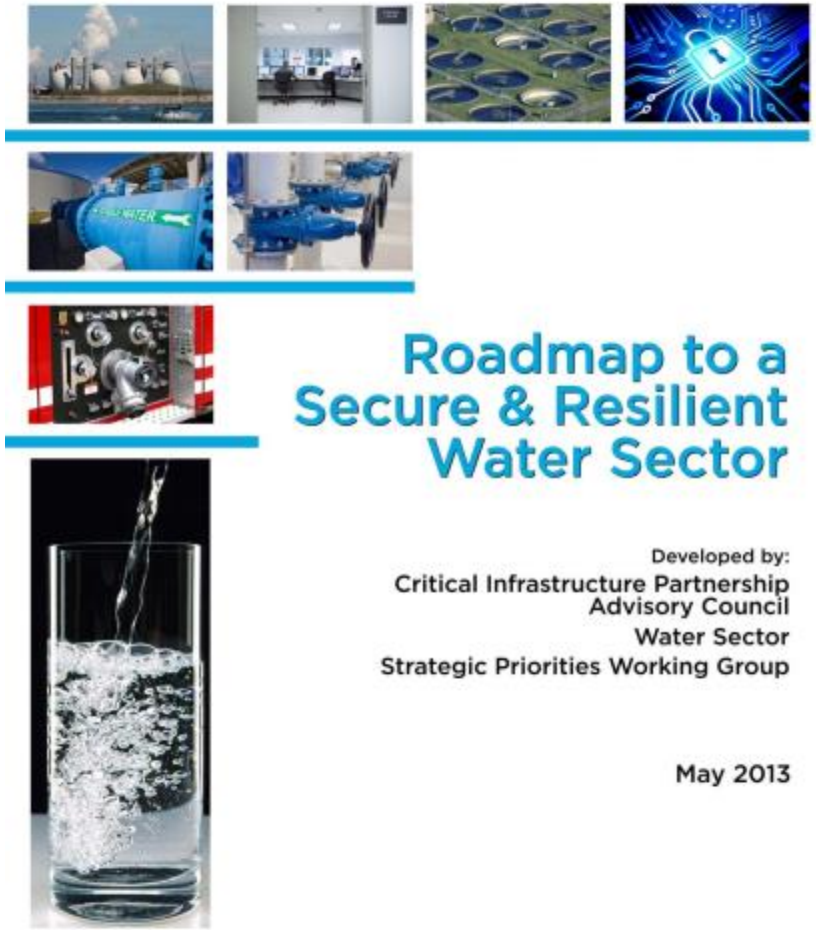
Following the Energy Sector's Roadmap

Carol Hawk
CEDS R&D Program Manager

U.S. DEPARTMENT OF ENERGY | Electricity Delivery & Energy Reliability

برخی از اقدامات کشورها در خصوص امن سازی زیرساخت های حیاتی و حساس حوزه انرژی





دفاع در عمق چیست

- دفاع در عمق عبارت است از استراتژی استفاده از لایه‌های مختلف دفاعی جهت مقابله با مسائل چندگانه امنیتی
- راهبرد عمل‌گرایانه برای دستیابی به امنیت اطلاعات
- ایجاد توازن میان ظرفیت حفاظت از اطلاعات با توجه به هزینه، عملکرد و ملاحظات عملیاتی

آژانس امنیت ملی آمریکا، راهبرد دفاع در عمق را ابزاری برای دستیابی به اعتماد اطلاعاتی تعریف کرده است و بیان نموده که ایجاد اعتماد اطلاعاتی هدف اصلی از اجرای راهبرد دفاع در عمق است که در نتیجه آن به یک ابزار دفاعی قابل اطمینان در برابر حملات سایبری دست یافته میشود.

دفاع در عمق چیست

راهبرد دفاع در عمق یک مدل حفاظتی و لایه‌ای قدرتمند برای اجزاء مهم سیستم‌های اطلاعاتی است، و یکی از روش‌های دفـاعـی در آن، دفاع لایه‌ای یا چند لایه است. هدف از دفاع لایه‌ای بـه کـارگـیـری از چندین مکانیزم تشخیص، نظارتی و حفاظتی است تا یـک مـهـاجـم مجبور به عبور از موانع مختلف بازرسی جهت دستیابی به اطـلاعـات حیاتی گردد. راهبرد دفاع در عمق نه تنها باید از نقض امنیت جلوگیری کند، بلکه باید حملات را شناسایی کرده و به آنها پاسخ دهد و عواقب ناشی از نقض امنیت را کاهش دهد.

چارچوب استراتژیک معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

- از دیدگاه استراتژی دفاع در عمق، دفاع تنها استفاده از تکنولوژی‌های خاص برای مقابله با ریسک‌ها نیست، بلکه امنیت باید یکی از اجزای سیستم باشد و در تمامی مراحل تولید، اجرا، پیکربندی و ... دیده شده باشد.
- اجرای استراتژی دفاع در عمق موثر، نیازمند طرح جامع و دسته بندی منابع سازمان در راستای فراهم کردن لایه‌های حفاظتی موثر است.

اصول متدولوژی دفاع در عمق از دیدگاه پدافند غیرعامل

- آگاهی از تهدیدات امنیتی که مراکز حیاتی و حساس و مهم با آن‌ها مواجه هستند.
- تعیین کمی و کیفی تهدیدات
- استفاده از منابع کلیدی جهت کاهش تهدیدات امنیتی
- تعریف نمودن صلاحیت هر یک از منابع و شناسایی نواحی که همپوشانی دارند.
- رعایت کردن استاندارد ها امنیتی موجود یا در حال ظهور برای کنترل‌های خاص.
- ابداع و تغییر کنترل‌های خاصی که برای سازمان مهم هستند.

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

- در سازمان‌ها و مراکز علمی معتبر دنیا مانند NIST، SANS، و ... بر روی این موضوع فعالیتهایی انجام پذیرفته است اما نوع و وجوه متنوع و خاص منظوره تهدیدات و آسیب پذیریهای متصور بر روی سرمایه‌های ملی سایبری و همچنین فضای سایبری کشور و عدم پاسخگو بودن روش‌های فوق، ضرورت توجه جدی به بومی سازی متدولوژی دفاع در عمق، با تکیه بر توان داخلی و استفاده حداکثری از مزیت های بالقوه و بالفعل سایبری کشور، برای افزایش قدرت بازدارندگی سایبری کشور را بیش از پیش نمایان می سازد

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

منطبق بر سه اصل دفاع *راهبردی*، *دفاع عملیاتی* و *دفاع فنی*

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

- برای نیل به معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق ماتریسی ۳*۳ تعریف میگردد که
  - ✓ در سطرهای این ماتریس لایه تهدیدات، لایه نیازمندیهای عملیاتی و لایه محصولات، خدمات و فناریها قرار دارد.
  - ✓ در ستونهای این ماتریس سه اصل دفاع راهبردی، دفاع عملیاتی و دفاع فنی قرار دارد.
- برای هریک از سطرها و ستونها مکانیزم دفاع در عمق بصورت رابطه ای برقرار خواهد شد.

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

دفاع فنی

دفاع عملیاتی

دفاع راهبردی

لایه تهدیدات

لایه نیازمندیهای عملیاتی

لایه محصولات، خدمات و فناوری

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

بررسی لایه تهدیدات

- این لایه براساس تهدیدشناسی به روش برداری (Vector Attack) تهیه گردیده است
- در این روش موجودیت های تهدیدات سایبر به قسمتهای مختلفی تقسیم شده است. این تقسیم بندی تمام موجودیت های درگیر از عوامل انسانی تهدید، انگیزه های انجام حملات و مسائل فنی گرفته تا نتایج نهایی که موردنظر حمله کننده است را شامل می گردد.
- هر حمله از ستون اول شروع می شود و زنجیره ای از عوامل ستون های میانی را می پیماید و به ستون انتهایی خاتمه می یابد، در این مدل نوع آسیب پذیری و نوع مکانیزم بکارگرفته شده در حمله نیز بیان میگردد.

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

بررسی لایه تهدیدات

اهداف کلان	نتایج	اهداف	مکانیزم و روش	آسیب پذیری ها	روش های کلان	عامل تهدید
بهره برداری سیاسی	تعیین موقعیت و وضعیت	اهداف ملی	Spoof	سیاستها ، کاربران، رفتارهای غیرمسئولانه	انتشار اخبار و اطلاعات	ارتش های ملی
بهره برداری اقتصادی	کنترل	تاسیسات صنعتی	Modify	آسیب پذیرهای پروتکل ها ، نرم افزارها ، سخت افزارها	نفوذ در عمق	جاسوسان
برتری استراتژیک	تحریف	سازمان های اجرایی	Bypass		سوء استفاده از پروتکل	مجرمین شبکه
برتری تاکتیکی	دسترسی	داده ها	Re-route	آسیب پذیریهای نرم افزارهای پایه DB، OS	مقیم در سخت افزار	ارتش های سایبری
اهداف ملی	منع یا انکار	Cloud	Copy		کنترل زیرساخت	مزدوران
اهداف نظامی	سرقت	خدمات	Re-play	آسیب پذیریهای سامانه های کلیدی در کلیه مراحل SDLC	Stealth	رقیبان اقتصادی
جاسوسی صنعتی	Mis‐direction	شبکه	Deny			گروهای هکرهای
صدمات عمده		Computer	Probe			معارضین سیاسی
چالش وتنش		Component	Probe			تروریست ها
		پردازش	Scan			طرفدارن جریان باز
		حساب کاربری	Flood			اقدامات ضد اجتماعی

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

بررسی لایه نیازمندیهای عملیاتی

انسان افزار

سامانه افزار

سازمان افزار

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

بررسی لایه نیازمندیهای عملیاتی

انسان افزار

- **هدف عملکردی از دیدگاه پدافندی** : تربیت نیروی متخصص برای توسعه دفاعی فضای سایبر و افزایش سطح تجربیات جهت نیل به فناوری های رقابتی و پیشرفته در این حوزه

سامانه افزار

- **هدف عملکردی از دیدگاه پدافندی** : خرید ، سفارش، تولید و حمایت از محصولات دفاعی داخلی، ارزیابی امنیتی محصولات نرم افزاری، تولید محصولات نرم افزاری پایه مانند سیستم عامل، پایگاه داده و سخت افزاری

سازمان افزار

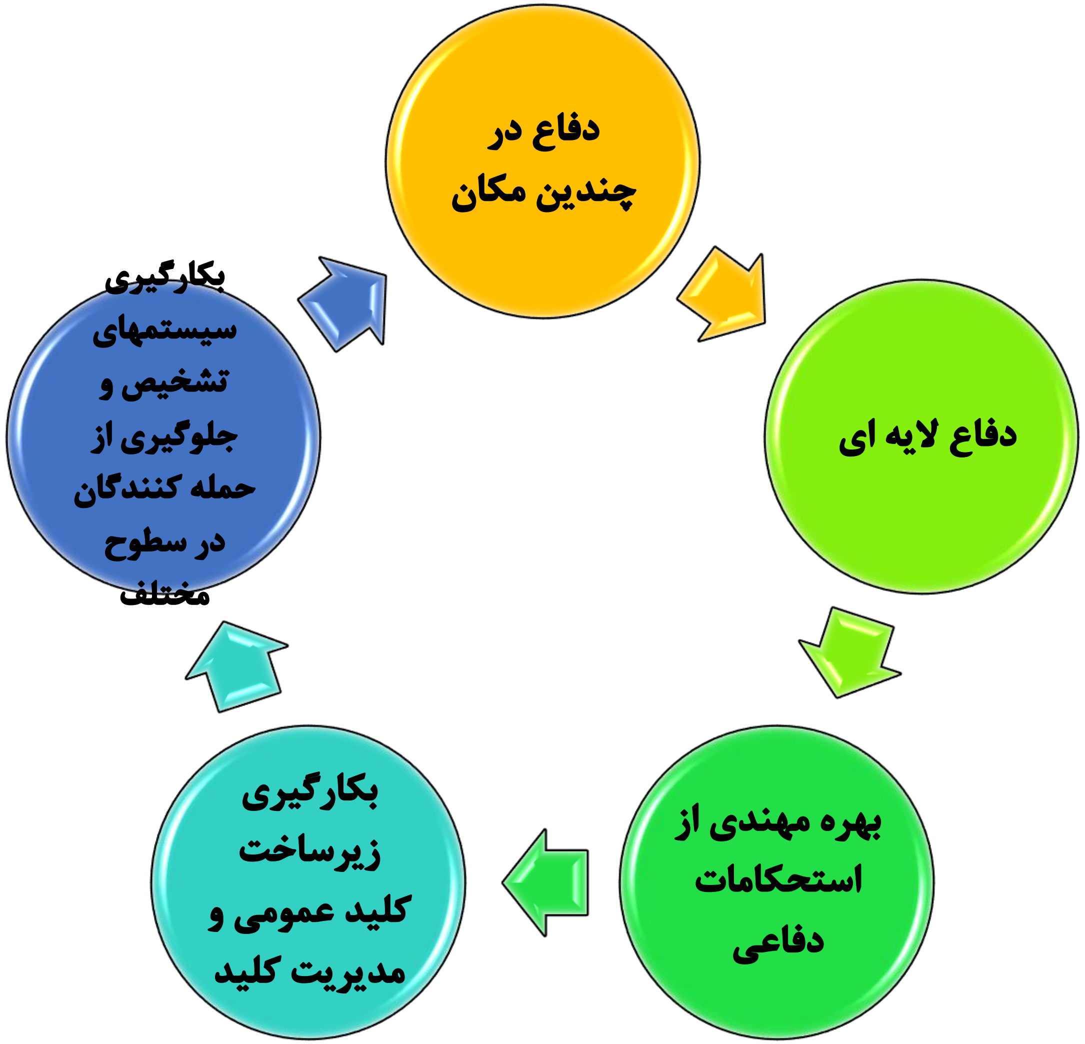
- **هدف عملکردی از دیدگاه پدافندی** : نیازمندی های فرآیندها و مدیریت کلان جهت سیاست گذاری و ارائه خطوط راهنما و توصیه نامه ها، همچنین بررسی نیازمندی های زیرساختی حوزه سایبر

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

بررسی لایه محصولات/خدمات/فناوری

- ابتدا بایستی محصولات و خدمات موردنیاز را تعیین کنیم و سپس با توجه به اینکه هریک از این محصولات و خدمات به چه فناوری هایی وابسته اند و از چه فناوری هایی بهره می برند، فناوری های موردنیاز را مشخص سازیم
- به ازای هر محصول، یکسری نیازمندی وجود دارند که پیشرانه تولید آن می شوند و به عبارت دیگر، لزوم تولید یک محصول مشخص را تعیین می کنند.
- نیازمندیهای سازمانی به همراه طرح دفاع سایبری کشور از مهمترین تبیین کننده های این نیازمندیها هستند.
- هر محصول برای تولید نیازمند یکسری از فناوری هاست که یا باید از پیش آماده باشند و یا در خلال تولید محصول فراهم آیند.

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق



ابزارها و مکانیزمها

فلسفه معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

- دفاع چند گانه بر اساس متدولوژی‌های دفاع در عمق و دفاع لایه به لایه مطابق با ملاحظات پدافند غیرعامل
- تشکیل و جداسازی نواحی عملکردی بر اساس نیازمندی‌ها و سطوح امنیتی-پدافندی
- هم افزایی کارآمد محصولات امن و امنیتی بومی

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع راهبردی

لایه سیاستهای فرماندهی،

دفاعی و اداره

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع راهبردی

بنا بر ماتریس تعریف شده، ستون راهبردی بایستی برای سطرهای لایه تهدیدات، لایه عملیاتی و لایه محصولات/خدمات/فناوری، اصول و راهبردهایی را مشخص نماید.

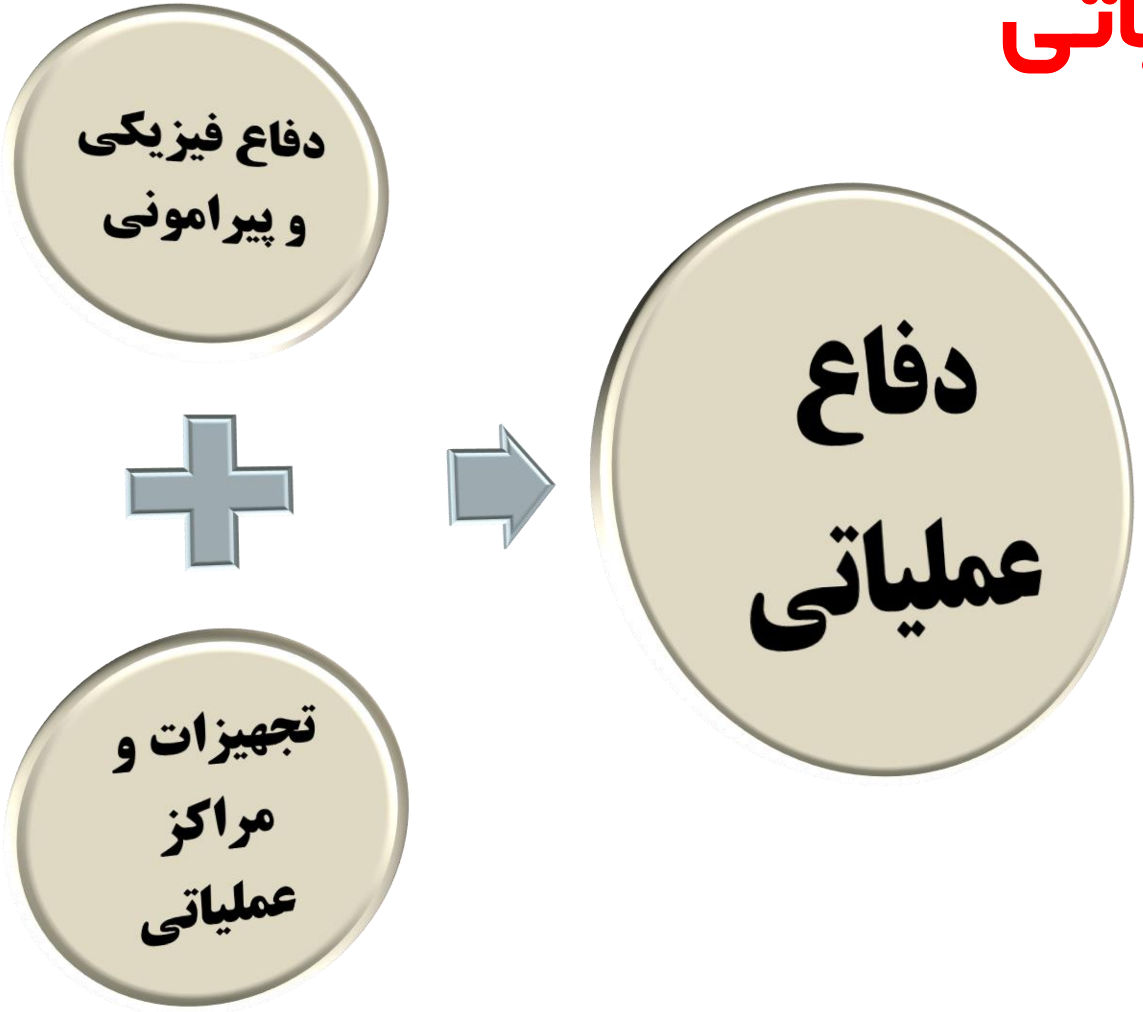
معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

- تدوین سیاستهای فرماندهی، دفاعی و اداره
- ایجاد تشکیلات دفاعی سازمان
- دستهبندی سرمایه ها و تعیین کنترلهای لازم
- تدوین مکانیزمهای مدیریت تداوم کسب و کار سازمان(BCP)
- تدوین دستورات و الزامات مدیریت ارتباطات
- تدوین دستورات و الزامات دفاع فیزیکی و کنترل دسترسی
- تدوین دستورات و الزامات نگهداری و توسعه سیستمها

اصل دفاع راهبردی

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع عملیاتی



معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع عملیاتی

دفاع فیزیکی و پیرامونی

- سامانه نظارت تصویری CCTV
- سامانه حفاظت پیرامونی
- سامانه های هوشمند الکترونیکی
- سامانه های کنترل، بازرسی و شناسایی
- سامانه های اعلام و اطفای حریق

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع عملیاتی

- تجهیزات و مراکز عملیاتی
  - مرکز عملیات امنیت (SOC)
  - مرکز پاسخگویی به رخدادهای سایبری (CSIRT)
  - جمع آوری و بررسی ادله قانونی (Forensic)
  - مدل سازی تهدیدات Threat) (Modeling
  - ارزیابی و مدیریت آسیب پذیری Vulnerability) Assessment/Management)
  - مرکز رصد، پایش، مراقبت، تشخیص رخدادهای سایبری

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی

لایه های پدافند سایبری نگاشت شده بر اصل دفاع فنی

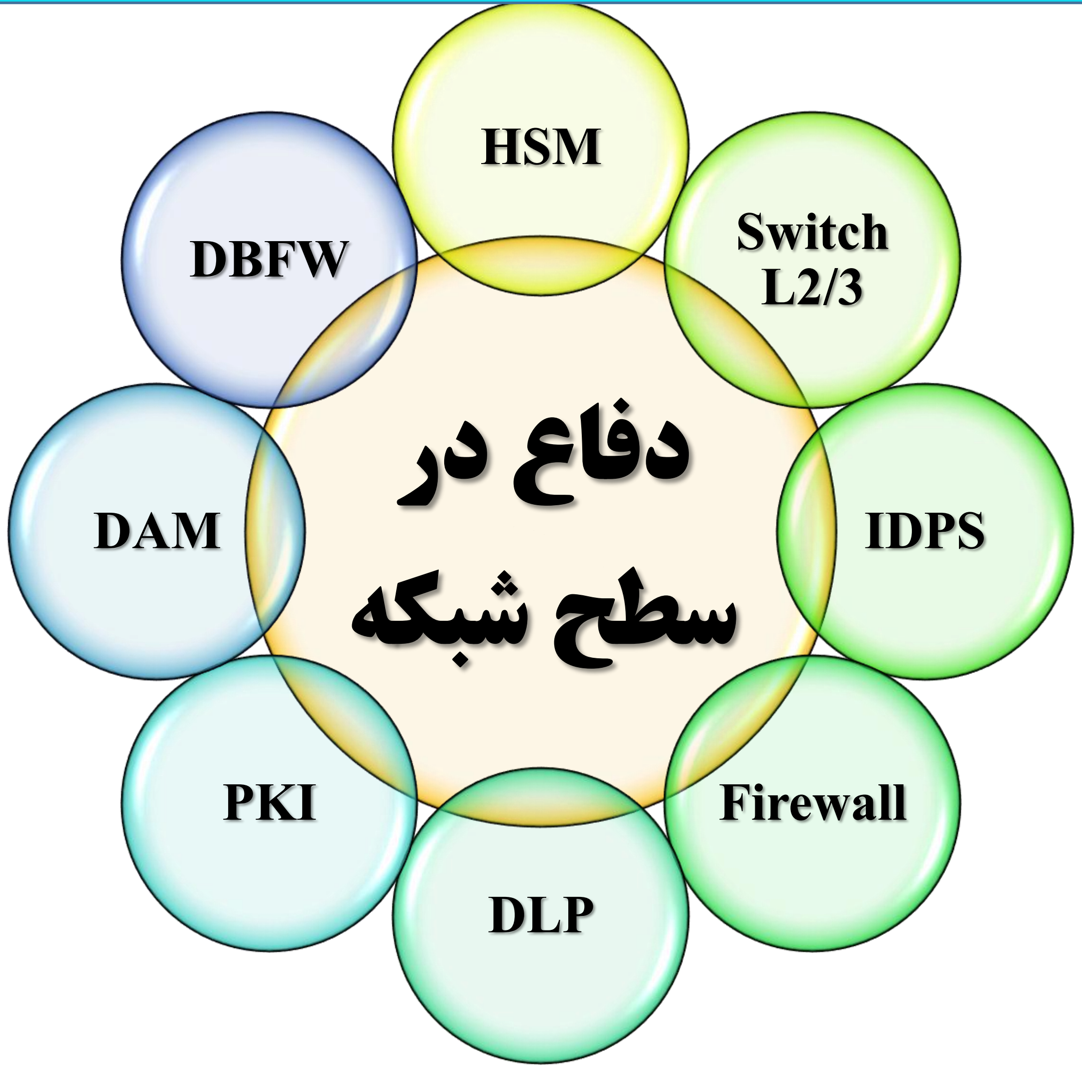
- دفاع در سطح سیستم عامل
- دفاع در سطح داده و محتوا
- دفاع در سطح برنامه های کاربردی
- دفاع در نقاط انتهایی (کاربران)
- دفاع در سطح شبکه سازمان
- دفاع پیرامونی و مرزبانی

معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی

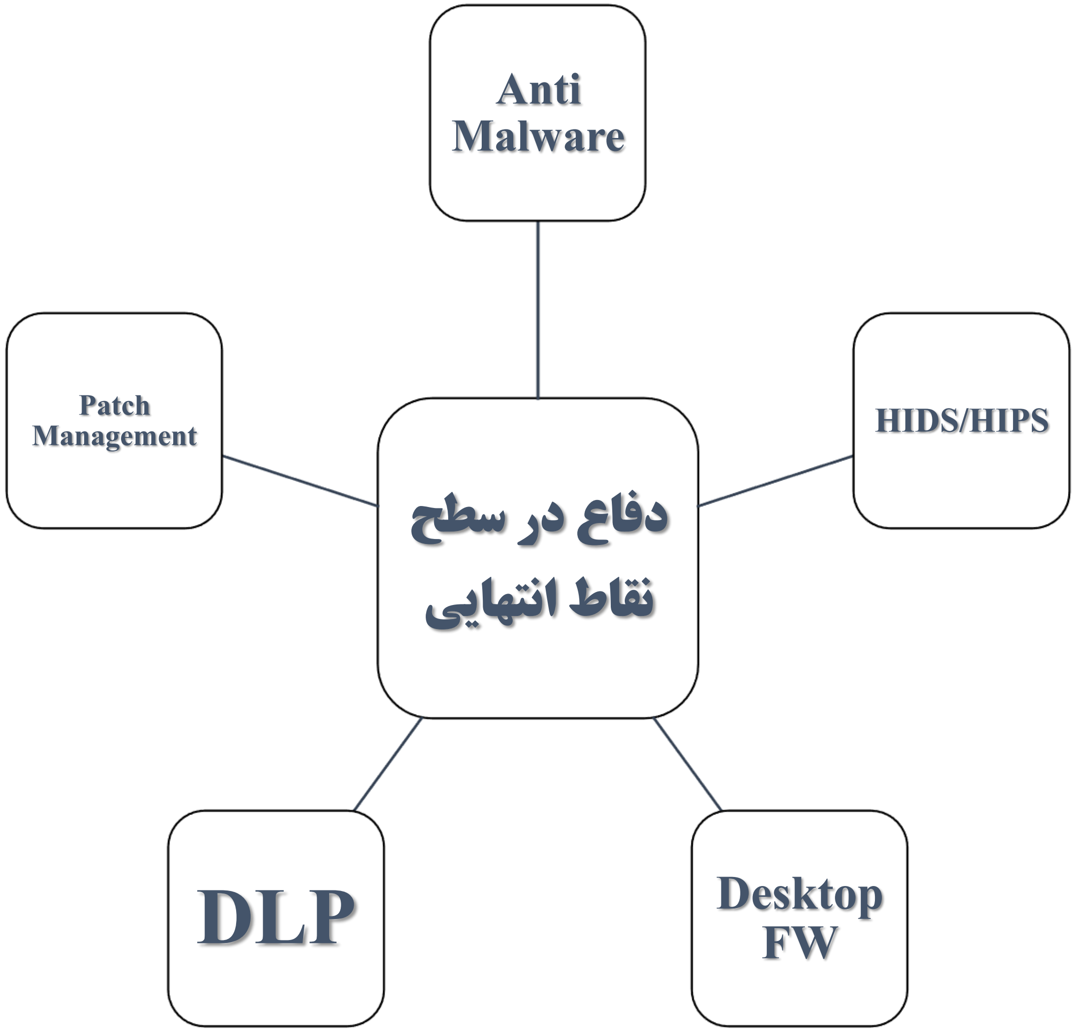
معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی



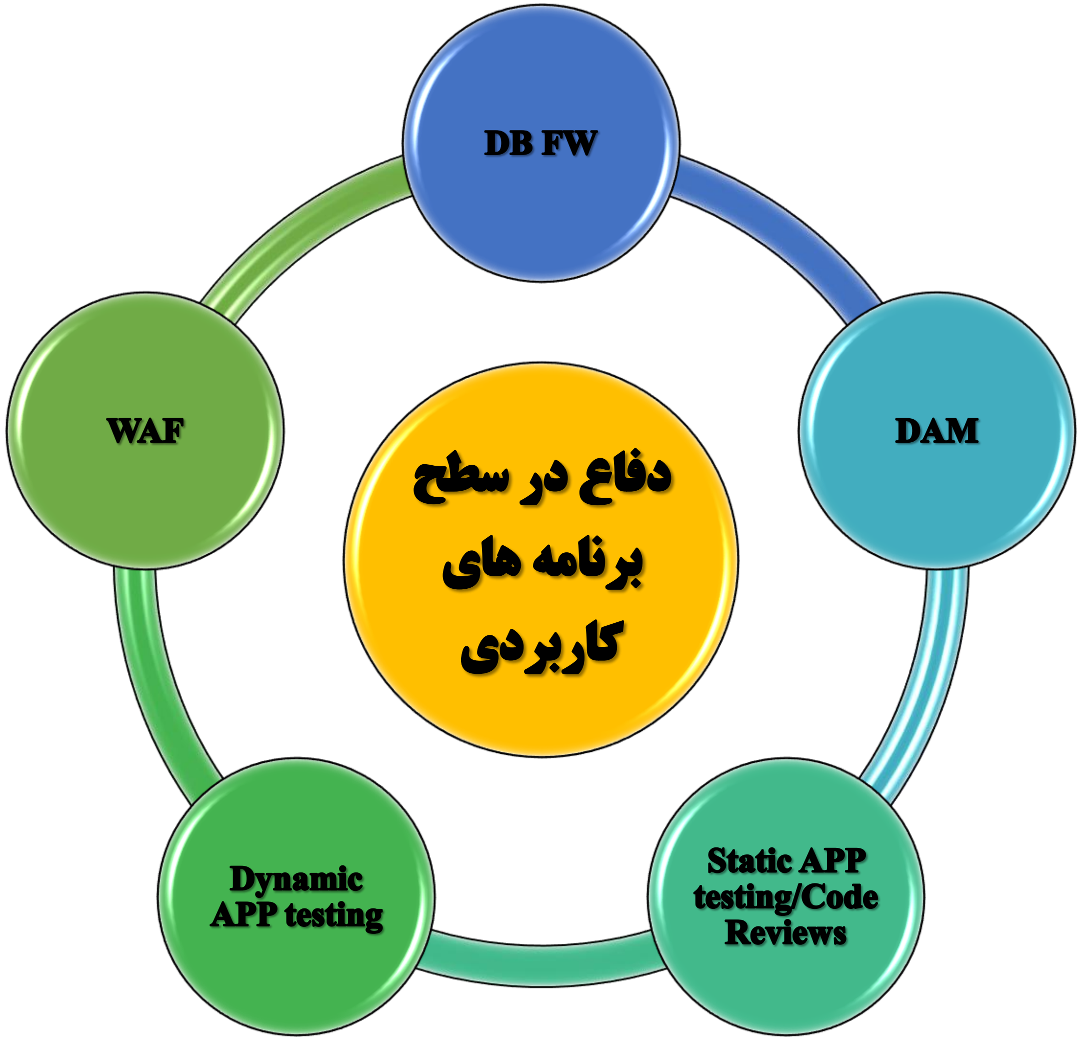
معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی



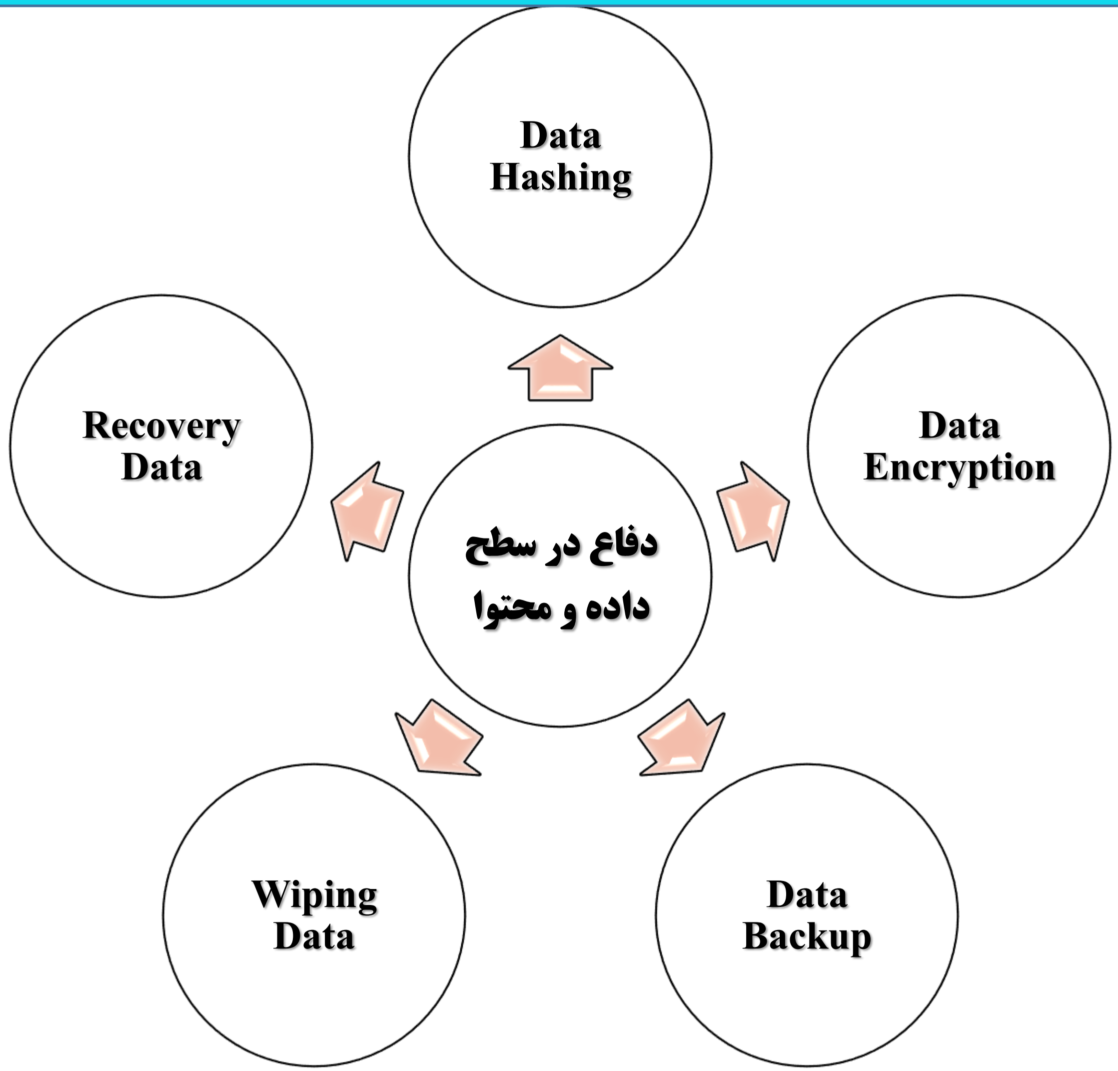
معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی



معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی



معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اصل دفاع فنی

معماری بومی پدافند سایبری مبتنی

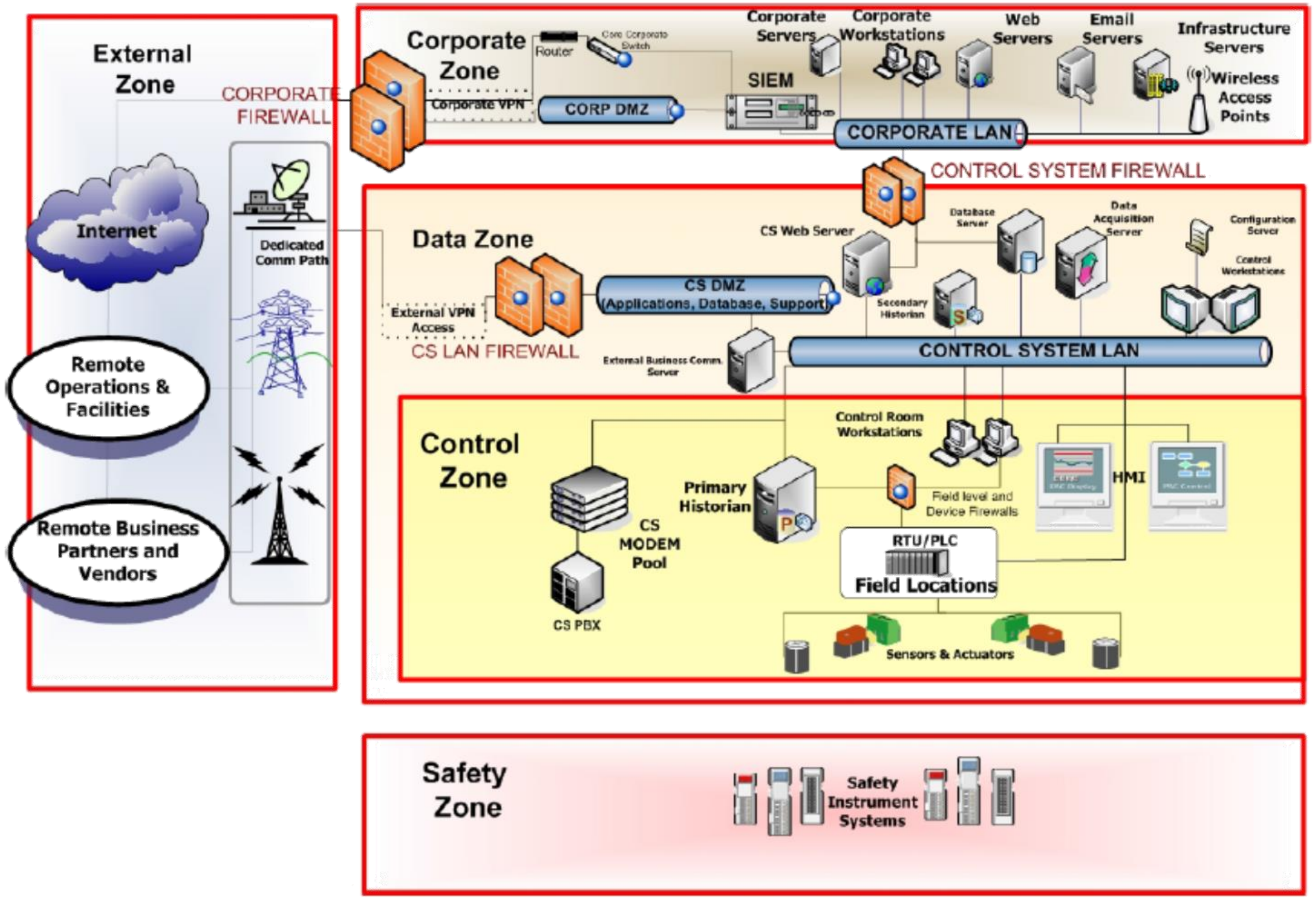
بر متدولوژی دفاع در عمق

در شبکه های صنعتی

تفاوت بین امنیت فناوری اطلاعات با امنیت سیستمهای کنترل صنعتی

شبکه ها و کامپیوترهای فناوری اطلاعات	سیستم های کنترل صنعتی
درصورت از دست دادن داده و یا بروز وقفه های ناخواسته ، می توان سیستم را با راه اندازی مجدد و یا برگرداندن فایل های پشتیبان به حالت اولیه برگرداند.	از دست دادن داده و یا بروز وقفه قابل تحمل نیست و ممکن است نتایج مهلکی را به دنبال داشته باشد
با تاخیر ناخواسته می توان کنار آمد	تاخیر زیاد قابل تحمل نیست
درصورت بروز مشکلات حاد برای سیستم با راه اندازی مجدد آن می توان مشکل ناخواسته را به نوعی حل کرد!	کارکرد سیستم می بایست همواره عاری از خطاء باشد . از کار افتادن سیستم حتی برای لحظاتی اندک می تواند فاجعه آمیز باشد
از نرم افزارهای آنتی ویروس استفاده زیاد می شود	بکارگیری نرم افزارهای آنتی ویروس در اکثر موارد مشکل است ، چراکه تاخیر قابل تحمل نمی باشد .
ارایه دوره های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی بسیار متداول است	ارایه دوره های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی کم است
از رمزنگاری استفاده می شود	تعداد بسیار زیادی از سیستم های کنترل صنعتی داده و پیام های کنترلی را به صورت غیر رمز شده ارسال می نمایند.
تست نفوذ به صورت ادواری انجام می شود	تست نفوذ به صورت ادواری در شبکه کنترلی انجام نمی شود و زمانی هم که این کار انجام می شود می بایست این کار با دقت صورت پذیرد تا باعث بروز اختلال نگردد .
پیاده سازی **patch** نرم افزارها به صورت ادواری انجام می شود	پیاده سازی **patch** نرم افزاری می بایست با دقت صورت پذیرد و معمولا" مستلزم هماهنگی با شرکت فروشنده تجهیزات کنترل صنعتی می باشد
ممیزی امنیت اطلاعات لازم است و معمولا" به صورت ادواری انجام می شود	ممیزی امنیت اطلاعات بطور ادواری انجام نمی شود
تجهیزات معمولا" هر سه تا پنج سال جایگزین و یا ارتقاء می یابند	تجهیزات استفاده شده برای مدتی طولانی و بدون جایگزینی استفاده می گردند .

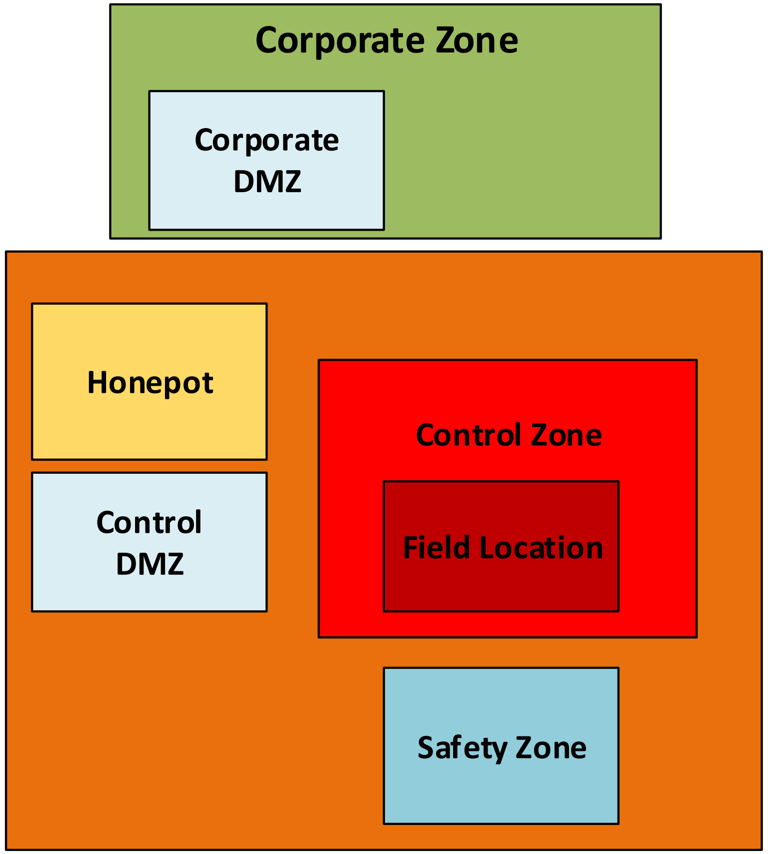
مدل مرجع پیاده سازی متدولوژی دفاع در عمق در ICS



راهکارهای پدافندی کنترل صنعتی بومی در معماری دفاع در عمق

- معماری لایه‌بندی شده
- فایروال کنترل صنعتی بومی با قابلیت بازرسی عمیق پروتکل‌های کنترل صنعتی
- سامانه تشخیص نفوذ صنعتی بومی با قابلیت شناسایی امضای تهدیدات کنترل صنعتی
- SIEM کنترل صنعتی بومی با قابلیت همبسته سازی رخدادهای مبتنی بر IT و OT
- راهکارهای DLP بومی
- راهکارهای هانی‌پات بومی
- راهکارهای DAM بومی
- ضدبدافزار بومی

نمونه معماری‌های مرجع بر اساس سطح پدافندی در صنعت



معماری کلی سطح پدافندی حیاتی و حساس

تعیین ناحیه‌های امنیتی

بهترین نقطه شروع برای طراحی استراتژی دفاع در عمق، تعیین دقیق نواحی امنیتی است

- **External zone**: ناحیه ارتباط با اینترنت، **peer**ها و سرورهای پشتیبان خارجی. این ناحیه پرخطرترین منطقه، اما کم اولویت‌ترین آن‌ها ازنظر امنیتی است.
- **Corporate Zone**: ناحیه اتصال به سرورهای همکار، مانند سرورهای **Email**، سرورهای **DNS** و ... این ناحیه نیز به دلیل حجم سرورهایی که در آن قرار دارد و اتصال آن با ناحیه خارجی ناحیه امنیتی پرخطری به شمار می‌رود، اولویت امن سازی آن از ناحیه خارجی بیشتر و از سایر نواحی کمتر است.

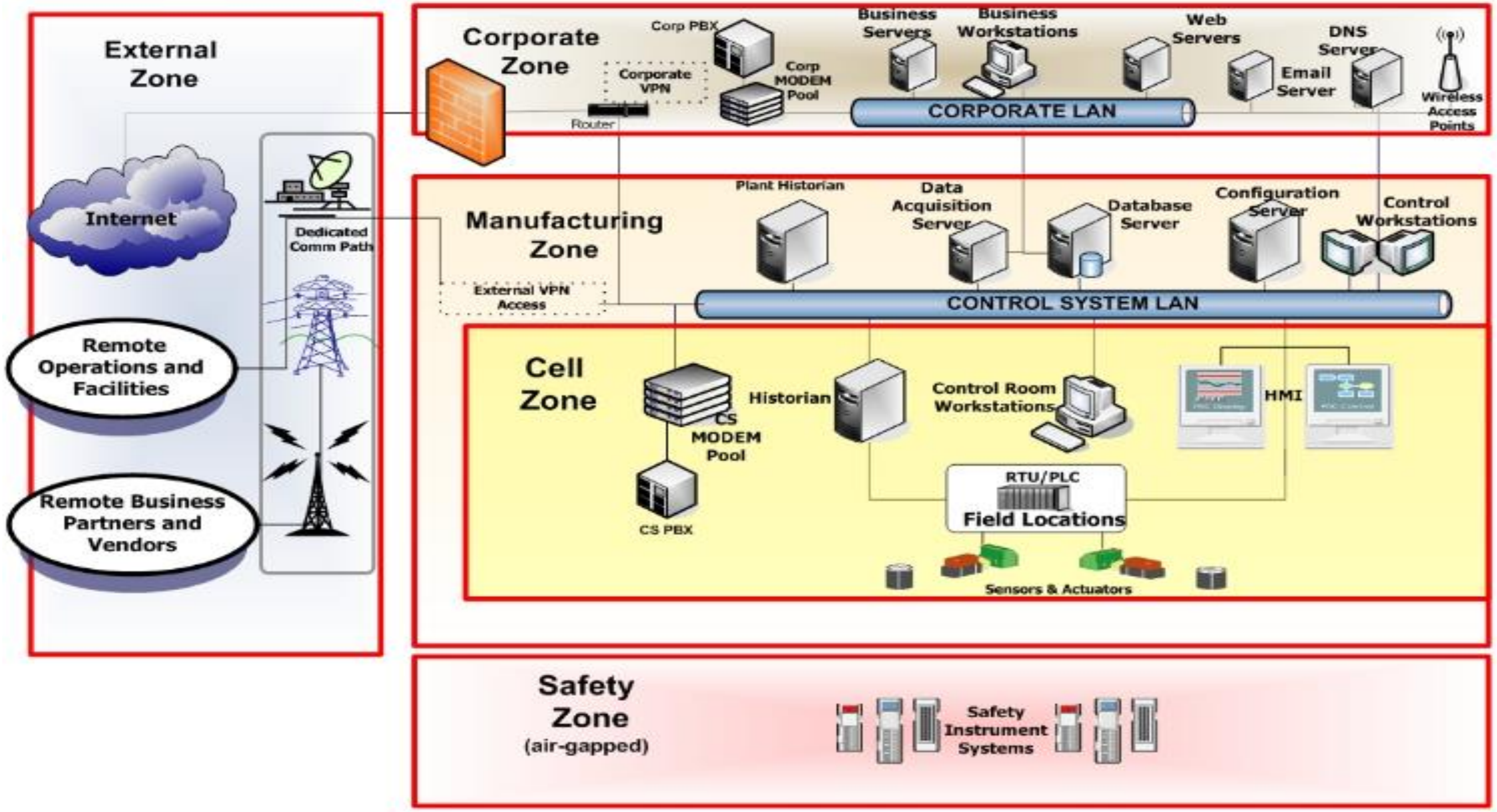
تعیین ناحیه‌های امنیتی

بهترین نقطه شروع برای طراحی استراتژی دفاع در عمق، تعیین دقیق نواحی امنیتی است

- **Manufacturing/Data Zone**: این ناحیه، ناحیه ذخیره و مدیریت داده‌ها به شمار می‌رود و ناحیه تبادل داده‌ها و اطلاعات با سایر نواحی به شمار می‌رود. با توجه به حجم بالای اطلاعات مهم که از طریق این ناحیه تبادل می‌شود، این ناحیه ازنظر امنیتی پرخطر به شمار می‌رود و امن سازی آن نیز اولویت بالاتری از نواحی قبلی دارد.
- **Cell Zone**: این ناحیه محل قرارگیری کنترل‌کننده‌هایی مانند **PLC**، **HMI** و ... است. اولویت امنیتی این ناحیه بسیار بالاست.
- **Safety Zone**: محل قرارگیری تجهیزات کنترل امنیتی است. ناحیه‌ای کم‌خطر محسوب می‌شود ولی حفظ امنیت آن بالاترین اولویت را بین سایر نواحی داراست.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

تعیین ناحیه‌های امنیتی



یک سیستم کنترل صنعتی نمونه پس از ناحیه بندی

ایجاد نواحی DMZ

- لایه بعدی برای ایجاد استراتژی دفاع در عمق، تعریف چندین ناحیه به‌عنوان ناحیه DMZ و جداسازی این نواحی از سایر نواحی است.
- نواحی DMZ باید بر اساس کارکرد و مجوز دسترسی جداسازی شوند.
- نواحی DMZ درواقع نواحی هستند که با شبکه خارجی مانند اینترنت در تعامل مستقیم هستند.
- جداسازی این نواحی موجب می‌شود که در صورت رخ دادن حمله‌ای از طریق اینترنت، حمله در این ناحیه باقی بماند و به سرورهای اصلی که حاوی اطلاعات حساس هستند، آسیب کمتری وارد شود.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

استفاده از فایروال

فایروال‌ها قوانین محکمی را برای ارتباط بین نواحی مختلف تعریف می‌کنند

- **Packet Filter Firewalls**: این فایروال در لایه network کاربرد دارد و بسته‌هایی را بین شبکه‌های مختلف تبادل می‌شوند، تحلیل می‌کند و بر اساس قوانین تعریف شده به برخی از بسته‌ها اجازه تبادل می‌دهد و برخی از بسته‌ها را حذف می‌کند. انواع فیلترینگ های مبتنی بر جزئیات بسته های در حال تبادل نظیر payload بسته ها، قابلیت بازرسی عمیق بسته ها (DPI) را فراهم می کند که سطح دقیق تری از نظارت بر روی بسته های در حال انتقال بر پایه پروتکل های کنترل صنعتی را فراهم می کند.

- **Proxy Gateway Firewalls**: این فایروال‌ها در نقش یک واسط proxy، شبکه‌هایی را که از آن محافظت می‌کنند پنهان می‌کنند. در لایه Application عمل می‌کند و مانند یک gateway سر راه ارتباط قرار می‌گیرد و اجازه هیچ ارتباط تعریف‌نشده‌ای را نمی‌دهد و تمامی ارتباطات باید از آن عبور کند. در شبکه‌های کنترل صنعتی این نوع فایروال برای جداسازی لایه‌های کنترل و Business و همچنین برای محافظت از نواحی DMZ مناسب است

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

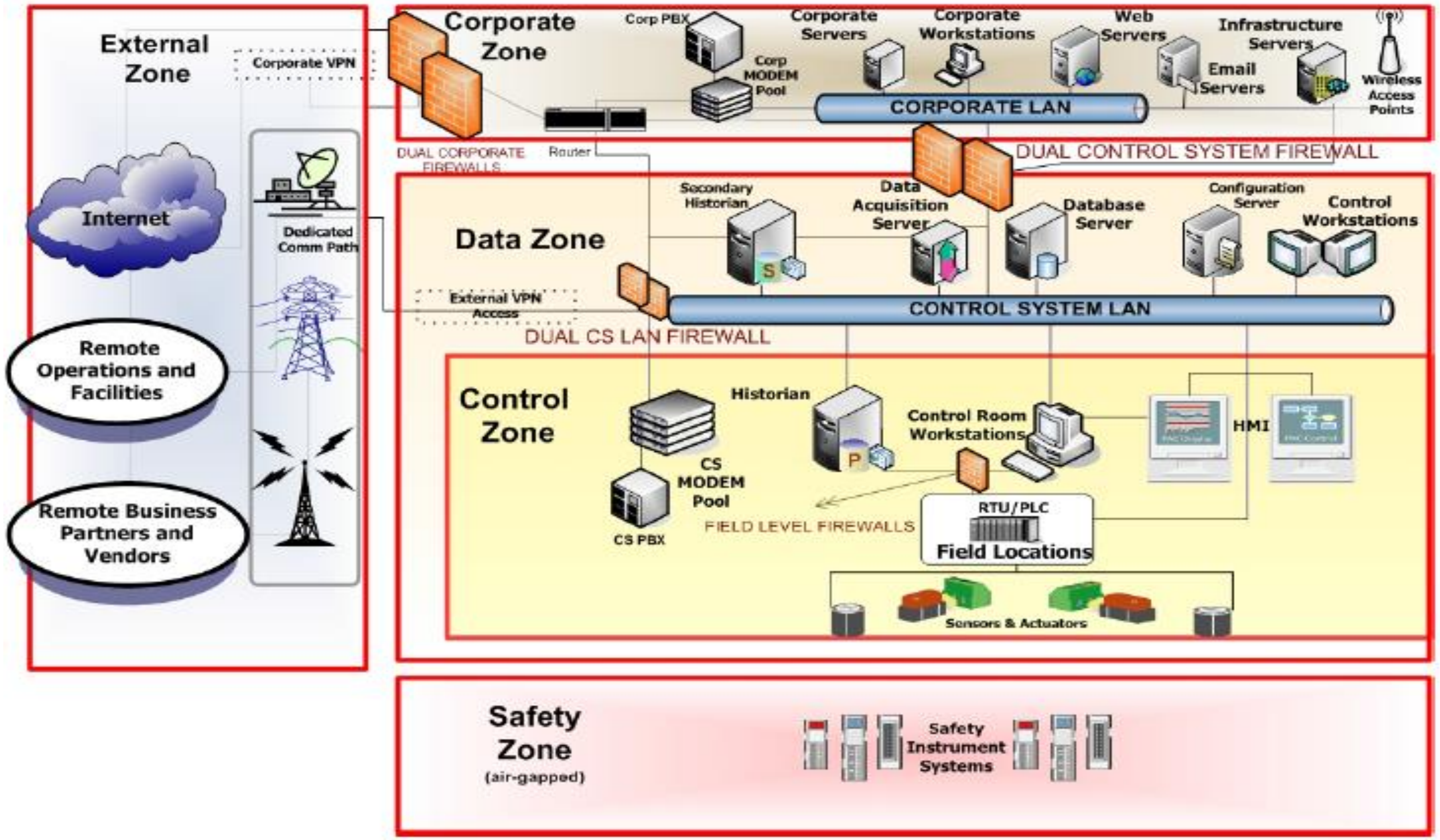
استفاده از فایروال

- **Host Firewalls:** فایروال‌های Host راهکارهای نرم‌افزاری هستند که از پورت‌ها و سرویس‌های سیستمی که روی آن نصب شده است، محافظت می‌کند. بسیاری از سیستم‌عامل‌ها در حال حاضر دارای فایروال Host هستند که می‌توان با تعریف قوانین مناسب روی این فایروال‌ها ترافیک پورت‌ها و سرویس‌های سیستم را محدود کرد. این نوع فایروال نیز در شبکه‌های کنترل صنعتی اهمیت زیادی دارد و باید روی تمامی سرورها نصب و به‌خوبی پیکربندی شود.

- **PLC/Field Level Firewalls:** فایروال‌هایPLC فایروال‌های سخت‌افزاری هستند که مستقیماً به خطوط متصل به Deviceها وصل می‌شوند این فایروال‌ها قابلیت‌های امنیتی را به PLCها، RTUها و سیستم‌های کنترلی اضافه می‌کنند.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

استفاده از فایروال



سیستم کنترل صنعتی نمونه پس از اضافه شدن فایروالها

استفاده از سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ به بررسی الگوهای خطرساز در تبادلات شبکه می‌پردازند و در صورت کشف الگوهای خطرساز یا ناشناخته آن‌ها را به‌عنوان احتمال حمله و نفوذ به سیستم گزارش می‌دهند.

مهم‌ترین نکاتی که باید در سیستم‌های تشخیص نفوذ در سیستم‌های کنترل صنعتی مورد توجه قرار بگیرند، عبارت‌اند از:

- استفاده از بسته‌ها و ابزارهای تشخیص نفوذ مختص سیستم‌های ICS/SCADA
- استفاده از سیستم‌های تشخیص نفوذ در پشت فایروال‌ها

استفاده از سیستم‌های تشخیص نفوذ

- استفاده از فایل‌های log به‌عنوان ابزاری برای تشخیص نفوذ
- ابزارهای Security Information & Event Management (SIEM) می‌توانند دیدگاهی برای تشخیص الگوی نفوذ ایجاد کنند.
- سیستم تشخیص نفوذ به‌گونه‌ای پیکربندی گردد که هشدارهای مناسب را در کوتاه‌ترین زمان به افراد ذیربط بدهد.
- از honeypotهای داخلی برای تشخیص سریع فعالیت‌های مشکوک در شبکه استفاده شود.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

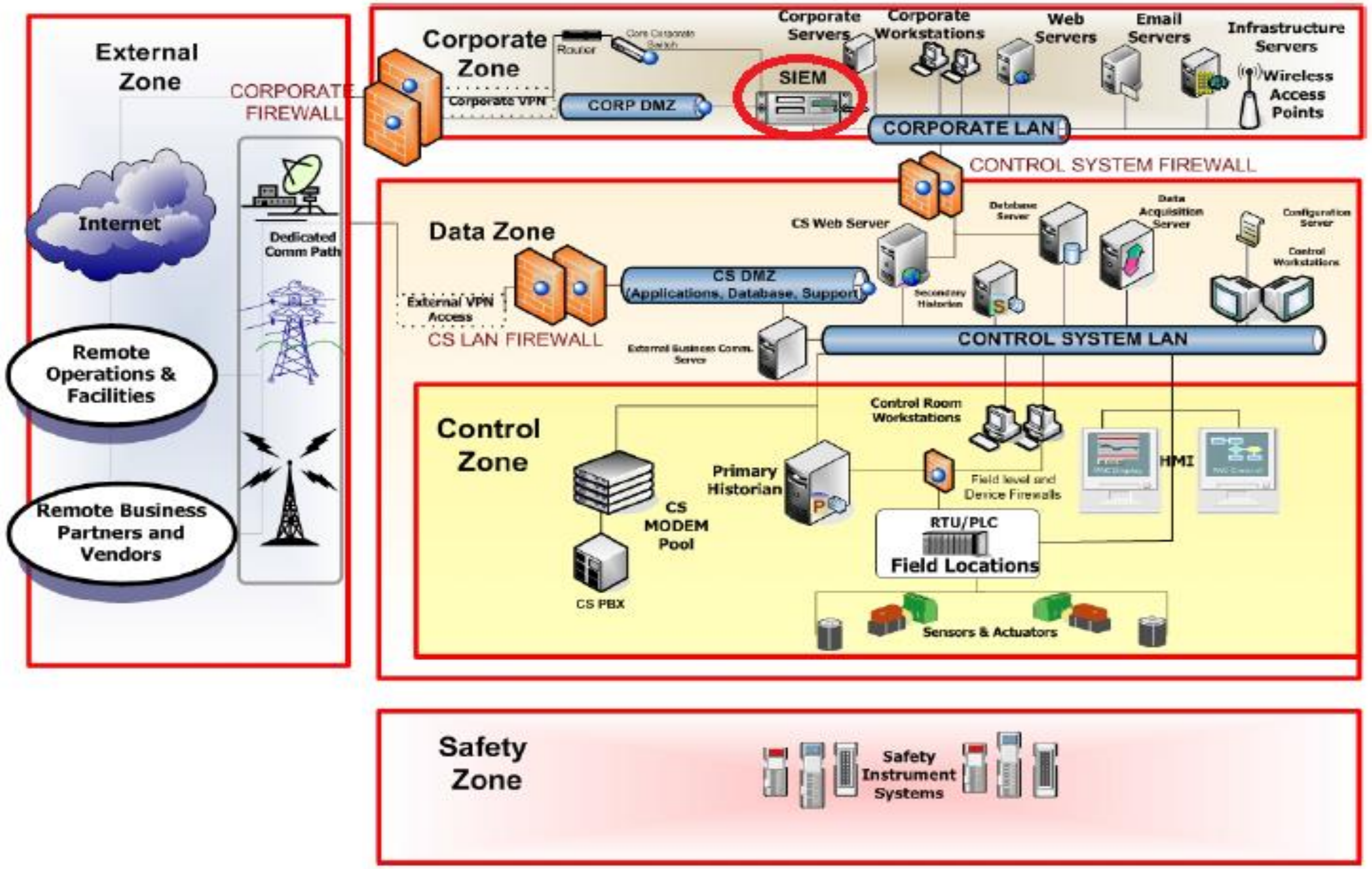
سامانه مدیریت اطلاعات و رخدادهای امنیتی(SIEM)

یکی از موارد مهم در استراتژی دفاع در عمق نحوه عملکرد سیستم در هنگام رخ دادن رویدادها و ثبت تمامی اطلاعات موردنیاز برای ردگیری و پیگیری آن رویداد است.

- سامانه Security Incident Event Management (SIEM) وظیفه مانیتورینگ و ثبت رویدادها را به‌صورت مرکزی انجام می‌دهد و به جمع‌آوری logتمامی ابزارهای امنیتی شامل IDS logs، Firewall logs و Log سایر اجزا سیستم می‌پردازد.
- ابزار SIEM بیشترین استفاده را زمانی دارد که حمله‌ای در سیستم رخ می‌دهد و تحلیلگر سیستم می‌تواند با کنار هم گذاشتن Logها، روش حمله، فرد حمله‌کننده و ... را کشف کند.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

اضافه شدن SIEM و IDS به سیستم کنترل صنعتی نمونه



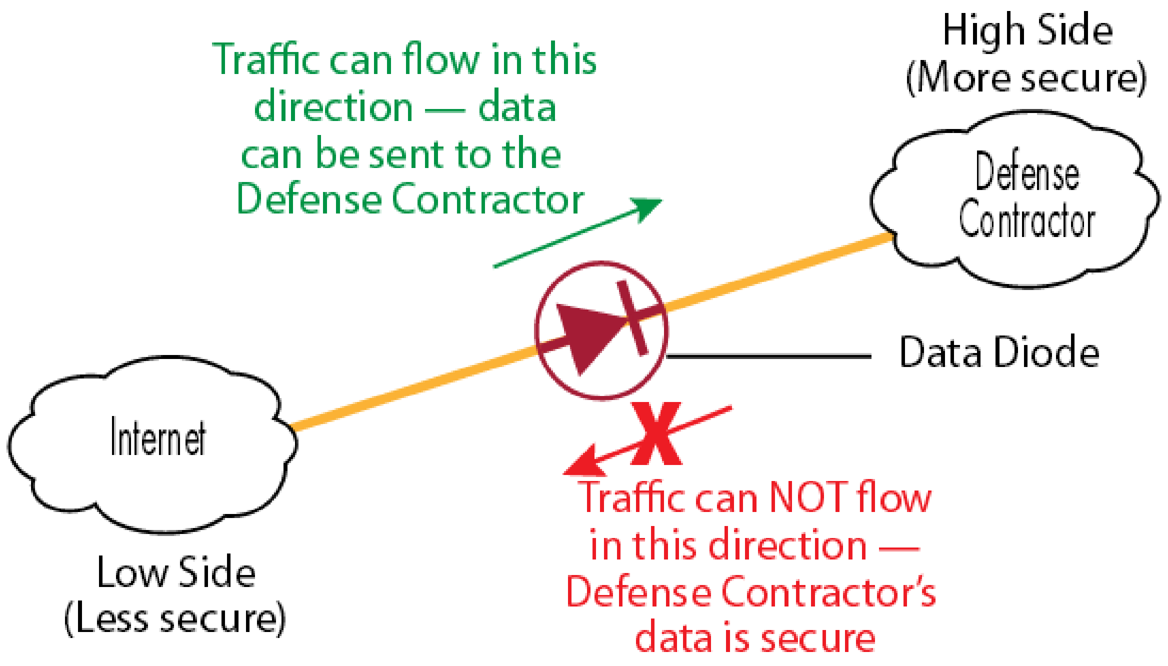
سامانه مدیریت اطلاعات و رخدادهای امنیتی(SIEM)

استفاده از دیتادیود برای یک‌طرفه سازی ارتباط

- دیتادیود به لینک‌های ارتباطی در شبکه گفته می‌شود که ترافیک روی آن‌ها به‌صورت یک‌طرفه ارسال می‌شود و امکان برگشت اطلاعات روی این لینک‌ها و این مسیرها وجود ندارد.
- در این روش دفاعی درصورتی‌که به هر نحو نفوذگر بتواند از سد سیستم‌های دفاعی گذشته و اطلاعاتی را وارد سیستم کنترل صنعتی کند (برای مثال درخواستی را به سیستم ارسال کند) به‌هیچ‌وجه نمی‌تواند پاسخی از سمت سیستم دریافت کند و درنتیجه محرمانگی داده‌ها حفظ خواهد شد.
- در تمامی لینک‌های شبکه که مسیر ارتباط یک‌طرفه است و نیازی به برگشت اطلاعات وجود ندارد، باید از دیتا دیودها استفاده شود.

استفاده از دیتادیود برای یک‌طرفه سازی ارتباط

نحوه عملکرد دیتادیودها



ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

تعریف سیاست‌های امنیتی

- تعریف سیاست‌های امنیتی قدم مهمی در امن سازی سیستم‌های کنترل صنعتی است.
- بسیاری از سیاست‌های امنیتی که در سیستم‌های IT تعریف می‌شوند، در سیستم‌های کنترل صنعتی نیز کاربرد دارند.
- سیاست امنیتی سندی است که برنامه‌های یک سامانه را برای محافظت از سرمایه‌های فیزیکی و اطلاعاتی مشخص می‌کند.

تعریف سیاست‌های امنیتی

نکاتی که برای تعریف سیاست‌های امنیتی اهمیت زیادی دارند عبارت‌اند از:

- سیاست باید عملی و قابل‌اعمال باشد.
- سیاست تعریف شده نباید روی کارایی سیستم تأثیر بگذارد.
- سیاست تعریف شده نباید هزینه زیادی را به سیستم وارد کند.
- سیاست‌ها باید با مشورت مدیر سیستم و مجری سیستم تعیین شود.
- سیاست‌ها باید به‌روز باشند و بر اساس تغییرات فناوری‌ها و نیازمندی‌های سازمان تغییر کنند.
- تعیین دسترسی افراد به دارایی‌ها باید در این بخش مشخص شود.

تعریف سیاست‌های امنیتی

ساختار هر سیاست امنیتی از اجزای زیر تشکیل می‌شود:

- عبارتی در رابطه با موضوع سیاست
- چگونگی اجرای سیاست در محیط سازمان
- نقش و مسئولیت افراد مختلف تأثیرگذار در سیاست
- سیاست به چه میزان انعطاف‌پذیر است؟
- اعمال، فعالیت‌ها و فرایندهای مجاز و غیرمجاز
- موارد سخت‌گیری و عدم انعطاف سیاست

دسترسی راه دور امن

امروزه بسیاری از تکنولوژی ها، دسترسی راه دور را به‌عنوان یک قابلیت مهم به امکانات خود اضافه کرده‌اند؛ اما برای امن سازی ارتباطات و دسترسی‌های راه دور نیاز به استفاده از تکنولوژیها و پروتکل‌های امن سازی این بستر است که ازجمله آن‌ها می‌توان به VPNها و احراز هویت‌های چندفاکتوره اشاره کرد.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

دسترسی راه دور امن

مهم‌ترین نکات برای پیاده‌سازی دسترسی راه دور امن در سیستم‌های کنترل صنعتی :

- تغییر پورت TCP برای پروتکل‌های راه دور معروف
- تغییر پیکربندی VPN به‌گونه‌ای که امکان استفاده از split tunneling وجود نداشته باشد.
- ثبت تمامی نشست‌های راه دور ایجاد شده، در سیستم رویدادنگاری
- استفاده از احراز هویت چندفاکتوره برای تمامی نشست‌های راه دور
- رمزنگاری همه ارتباطات روی شبکه‌های غیرقابل‌اعتماد
- استفاده از رمزهای بسیار پیچیده برای کاربران راه دور
- محدود کردن دسترسی راه دور به بخش کوچکی از شبکه. برای مثال دسترسی فقط به ناحیه DMZ وجود داشته باشد و دسترسی به سایر سرورها از طریق این ناحیه انجام شود.
- اطمینان از اینکه سیستم تشخیص نفوذ (IDS) تمامی ترافیک راه دور را مورد بررسی قرار می‌دهد.

امن سازی ارتباطات بی‌سیم

استفاده از اتصالات بی‌سیم به سیستم‌های کنترل صنعتی، ریسک‌های جدیدی را به این سیستم‌ها اضافه کرده است

مهم‌ترین راهکارها برای امن سازی ارتباطات بی‌سیم راه دور عبارت‌اند از:

- تعریف سیاست‌های امنیتی برای LANهای بی‌سیم (WLANها)
- جداسازی LANهای بی‌سیم از LANهای سیمی با استفاده از یک فایروال
- دسترسی به WLANها تنها پس از احراز هویت امکان‌پذیر باشد.

امن سازی ارتباطات بی‌سیم

- ترافیک WLAN با استفاده از الگوریتم‌های رمزنگاری قوی رمز شود.
- توان آنتن‌های بی‌سیم برای منطقه محدودی تعریف شود و خارج از منطقه دسترسی به آنتن‌ها امکان‌پذیر نباشد.
- پویش برای یافتن نقاط دسترسی غیرمجاز به شبکه بی‌سیم به‌صورت متناوب انجام شود.
- انتقال SSID beacon غیرفعال شود.
- از آدرس IPهای ایستا در شبکه WLAN استفاده شود.
- اطمینان از اینکه بسته‌های ARP برادکست شده در شبکه سیمی در شبکه بی‌سیم منتقل نمی‌شوند.
- Wi-Fi Protected Setup (WPS) را غیرفعال کنید و به‌صورت متناوب از غیرفعال بودن آن مطمئن شوید.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

مدیریت وصله‌ها و استفاده از آخرین وصله‌ها

- مدیریت وصله‌ها مؤلفه بسیار مهمی در امنیت سیستم‌های کنترل صنعتی به شمار می‌رود. در بسیاری از موارد تنها راه‌حل برای مقابله با آسیب‌پذیری‌های کشف شده استفاده از وصله‌های منتشر شده برای آسیب‌پذیری است.
- مشکلی که در استفاده از وصله‌ها وجود دارد این است که گاهی ممکن است استفاده از وصله کارکرد سیستم را با اختلال مواجه کند

مهم‌ترین نکات برای مدیریت وصله‌ها عبارت‌اند از:

- مدیریت سیستم باید همواره آخرین اطلاعات از آسیب‌پذیری‌های کشف شده در رابطه با سیستم ICSمورد مدیریت خود را به دست بیاورد.
- مدیریت سیستم باید همواره اطلاعات کاملی از آخرین وصله‌های منتشر شده برای تمامی نرم‌افزارها و سخت‌افزارهای سیستم ICSمورد مدیریت خود به دست آورد.
- از تحلیل ریسک برای فهمیدن اینکه استفاده از یک وصله چه فواید و چه ضررهایی برای سیستم دارد استفاده کند.
- به‌کارگیری و تست آخرین وصله‌های امنیتی در محیط تست و سپس به‌کارگیری وصله‌ها در محیط واقعی

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

امن سازی دسترسی فیزیکی

- نگه‌داشتن تجهیزات و سرورهای سیستم‌های کنترل صنعتی در مکانی امن با استانداردهای لازم یکی از اولین اصول برای داشتن یک سامانه کنترل صنعتی امن است.
- امنیت فیزیکی از چند جهت باید مورد توجه قرار بگیرد. اول امنیت در برابر حوادث طبیعی و دوم امنیت در برابر دسترسی فیزیکی افراد غیرمجاز.

برخی از اصولی که برای حفظ امنیت سرورها و تجهیزات در برابر حوادث طبیعی و غیرعمدی ضروری است:

- در دسترس بودن تجهیزات یدکی که در صورت خرابی یک تجهیز بتوان از آن‌ها به‌عنوان پشتیبان استفاده نمود.

- نصب سنسورهای کنترل رطوبت و دما

امن سازی دسترسی فیزیکی

- نصب سیستم‌های تصفیه هوا
- استفاده از تجهیزات آتش‌نشانی و اعلام حریق مجهز به سنسورهای حساس به دود
- تجهیز به سیستم‌های کنترل برق که در هنگام تغییرات ولتاژ برق شهری، اقدام به توزیع یکنواخت و با ولتاژ ثابت برق به مرکز نماید.
- تجهیز به سیستم‌های پشتیبان برق که در صورت قطع برق شهری، به‌صورت آنی و خودکار به تأمین برق آن اقدام نموده و در مدت زمان طولانی هم بی‌وقفه، قادر به سرویس‌دهی باشد.
- چیدمان تجهیزات به‌گونه‌ای باشد که در مواقع لازم، امکان عبور از میان آن‌ها به‌آسانی صورت پذیرد.

امن سازی دسترسی فیزیکی

سیاست‌هایی که برای امنیتی فیزیکی سامانه در برابر افراد غیرمجاز باید رعایت شود، عبارت‌اند از:

- در سیاست‌های ورود به محل قرارگیری تجهیزات، باید مواردی چون سامانه‌های دزدگیر، تعداد و نوع کلیدها و دارندگان آن‌ها، زمان مجاز برای ورود هر شخص یا سازمان ازجمله افرادی که نظافت محل را بر عهده دارند، باید مشخص باشد.
- لازم است مشخص شود که مراجعان، مجاز به رفت‌وآمد در کدام بخش‌های سازمان هستند.
- تهیه‌ی فهرست تجهیزات موجود شامل شماره سریال و شرح فیزیکی وسایل، از مسائل مهمی است که در هنگام تدوین سیاست‌های امنیتی نباید نادیده گرفته شود.
- داشتن برنامه‌ای مشخص برای دور انداختن و از بین بردن کاغذهایی که دربرگیرنده‌ی اطلاعات مهم هستند نیز از ضروریات یک سیاست امنیتی است.

پیش‌بینی رویدادها و واکنش مناسب به رویدادها

یک سیستم کنترل صنعتی باید تا حد امکان رویدادهایی را که ممکن است در سیستم روی بدهد پیش‌بینی کند و واکنش مناسب را در هنگام رویداد نشان دهد.

رویه پیش‌بینی رویداد و واکنش مناسب شامل فعالیت‌های زیر است:

- تشخیص رویداد
- پاسخ به رویداد
- بازیابی سیستم پس از رویداد

پیش‌بینی رویدادها و واکنش مناسب به رویدادها

مهم‌ترین نکات برای به‌کارگیری یک برنامه مناسب برای واکنش به رویدادها در سیستم‌های کنترل صنعتی به‌صورت زیر است:

- تعریف یک برنامه در واکنش به حمله که در آن نقش هریک از کارکنان برای کنترل حمله مشخص باشد. به صورتی که هر فرد بداند هنگام رخ دادن یک حمله چه وظیفه‌ای دارد.
- مشخص کردن افرادی با عنوان مدیر حمله که در هنگام رخ دادن حمله تصمیم‌های کلیدی را اتخاذ کنند.
- گروهی از کارکنان باید رویدادهای غیرمتعارفی را که در سیستم رخ می‌دهد به گروه دیگری که مسئول تصمیم‌گیری هستند اطلاع دهند. نحوه اطلاع‌رسانی و مواردی که باید گزارش شوند باید از پیش تعریف شده و مدون باشد.
- پس از بازیابی سیستم باید گزارشی از تمامی آنچه در سیستم رخ داده شد، تدوین شود و در اختیار مدیران سیستم قرار بگیرد تا بر اساس این گزارش مشکلات و نواقص برنامه واکنش به رویداد مشخص و اصلاح شود.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

پشتیبان گیری و بازیابی سیستم پس از رویداد

- پس از یک رویداد و آسیب‌هایی که یک رویداد به یک سیستم می‌زند، سیستم باید بتواند به حالت قبلی خود بازگردد و کار خود را از سربگیرد.
- حذف تمامی اثراتی که رویداد روی سیستم گذاشته است و بازگرداندن داده‌های باارزشی که از بین رفته است بسیار مشکل است، مگر اینکه سیستم دارای یک سیستم پشتیبان باشد و اطلاعات باارزش خود را در سیستم پشتیبان نیز نگهداری کند.

مهم‌ترین نکات برای بازیابی یک سیستم آلوده پس از رخ دادن یک رویداد را می‌توان به‌صورت زیر خلاصه کرد:

- اطمینان حاصل شود که سیستم‌هایی که دارای اطلاعات و داده‌های باارزش هستند به‌صورت روزانه یا هفتگی پشتیبان گیری شوند.
- داده‌های روی سیستم پشتیبان تست و بازسازی شوند تا اطمینان حاصل شود که در مواقع لازم این داده‌ها قابل‌استفاده خواهند بود.
- سرورهای پشتیبان در مکان‌های امن فیزیکی محافظت شوند.
- اطلاعات پشتیبان به‌صورت رمزنگاری شده ذخیره شود.

آموزش اصول امنیتی-پدافندی به کاربران سیستم‌ها

- مدیران امنیت شبکه علاوه بر گذراندن دوره‌های اصلی امنیت شبکه، باید دوره‌های آموزشی مداومی را نیز داشته باشند تا همواره اطلاعات امنیتی خود را به‌روز کنند و از آخرین تغییرات، حملات و آخرین اطلاعات در شبکه‌ها اطلاع پیدا کنند.
- دوره‌های آموزش امنیت باید بر اساس سطح دسترسی کاربران به سیستم‌ها متفاوت باشد و مدیر سیستم باید همواره آخرین اطلاعات منتشر شده در زمینه امنیت را بر اساس نیاز کاربران سیستم در اختیار کاربران گذاشته و آن‌ها را موظف به مطالعه و به‌کارگیری اطلاعات کند.

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

به‌کارگیری مکانیسم‌های رمزنگاری

- هر ارتباط بین هر دو زیر سیستم در یک سیستم کنترل صنعتی باید به‌صورت رمز شده انجام شود.
- برخی از تجهیزات و پروتکل‌ها خود امکان رمزنگاری را دارند که فعال‌سازی این امکان در آن‌ها ضروری است
- تجهیزاتی که امکان رمزنگاری به‌صورت توکار ندارند باید با تجهیزات اضافی برای رمزنگاری مجهز شوند
- هر زیرسیستم ابتدا اطلاعات را رمز کرده و سپس به زیرسیستم دیگری ارسال کند.

امن سازی ارتباطات VSAT

مهم‌ترین نکات برای امن سازی ارتباطات VSAT:

- **پورت telnetدر این تجهیزات بسته شود و یا در صورت نیاز پورت پیش‌فرض با پورت امن دیگری نظیر sshجایگزین شود.**
- **تغییر گذرواژه‌های پیش‌فرض برای اتصال به VSATها اجباری باشد.**
- **امکان تعریف گذرواژه‌های ساده و قابل حدس برای اتصال به VSATها وجود نداشته باشد**

ملاحظات و الزامات سازمان پدافند غیرعامل کشور درخصوص امن سازی تجهیزات کنترل صنعتی

استفاده از سرورهای AAA

- افزایش تعداد سرورهای شبکه در پی راه‌اندازی سرویس‌های مختلف وجود پایگاه داده های مختلف با سیاست‌های متنوع و ... دسترسی‌های متنوعی برای هر فرد به منابع مختلف ایجاد خواهد کرد به‌طوری‌که پس از مدتی جهت اضافه کردن کاربر جدید به سیستم، نیاز به تعریف آن در چندین سرور وجود خواهد داشت.
- تعریف و پیاده‌سازی **AAA Server** یکی از تدبیرهاست که بر دسترسی کاربران به منابع شبکه به صورت متمرکز نظارت خواهد داشت.
- سرور **AAA** یک سرور است که امکان دسترسی کاربران را به منابع کامپیوتری شبکه فراهم می‌کند.
- این سرور، سرویس‌های **Authentication**، **Authorization** و **Accounting** را به‌صورت متمرکز فراهم می‌آورد و نتیجه استفاده از سرور **AAA** این است که سطح امنیت را در پروسه احراز هویت و کنترل دسترسی به‌صورت چشمگیری افزایش می‌دهد.

بازبینی کد برنامه

- بسیاری از مشکلات امنیتی در سیستم‌های کنترل صنعتی ناشی از سهل‌انگاری در تولید کد محصولات و عدم بازبینی کد برای بررسی نقاط آسیب‌پذیر آن است.
- برای بررسی آسیب‌پذیری‌های موجود در کد برنامه‌ها می‌توان از ابزارهای تحلیل کد استفاده کرد.
- این ابزارها معمولاً نمی‌توانند تمام آسیب‌پذیری‌های موجود را در کد کشف کنند؛ اما قادر به تشخیص برخی از آسیب‌پذیری‌های کد هستند.

اعتبارسنجی ورودی

- بررسی اعتبارسنجی داده‌ها از مهم‌ترین قسمت‌ها در بررسی کد محصولات کنترل صنعتی است.
- ورودی‌های غیر معتبر مانند اسکریپت‌ها، کاراکترهای غیرمجاز در پرس‌وجوهای SQL، نوع و اندازه‌ی غیر معتبر داده‌ها و ... در ورودی می‌توانند موجب حملاتی مانند سرریز بافر، تزریق SQL و Cross Site Scripting شده و دسترسی‌های غیرمجاز را فراهم آورند.
- اعتبارسنجی باید روی تمام ورودی‌ها انجام شود. هدرها، کوکی‌ها، پرس‌وجوها و کلیه‌ی مناطق ورود داده باید مورد اعتبارسنجی قرار گیرند. در این مکانیسم می‌بایست پارامترهایی که اولاً فرمت مطلوب را ندارند و ثانیاً در بازه‌ی قابل‌قبول (ازنظر طول، نوع و ...) نیستند، رد شوند.

رفع مشکل سرریز بافر

- سرریز بافر یکی از معمول‌ترین آسیب‌پذیری‌های امنیتی می‌باشد که هنگامی‌که اعتبارسنجی کافی روی اندازه‌ی داده‌های ورودی انجام نگرفته باشد، رخ می‌دهد. از این شکاف می‌توان برای جایگزینی محتوای حافظه استفاده کرد.
- هنگامی‌که داده نوشته‌شده در بافر بیش از طول بافر باشد، داده‌ی اضافی در فضای حافظه همسایه ریخته می‌شود.
- توسط حمله‌ی سرریز بافر، این فضای حافظه می‌تواند جایگزین شده و درنتیجه پروسه در حال اجرا کنترل اجرایی خود را از دست می‌دهد.
- نفوذگر می‌تواند از موقعیت سرریز بافر برای اجرای دستورات مختلف استفاده کند. بدین ترتیب که با حمله‌ی سرریز بافر، نفوذگر می‌تواند آدرس کد خود را در حافظه جایگزین کند و درنتیجه بعد از اتمام اجرای برنامه‌ی جاری، کد نفوذگر اجرا خواهد شد.
- تمام فیلدهای ورودی باید حدود مشخصی ازنظر طول و نوع داده‌ی ورودی داشته باشند. برنامه‌ی کاربردی باید طوری طراحی شده باشد که با توجه به محدوده‌ی آرایه‌ها و بافرها در هر دسترسی، مقداری متجاوز از حدود آن‌ها را وارد نکند.

رفع آسیب‌پذیری XSS

- آسیب‌پذیری cross site scripting هنگامی رخ می‌دهد که نفوذگر از یک web application برای ارسال کدی خطرناک به شکل یک اسکریپت به کاربری دیگر استفاده می‌کند.
- نفوذگر از XSS برای ارسال اسکریپت مخرب، به یک کاربر قابل اعتماد استفاده می‌کند.
- . برای جلوگیری از XSS باید از ورودی کاربر به شکل HTML جلوگیری کرد و یا حداقل تنها اجازه‌ی استفاده از tagها و کاراکترهای ویژه‌ای را داد و کاراکترهای زیر را از ورودی حذف کرد: <، >، (،)، #، &

رفع آسیب‌پذیری تزریق SQL

- در سیستم‌های کنترل صنعتی که از پایگاه داده استفاده می‌شود، آسیب‌پذیری تزریق SQL می‌تواند بسیار خطرساز باشد.
- نقطه آسیب‌پذیر در این سیستم‌ها آنجاست که تولید پرس‌وجو به‌صورت پویا، از داده‌هایی که وارد می‌کند ساخته شود و یک نفوذگر حرفه‌ای که با زبان SQL آشناست، می‌تواند محتویات این فیلدها را با دستورات SQL دلخواهش پر کند و باعث ایجاد دسترسی‌های خطرناکی به اطلاعات موجود در بانک شود.
- قبول کاراکترهای غیرمجاز در پرس‌وجوهای SQL مشکلی است که به‌واسطه‌ی آن، پرس‌وجوها در داده‌های ورودی جاسازی شده و دستوراتی جعلی را در پایگاه داده‌ها اجرا می‌کنند.
- برای جلوگیری از این حمله ورودی‌هایی که با استفاده از آن‌ها پرس‌وجویی به پایگاه داده ساخته می‌شود باید به خوبی اعتبارسنجی شود و کاراکترهای مخرب مانند ' ; - -- حذف شوند.

ضرورت بومی سازی صنعت سایبری

به ویژه سامانه های پایه و اساسی

سایبری

ضرورت بومی سازی صنعت سایبری به ویژه سامانه های پایه و اساسی سایبری

- در شرایطی که قراردادهای بین المللی با شرکتهای فناوری خارجی به شدت تحت تاثیر مسائل سیاسی روز قرار دارند و اینگونه تکنولوژی‌ها اصولاً در اختیار آمریکا و چند کشور اروپایی قرار دارند، انعقاد قرارداد خرید سامانه های امنیت سایبری بصورت مستقیم یا غیر مستقیم از آن‌ها اساساً نادرست بوده و در کل به صلاح امنیت ملی کشور نیست.

- صنعت تولید و توسعه نرم‌افزارهای بزرگ سازمانی در اختیار شرکت‌هایی است که بطور کلی یا جزیی در کشورهای پیشرفته و ذاتاً استعمارگر قرار دارند و از آنجاییکه این کشورها عموماً دارای مواضع خصمانه پنهان و آشکار سیاسی و اقتصادی بر علیه کشورهای مستقل و یا در حال ترقی هستند، بنابراین خریداری فناوری سیستم‌های امنیتی از چنین مراجعی بهترین فرصت را برای نفوذ و نظارت بر سیستم‌های اطلاعاتی سازمانهای داخلی کشورها در اختیار متخاصمان قرار می‌دهد.

ضرورت بومی سازی صنعت سایبری به ویژه سامانه های پایه و اساسی سایبری

- فناوری تولید و روشهای شناسایی الگوها و قابلیت‌های فنی یک سامانه امنیت شبکه تجهیزات مورد استفاده در زیرساختهای حیاتی و حساس در شناسایی و مقابله با حملات پیچیده، خود یکی از پارامترهایی است که باید اکیداً مخفی و محرمانه نگاه داشته شود.

- هرچند سامانه های امنیتی و دفاعی امکان افزودن تشخیص الگوهای متفاوتی از حملات توسط مدیران سیستم را مهیا می‌نماید ولی با توجه به پیشرفت‌های روز افزون فن‌آوری اطلاعات و کشف خلل و کاستی‌های امنیتی، در طول زمان بهره برداری می‌بایست امکان اعمال تغییرات، به‌روز آوری و افزودن امکانات جدید مهیا باشد.

ضرورت بومی سازی صنعت سایبری به ویژه سامانه های پایه و اساسی سایبری

- آشنایی شرکت‌های تولید کننده و متخصصین آن‌ها به فن‌آوری ساخت یک نرم‌افزار امنیتی یا زیرساختی در شرایط خاص بین‌المللی یا بروز بحران می‌تواند انگیزه لازم برای همکاری این شرکت‌ها یا متخصصین آن‌ها با دولت‌ها را به منظور نفوذ به سیستم‌های اطلاعاتی مصرف کننده ایجاد کند.

- در شرایطی که روش کار و استراتژی‌های محصولات خارجی عموماً شناسایی شده‌اند، یک سازمان یا کشور متخاصم بسادگی می‌تواند با خرید سامانه امنیتی یا زیرساختی مشابه در شرایط آزمایشگاهی روش حمله به کشور را تجربه نماید. لذا هیچ محصولی همانند یک محصول تولید داخل نمی‌تواند بصورت دقیق ناظر بر استفاده از مجموعه اطلاعات موجود در سیستم‌های اطلاعاتی و شبکه‌های داخلی کشور باشد.

ضرورت بومی سازی صنعت سایبری به ویژه سامانه های پایه و اساسی سایبری

- تقریباً تمام شرکت‌های بزرگ خدمات اینترنتی مانند Google، Yahoo، ...و نیز آن‌ها که به تولید تجهیزات امنیت اطلاعات در رده سازمانی می‌پردازند، متعهد به ارائه سرویس‌های خاص اطلاعاتی به سازمانها و سرویس‌های امنیتی کشورهای متبوع خود هستند.

- یک سامانه امنیتی یا زیرساختی تولید داخل از قابلیت سفارش‌سازی و تطبیق رفتاری کامل با نیازهای مشتری برخوردار است و امکان بهینه سازی و توسعه مداوم بر اساس نیازهای مشتری بومی را دارد.

ضرورت بومی سازی صنعت سایبری به ویژه سامانه های پایه و اساسی سایبری

- هزینه خرید، نگهداری، آموزش استفاده، اعمال تغییرات، رفع مشکلات و از همه مهمتر دردسترس بودن کد برنامه و حصول اطمینان از نداشتن راه‌های نفوذ مخفی در نرم‌افزار از جمله مهمترین دلایلی است که تهیه یک محصول داخلی را بر نسخه خارجی ارجح می‌کند.

- پیچیدگی فن‌آوری سامانه های امنیتی بستری مناسب برای تعبیه راه‌های نفوذ پنهانی و سیستمهای جاسوسی اطلاعات است. به بیان دیگر فروش این‌گونه سیستم‌ها حتی بصورت غیر مستقیم و با واسطه به کشورهایی مانند ایران، از جمله آرزوهای بسیار بزرگ کشورهای صاحب این فن‌آوری برای دست‌یابی به اطلاعاتی از شبکه‌های دیگر کشورها است.

آزمایشگاه و مراکز ارزیابی امنیتی-پدافندی محصولات سایبری

- استخراج شاخص های ارزیابی و رتبه بندی آزمایشگاهها در چهار حوزه نرم افزار، سخت افزار، شبکه و تجهیزات شبکه، الگوریتم و پروتکل Lab evaluation_Software.xlsx Lab_evaluation_HARDWARE.xlsx
- استخراج شاخص های ارزیابی پدافندی محصولات سایبری (سامانه مدیریت اطلاعات و رخدادهای امنیتی، دیواره آتش، دیواره آتش نسل بعدی، دیواره آتش لایه برنامه های کاربردی، مدیریت یکپارچه تهدیدات، سامانه تشخیص/جلوگیری از نفوذ) IPS IDS.xlsx-SOC Evaluation.xlsx
- ساماندهی و رتبه بندی آزمایشگاه ها و مراکز ارزیابی امنیتی سایبری کشور

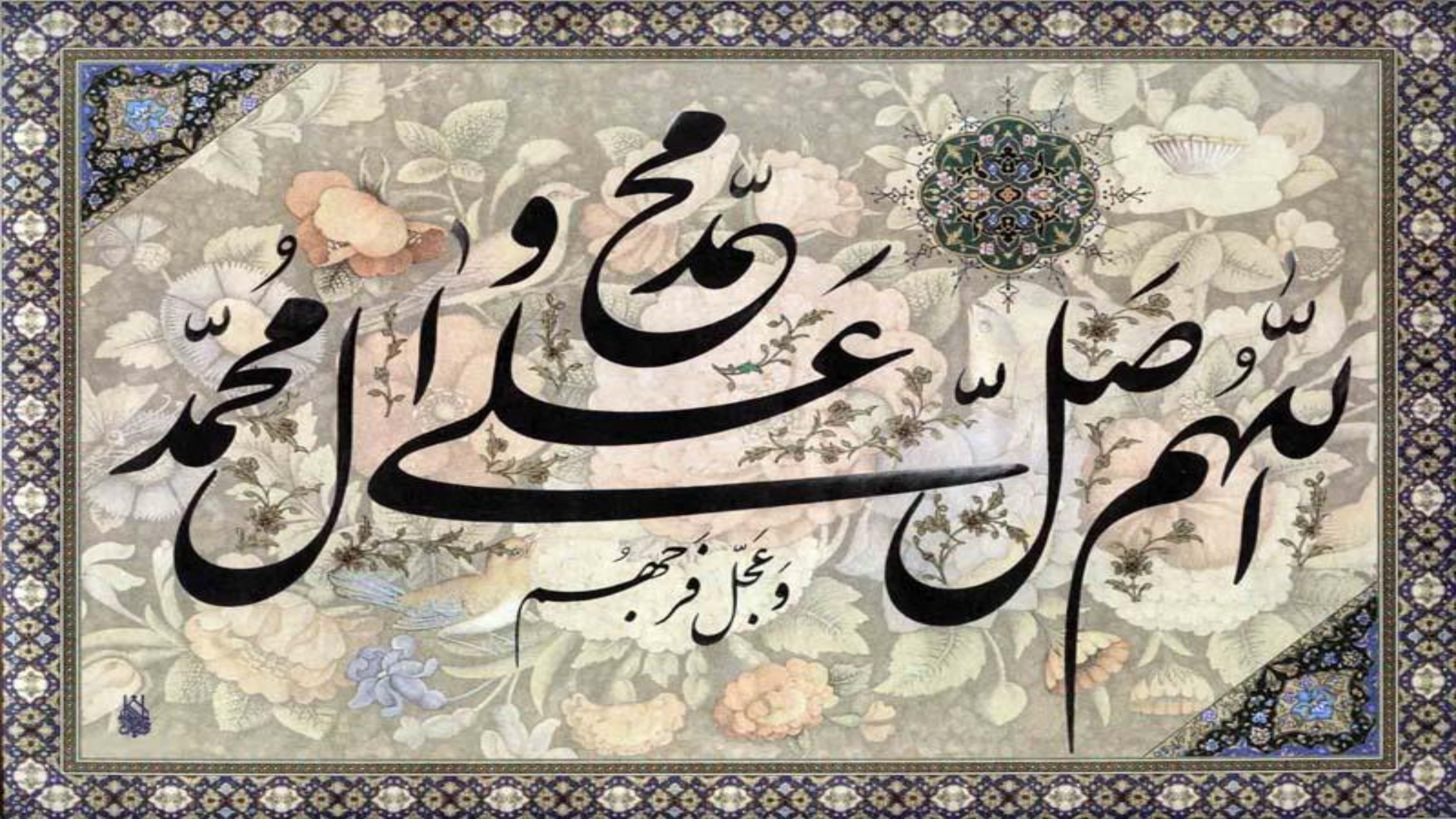
Nitro Zeus

پروژه نیترو زئوس

- یک مستند جدید با نام Zero Days، برای اولین بار در فستیوال فیلم برلین به نمایش درآمد.
- این مستند توسط آلکس گیبنی ساخته شده و تلاش‌های مشترک آمریکا و اسراییل برای طراحی خرابکاری در ایران را افشا می‌کند.
- پروژه کاملا عملیاتی با هدف فلج کردن و از کار انداختن برخی از زیرساخت های حیاتی در ایران

پروژه نیترو زئوس

- بد افزاری نظیر استاکس نت، تنها بخش کوچکی از این پروژه بزرگ بوده است.
- پروژه Nitro Zeus البته ریشه های خود را در دولت بوش دارد، ولی به شکل کامل در سال ۲۰۰۹ و ۲۰۱۰ به تکامل رسیده است.
- این برنامه یک تلاش ۷ ساله، زیر نظر فرماندهی امنیت سایبری(Cyber Command)و سازمان امنیت ملی NAS آمریکا، بود.
- طرحی را برای مقابله با ایران در صورت شکست خوردن مذاکرات


اللهم صل علی محمد و آل محمد
و عجل فرجهم

قرارگاه پدافند سایبری کشور

سازمان پدافند غیر عامل کشور

اسناد و طرح های قرارگاه

پدافند سایبری کشور

هادی کریمی نیسیانی

معاونت فنی قرارگاه پدافند سایبری کشور

بسم الله الرحمن الرحیم

اگر مدیران کشور اهمیت این مسئله را درک نکنند و پدافند غیرعامل به طور شایسته توسعه پیدا نکند، کشور در معرض تهدیدهای بعضاً غیرقابل جبران قرار خواهد گرفت، بنابراین مسئولان بخش‌های مختلف کشور چه بخشهای نظامی و چه بخشهای غیرنظامی، باید با پدافند غیرعامل همکاری کامل و لازم انجام دهند.

بیانات رهبر معظم انقلاب اسلامی

در دیدار رئیس و مسئولان سازمان پدافند غیرعامل کشور

اسناد و طرح های سازمان پدافند غیر عامل - قرارگاه پدافند سایبری کشور جهت کاهش آسیب پذیری ها و امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر کشور

طرح های شش گانه پدافند سایبری

- پاسخ به شرایط اضطراری سایبری (CERP)
- امن سازی اضطراری سایبری
- مصون سازی سایبری
- طرح تداوم فعالیت های ضروری زیرساخت (BCP)
- طرح بازیابی از حوادث و حملات سایبری (DRP)
- طرح رزمایش سایبری

طرح های سازمان پدافند غیرعامل کشور- قرارگاه پدافند سایبری کشور

- **طرح پاسخ اضطراری سایبری (CERP) (حوزه بانکی، حوزه انرژی، حوزه ارتباطات، حوزه حمل و نقل)**
- **طرح امن سازی اضطراری**
- **طرح مصون سازی زیرساخت های سایبری و وابسته به سایبر کشور**

طرح های سازمان پدافند غیرعامل کشور- قرارگاه پدافند سایبری کشور

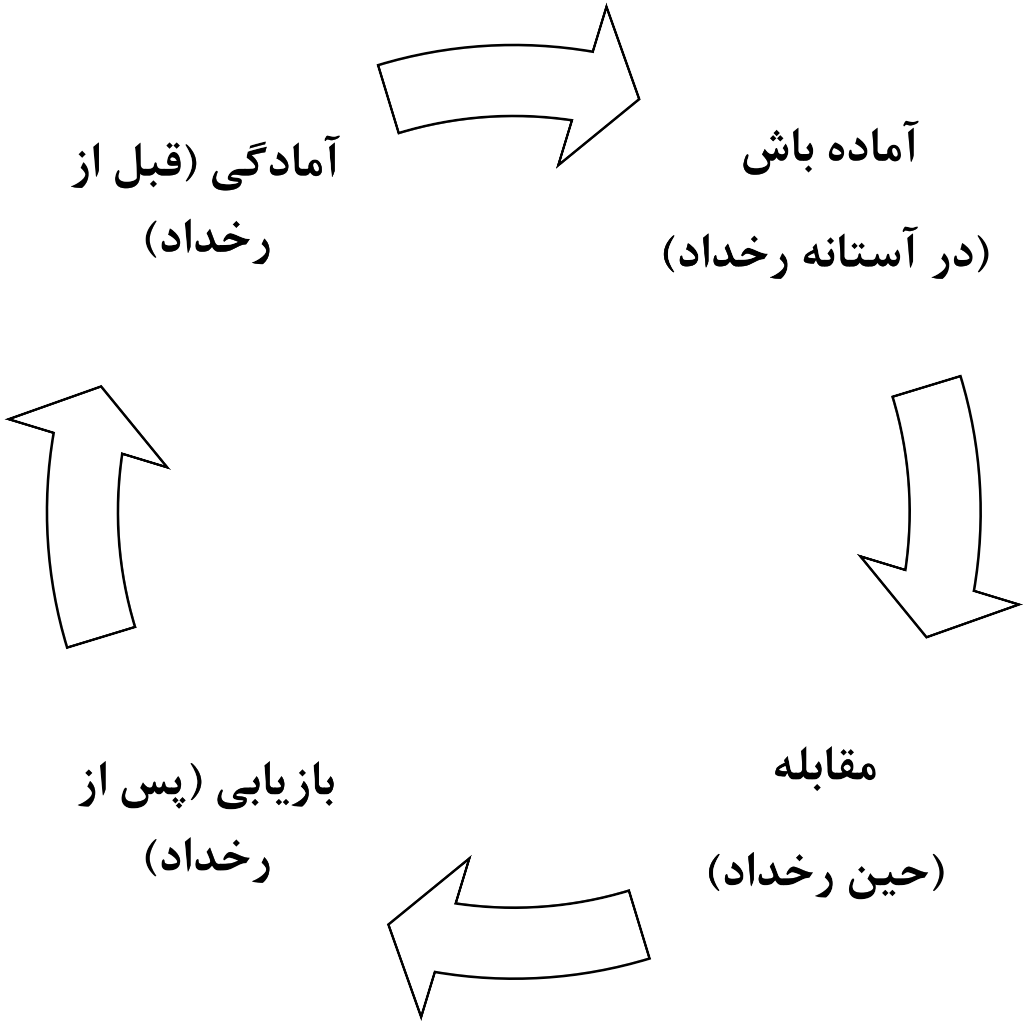
- **طرح تداوم فعالیت های ضروری زیرساخت (BCP)**
- **طرح پشتیبان گیری و بازیابی از فاجعه (DRP)**
- **طرح کنترل آمادگی ها و رزمایش**

طرح های پاسخ به شرایط اضطراری در حوزه سایبری (CERP)

- پاسخ به شرایط اضطراری سایبری در حوزه **انرژی**
- پاسخ به شرایط اضطراری سایبری در حوزه **حمل و نقل**
- پاسخ به شرایط اضطراری سایبری در حوزه **بانکی**
- پاسخ به شرایط اضطراری سایبری در حوزه **حمل و نقل شهری**

طرح پاسخ اضطراری سایبری (CERP)

چارچوب و الگوی طرح پاسخ اضطراری به تهدیدات سایبری



اقدامات اجرایی مراحل طرح پاسخ به شرایط اضطراری سایبری

مرحله آمادگی (قبل از رخداد)

هدف اصلی از این پاسخ آن است که حملات سایبری احتمالی به زیرساخت ها، تاثیر خاصی بر عملکرد طبیعی آن و نحوه خدمت رسانی مستمر و پایدار نداشته باشد و بتوان در کمترین زمان، منشا حمله را شناسایی و از ورود خسارت جلوگیری شود. در این مرحله بایستی از **قابلیت آماده سازی** برای مواجه شدن با شرایط اضطراری سایبری برخوردار بوده و بتوان قبل از وقوع رخداد، **امن سازی اضطراری** صورت پذیرفته و با بهره گیری از **رصد و پایش و تشخیص** در سریع ترین زمان ممکن، شناسایی حملات سایبری انجام شود.

اقدامات اجرایی مراحل طرح پاسخ به شرایط اضطراری سایبری

مرحله آماده باش (در آستانه رخداد)

هدف از این مرحله، تشدید آمادگی های لازم، هشدار به زیرمجموعه ها، ابلاغ آماده باش رسمی به عوامل مدیریت بحران در مرکز داده و سایر مراکز تابعه برای مواجهه با حملات سایبری متناسب با تعیین وضعیت سایبری است. در این فاز، تمام اقدامات مرحله قبل بایستی صورت گرفته باشد و مدیران و کارشناسان بایستی برای مواجهه با حمله سایبری در آمادگی کامل باشند

اقدامات اجرایی مراحل طرح پاسخ به شرایط اضطراری سایبری

مرحله مقابله (حین رخداد)

هدف اصلی در این مرحله، مدیریت صحنه عملیاتی، خنثی سازی تهاجم، انسداد و انحراف مسیرهای تهاجم، کاهش صدمات و خسارات ناشی از تهاجم سایبری، جلوگیری از گسترش دامنه حملات به بخش‌های دیگر، تعیین منشا حمله و مشخصات مهاجم است.

اقدامات اجرایی مراحل طرح پاسخ به شرایط اضطراری سایبری

مرحله بازیابی (پس از رخداد)

پس از وقوع حمله سایبری باید اقدامات لازم برای بازیابی شرایط عادی و تداوم کسب وکار، به سرعت اجرایی شود و زمان از دسترس خارج شدن، به حداقل ممکن کاهش یابد. مدیریت رخداد سایبری، کاهش خسارات ناشی از حمله و پرهیز از پیامدهای فاجعه‌بار در این مرحله انجام می شود.

طرح امن سازی اضطراری

امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

سازمان پدافند غیرعامل کشور

اقدامات امن سازی اضطراری

زیرساخت های سایبری و وابسته به سایبر کشور

قرارگاه پدافند سایبری کشور

دی ماه ۱۳۹۷

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

۱. بررسی و شناخت گلوگاه های زیرساخت های سایبری و وابسته به سایبر و تهیه فهرست کاملی از آنها

۲. دسته بندی، اولویت بندی گلوگاه های شناسایی شده به دسته های قابل رسیدگی در اسرع زمان، قابل رسیدگی در میان مدت (حداکثر یک ماه)، قابل رسیدگی در بلند مدت (تا شش ماه)، قابل رسیدگی در زمان های طولانی تر و گلوگاه های غیرقابل رفع ولی قابل مدیریت.

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

۳. گزارش اقدامات انجام شده به مدیریت زیرساخت و دستگاه متولی

۴. گزارش اقدامات انجام شده به مبادی ذیربط

۵. انجام بازرسی های اضطراری غیرمترقبه و درصورت نیاز بازنگری معماری امنیتی و پدافندی زیرساخت در تمام سطوح اعم از سطح کاربری، سطح شبکه، سطح ارتباطات بر اساس معماری امن و لایه به لایه مبتنی بر دفاع در عمق

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

۶. عدم اتصال شبکه کنترل صنعتی در هر سطح و به هر میزانی به شبکه اینترانت اداری و شبکه اینترنت

۷. تشدید کنترل دسترسی شرکت های پیمانکار

۸. قطع دسترسی از راه دور (خارج از کشور) به زیرساخت های حیاتی و حساس و انجام فرایندهای تعمیر، نگهداری و به روز رسانی بصورت محلی و غیربرخط و اکتفا به مشاوره حداقلی با پیمانکار خارجی

۹. برگزاری تمرین و رزمایش به منظور حصول اطمینان از حل مشکل گلوگاه ها

۱۰. گزارش اقدامات انجام شده در رزمایش به مبادی ذیربط

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

طرح تداوم فعالیت های ضروری زیرساخت

۱. تهیه، تدوین و اجرای طرح تداوم فعالیت های ضروری زیرساخت

۲. تهیه، تدوین و اجرای طرح بازیابی پس از حادثه

۳. برگزاری رزمایش جهت تمرین کارآمدی طرح تداوم فعالیت های ضروری و طرح بازیابی پس از حادثه

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

ایجاد، تقویت و ارتقای سامانه رصد، پایش، تشخیص و هشدار تهدیدات و حملات سایبری در دو سطح سیستمهای کنترل صنعتی و سامانه های فناوری اطلاعات و ارتباطات جهت مانیتورینگ ۲۴*۷

اقدامات امن سازی اضطراری زیرساخت های سایبری و وابسته به سایبر

۵. ملاحظات حفاظتی، امنیتی و آموزشی نیروی انسانی

۱. بازنگری در اجرای کامل دستورالعمل حفاظتی و امنیتی کارکنان شاغل (نظیر اصول حیطه بندی، طبقه بندی و ...) و حصول اطمینان از اجرای کامل

۲. افزودن سامانه های احراز هویت دو یا چند مرحله ای نظیر سامانه های بیومتریک برای تردد و دسترسی کارکنان به نقاط کلیدی زیرساخت

۳. تهیه و اجرای طرح پالایش نیروی انسانی

۴. حراست دستگاه با توجه به افزایش تهدیدات، کنترل مضاعف در صلاحیت ها و دسترسی های نیروی انسانی را مورد توجه جدی قرار دهد.

۵. بازنگری در طرح ها و تشدید کنترل های حفاظت فیزیکی مراکز و زیرساخت های حیاتی و حساس

الزامات و ملاحظات پدافند سایبری برای امن سازی اضطراری سامانه های سایبری

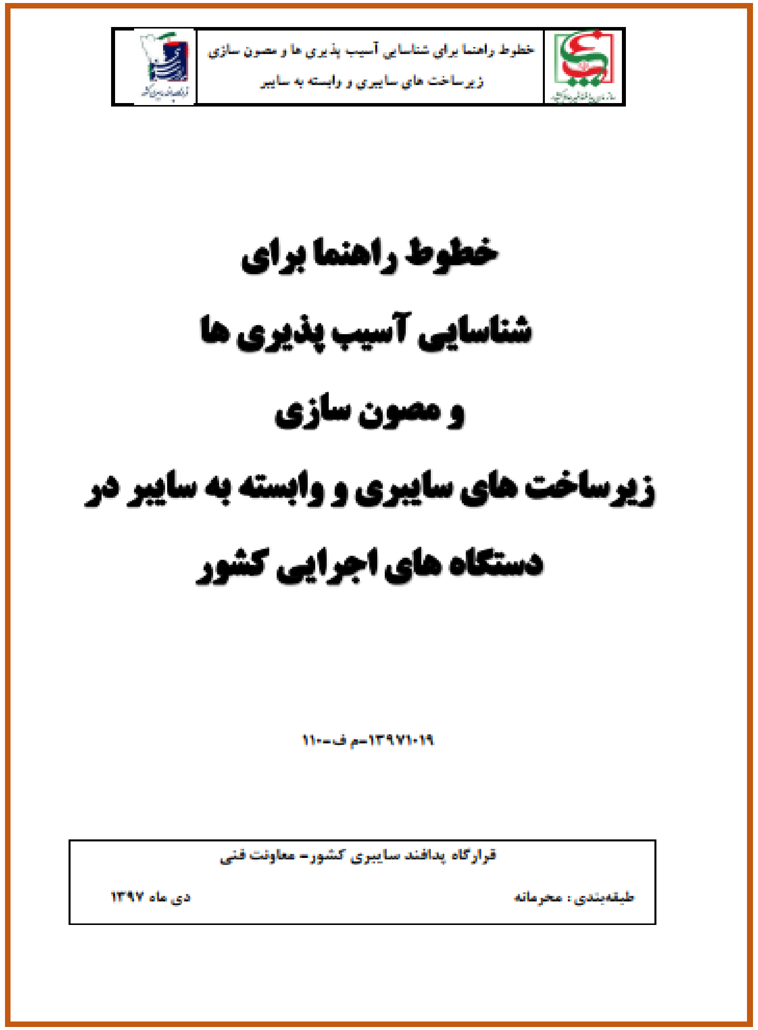
- امن سازی سیستم عامل CentOS
- امن سازی سیستم عامل Ubuntu
- امن سازی سیستم عامل ویندوز سرور

الزامات و ملاحظات پدافند سایبری برای امن سازی اضطراری سامانه های سایبری

- آسیب پذیری های سوویچ ها و روترهای سیسکو و Huawei
- امن سازی اضطراری سوییچ ها و روترهای سیسکو و Huawei
- امن سازی اضطراری پروتکل OPC

خطوط راهنما برای شناسایی آسیب پذیری ها و مصون سازی زیرساخت های سایبری و وابسته به سایبر

خطوط راهنما برای شناسایی آسیب پذیری ها و مصون سازی زیرساخت های سایبری و وابسته به سایبر



خطوط راهنما برای شناسایی آسیب پذیری ها و مصون سازی
زیرساخت های سایبری و وابسته به سایبر

خطوط راهنما برای
شناسایی آسیب پذیری ها
و مصون سازی
زیرساخت های سایبری و وابسته به سایبر در
دستگاه های اجرایی کشور

۱۳۹۷۱۰۱۹-م ف-۱۱۰۰

قرارگاه پدافند سایبری کشور- معاونت فنی

طبقه‌بندی : محرمانه

دی ماه ۱۳۹۷

اسناد بالادستی برای اجرای ماموریت

بند ب–۴ از ماده ۱۰ اساسنامه مصوب سازمان پدافند غیرعامل

بند پ ماده ۱۰۷ قانون برنامه ششم توسعه

بند ۲–۵۳ سیاست های کلی نظام در برنامه ششم توسعه

بند پ ماده ۱۰۶ قانون برنامه ششم توسعه

ماده ۱۰۹ قانون برنامه ششم توسعه

دسته بندی آسیب پذیری ها و راهکارهای اجرایی

آسیب پذیری هایی که رفع و یا حذف آنها نیاز به تغییرات قابل توجه در زیرساخت مربوطه دارد

- طرح های مصون سازی تفصیلی میان مدت

آسیب پذیری هایی که برای رفع آنها نیاز به برنامه و طرح مناسب می باشد

- اجرای برنامه کوتاه مدت برای امن سازی

آسیب پذیری هایی که می توان در حداقل زمان ممکن، مرتفع نمود (فوریتی)

- امن سازی اضطراری

اقدامات پیشنهادی

گام صفر : سازماندهی و آموزش تیم های اجرایی

گام اول: شناسایی، ارزش گذاری و اولویت بندی دارایی ها

گام دوم : استخراج تهدیدات و آسیب پذیری های سایبری

گام سوم : تعیین مخاطرات سایبری و پیامدسنجی مخاطرات

اقدامات پیشنهادی

گام چهارم : تدوین راهکارهای پدافند سایبری جهت مصون سازی مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر مطابق با معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

گام پنجم: تدوین راهکارهای کاهش اثرات یا مقابله با حملات سایبری

گام ششم: سنجش میزان آمادگی زیرساخت های حیاتی و حساس در برابر حملات سایبری

اقدامات پیشنهادی

گام صفر : سازماندهی و آموزش تیم های اجرایی

تشکیل تیم و سازماندهی تیم ها یا نخبه و خبره برای بررسی و کشف آسیب پذیری

برگزاری آموزش های ارتقاء توانمندی های سایبری و پدافند سایبری با دوره های طولی و عرضی برای کارشناسان و مدیران زیرساختهای سایبری و وابسته به سایبر در سطوح مختلف

اقدامات پیشنهادی

گام اول: شناسایی، ارزش گذاری و اولویت بندی دارایی ها

شناسایی دارایی ها، مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر

تعیین سطح اهمیت دارایی ها، مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر به سطوح ویژه، حیاتی، حساس، مهم و فاقد طبقه بندی

اقدامات پیشنهادی

گام دوم : استخراج تهدیدات و آسیب پذیری های سایبری

- احصای تهدیدات سایبری مترتب در مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر ترسیم بردار تهدیدات
- تدوین سناریوی تهدید پایه و سناریوهای تهدیدات محتمل
- شناسایی آسیب پذیری های سایبری مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- ترسیم ماتریس تهدید–آسیب پذیری–دارایی برای بررسی برهم کنش تهدیدات و آسیب پذیریها بر روی دارایی ها و تحلیل برهم کنش تهدیدات–آسیب پذیری ها

اقدامات پیشنهادی

گام سوم : تعیین مخاطرات سایبری و پیامدسنجی مخاطرات

تعیین مخاطرات سایبری (اعمال تهدیدات بر آسیب پذیری ها)

پیامدسنجی مخاطرات و وزن دهی به هر یک و تقسیم نمودن پیامدها به سه سطح اولیه، ثانویه و نهایی

محاسبه مخاطره و تعیین خطر قابل قبول

اقدامات پیشنهادی

تدوین راهکارهای پدافند سایبری جهت مصون سازی مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر مطابق با معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

گام چهارم : تدوین راهکارهای پدافند سایبری جهت مصون سازی مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر مطابق با معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق

اجرای راهکارهای پدافند سایبری جهت مصون سازی مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر و نظارت بر حسن انجام کار

اقدامات پیشنهادی

گام پنجم: تدوین راهکارهای کاهش اثرات یا مقابله با حملات سایبری

تدوین راهکارهای مقابله با حملات (تهیه دستورالعمل های مدیریتی امنیت و پدافند سایبری، تعریف فرایندهای کاری قبل، در آستانه، حین و پس از حادثه، تشکیل تیم CSIRT و ...) و نظارت بر حسن انجام کار

تدوین طرح تداوم خدمات و فعالیت های ضروری (BCP) در صورت بروز بحران سایبری و اجرای طرح

اقدامات پیشنهادی

گام ششم: سنجش میزان آمادگی زیرساخت های حیاتی و حساس در برابر حملات سایبری

برگزاری ارزیابی های امنیتی، تست نفوذ، تمرین و رزمایش های سایبری به منظور سنجش میزان آمادگی زیرساخت برای مواجه با رخدادها و حملات سایبری

به روز رسانی راه کارهای پدافند سایبری با توجه به تهدیدات و آسیب پذیری های جدید

الزامات و ملاحظات پدافند سایبری در پروژه های کشوری و فناوری های نوین

1. الزامات و ملاحظات پدافند سایبری در پروژه انتخابات الکترونیک
2. الزامات و ملاحظات پدافند سایبری در پروژه دیسپچینگ ملی برق کشور
3. الزامات و ملاحظات پدافند سایبری در پروژه شبکه ملی هوشمند برق

الزامات و ملاحظات پدافند سایبری در پروژه های کشوری و فناوری های نوین

4. الزامات و ملاحظات پدافند سایبری در پروژه مانیتورینگ ایستگاه های راه دور گاز
5. الزامات و ملاحظات پدافند غیرعامل برای پروژه رسانه تعاملی فراگیر در سازمان صداوسیما (IPTV)
6. الزامات و ملاحظات پدافند سایبری در پروژه طرح فهام

الزامات و ملاحظات پدافند سایبری در پروژه های کشوری و فناوری های نوین

7. الزامات و ملاحظات پدافند سایبری در پروژه امن سازی پروتکل کنترل صنعتی IEC60870-5-104

8. الزامات و ملاحظات پدافند سایبری در پروژه امن سازی پروتکل کنترل صنعتی OPC

9. الزامات و ملاحظات پدافند سایبری در پروژه بومی سازی پروتکل های کنترل صنعتی

الزامات و ملاحظات پدافند سایبری در پروژه های کشوری و فناوری های نوین

10. الزامات و ملاحظات پدافند سایبری برای ارائه دهندگان راه حل های امنیتی مدیریت شده (MSSP)

11. الزامات و ملاحظات پدافند سایبری در رایانش ابری و امنیت آن در سطح ملی

12. الزامات و ملاحظات پدافند سایبری در سیستم عامل های ویندوز و لینوکس در سطح ملی

الزامات و ملاحظات پدافند سایبری در پروژه های کشوری و فناوری های نوین

13. الزامات و ملاحظات پدافند سایبری در امن سازی سوویچ ها و روترهای پرظرفیت سیسکو و Huawei

14. شناسایی برخی از ایمپلنت ها در تجهیزات سیسکو و Huawei

الزامات و ملاحظات پدافند سایبری برای امن سازی اضطراری سامانه های سایبری

- آسیب پذیری های سوویچ ها و روترهای سیسکو و Huawei
- امن سازی اضطراری سوییچ ها و روترهای سیسکو و Huawei
- امن سازی اضطراری پروتکل OPC

نظام عملیاتی پدافند سایبری

محدوده زمانی عملیات پدافند سایبری

«پیش از جنگ سایبری»

«در آستانه‌ی جنگ سایبری»

«حین جنگ سایبری»

«پس از جنگ سایبری»

سطوح عملیات پدافند سایبری

ملی

حوزه‌ای

زیرساختی

رویکردهای عملیات پدافند سایبری

«پیش‌گیرانه»

«پیش‌کنش‌گرانه»

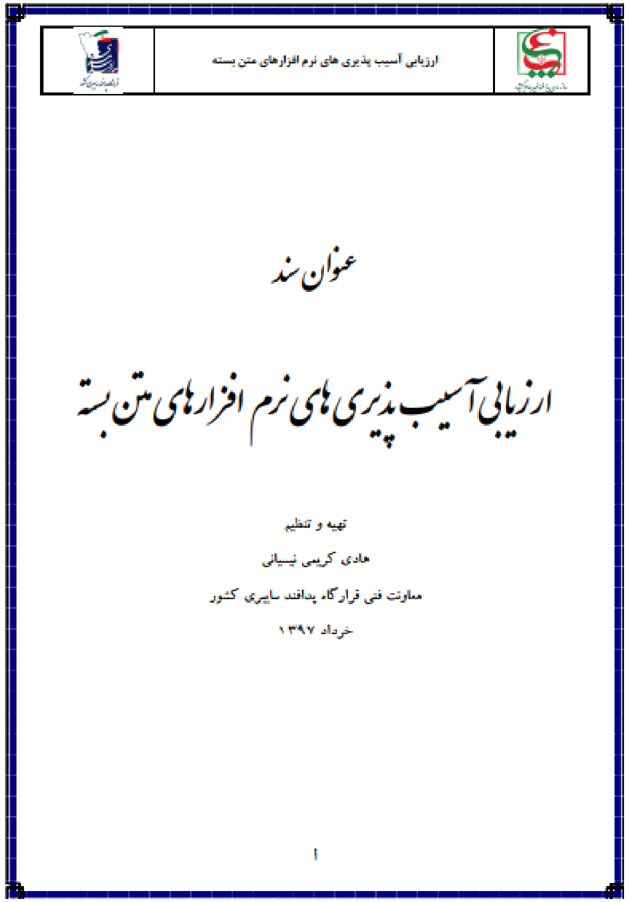
«واکنش‌گرایانه»

«منفعلانه»


انرژی
ارتباطات و
فضای سایبری
کشور
حمل و نقل
پولی و
مالی
سلامت
شهری
سامانه های
ملی
نظام عملیاتی
پدافند
سایبری

۵- طرح ها و پروژه های مصون سازی زیرساخت های سایبری و وابسته به سایبر

2. ارزیابی آسیب پذیری های نرم افزارهای مورد استفاده در زیرساخت های کشور



ارزیابی آسیب پذیری های نرم افزارهای متن بسته

عنوان سند

ارزیابی آسیب پذیری های نرم افزارهای متن بسته

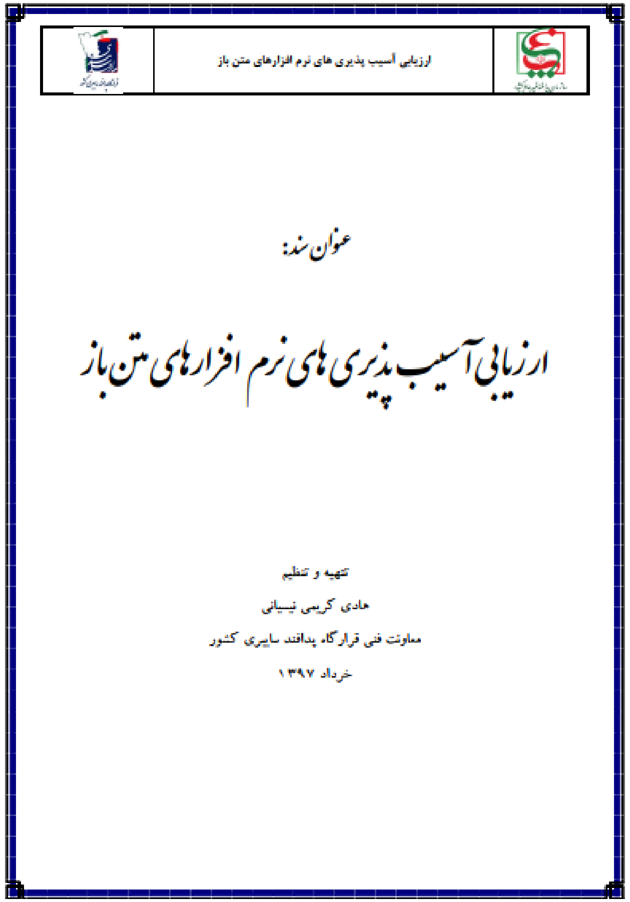
تهیه و تنظیم

هادی کریمی نیسیانی

معاونت فنی قرارگاه پدافند سایبری کشور

خرداد ۱۳۹۷

أ



ارزیابی آسیب پذیری های نرم افزارهای متن باز

عنوان سند:

ارزیابی آسیب پذیری های نرم افزارهای متن باز

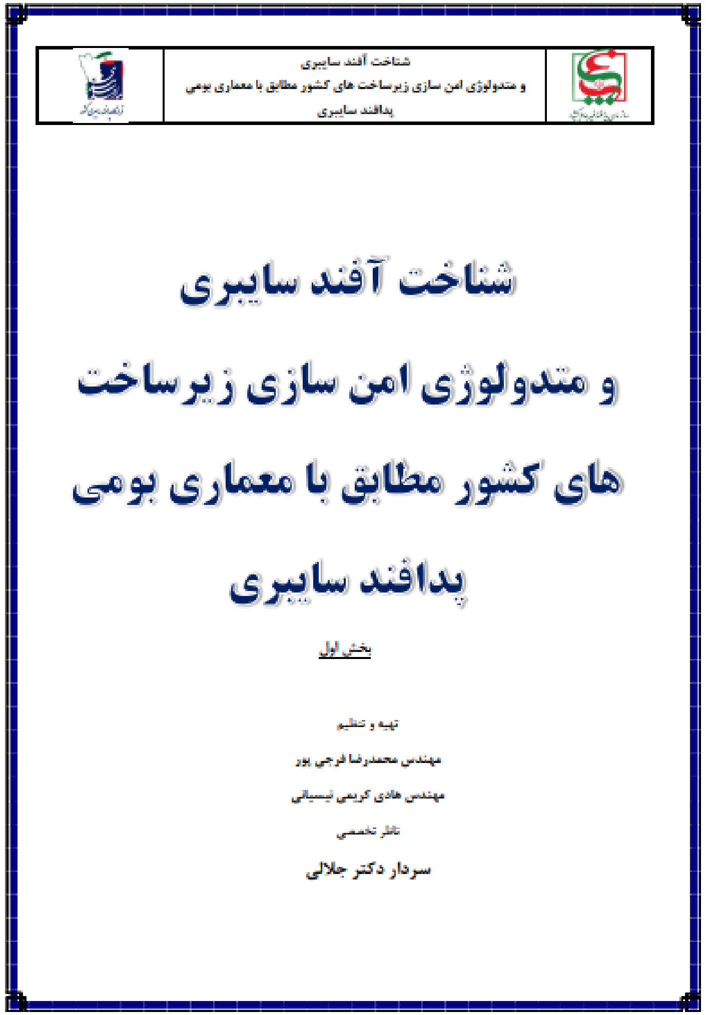
تهیه و تنظیم

هادی کریمی نیسیانی

معاونت فنی قرارگاه پدافند سایبری کشور

خرداد ۱۳۹۷

۵– طرح ها و پروژه های مصون سازی زیرساخت های سایبری و وابسته به سایبر



شناخت آفند سایبری
و متدولوژی امن سازی زیرساخت های کشور مطابق با معماری بومی
پدافند سایبری

شناخت آفند سایبری

و متدولوژی امن سازی زیرساخت

های کشور مطابق با معماری بومی

پدافند سایبری

بخش اول

تهیه و تنظیم

مهندس محمدرضا فرجی پور

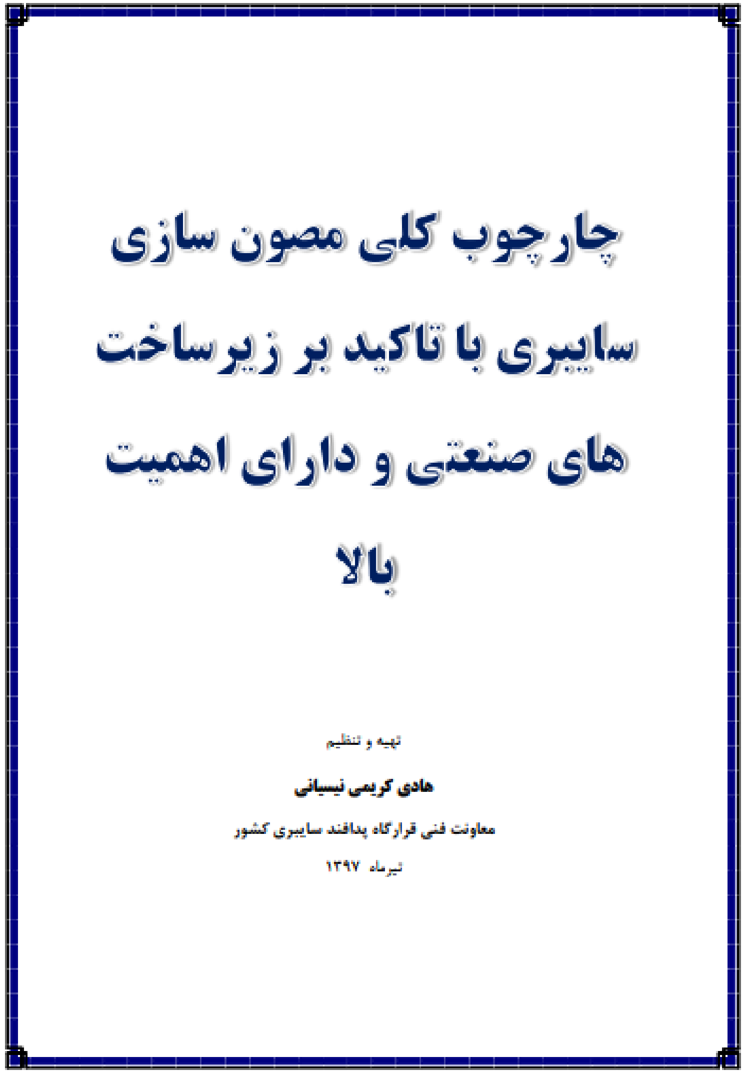
مهندس هادی کریمی نیسیانی

ناظر تخصصی

سردار دکتر جلالی

3. معماری بومی پدافند سایبری مبتنی بر متدولوژی دفاع در عمق و دفاع لایه به لایه

۵– طرح ها و پروژه های مصون سازی زیرساخت های سایبری و وابسته به سایبر


چارچوب کلی مصون سازی سایبری با تاکید بر زیرساخت های صنعتی و دارای اهمیت بالا

تهیه و تنظیم

هادی کریمی نیسیانی

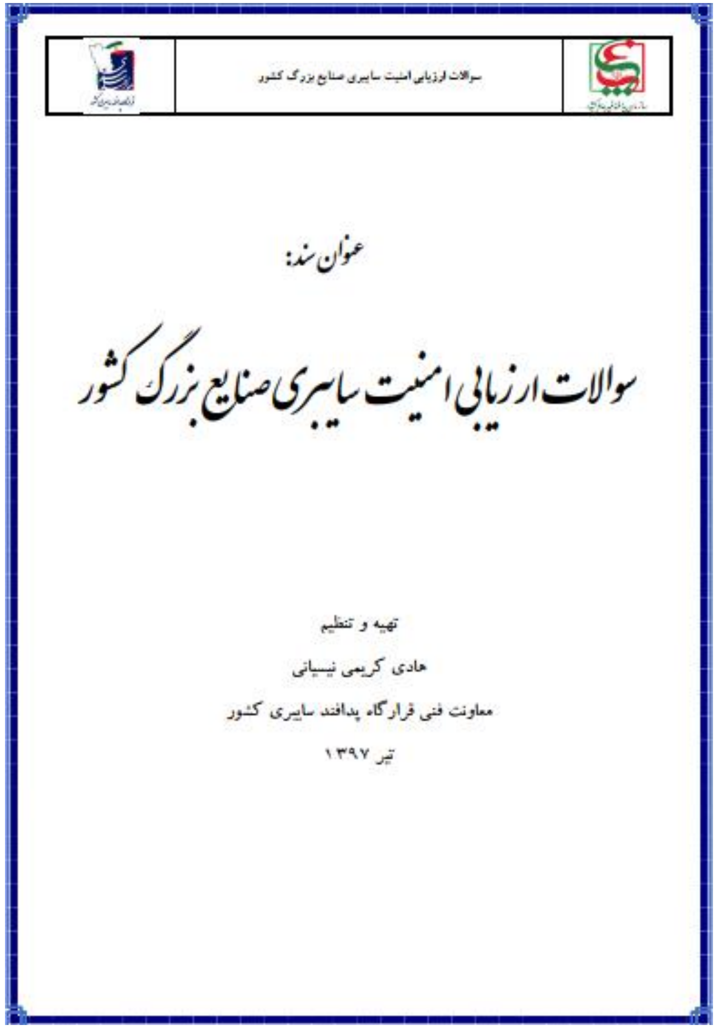
معاونت فنی قرارگاه پدافند سایبری کشور

تیرماه ۱۳۹۷

4. چارچوب کلی مصون سازی زیرساخت های سایبری و یا وابسته به سایبر با تاکید بر زیرساخت های صنعتی و دارای اهمیت بالا

۵- طرح ها و پروژه های مصون سازی زیرساخت های سایبری و وابسته به سایبر

9. **سوالات ارزیابی امنیت سایبری صنایع بزرگ**


سوالات ارزیابی امنیت سایبری صنایع بزرگ کشور

عنوان سند:

سوالات ارزیابی امنیت سایبری صنایع بزرگ کشور

تهیه و تنظیم

هادی کریمی نیسیانی

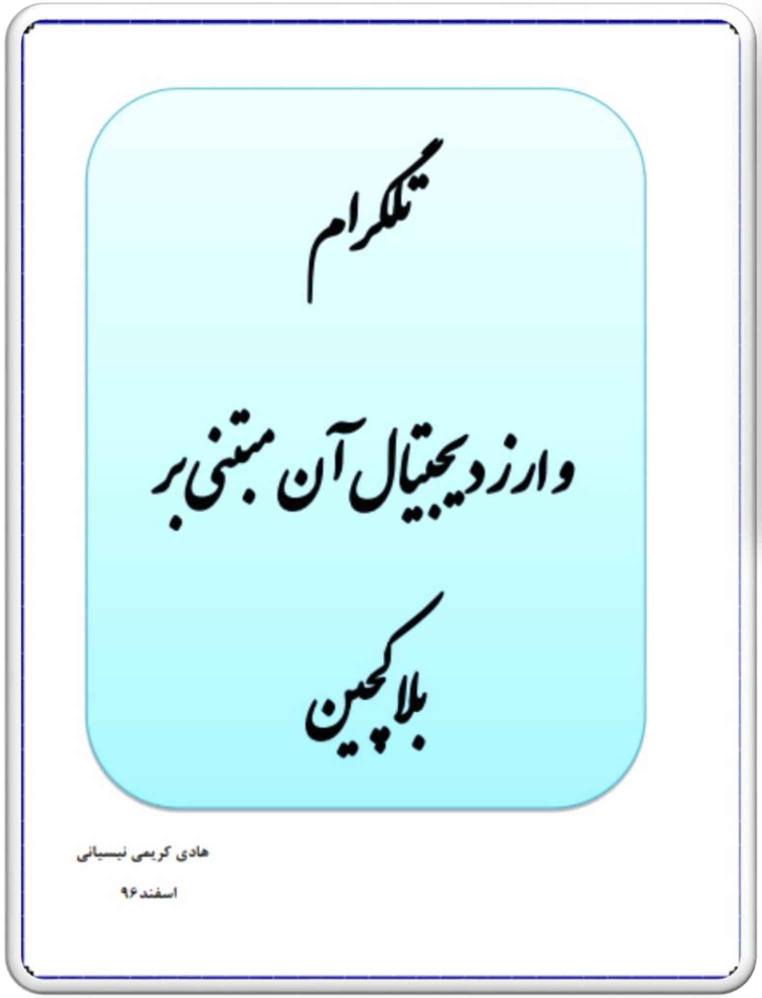
معاونت فنی قرارگاه پدافند سایبری کشور

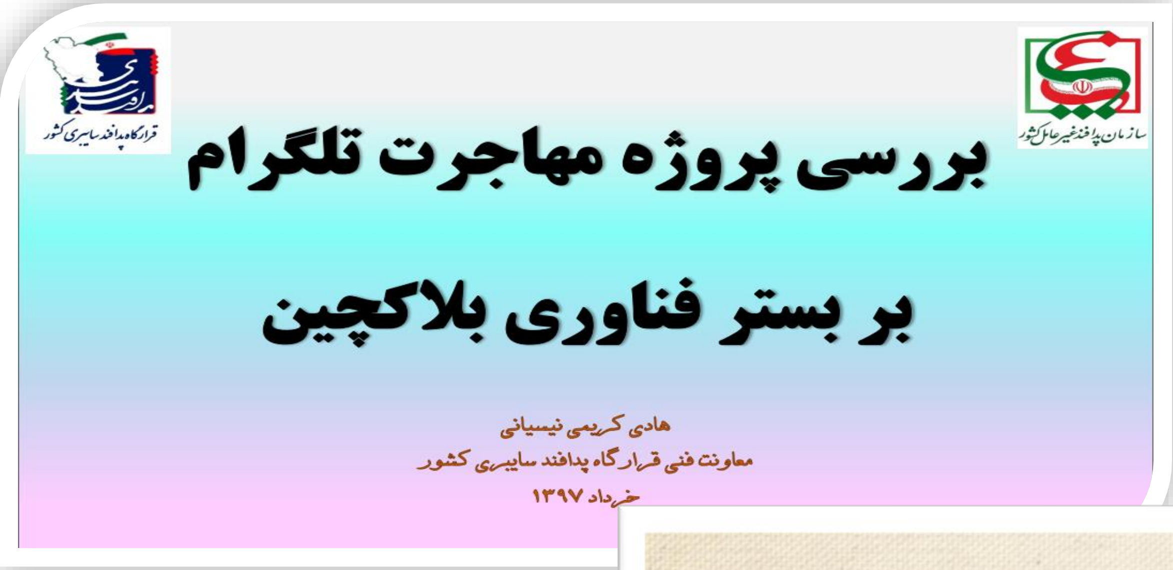
تیر ۱۳۹۷

مستندات شبکه های اجتماعی

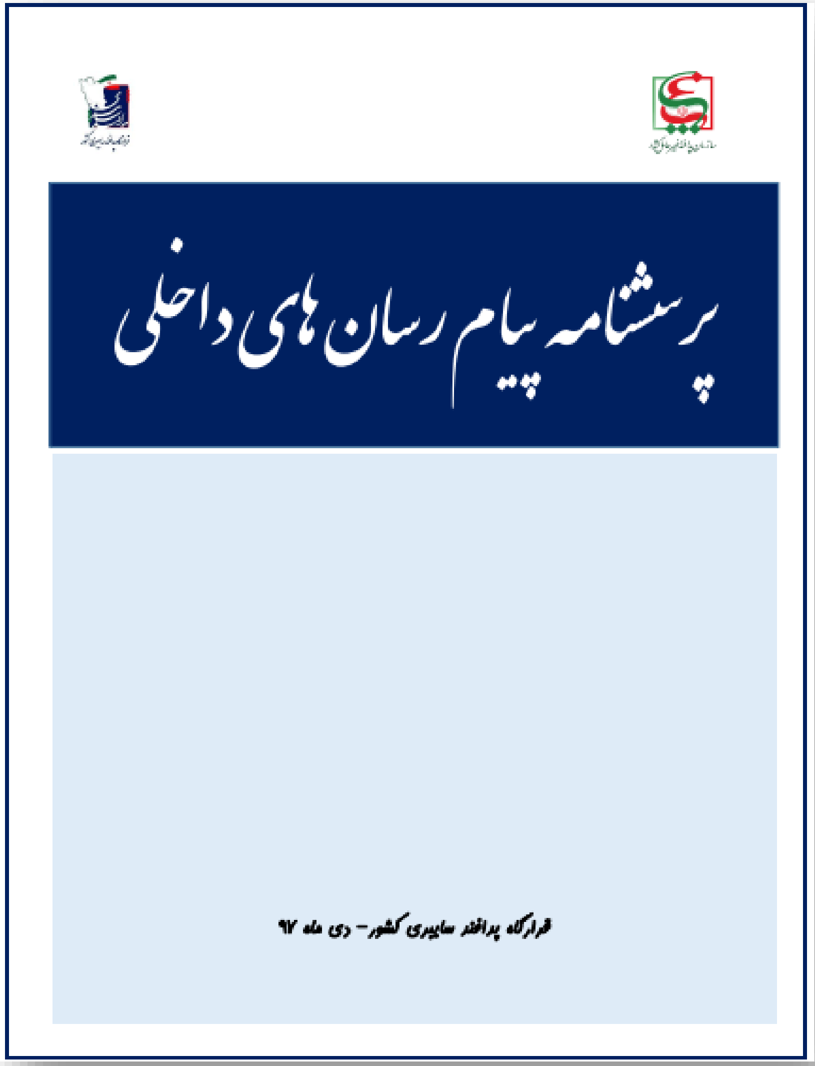
۶– مستندات شبکه های اجتماعی

1. تلگرام





۶- مستندات شبکه های اجتماعی


پرسشنامه پیام رسان های داخلی

قرارگاه پدافند سایبری کشور- دی ماه ۹۷

2. پرسشنامه ارزیابی پیام رسان های داخلی

آیین نامه نحوه استفاده هوشمندانه از تلفن هوشمند در مراکز حیاتی و حساس

۷– آیین نامه نحوه استفاده هوشمندانه از تلفن هوشمند در مراکز حیاتی و حساس


آیین نامه نحوه استفاده

هوشمندانه و امن از

تلفن همراه هوشمند

در مراکز حیاتی و حساس کشور

سازمان پدافند غیرعامل کشور


دستورالعمل نحوه استفاده

هوشمندانه و امن از

تلفن همراه هوشمند

و دستگاه های مشابه در

مراکز حیاتی و حساس کشور

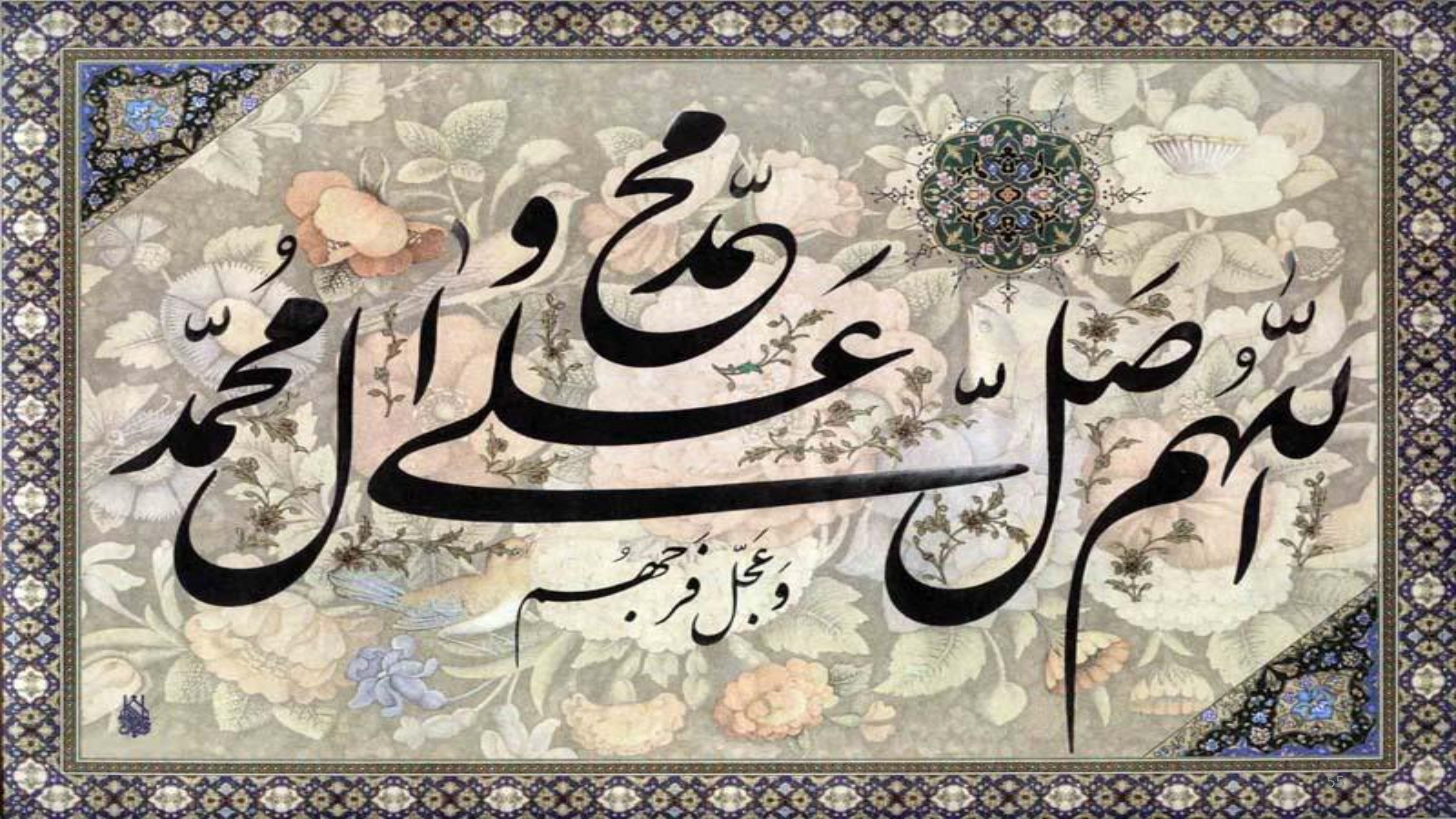
شهریورماه ۱۳۹۲

قرارگاه پدافند سایبری کشور

۱

1. آیین نامه نحوه استفاده هوشمندانه از تلفن هوشمند در مراکز حیاتی و حساس

2. دستورالعمل نحوه استفاده هوشمندانه و امن از تلفن همراه هوشمند و دستگاه های مشابه در مراکز حیاتی و حساس کشور


اللّهمّ صلّ علی محمّد و آل محمّد
وَ عَجّل فرجهُم

فناوری های نوین سایبری

چالش ها – فرصت ها

با رویکرد پدافند سایبری

هادی کریمی نیسیانی

معاونت فنی قرارگاه پدافند سایبری کشور

خرداد ۱۴۰۰

قرارگاه پدافند سایبری کشور

سازمان پدافند غیرعامل کشور


بسم الله الرحمن الرحیم

اگر مدیران کشور اهمیت این مسئله را درک نکنند و پدافند غیرعامل به طور شایسته توسعه پیدا نکند، کشور در معرض تهدیدهای بعضاً غیرقابل جبران قرار خواهد گرفت، بنابراین مسئولان بخش‌های مختلف کشور چه بخشهای نظامی و چه بخشهای غیرنظامی، باید با پدافند غیرعامل همکاری کامل و لازم انجام دهند.

بیانات رهبر معظم انقلاب اسلامی

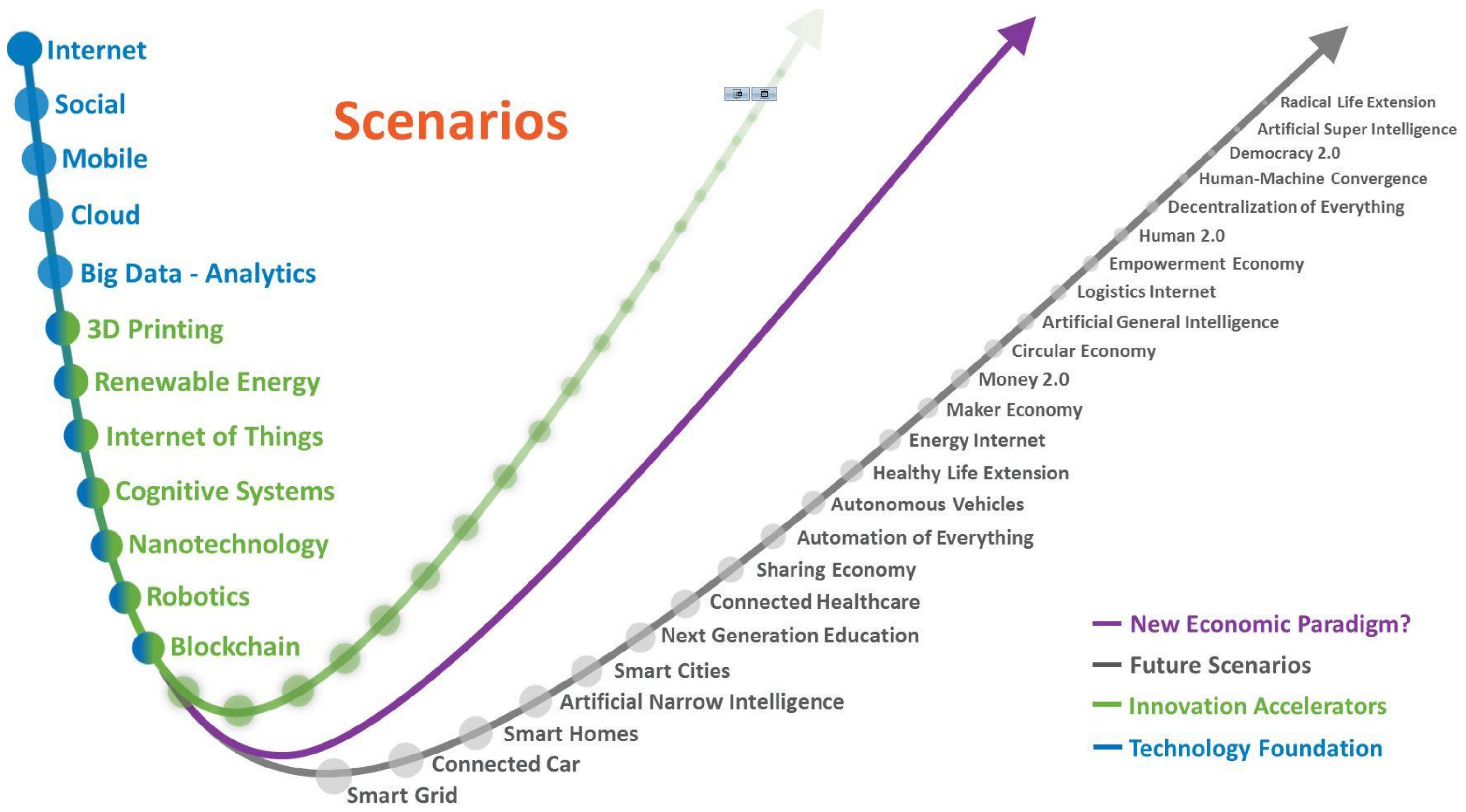
در دیدار رئیس و مسئولان سازمان پدافند غیرعامل کشور

فناوری های نوین تحول آفرین در حوزه سایبر
فرصت ها و چالش ها

فناوری های نوین تحول آفرین در حوزه سایبر

- انقلاب وب (مهاجرت از وب ۱ و ۲ به وب ۳ و ۴)
- انقلاب در صنعت پول، بانکداری و پرداخت (Cryptocurrency)
- Blockchain
- محاسبات کوانتومی
- Data Science(Big Data, Data Mining, Data Analysis)
- Cloud Computing, Fog Computing & Edge Computing
- هوش مصنوعی(Artificial Intelligence)
- IOT & IIOT

سناریوهای جدید

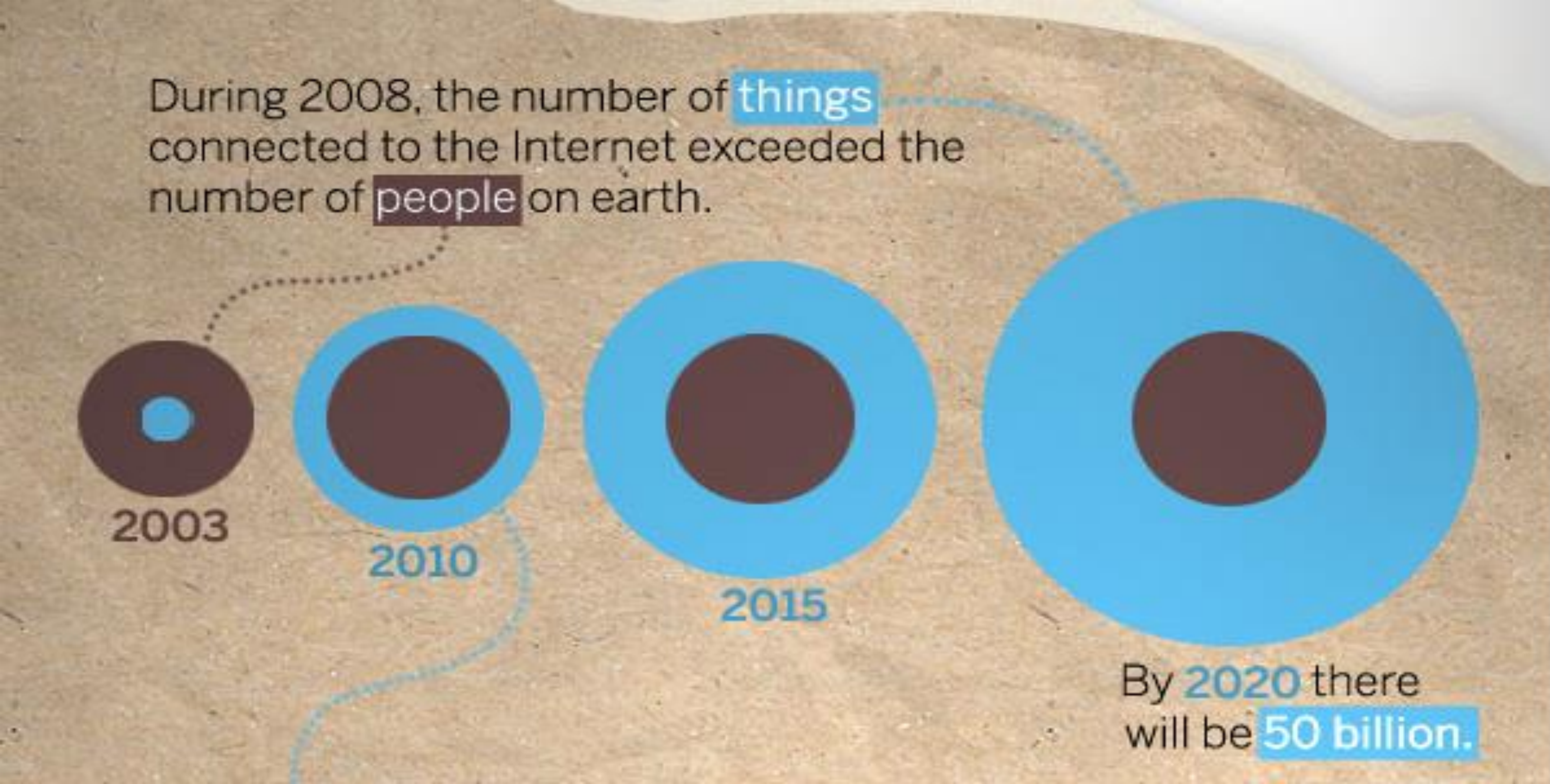


فناوری اینترنت اشیا

Internet Of Things

تعریف اینترنت اشیاء (IOT)

- مجموعه استانداردها، پروتکلها، دستگاهها و فناوریهای لازم برای برقراری ارتباط و انتقال اطلاعات بین دستگاههای هوشمند با یکدیگر و با انسان در سطح جهانی.
- هدف اصلی طراحی این شبکه، به اشتراک گذاردن اطلاعات موجود در هر شیء میان سایر اشیاء مرتبط با آن، درهر زمان و در هر مکان مورد نیاز است.
- در واقع اینترنت اشیاء، به معنی امکان برقراری ارتباط تمام اشیاء با یکدیگر IOT، و با انسانهاIOP، به همراه شناسایی و کشف آنها تحت یک شبکه یکپارچه است (هدف IOE)
- ایده اتصال زنجیره ای دستگاهها و اشیاء در سطح جهانی با ظهور فناوری RFID مطرح شد.
- فناوری IoTروشهای ارتباطی مختلف مانند، RFID، Zigbee، Wi-Fi، 3G/4G/5Gدستگاههای فشرده و حسگرها را با یکدیگر ترکیب میکنند



Sources: Cisco IBSG, Jim Cicconi, AT&T , Steve Leibson, Computer History Museum, CNN, University of Michigan, Fraunhofer

تعریف اینترنت اشیاء (IOT)

از نقطه‌نظر مفهومی، اینترنت اشیاء بر اساس **<u>سه رکن اساسی</u>** ساخته می‌شود که مرتبط با قابلیت‌های اشیاء هوشمند است.

<u>قابلیت شناسایی</u>،

هر شیء بتواند خودش را بشناساند

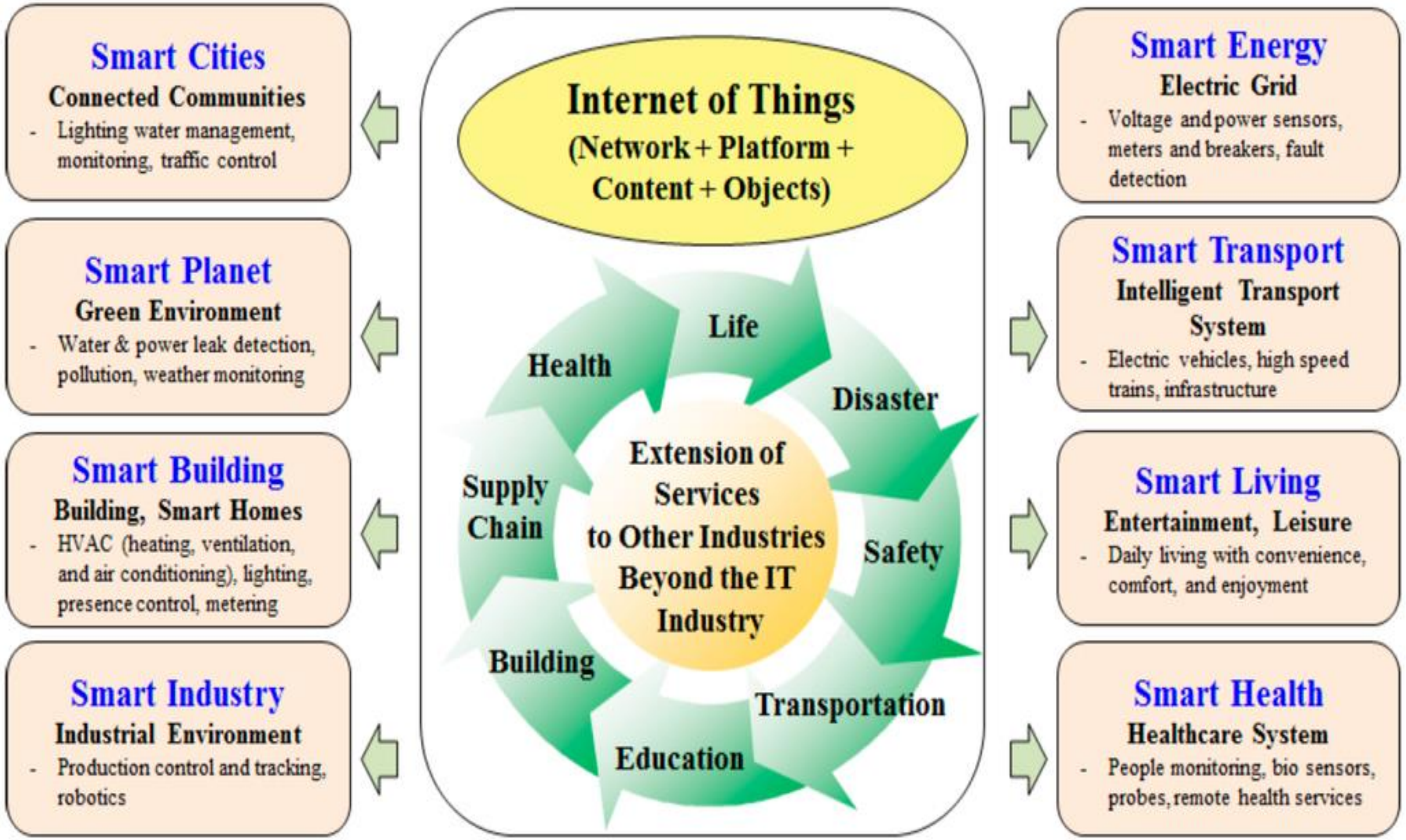
<u>قابلیت برقراری ارتباط</u>،

هر شیء بتواند ارتباط برقرار کند

<u>قابلیت تعامل</u>،

هر شیء بتواند تعامل کند

ابعاد مختلف هوشمندی در اینترنت اشیاء



استانداردهای ITU برای IoT & IIoT

استانداردهای عمومی اینترنت اشیا

General
Y.4000-Y.4049
SG-13, SG-16

زیرساخت، اتصال و شبکه اینترنت اشیا

Infrastructure, connectivity and networks
Y.4250-Y.4399
SG-13, SG-16

مدیریت، کنترل و کارایی در اینترنت اشیا

Management, control and performance
Y.4700-Y.4799
SG-16, SG-20

تعاریف و اصطلاحات مربوط به اینترنت اشیا

Definitions and terminologies
Y.4050-Y.4099
SG-13

چارچوب، معماری و پروتکل‌های اینترنت اشیا

Frameworks, architectures and protocols
Y.4400-Y.4549
SG-13, SG16, SG11

شناسه و امنیت در اینترنت اشیا

Identification and security
Y.4800-Y.4899
SG-16

الزامات و مطالعات موردی اینترنت اشیا

Requirements and use cases
Y.4100-Y.4249
SG-13, SG16

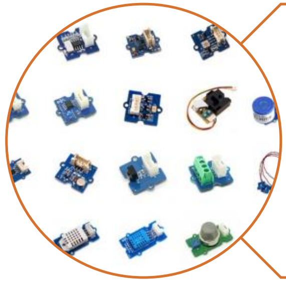
سرویس ها، برنامه‌های کاربردی، محاسبات و پردازش داده در اینترنت اشیا

Services, applications, computation and data processing
Y.4550-Y.4699
SG-13, SG16, SG20

سنجش و ارزیابی اینترنت اشیا

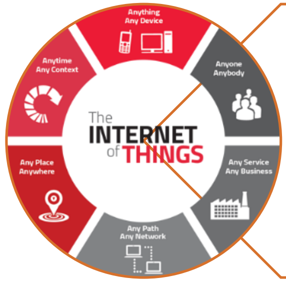
Evaluation and assessment
Y.4900-Y.4999
SG-5

اکوسیستم اینترنت اشیاء



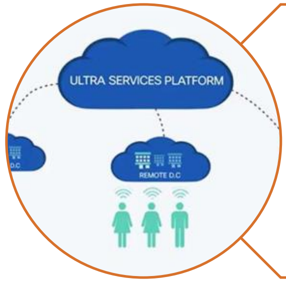
سخت افزار

(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)



شبکه مخابراتی ارتباطی

(شامل شبکه انتقال مبتنی بر IP و شبکه دسترسی)



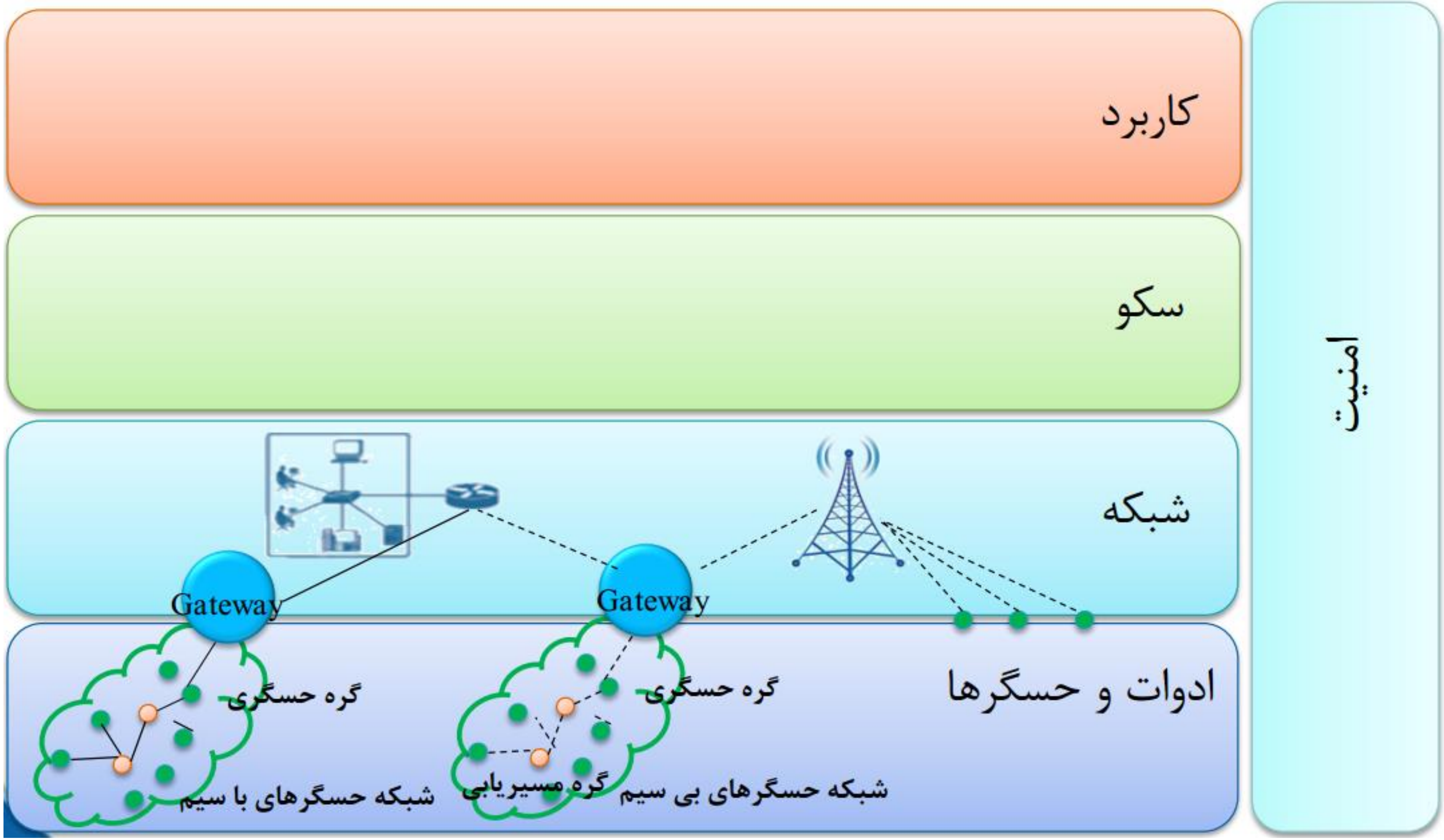
بستر ابری

(مرکز داده، پلتفرم تحلیل کلان داده و میان افزار ارایه سرویس)

برنامه‌های کاربردی

(شامل توسعه‌دهندگان سرویس و سرویس‌گیرندگان)

اکوسیستم اینترنت اشیاء



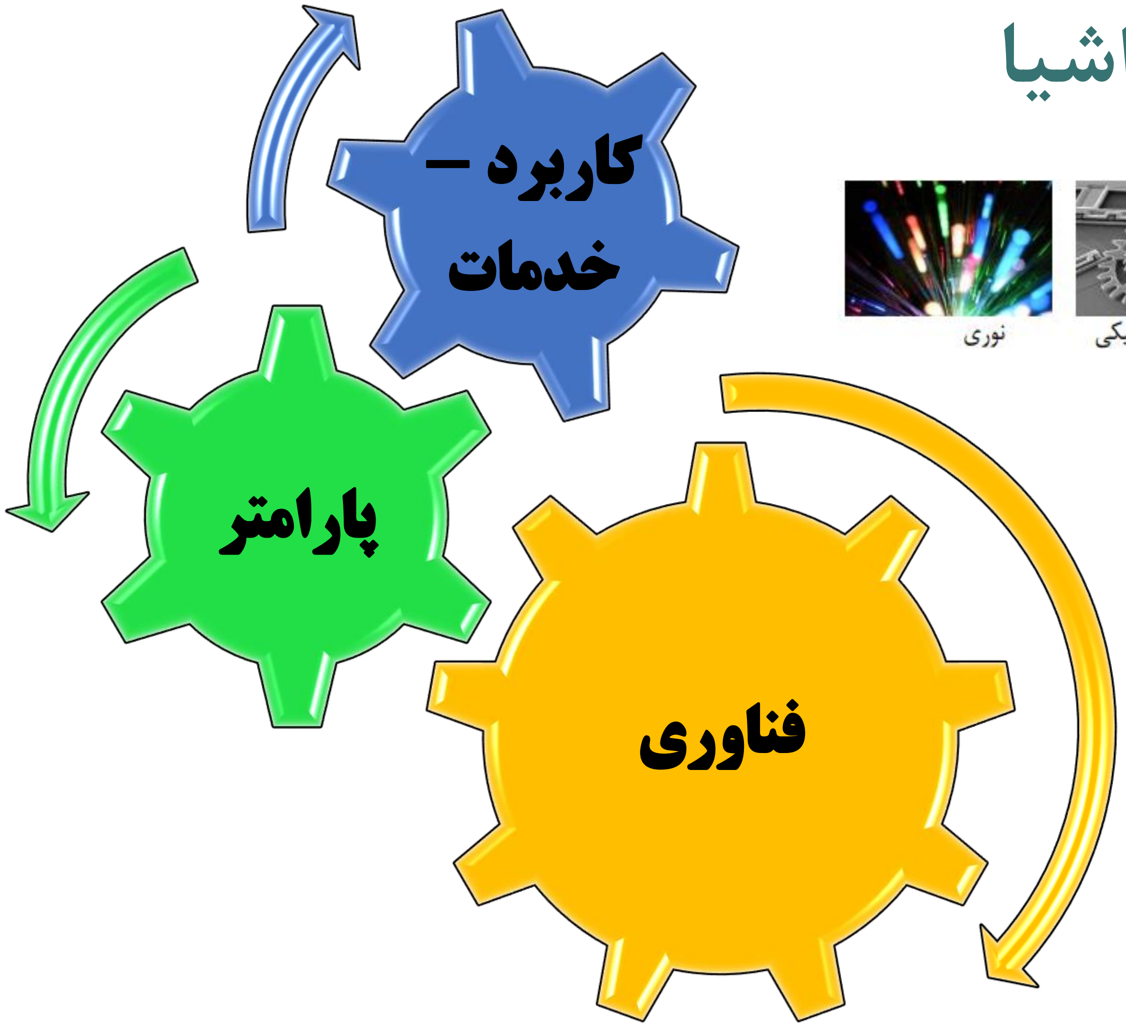
اکوسیستم اینترنت اشیاء

سخت افزار
(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)

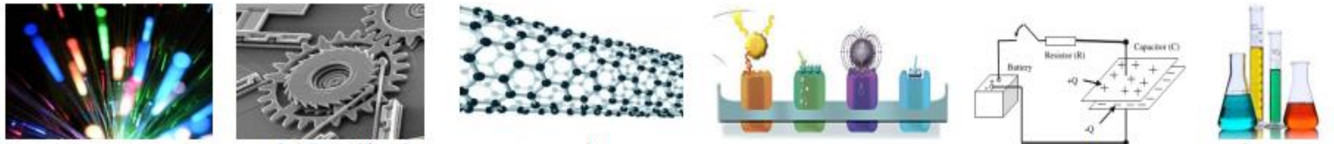
- حسگر یا سنسور کمیت های فیزیکی مانند فشار، حرارت، رطوبت، دما، و ... را به کمیت های الکتریکی پیوسته (آنالوگ) یا غیرپیوسته (دیجیتال) تبدیل می کند.
- در واقع سنسور یک وسیله الکتریکی است که تغییرات فیزیکی یا شیمیایی را اندازه گیری می کند و آن را به سیگنال الکتریکی تبدیل می نماید

اکوسیستم اینترنت اشیاء

سخت افزار
(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)



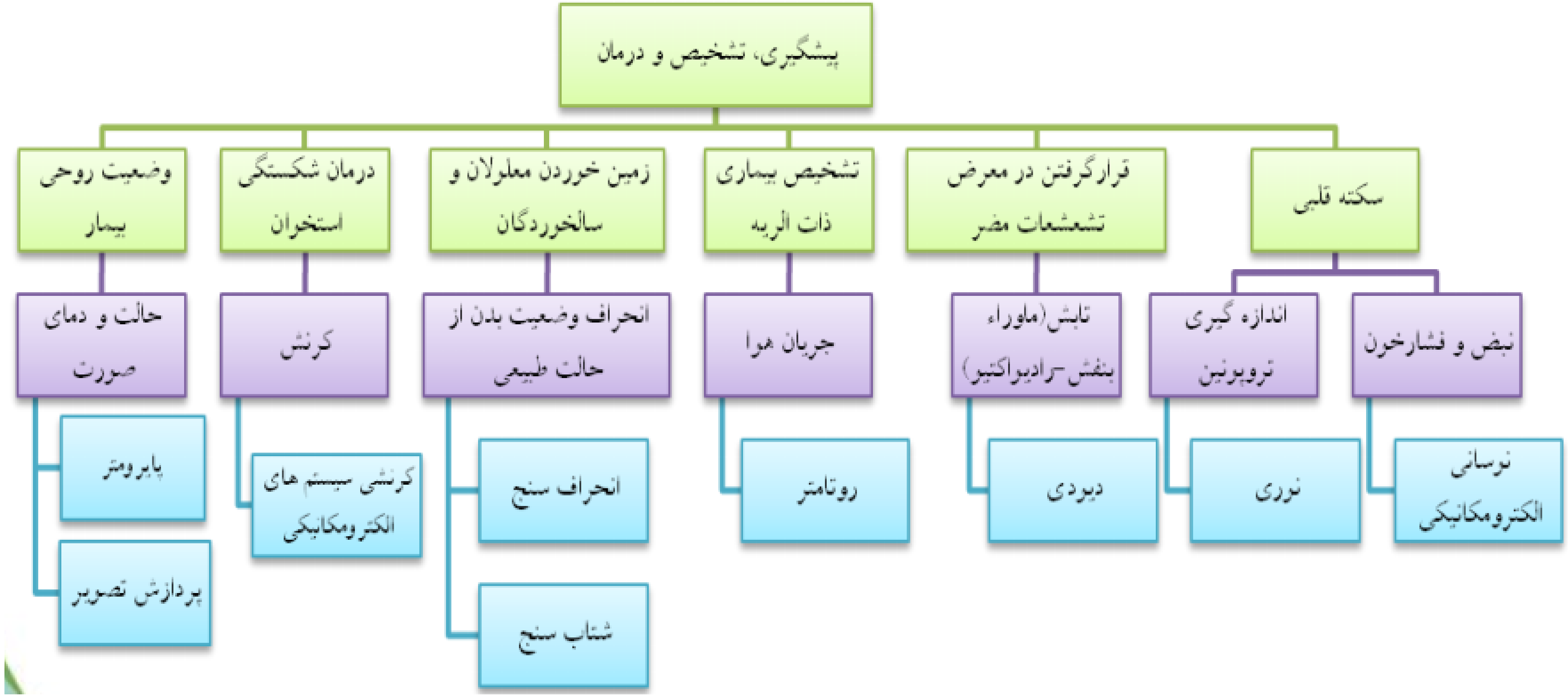
طبقه بندی حسگر در اینترنت اشیا



اکوسیستم اینترنت اشیاء

سخت افزار
(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)

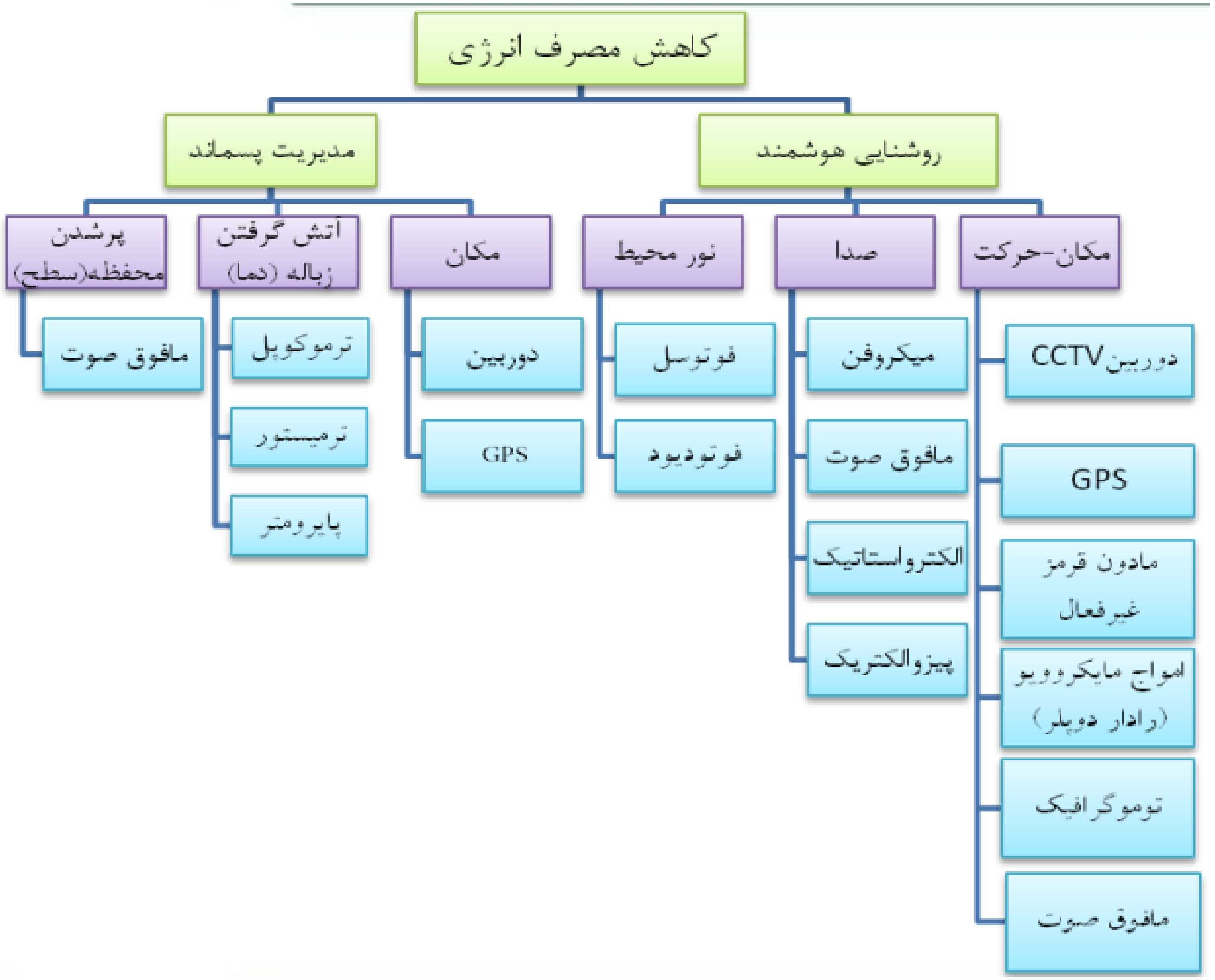
حسگرهای مورد استفاده در سلامت هوشمند



اکوسیستم اینترنت اشیاء

سخت افزار
(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)

حسگرهای مورد استفاده در شهر هوشمند



اکوسیستم اینترنت اشیاء

اهمیت حوزه حسگرهای اینترنت اشیا

امنیت اینترنت اشیا درگرو امنیت شبکه حسگرها است.

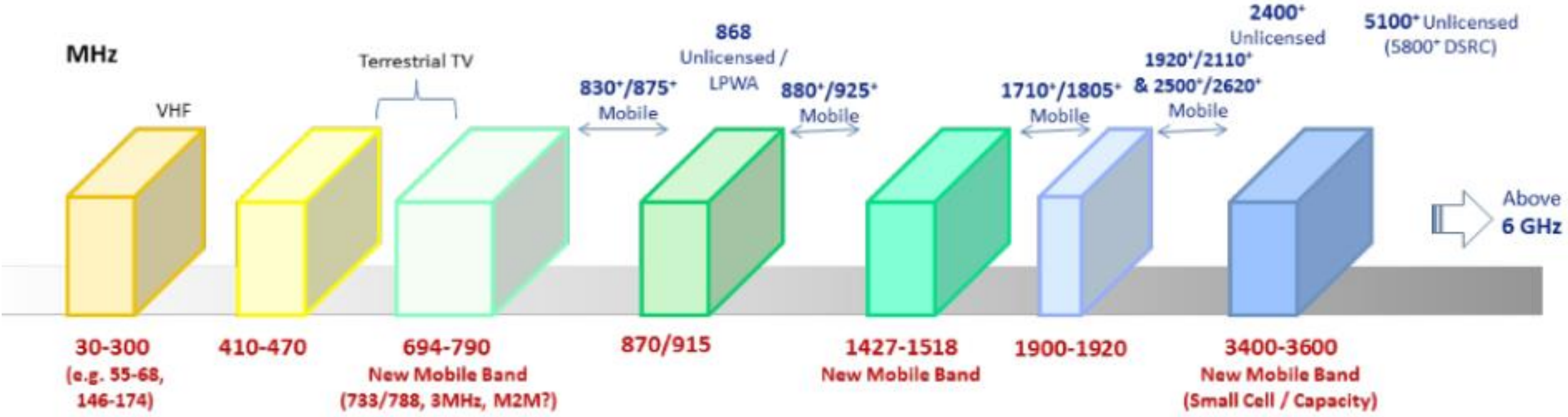
حسگرها به عنوان زیرساخت، پیشران و شکل دهنده بازار IoT محسوب میشوند

حجم بالای نیاز بازار و تولیدات مجموعه های سخت افزاری حسگری در اینترنت اشیا منجر به صرفه اقتصادی در ورود به ساخت مجموعه های حسگری می شود

سخت افزار
(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)

اکوسیستم اینترنت اشیاء

- نیازمندیهای طیف فرکانسی IoT و IIoT



اکوسیستم اینترنت اشیاء

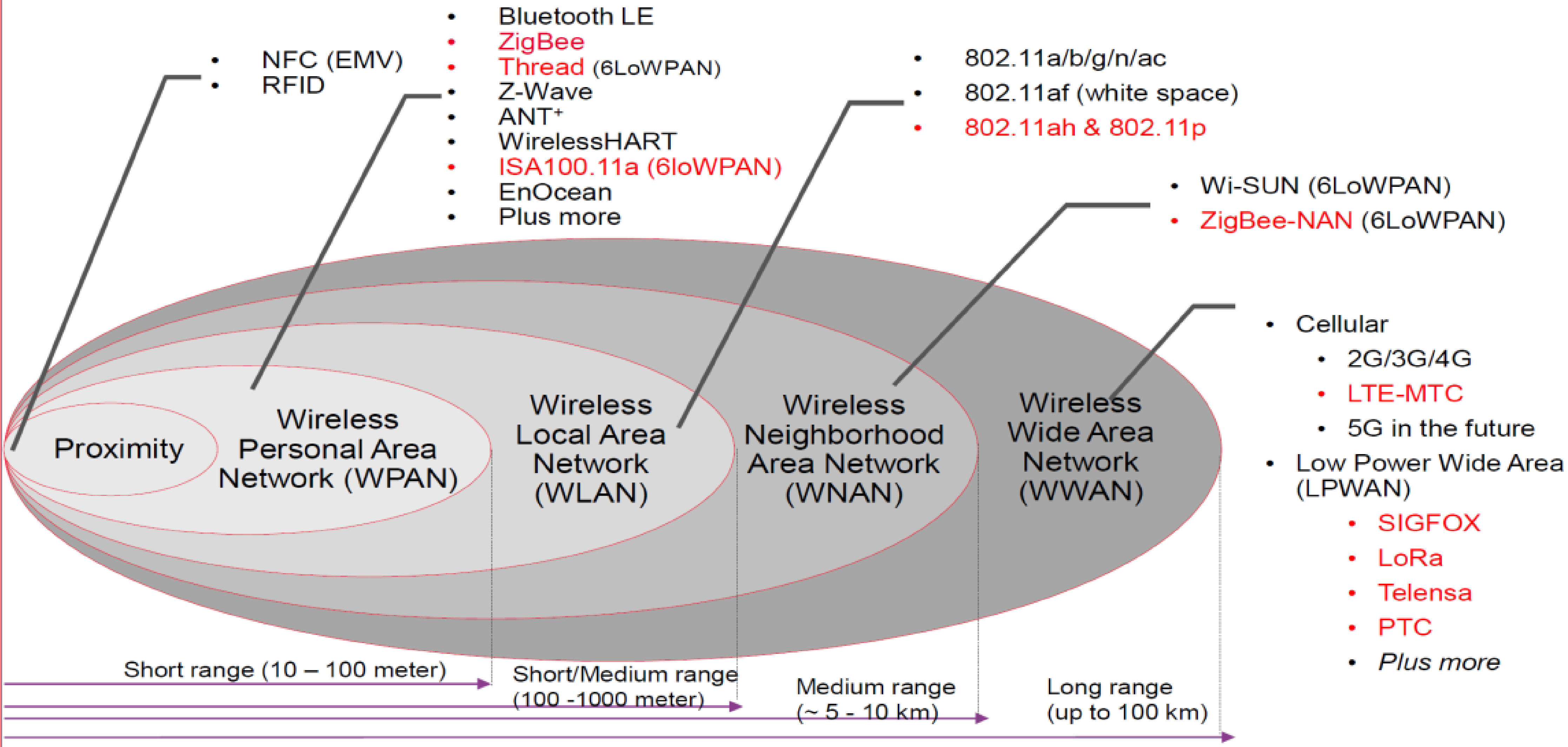
شبکه مخابراتی ارتباطی

فناوری های بیسیم

مطرح در IOT & IIOT

اکوسیستم اینترنت اشیاء

شبکه مخابراتی ارتباطی



اکوسیستم اینترنت اشیاء

شبکه مخابراتی ارتباطی

- **Wireless Sensor Network (WSN)**
  - **Short Range**
    - Body Area Network(BAN)
    - Home Area Network(HAN)
    - Personal Area Network(PAN)
    - Local Area Network(LAN)
  - **Long Range**
    - Low Power Wide Area Network(LPWAN)
    - Wide Area Network(WAN)

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

IEEE 802.11

- Data Rate: Up to 2Mbps in the 2.4GHz band
  - Modulation Scheme: FHSS (Frequency-hopping spread spectrum)

or DSSS (direct-sequence spread spectrum)

- Security: WEP & WPA

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

IEEE 802.11.a

- Data Rate: In the **5GHz band up to 54Mbps**
  - Modulation Scheme: **OFDM**
  - Security: WEP & WPA
  - **Eight available channels**.
  - **Less potential for radio frequency interference than 802.11b and 802.11g**.
  - Better than 802.11b at supporting multimedia voice, video and large image applications in densely populated user environments.

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

IEEE 802.11.g

- Data Rate: **Up to 54Mbps in the 2.4GHz band**
  - Modulation Scheme: Orthogonal Frequency Division Multiplexing (**OFDM**) above 20Mbps, DSSS with CCK below 20Mbps
  - Security: WEP & WPA
  - May replace 802.11b.
  - **Improved security enhancements over 802.11**.
  - Compatible with 802.11b.
  - 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three nonoverlapping channels.

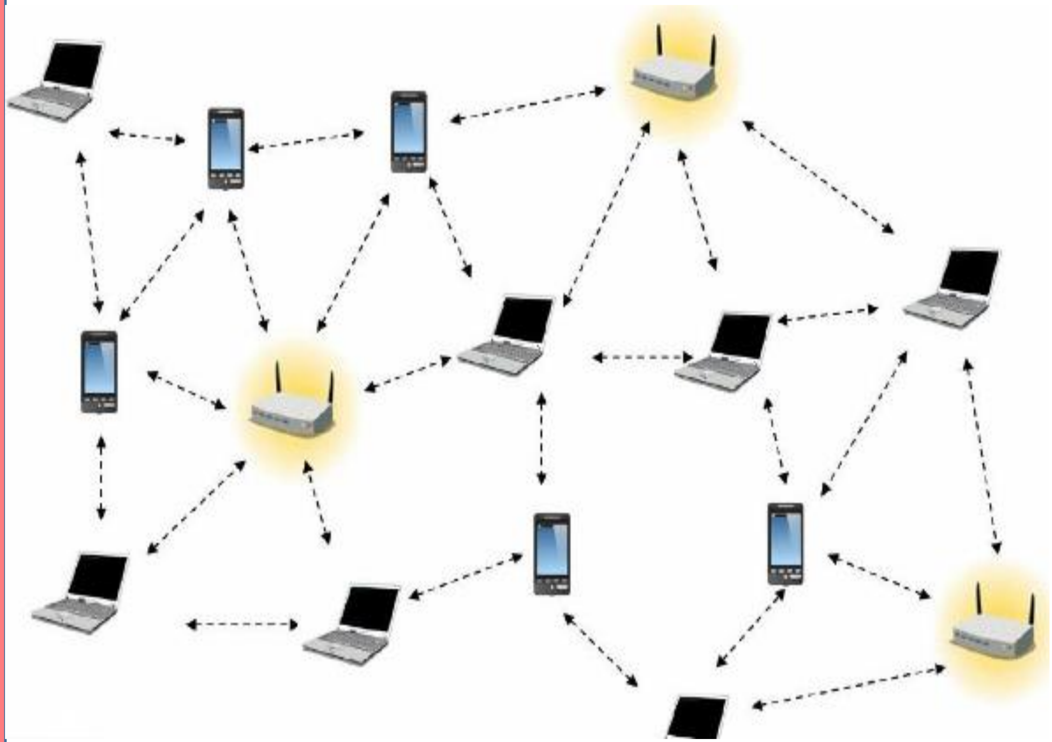
اکوسیستم اینترنت اشیاء - شبکه مخابراتی ارتباطی

IEEE 802.11

802.11a	Wireless network operating in the 5 GHz ISM band with data rate up to 54 Mbps
802.11b	Wireless network operating in the 2.4 GHz ISM band with data rates up to 11 Mbps
802.11e	Quality of service and prioritisation
802.11f	Handover
802.11g	Wireless network operating in 2.4 GHz ISM band with data rates up to 54 Mbps
802.11h	Power control
802.11i	Authentication and encryption
802.11j	Interworking
802.11k	Measurement reporting
802.11n	Wireless network operating in the 2.4 and 5 GHz ISM bands with data rates up to 600 Mbps
802.11s	Mesh networking
802.11ac	Wireless network operating below 6GHz to provide data rates of at least 1Gbps per second for multi station operation and 500 Mbps on a single link
802.11ad	Wireless network providing very high throughput at frequencies up to 60GHz
802.11af	Wi-Fi in TV spectrum white spaces (often called White-Fi)

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

Ad hoc



- اتصال دو کلاینت بیسیم بطور مستقیم
- پیاده سازی بدون بدون نیاز به WAP
- مانند شبکه های Peer-to-peerبدون نیاز به سرور
- هر عنصر مسئول امنیت خود بوده
- مدیران شبکه مجاز هستند که WEPرا پیکربندی کنند
- حداکثر سرعت انتقال فعلاً 11Mbpsاست

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

Ad hoc

Some Ad hoc routing Protocols

Reactive routing protocols

Dynamic Source Routing (DSR)
- Location-Aided Routing (LAR)
- Ad Hoc On-Demand Distance Vector (AODV)
- Power-Aware Routing (PAR)
- Associativity-Based Routing (ABR)
- Signal Stability Based Adaptive Routing (SSA)
- Link Reversal Algorithm
- Temporally-Ordered Routing Algorithm (TORA)
- Cluster Based Routing Protocols (CBRP)

Proactive routing protocols

Destination-Sequenced Distance Vector (DSDV)
- Optimized Link State Routing (OLSR)
- Cluster head Gateway Switch Routing CGSR (hierarchical)
- Wireless Routing Protocol (WRP)
- Global State Routing (GSR)
- Fisheye State Routing (FSR)
- Hierarchical State Routing (HSR)
- Zone-based Hierarchical Link State Routing Protocol (ZHLS)

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

Zigbee

- دستگاههای مبتنی بر ZigBee در باندهای بدون لیسانس ISMکار می کنند.
- عمومی ترین پیکربندی در باند 2.4 GHzاست.
- حداکثر سرعت انتقال، ۲۵۰کیلوبیت برثانیه با مدولاسیون QPSK
- نسخه آمریکایی در باند 915MHz با نرخ بیت 40 Kbps با استفاده از مدولاسیون BPSK
- نسخه اروپایی در باند 868 MHz با نرخ بیت 20 Kbps
- مصرف توان کم
- قابلیت اطمینان نسبتا بالا، تصدیق هویت گرههای معتبر، رمزنگاری برای امنیت و مسیریابی داده
- برد ۱۰تا ۱۰۰متر با توجه به قدرت فرستنده و ویژگیهای محیط

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

Z-Wave

Specification	z-wave support
Standard	ITU-T G.9959 (PHY and MAC)
RF Frequency Range	868.42 MHz in Europe, 908.42 MHz in US
Data rate	9.6, 40, 100 Kbps
Maximum Nodes	232
Architecture	Master and slave in mesh mode
MAC layer	CSMA/CA
RF PHY modulation	FSK (for 9.6kbps and 40 kbps), GFSK with BT=0.6 (for 100 kbps)
Coding	Manchester(for 9.6kbps), NRZ(for 40 and 100 kbps)
Distance	30 meter in indoors, 100 meters in outdoors

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

Z-Wave

*انتقال ویدئوی HDبه صورت بی سیم با فرکانس 60GHz
*کنترل درب گاراژ در فرکانس 315MHz
*پایش درجه حرارت از راه دور در فرکانس MHz433
*اخذ داده در فرکانس 915MHz
*کنترل روشنایی، امنیت و کنترل آب و هوا
*آشکارسازی دود، قفل های درب، حسگرهای امنیتی
*HVAC (Heating, Ventilation and Air Conditioning)
*کنترل و پایش
*کاربردهای M2M

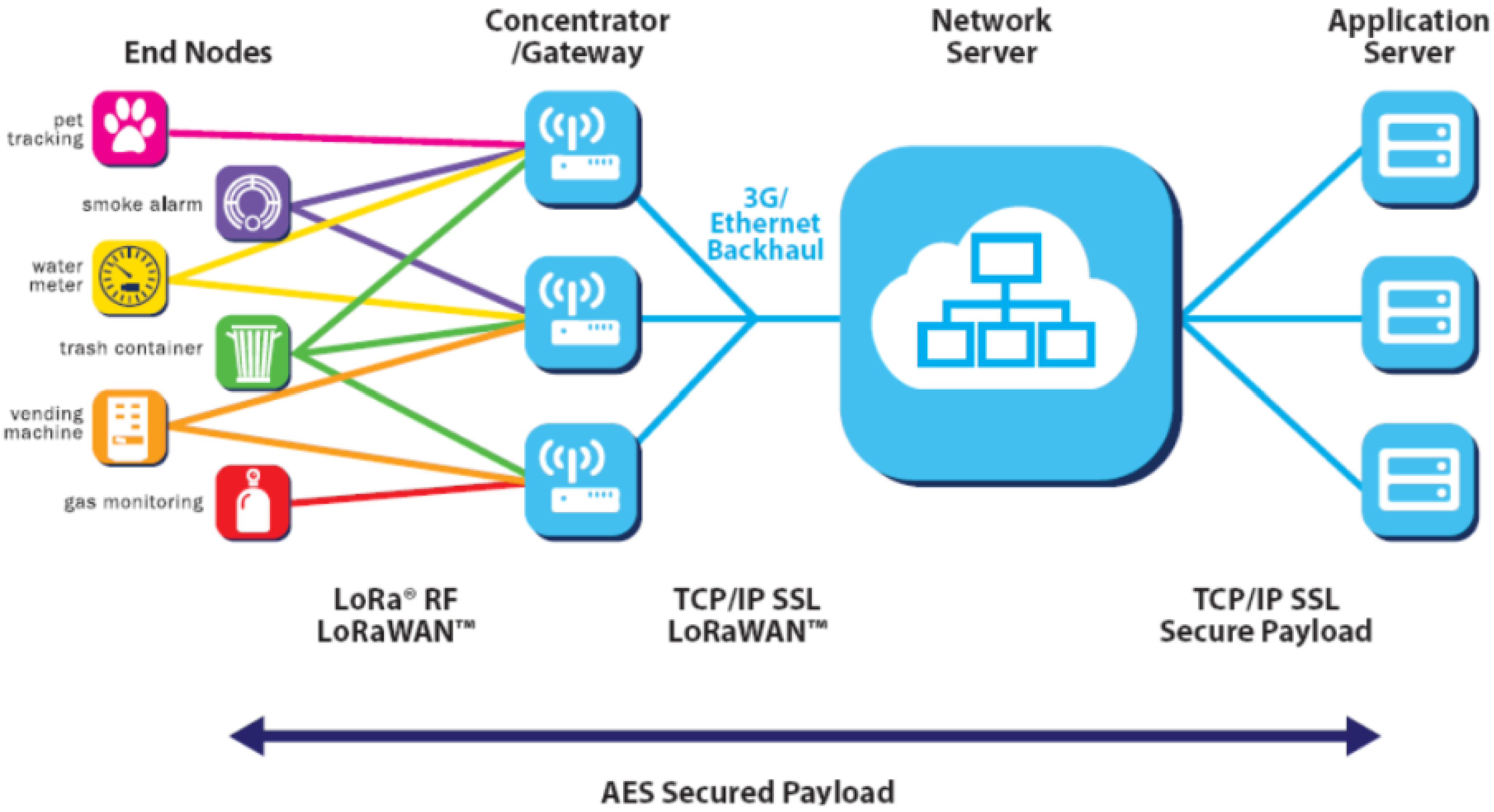
اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

LoRaWAN

- LoRaWANدارای اکوسیستم باز است بدین معنی که نرم افزار باز زیادی وجود داشته و فروشندگان زیادی در دسترس هستند.
- این استاندارد قابلیت همکاری متقابل میان اشیای هوشمند را بدون نیاز به نصب تجهیزات پیچیده محلی، فراهم کرده و به کاربر، توسعه کننده و تجارت گسترش اینترنت اشیا، آزادی عمل داده است.

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

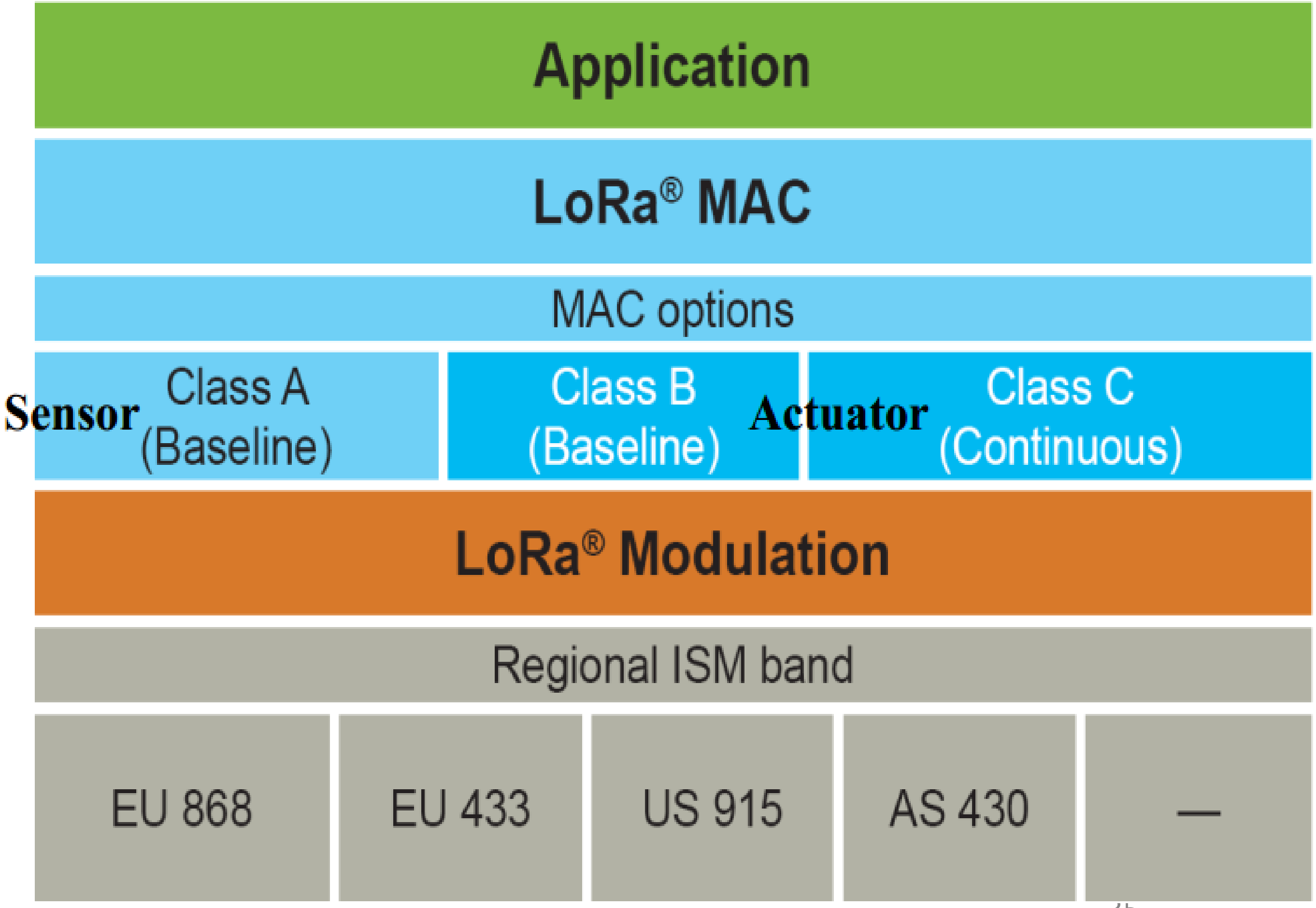
LoRaWAN



اکوسیستم اینترنت اشیاء - شبکه مخابراتی ارتباطی

LoRaWAN

- EUI 64bit Associate IP6 to LoRa sensors
- A unique network key to ensure security at the network layer
- A unique application key to ensure end-to-end security at the application layer,
- A device-specific key to secure the joining of a node to the network.



اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

6LOWPAN / IEEE.802.15.4

- در اینترنت اشیا به جهت مصرف کم باطری معمولا سرعت کم و قدرت کم داریم به عبارت دیگر نودهای محدود شده و شبکه محدود شده داریم.
- پروتکل های**Full Stack** برای لایه شبکه معمولا استفاده نمی شوند.
- برای لایه شبکه اینترنت اشیا پروتکل های محدود شده در نظر گرفته شده است.
- این پروتکل برای سرعت کم و قدرت کم در شبکه های بی سیم شخصی (**WPAN**)استفاده می شود.

اکوسیستم اینترنت اشیاء - شبکه مخابراتی ارتباطی

6LOWPAN / IEEE.802.15.4

- حداکثر اندازه فریم ۱۲۷است که ۲۵بایت هدر، ۲۱بایت برای امنیت و ۸۱بایت Payload.

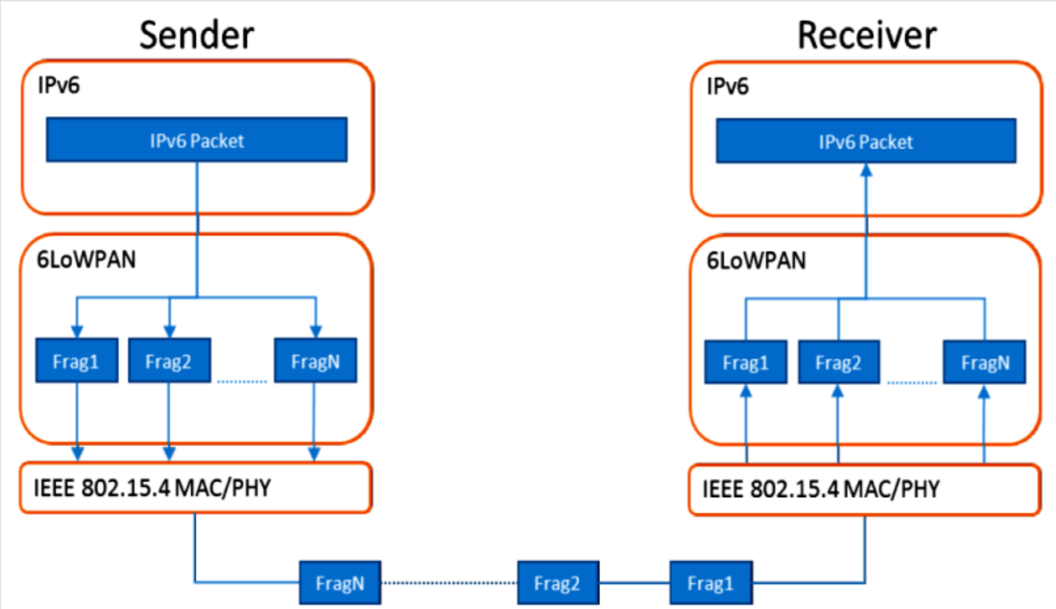
- برای ارتباط فناوری IPv6و IEEE.802.15.4یک لایه نیاز است که انطباق ساده بین الزامات لایه IPv6و قابلیتهای لایه پیوند را فراهم کند، این لایه 6LoWPAN نامیده میشود.

- در حقیقت ۶LoWPANپروتکل IPv6است که برای ابزارهای کم توان و با قابلیت پردازش محدود طراحی شده است.

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

6LOWPAN / IEEE.802.15.4

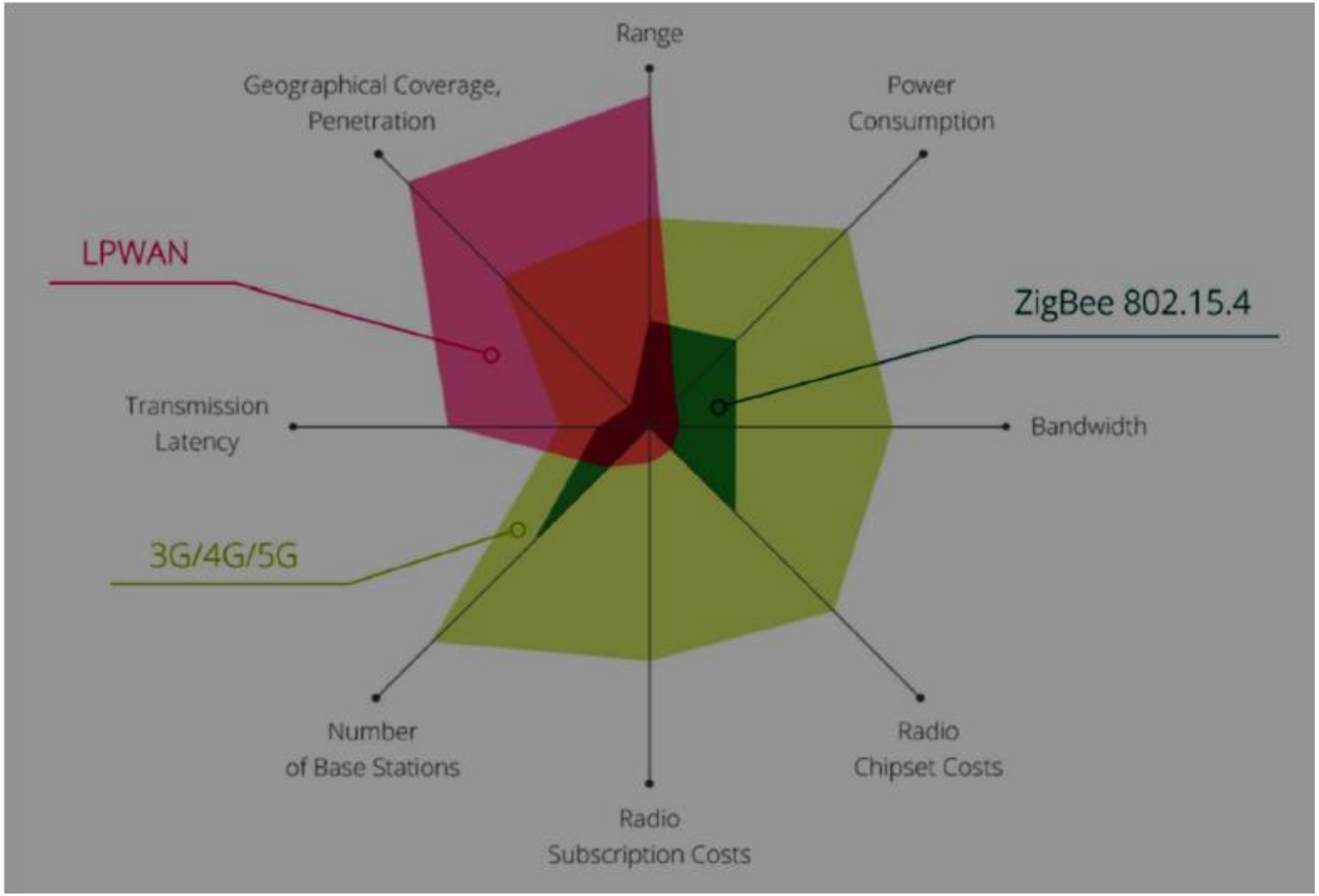
- گروه 6LoWPAN چگونگی کپسوله کردن و سازوکار فشرده سازی هدر آن را تعریف کرده است، به این ترتیب بسته های IPv6 میتوانند روی شبکه های مبتنی بر IEEE 802.15.4 ارسال یا دریافت شوند.



در فرستنده بسته را قطعه قطعه میکند و در گیرند مجددا آنرا سوار میکند

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

فناوری LPWAN در مقایسه با سایرین



اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

مقایسه فناوری های شبکه بی سیم گستره کوتاه

فناوری/مشخصات	نوع شبکه	باند فرکانس	توپولوژی	مصرف توان	نرخ بیت	گستره تحت پوشش	کاربرد	هزینه
ANT+	PAN	2.4GHz	P2P,Star,Tree ,Mesh	خیلی کم	1Mbps	Up to 100m	ورزش و تناسب اندام	کم
Bluetooth	PAN	2.4GHz 2.4835GHz	Star	کم	2.1Mbps	9-90m	تبادل داده، هدست	کم
BLE	PAN	2.4GHz 2.4835GHz	Star	خیلی کم	260Kbps	5-10m	سلامتی و تناسب اندام	کم
KNX	LAN	868MHz	Star,Tree,Me sh	خیلی کم	1.2Kbps	800m	اتوماسیون ساختمان	متوسط
NFC	PAN	13.56MHz	P2P	خیلی کم	400Kbps	<10cm	پرداخت، اشتراک، دسترسی	کم
RFID	PAN	13.56MHz Etc.	P2P	خیلی کم	400Kbps	<3m	ردیابی، شناسایی	کم
THREAD	LAN	2.4GHz 2.4835GHz	Star, Mesh	خیلی کم	250Kbps	800m	شبکه سنسور، اتوماسیون ساختمان و صنعت	متوسط

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

مقایسه فناوری های شبکه بی سیم گستره کوتاه

فناوری /شاخص	NB-Fi	LoRaWAN	Sigfox	RPMA	Weightless	NB-IoT
باند فرکانس(MHz)	۸۶۸/۸	۸۶۸/۸	۸۶۸/۸	۲۴۰۰	۸۶۸/۸	۹۰۰،۸۰۰،۷۰۰
حداکثر گستره (متر)	۱۶۸۰۰	۷۲۰۰	۹۵۰۰	۴۶۰۰	۴۱۰۰	شبکه سلولی
حداکثر بودجه لینک(dBm)	۱۶۶	۱۵۱	۱۵۶	۱۶۳	۱۴۷	۱۶۴
پهنای باند(KHz)	۰/۱	۱۲۵	۰/۱	۱۰۰۰	۰/۲	۲۰۰
نرخ بیت داده(Kbps)	۰/۰۰۰۸-۰/۱۲	۰/۱۰۰-۳	۰/۶	(DL)۱۵۶ (UL)۶۲۴	۲/۱۶۰۰۰-۵	(DL)۲۰۰-۱۵۲ (UL)۱۴۴-۴۸
راندمان طیف	زیاد	خیلی کم	کم	متوسط	کم	زیاد
دروازه‌راه(BTS)	دو طرفه	یک‌طرفه	یک‌طرفه	یک‌طرفه	یک‌طرفه	دوطرفه
گره به ازای هر دروازه‌راه	۱۳۵۰۰۰۰	۴۰۰۰۰	۵۰۰۰۰	+۵۰۰۰۰۰	۵۰۰۰۰	+۵۰۰۰۰
مقیاس‌پذیری	زیاد	خیلی کم	کم	زیاد	کم	زیاد

اکوسیستم اینترنت اشیاء - شبکه مخابراتی ارتباطی

مقایسه فناوری های شبکه بی سیم گستره کوتاه

فناوری /شاخص	NB-Fi	LoRaWAN	Sigfox	RPMA	Weightless	NB-IoT
ظرفیت‌دمدولاسیون همزمان	۱۲۰۰۰۰	۸	۲۵	۴۰۰۰	۲۵	
امنیت(رمزنگاری)	XTEA-256	AES-128	16bit	AES-128	-	LTE Encryp.
استفاده از آنتن Sector	بله	خیر	خیر	خیر	خیر	
هزینه به ازای هر گره(دلار)	۱/۹۹	۲۹	۱/۹۹	۵	۱۹	۴-۲
طول عمر باطری(سال)	۱۰	۱۰	۱۰	۱۰	۱۰	+۱۰
زمان تجاری شدن محصول	۲۰۱۱	۲۰۱۴	۲۰۱۰	۲۰۱۰	۲۰۱۳	۲۰۱۷
تعداد توسعه تجاری	+۱۰۰	+۱۰۰	+۱۰۰	۳۰	۱۰	-
نوع کاربرد	روشنایی،سنجش از راه دور، ماشین به ماشین، انرژی	روشنایی، انرژی، پایش گاز، ردیابی اموال، زلزله	اتوماسیون خانه، پایش محیط، ردیابی حیوانات، پایش آب	روشنایی، انرژی، پایش چاه نفت، صنعت	ماشین به ماشین	سنجش انرژی، ماشین به ماشین

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

IoT Wireless Technologies
Frequency Bands

Technologies	Frequency	Data rate	Range	Power	Cost
2G/3G	Cellular bonds	10 Mb/s	Several km	High	High
802.15.4	2.4 GHz	250 kb/s	100m	Low	Low
Bluetooth	2.4 GHz	1.2.1.3 Mb/s	100m	Low	Low
LoRa	< 1 GHz	<50 kb/s	2-5 km	Low	Medium
LTE Cat 0/1	Cellular bonds	1-10 Mb/s	Several km	Medium	High
NB-IoT	Cellular bonds	0.1-1 Mb/s	Several km	Medium	High
SIGFOX	<1 GHz	Very low	Several km	Low	Medium
Weightless	<1 GHz	0.1-24 Mb/s	Several km	Low	Low
WI-Fi (11f/h)	2.4.5 <1GHz	0.1-1 Mb/s	Several km	Medium	Low
WirelessHART	2.4 GHz	250 kb/s	100m	Medium	Medium
ZigBee	2.4 GHz	250 kb/s	100m	Low	Medium
Z-Wave	908.42 MHz	40 kb/s	30m	Low	Medium

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

IoT Wireless Technologies
Frequency Bands

Parameter	WAVIoT	LoRa (LinkLabs)[1]	Sigfox[2]	LTE-M (exp.)	WIFI	Cellular
Minimum Data rate	8+ bps	150 bps	100 bps	64 kbps	High	High
Max Range, meters	50 000	10 000	10 000	5 000	100	Within coverage
Gateway sensitivity, dBm	-154	-137	-142	-123	-96	-114
Gateway antenna gain, dBi	16	9	9	16	8	14
Gateway cable loss, dB	2	2	6	2	2	2
Gateway mode	Full Duplex	Half Duplex	Half Duplex	Full Duplex	Full Duplex	Full Duplex
Nodes per gateway	2 000 000+	250 000	50 000	50 000	200	5 000
Node max output power, dBm	26	26	14	23	20	33
Max Link budget, dBm	194	170	159	163	122	159
Node bandwidth	100 Hz	125 kHz	100 Hz	192 kHz	20 MHz	200 kHz
Spectrum efficiency	High	Very Low	Low	High	High	High
Simultaneous demodulation capacity	8 192	8	25	64	13	64
Scalability	High	Very Low	Low	High	Limited	High
Minimum Node cost, USD	2	29	2	5	25	10
Battery life	20+ years	10 years	10 years	5 years	7 days	1 day

اکوسیستم اینترنت اشیاء – شبکه مخابراتی ارتباطی

معیار کلی انتخاب فناوری شبکه

- گذردهی کم، گستره کوتاه – ازجمله Zigbee و Bluetooth
- گذردهی بالا، گستره کوتاه : WiFi
- گذردهی کم، گستره بلند : LoRa، Sigfox، NB-IoT
- گذردهی بالا، گستره بلند : 4G، 5G و …

اکوسیستم اینترنت اشیاء – بستر ابری

Cloud / Fog / Edge

- رایانش ابری یک مدل از رایانش است که به جای منابع اختصاصی برای هر کاربر، به مجموعه منابع فیزیکی – ویا مجازی – مشترک تکیه میکند.
- یکی از خصیصه های کلیدی رایانش ابری ، انعطاف پذیری آن می باشد. این بدین معنیست که سرویس های رایانش ابری به کاربران این امکان را میدهند که حتی زمانی که از سرویس خود استفاده میکنند نیز، منابع سرویس خود را افزایش یا کاهش دهند

سرویس های مبتنی بر ابر (cloud-based services)

- تعریف NIST

رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی (مثل: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم‌کننده سرویس به سرعت فراهم شده یا آزاد (رها) گردد.

سرویس های مبتنی بر ابر (cloud-based services)

منظور از رایانش ابری استفاده از منابع محاسباتی (سخت افزار و نرم افزار) است که مجموعه ای از سرورها از طریق یک شبکه می باشد در این روش، بجای اینکه کاربر نرم افزارهای کاربردی مورد نیاز خود را بر روی کامپیوتر شخصی نصب کند، از طریق هر کامپیوتر متصل به شبکه خدمات مورد نیاز خود را بصورت وب سرویس دریافت می کند. نرم افزارهای کاربردی بر روی سرورهای پر سرعت شبکه نصب می شوند و کاربر می تواند به تمامی این نرم افزارها از طریق شبکه دسترسی پیدا کند.

Essential characteristics

- On demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Measured service

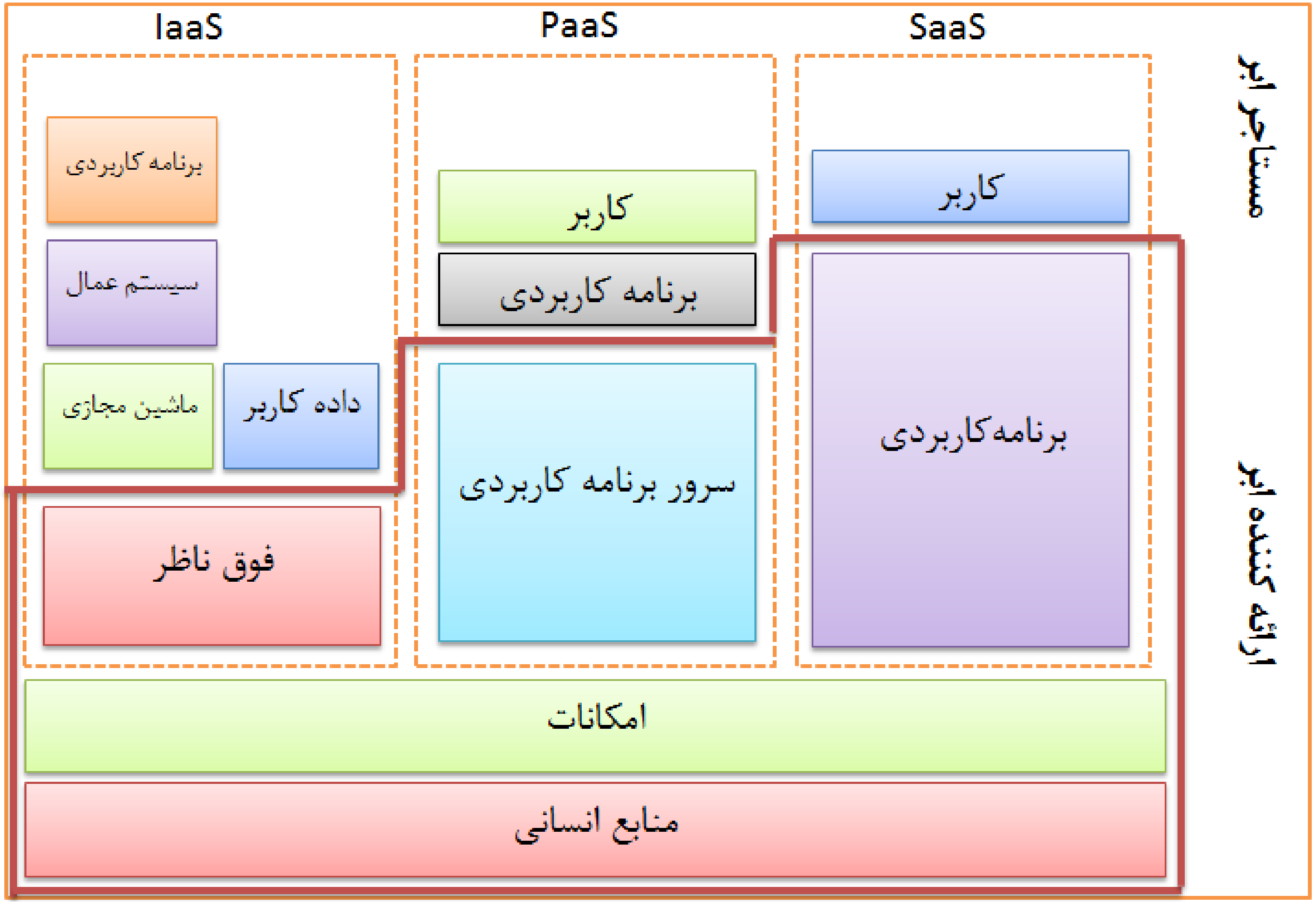
no-need-to-know
flexibility and elasticity
pay as much as used and needed
always on!, anywhere and any place

مدلهای رایانش ابری

- مدلهای بکار گیری (Deployment Models)
  - خصوصی
  - عمومی
  - سازمانی
  - ترکیبی
- مدلهای تحویل خدمات (Delivery Models)
  - Software as a service (SAAS)
  - Platform as a service (PAAS)
  - Infrastructure as a service (IAAS)

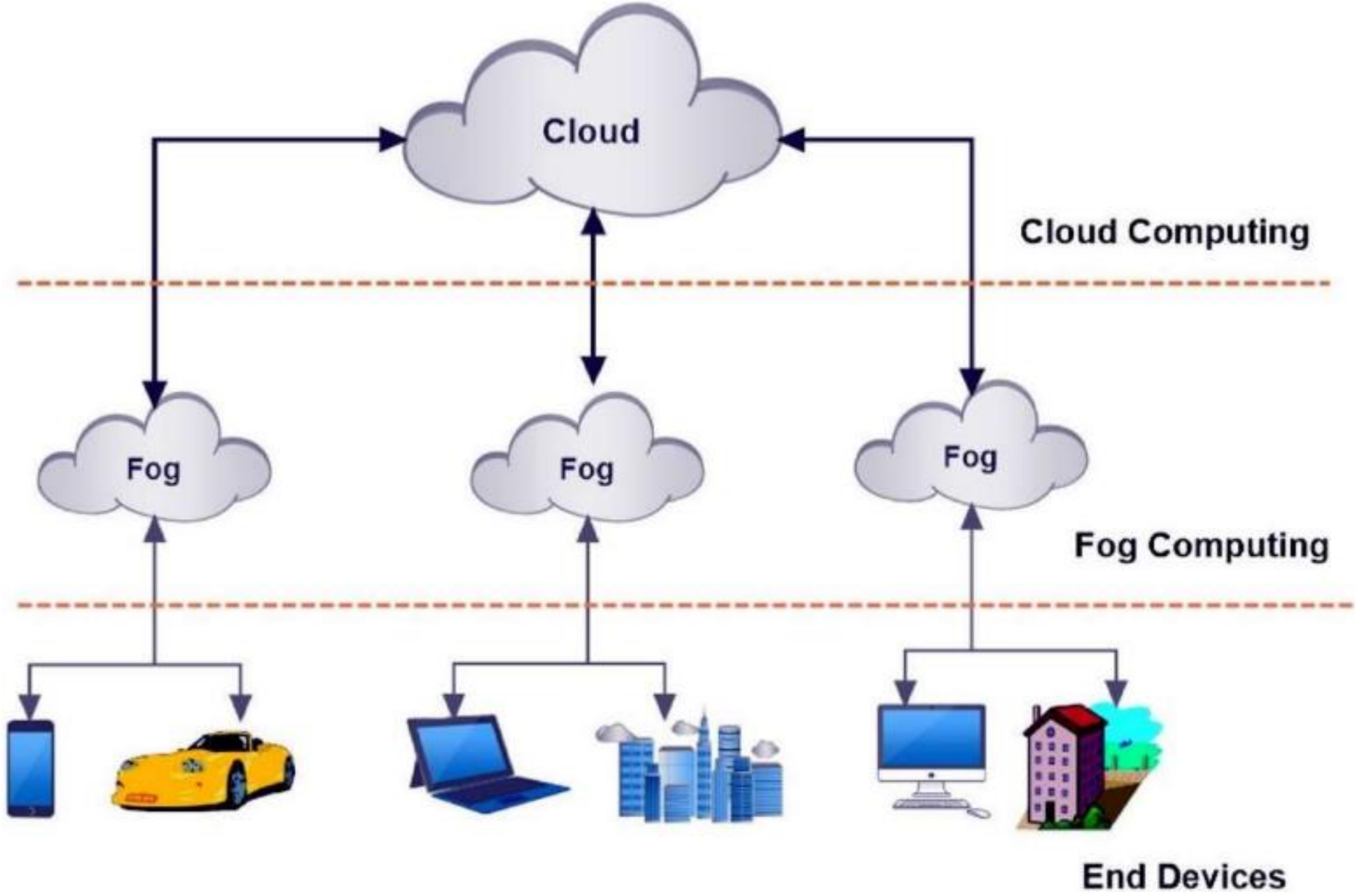
اکوسیستم اینترنت اشیاء – بستر ابری

مدل سرویس ابرو تقسیم وظایف امنیتی- ارائه شده توسط ENISA



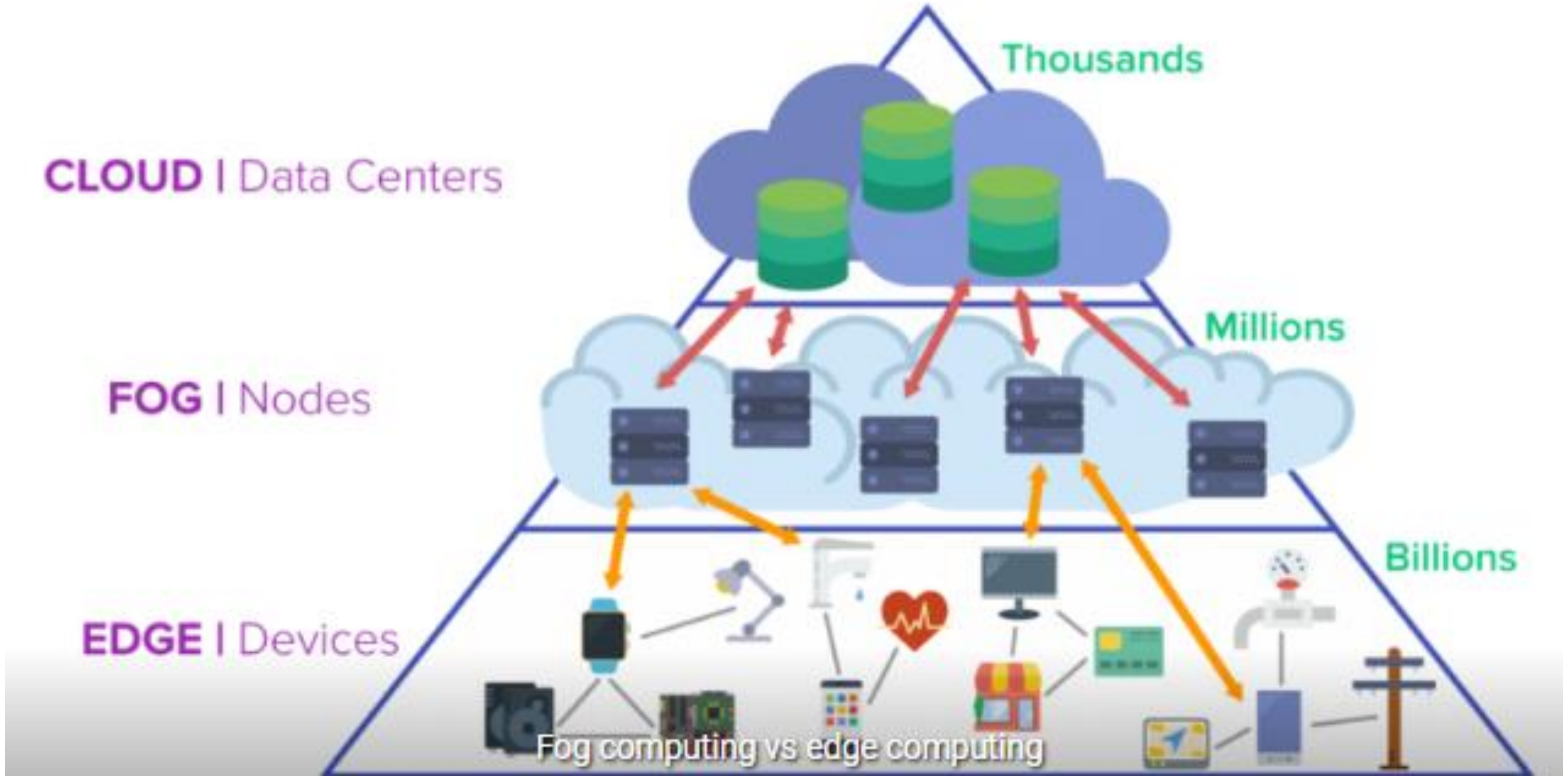
اکوسیستم اینترنت اشیاء – بستر ابری

Cloud / Fog / Edge



اکوسیستم اینترنت اشیاء – بستر ابری

Cloud / Fog / Edge



Examples of Cloud Storage systems:

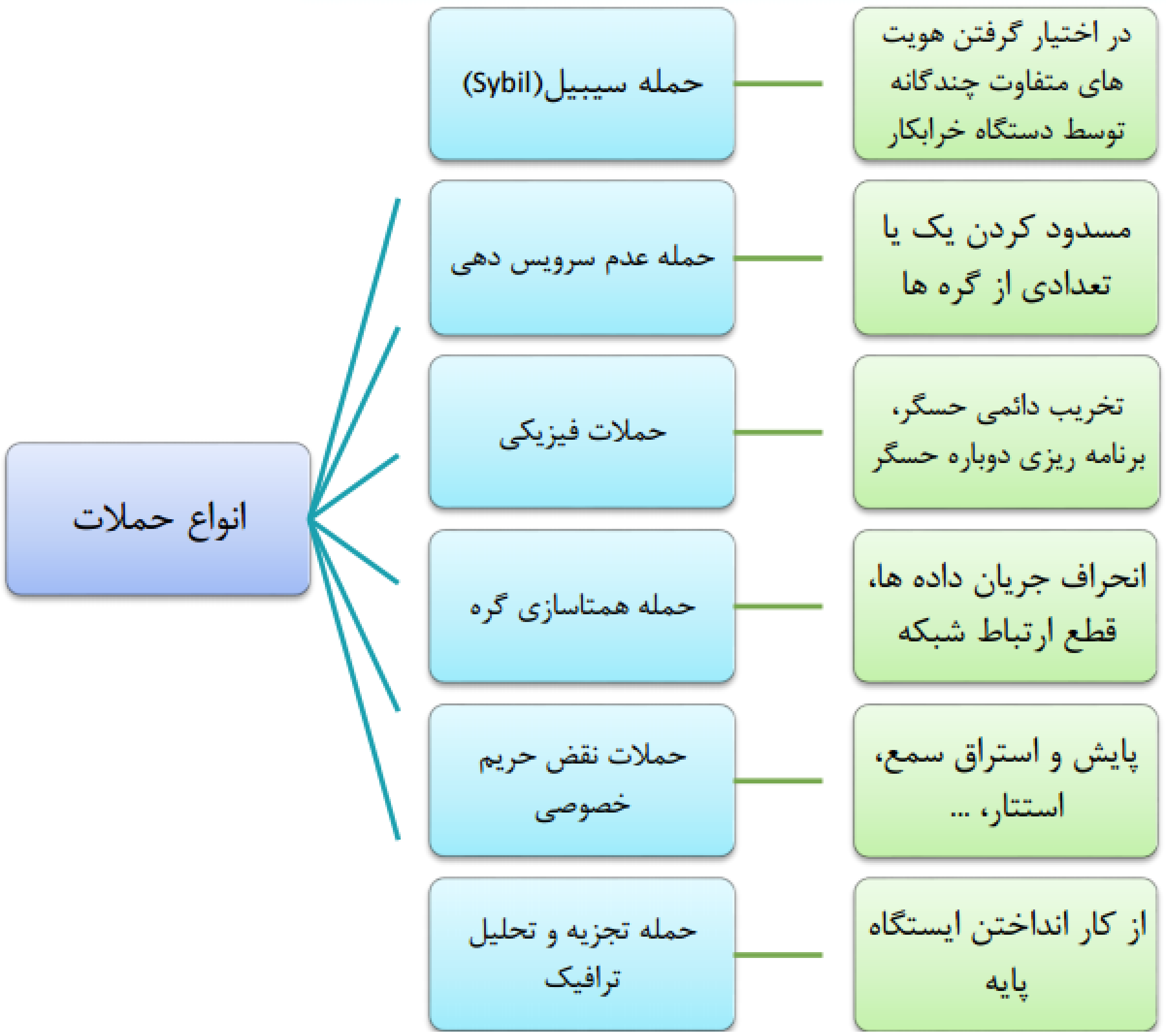
Dropbox

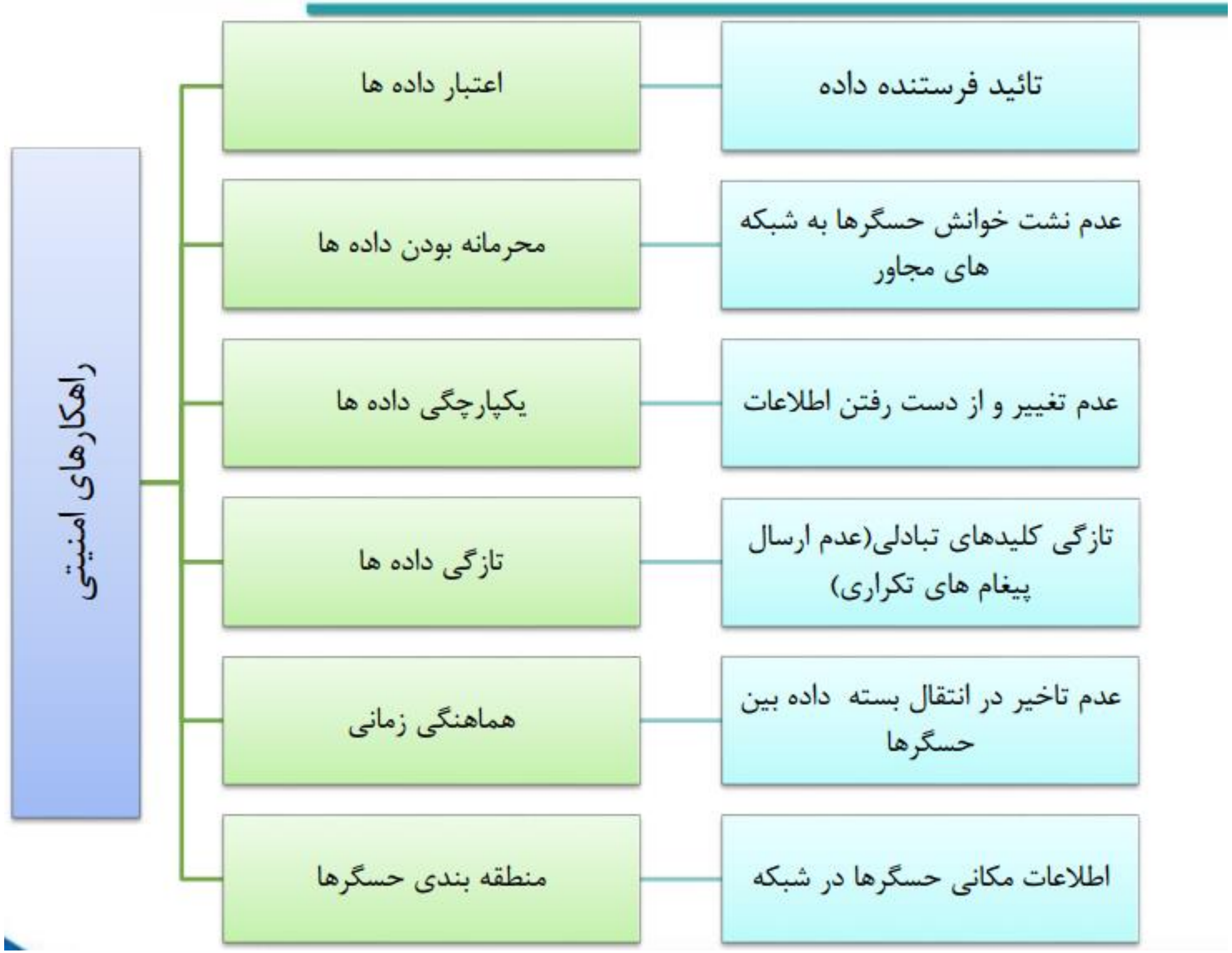
box

iCloud

Google Docs

SkyDrive


انواع حملات
حمله سیبیل(Sybil)
در اختیار گرفتن هویت های متفاوت چندگانه توسط دستگاه خرابکار
حمله عدم سرویس دهی
مسدود کردن یک یا تعدادی از گره ها
حملات فیزیکی
تخریب دائمی حسگر، برنامه ریزی دوباره حسگر
حمله همتاسازی گره
انحراف جریان داده ها، قطع ارتباط شبکه
حملات نقض حریم خصوصی
پایش و استراق سمع، استتار، ...
حمله تجزیه و تحلیل ترافیک
از کار انداختن ایستگاه پایه


راهکارهای امنیتی
اعتبار داده ها
تائید فرستنده داده
محرمانه بودن داده ها
عدم نشت خوانش حسگرها به شبکه های مجاور
یکپارچگی داده ها
عدم تغییر و از دست رفتن اطلاعات
تازگی داده ها
تازگی کلیدهای تبادلی(عدم ارسال پیغام های تکراری)
هماهنگی زمانی
عدم تاخیر در انتقال بسته داده بین حسگرها
منطقه بندی حسگرها
اطلاعات مکانی حسگرها در شبکه

پلتفرم های IOT و IIOT

عامل مدیریت مرکزی با قابلیتهای مختلف از تحلیل و نمایش داده گرفته، تا پردازش پیشرفته داده، امنیت، مصورسازی، حسابرسی و …	PaaS با قابلیت توسعه برنامه کاربردی	GW موجود در محیط	سیستم عامل موجود در محیط

پلتفرم های IOT و IIOT

پلتفرم های تجاری

Cisco ،IBM ،Microsoft ،Intel، Bosch ،Google ،ARM ،GE ، AT&T ،Oracle ،HP ،Amazon ، Samsung , …

پلتفرم های متن باز

Hub-of-All-ThingsیاHAT ، LinkSmart ،OpenIoT ، OpenRemote ،TerraSwarm ، Ericsson IoT-Framework ، ThingSpeak ،AirVantage، Exosite ،NinjaBlock ،Device Hub ،Mango ،Nimbits ، SiteWhere , …

سیستم عاملهای اینترنت اشیاء

،Contiki ،AllJoyn ، RIOT Spark ،Raspbian, …

پلتفرم های IOT و IIOT

پلتفرم های اینترنت اشیا و کاربردهای آن

نام شرکت	نام محصول	چیستی محصول	کاربرد محصول
	Cisco Application Enablement Platform	ارائه‌دهنده زیرساختی برای میزبانی برنامه‌های کاربردی و پویایی برنامه‌های کاربردی بین ابر و مه (Fog) و میان افزار	• پلتفرم های نفتی • خانه هوشمند • شهرهای هوشمند • ساخت ربات ها • ساخت و ساز هوشمند
	Cisco Jasper	PaaS و مرکز کنترل سرویس‌ها	• خانه هوشمند
IBM	IBM Watson	واتسون پلتفرم ساخت، راه‌اندازی (launch) و مدیریت اپلیکیشن‌ها و راهکارهای IoT است. پلتفرم اینترنت اشیاء با تمرکز بر لایه ارتباطی و توسعه اپلیکیشن ها با استفاده از محصول IBM blumix که پلتفرم ابری IBM است (تاکید این راهکار بر روی PaaS، مدیریت اتصال و دستگاه-ها، مدیریت داده، تحلیل داده و مدیریت ریسک است).	• ساختمان هوشمند • هوشمندسازی مزارع و کارخانه ها و ماشینهای هوشمند • حمل و نقل • اپلاینسهای متصل
Intel	Intel® IoT Platform	پلتفرم اینترنت اشیاء با تمرکز بر لایه ارتباطی	• خانه هوشمند • خودرو هوشمند

پلتفرم های IOT و IIOT

پلتفرم های اینترنت اشیا و کاربردهای آن

Bosch	Bosch IoT Suite	Bosch IoT Suite یک PaaS است که تمام قابلیت های میان افزارهای لازم برای ساختن برنامه های کاربردی از بالا به پایین را فراهم می‌کند.	• شهرهای متصل • صنایع متصل • خانه ها و ساختمان های متصل • حمل و نقل متصل • انرژی متصل
	Google Cloud platform	پلتفرم گوگل بخشی از ابر گوگل است که با استفاده از زیرساخت‌های گوگل، تحلیل داده‌ها و یادگیری ماشین را انجام می‌دهد.	• شهر هوشمند
	Google Brillo	پلتفرمی مختص پروژه خانه هوشمند که گجت‌های IOT را با یکدیگر، تلفن‌ها، تبلت‌ها و ابر لینک (مرتبط) می‌کند.	• خانه هوشمند
ARM	ARM mbed	فراهم‌کننده پلتفرم اینترنت اشیاء ARM mbed، سیستم عامل، سرویس‌های ابری، ابزار و اکوسیستم توسعه‌دهندگان تا بتوانند راهکارهای IoT را پیاده‌سازی و مستقر کنند.	• شهر هوشمند • خانه هوشمند (تجاری نشده) • پوشیدنی‌ها
AT&T	AT&T M2X	پلتفرم اینترنت اشیاء با تمرکز بر لایه ارتباطی و ذخیره‌سازی داده‌ها و برروی زیرساخت ابری	• راهکارهای مربوط به خودرو و وسایل نقلیه • مدیریت سرمایه و بازرگانی • شهرهای هوشمند • مراقبت‌های سلامتی و درمانی

پلتفرم های IOT و IIOT

پلتفرم های اینترنت اشیا و کاربردهای آن

Oracle	Oracle IoT	پلتفرم اینترنت اشیاء اوراکل، یک راهکار انتها به انتها برای معماری IoT و مقرون به صرفه، مقیاس‌پذیر و رقابتی است که PaaS ارائه می‌دهد.	• خدمات رفاهی • ساخت و ساز و مهندسی • بهداشت و مراقبت از سلامت • بیمه
HP	HPE IoT	ارایه یک پلتفرم IoT با تمرکز بر داده	• شهر هوشمند • نورپردازی هوشمند در سطح شهر • اندازه‌گیری هوشمند (در زمینه انرژی) • خودروهای متصل
Amazon	AWS IoT	پلتفرمی ابری برای تحلیل و مدیریت اینترنت اشیاء	• شهر هوشمند • انرژی • سیستم های ایمنی • خانه هوشمند • مراقبت های بهداشتی و سلامت
	The Azure IoT suite	پلتفرم بر پایه ابر مایکروسافت و با تمرکز بر لایه کنترل مرکزی و مدیریت و تحلیل داده‌های بزرگ به صورت بلادرنگ	• پایش از راه دور • پیش‌بینی تعمیرات
	Microsoft Soliar	پلتفرمی با تأکید بر ویژگی کیت توسعه اپلیکیشن‌هاست.	• smartfactoryadvisor
	Microsoft Research Lab of Things	یک پلت‌فرم برای تحقیقات آزمایشگاهی که راهکار ارتباطات داخلی بین دستگاه‌ها را ممکن می‌سازد و سناریوهای کاربردی را پیاده‌سازی می‌کند.	• مراقبت سلامت، • مدیریت انرژی، • خودکارسازی خانه
GE	predix	جمع‌آوری داده از ماشینهای صنعتی در محیط و تحلیلهایی در مقیاس صنعتی برای مدیریت عملکرد دارایی (APM) و بهبود عملیات با فراهم نمودن یک راه استاندارد برای اتصال	• هوشمندسازی ماشین آلات پیاده‌سازی

پلتفرم های IOT و IIOT

- **(H.A.T) Hub-of-All-Things**

یک پروژه چندرشته ای دانشگاهی است که از سال ۲۰۱۳آغاز به کار کرده است و در حال حاضر شش دانشگاه انگلیس روی آن کار میکنند. هدف اولیه این پروژه ایجاد یک پلتفرم خاص بازار چندوجهی است که فرصتهای خاص یک اقتصاد و تجارت جدید را با استفاده از داده های تولید شده در یک «خانه هوشمند» فراهم کند. این پروژه امکان مدیریت و کنترل داده توسط کاربر و کنترل دسترسی به دادهها را فراهم میکند.

پلتفرم های IOT و IIOT

- **OpenIoT**

یک پلتفرم متن باز و کاملاً نامتمرکز است که امکان شبکه شدن دستگاه ها را فراهم میکند. این پلتفرم مکانیزم پرداخت برای استفاده از سرویس ها را نیز ارائه میکند.

پلتفرم های IOT و IIOT

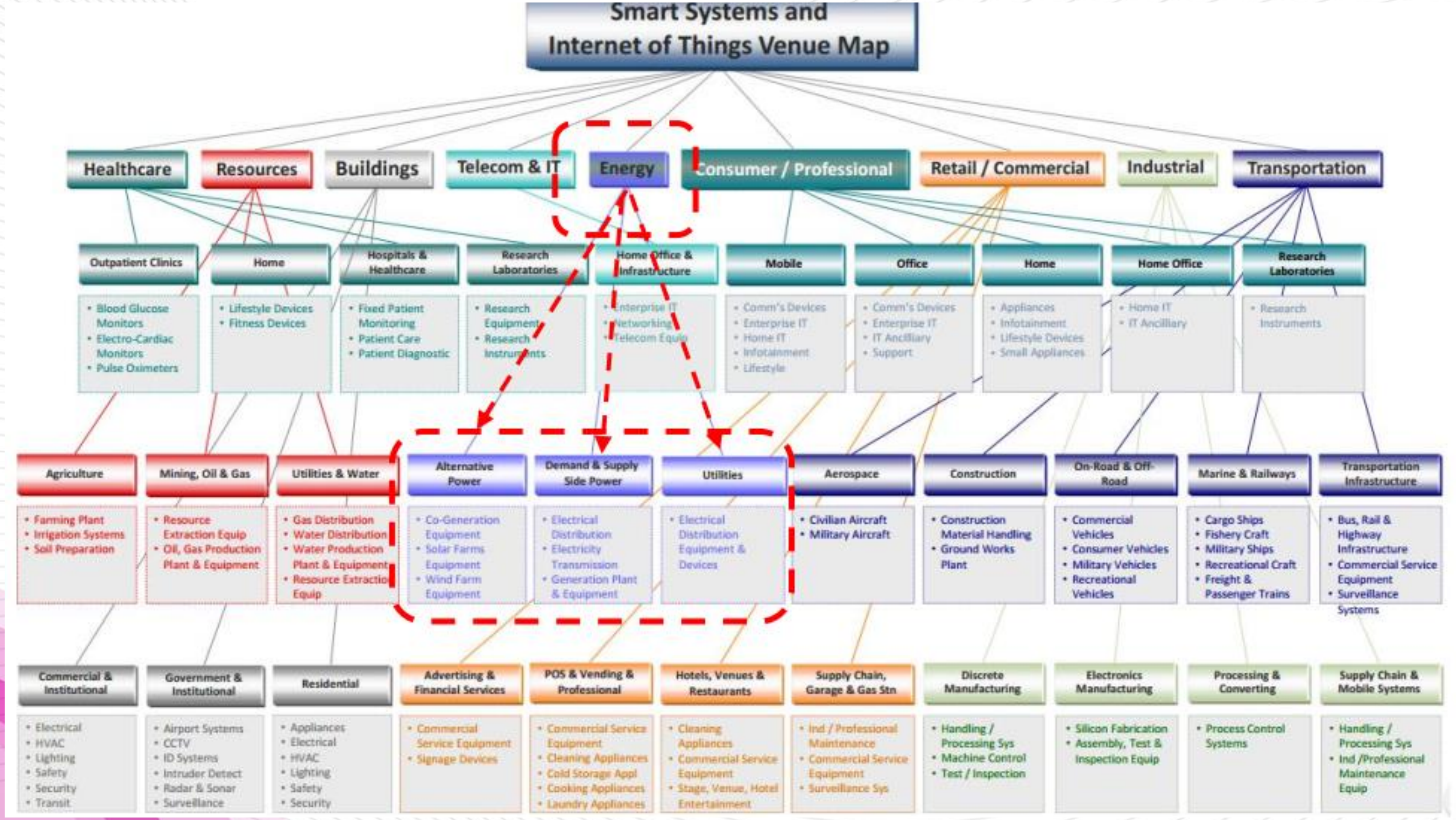
- **Mango**

Mango نرم افزار متن باز ماشین به ماشین مبتنی بر وب است که چندین پلتفرم را پشتیبانی میکند.

- ویژگیهای کلیدی آن عبارتند از: پشتیبانی از چندین پروتکل و پایگاه داده، قابلیت تعریف رخداد توسط کاربر و استخراج/وارد کردن داده

کاربردهای اینترنت اشیا

سیستم های هوشمند و نمودار اینترنت اشیاء



کاربردهای عمده اینترنت اشیاء

ارتباطات و فناوری اطلاعات

صنعت سلامت، بهداشت و پزشکی

صنعت حمل و نقل

نظامی

شهر هوشمند

حوزه انرژی و صنایع وابسته

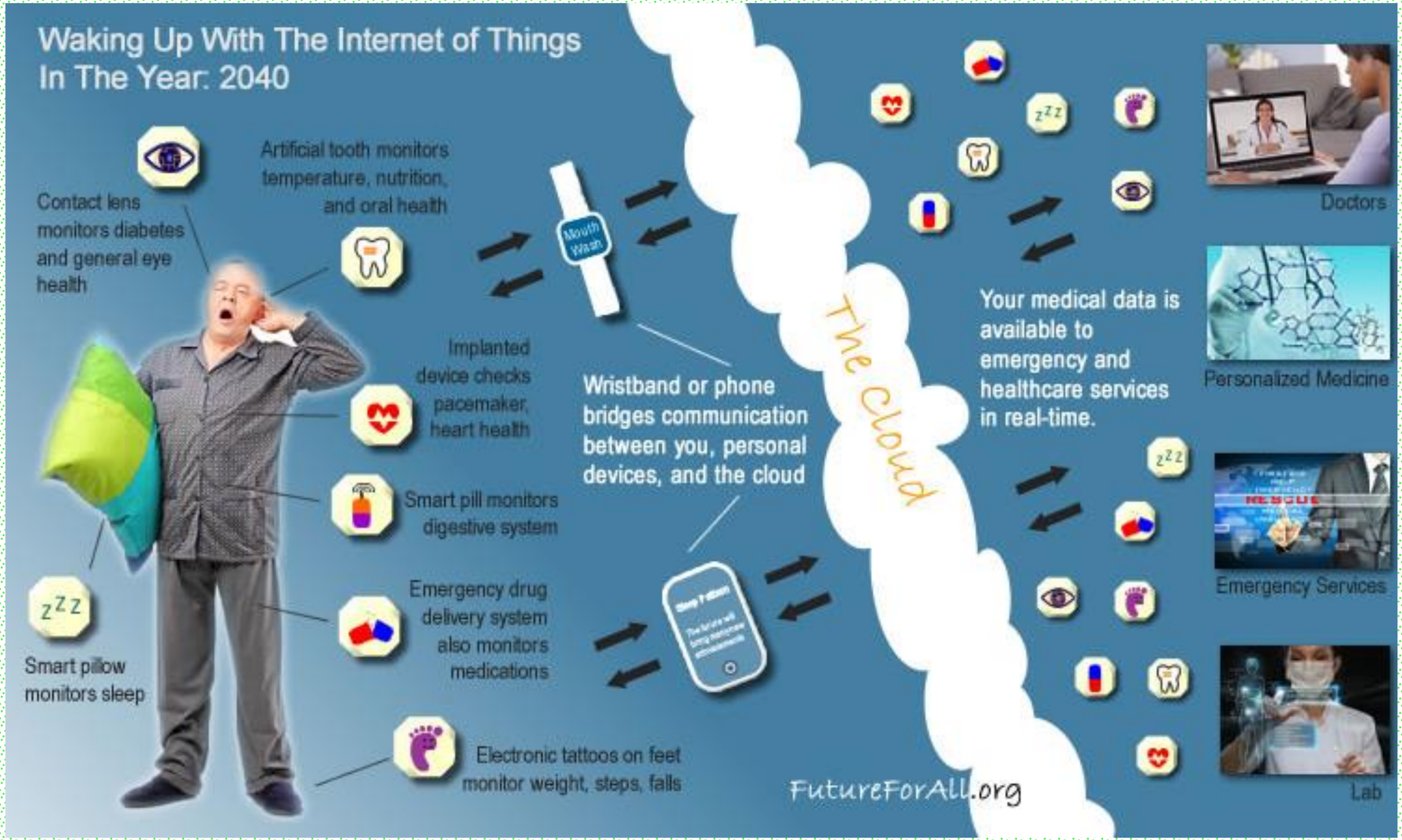
کاربردهای اینترنت اشیاء

سلامت، بهداشت و پزشکی

- جمع‌آوری داده‌های مرتبط با علائم حیاتی بیمار از طریق شبکه سنسورهای متصل به تجهیزات پزشکی و بدن بیمار
- ارسال داده‌های جمع‌آوری شده به بستر ابری مرکز پزشکی مربوطه (برای مثال، یک بیمارستان) برای ذخیره‌سازی و پردازش آنها
- تحلیل و مدیریت اطلاعات فراهم‌شده از طریق سنسورها
- تضمین دسترسی فراگیر (از هر جا و در هر زمان) و به اشتراک‌گذاری داده‌های پزشکی
- ارسال محتوای هوشمند به کاربر
- جمع‌آوری پارامترهای خاص مرتبط با بیماری‌های مزمن و شایع به صورت دوره‌ای
- هزینه های درمانی به طور قابل ملاحظه ای کاهش یافته و نتایج درمان بهبود می یابد
- کاشت تراشه‌های ارتباطی

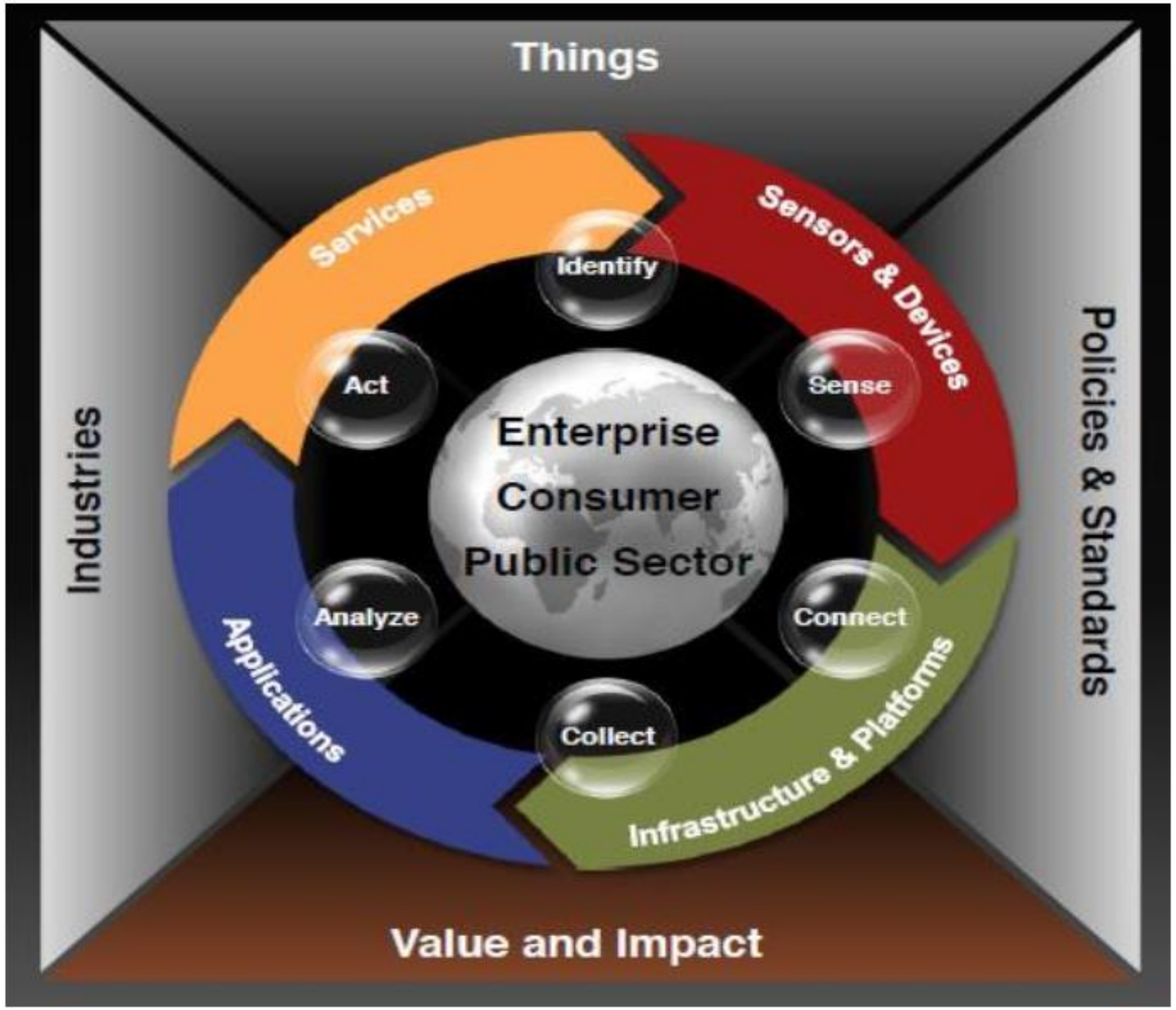
کاربردهای اینترنت اشیاء

سلامت، بهداشت و پزشکی



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

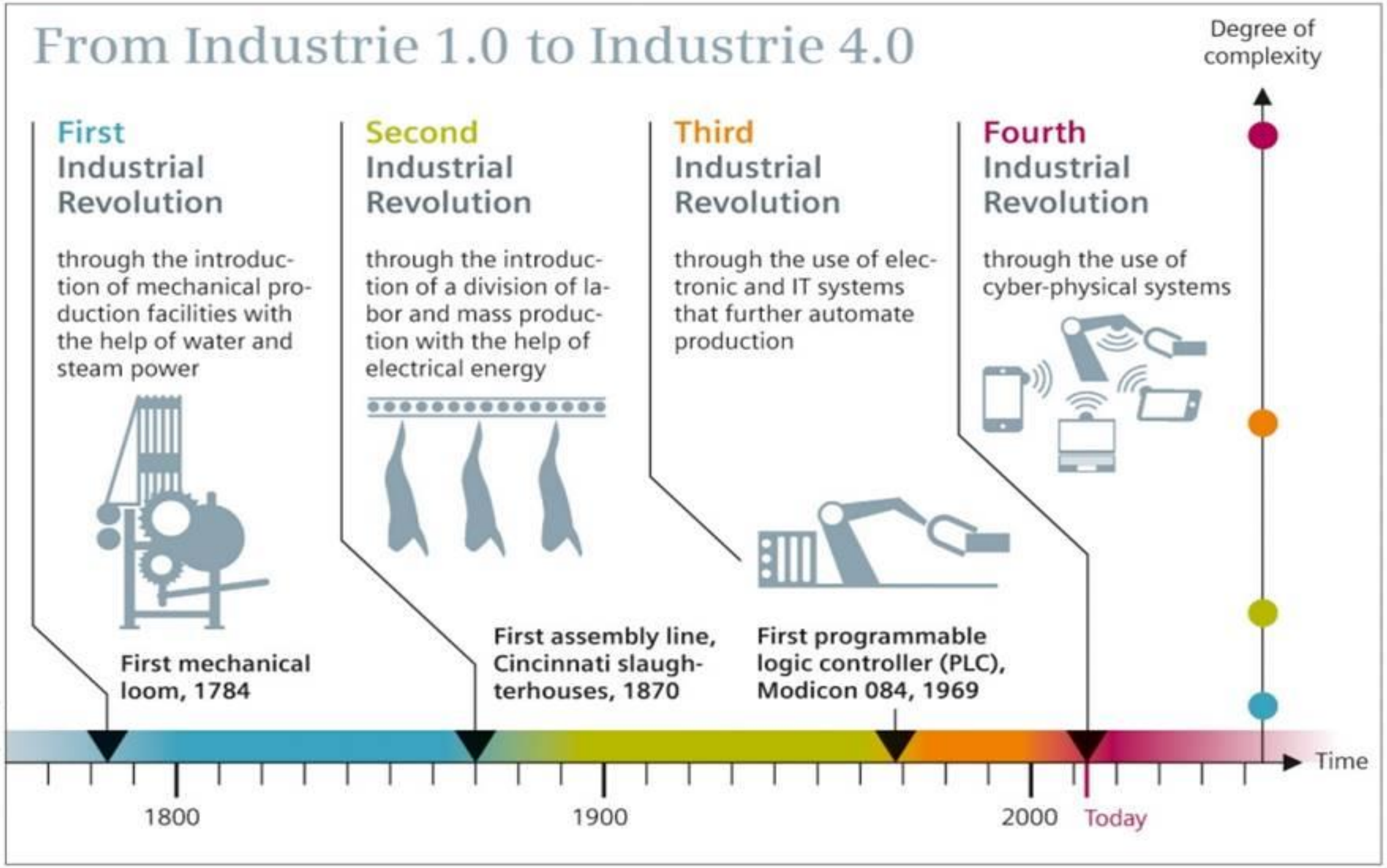


برخی از لایه های اینترنت اشیاء

کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

انقلاب چهارم صنعتی مبتنی بر فضای سایبری



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

- در نسل جدید صنعت، راهکار اینترنت اشیا در محیط های صنعتی (IIoT) منجر به توسعه سیستم های نوآورانه و کارآمد با هدف افزایش بهـره وری عملیـاتی و کاهش چشمگیر هزینه های تولید شده است.
- طیف گسترده ای از برنامه های کاربردی اینترنت اشـیا، تحـت چـارچوب هـای متفـــــاوتی بـــــه وجـــــود آمـــــده اســـــت

کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

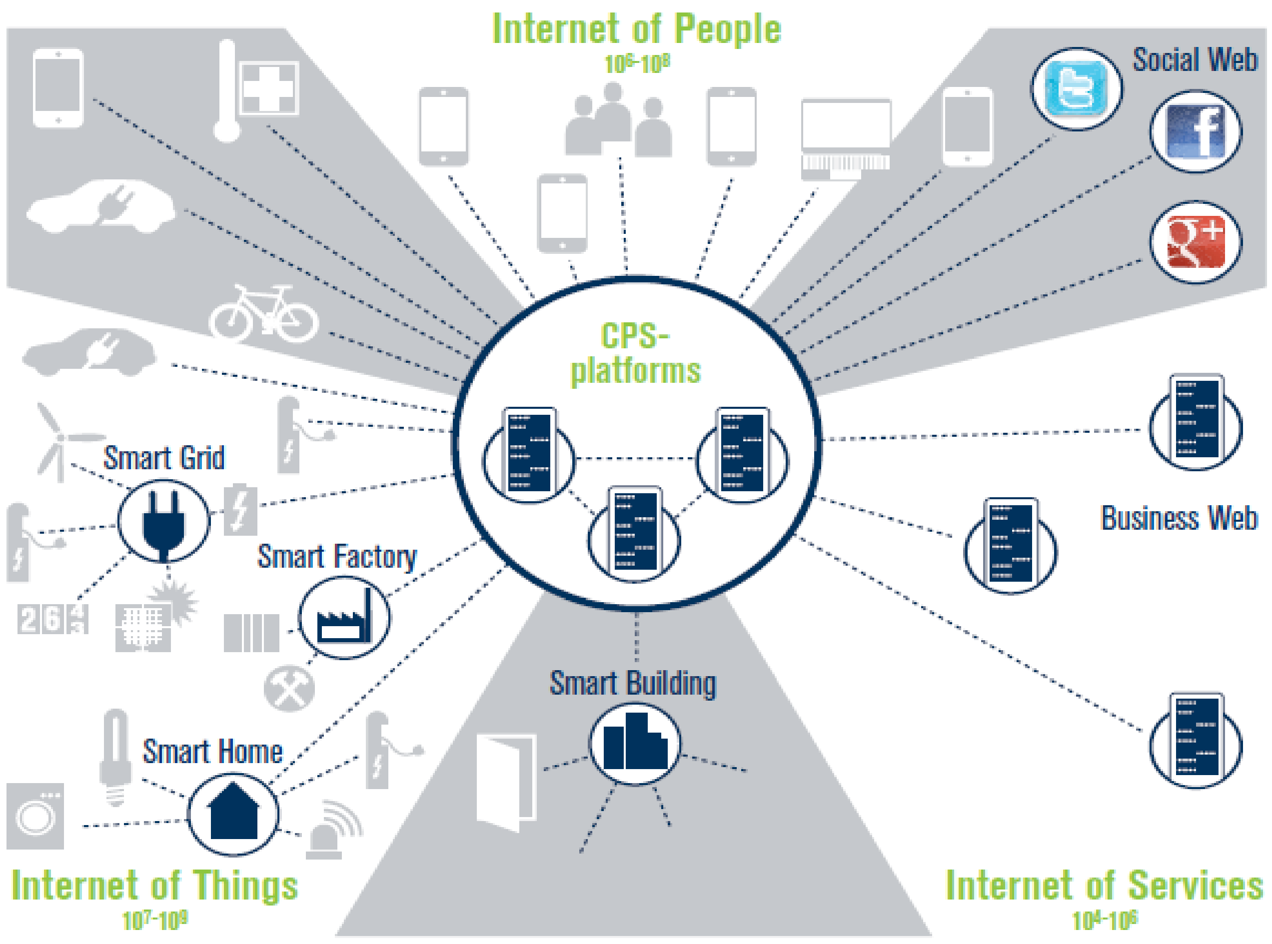
- صنعت ۴.۰ اصطلاحی است در برگیرنده مفاهیم فناوری و زنجیره ارزش، که برمبنای مفـاهیم نوینی نظیر سیستم‌های سایبری–فیزیکی، اینترنت اشیاءو اینترنت خدمات، شکل گرفته اسـت. صنعت ۴.۰ راهکار جامعی‌است که ایجاد کارخانه هوشمند را ممکن می‌سازد.

- Industry 4.0
- Cyber-Physical Systems (CPS)
- Internet of Things
- Internet of Services

- تمرکززدائی، رایانش بی‌درنگ و انعطاف پذیری گسترده در خدمات

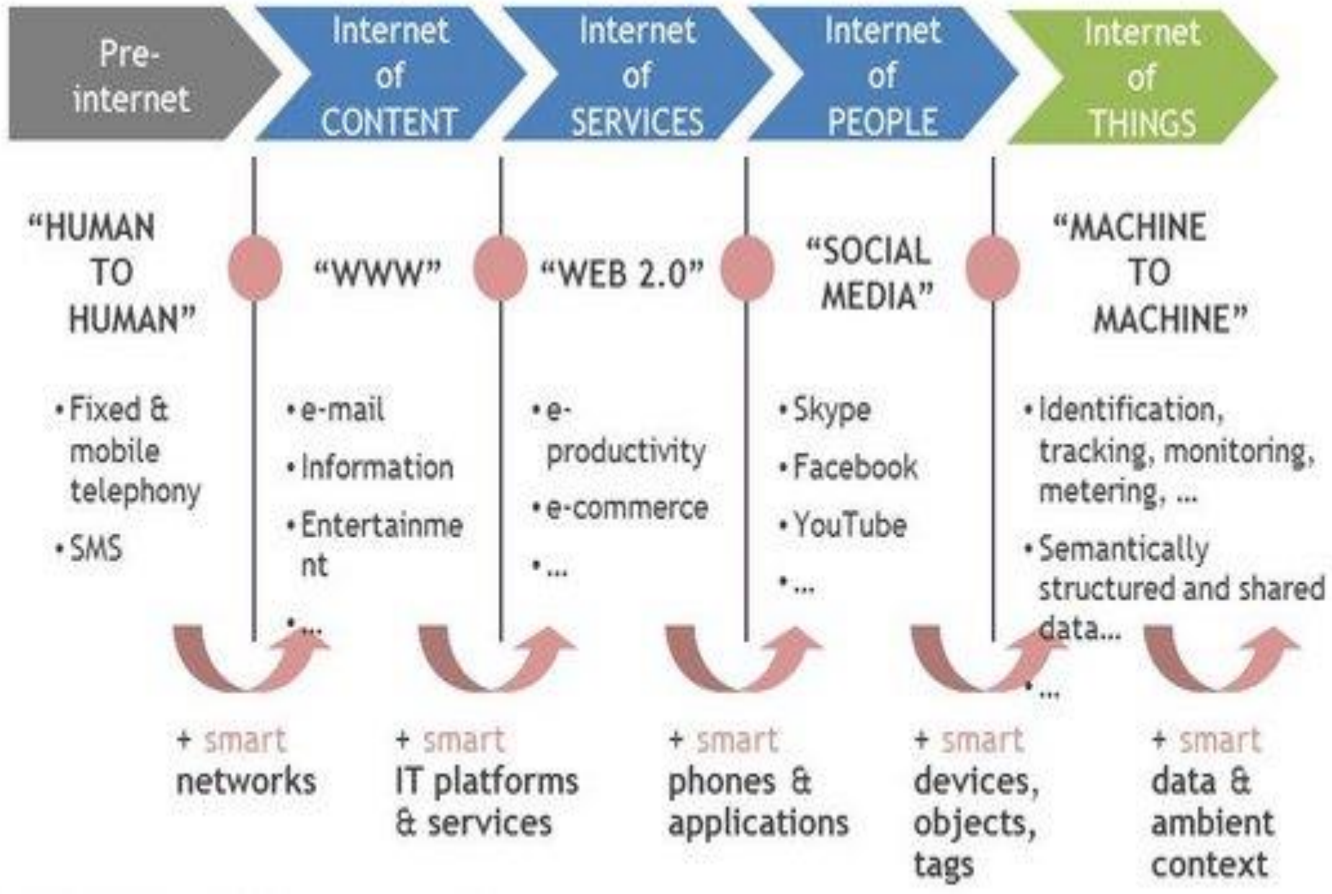
کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)



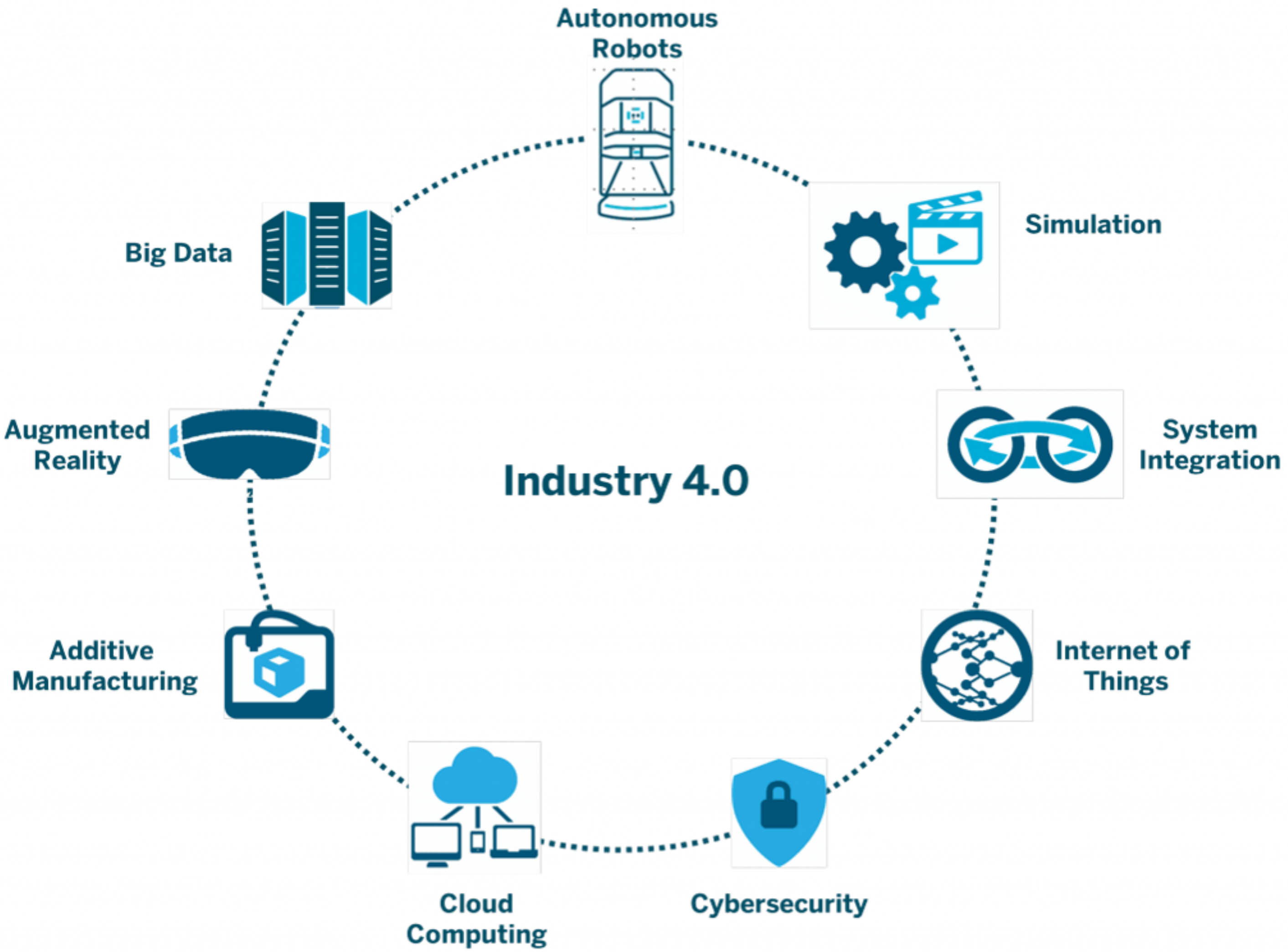
کاربردهای اینترنت اشیاء- زیرساخت های صنعتی (IIOT)

سیر تکاملی اینترنت و دستیابی به صنعت ۴.۰



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

- انقلاب صنعتی چهارم با کاربرد سیستم‌های سایبرفیزیکی در کارخانه‌ها شناسایی می‌شود. کارخانه‌های هوشمند با استفاده از CPS قادر خواهند بود همه فرآیندهای تولید و قطعات را از طریق شبکه‌های دیجیتال مورد پیگیری قرار دهند و تلفیق افقی کارآمدتری در زنجیره‌های تامین ایجاد می‌گردد.
- اتحادیه اروپا نیز در پروژه Horizon 2020 اقدامات موثری را در دستور کار خود قرار داده است که با سرمایه بالغ بر ۸۰ میلیارد یورو از سال ۲۰۱۴ تا ۲۰۲۰ اجرا خواهد شد. هدف این اقدام یک طیف گسترده از تحقیق و پژوهش از جمله۱۳.۵ میلیارد یورو متمرکز بر توسعه فناوری‌های صنعتی، ۳ میلیارد یورو برای بنگاه‌های تجاری کوچک و متوسط با رهبری فناوری‌های صنعتی و ۲.۸ میلیارد یورو برای پرکردن فاصله نوآوری بین جامعه دانشگاهی و توسعه تجاری فناوری می‌باشد.

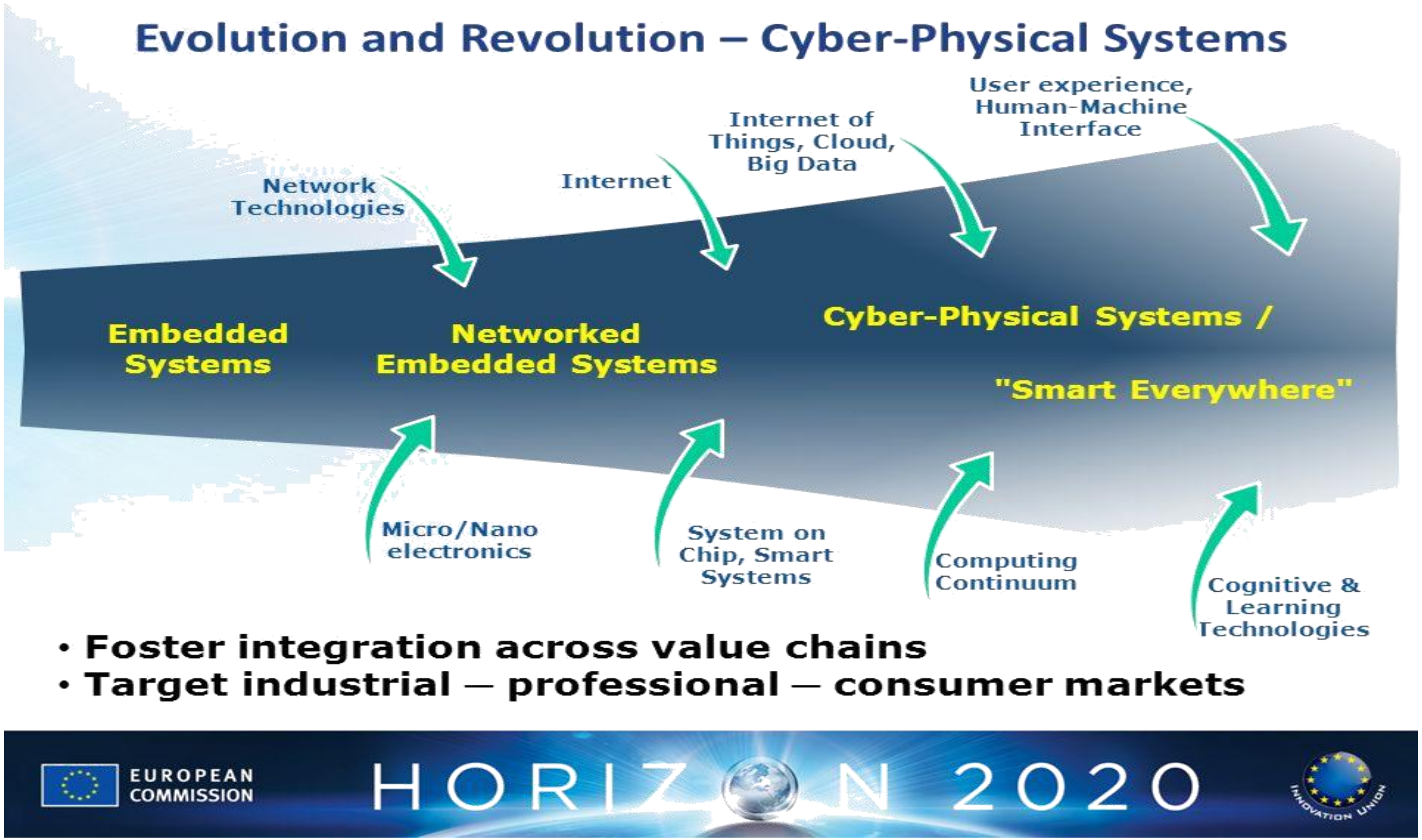
کاربردهای اینترنت اشیاء

سیستم‌های سایبری- فیزیکی و انقلاب چهارم صنعتی

- سیستم‌های سایبر- فیزیکی دنیای کاملا شبکه‌ای را خلق می‌نمایند که در آن، اشیاء هوشمند با یکدیگر ارتباط و تعامل برقرار می‌کنند.
- سیستم‌های سایبر-فیزیکی بیانگر گام تکاملی دیگری نسبت به سیستم‌های تعبیه شده موجود هستند.
- سیستم‌های تعبیه شده با اینترنت و داده‌ها و خدمات آنلاین موجود، تلفیق می‌شوند تا سیستم‌های سایبر فیزیکی را شرح دهند.

کاربردهای اینترنت اشیاء

سیستم‌های سایبری – فیزیکی و انقلاب چهارم صنعتی



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

برخی از مهمترین موارد هوشمند سازی زیرساخت ها در دنیا :

برزیل

- بزرگترین بازار را از لحاظ تعداد ارتباطات M2M در آمریکای لاتین
- بهره بردن از ۹.۹ میلیون اتصال ۶۶ درصد از ارتباطات M2M آمریکای لاتین در سال ۲۰۱۶

چین

- راه اندازی طرحی با نام حمایت ویژه از تحقیق و توسعه اینترنت اشیاء صنعتی با هزینه ۷۷۴ میلیون دلار و در بازه زمانی ۲۰۱۱ تا ۲۰۱۵

آلمان

سرمایه گذاری ۲۲۱ میلیون دلاری برای حمایت از صنعت، دانشگاه و تحقیق و توسعه در جهت پیشبرد زیرساخت های هوشمند

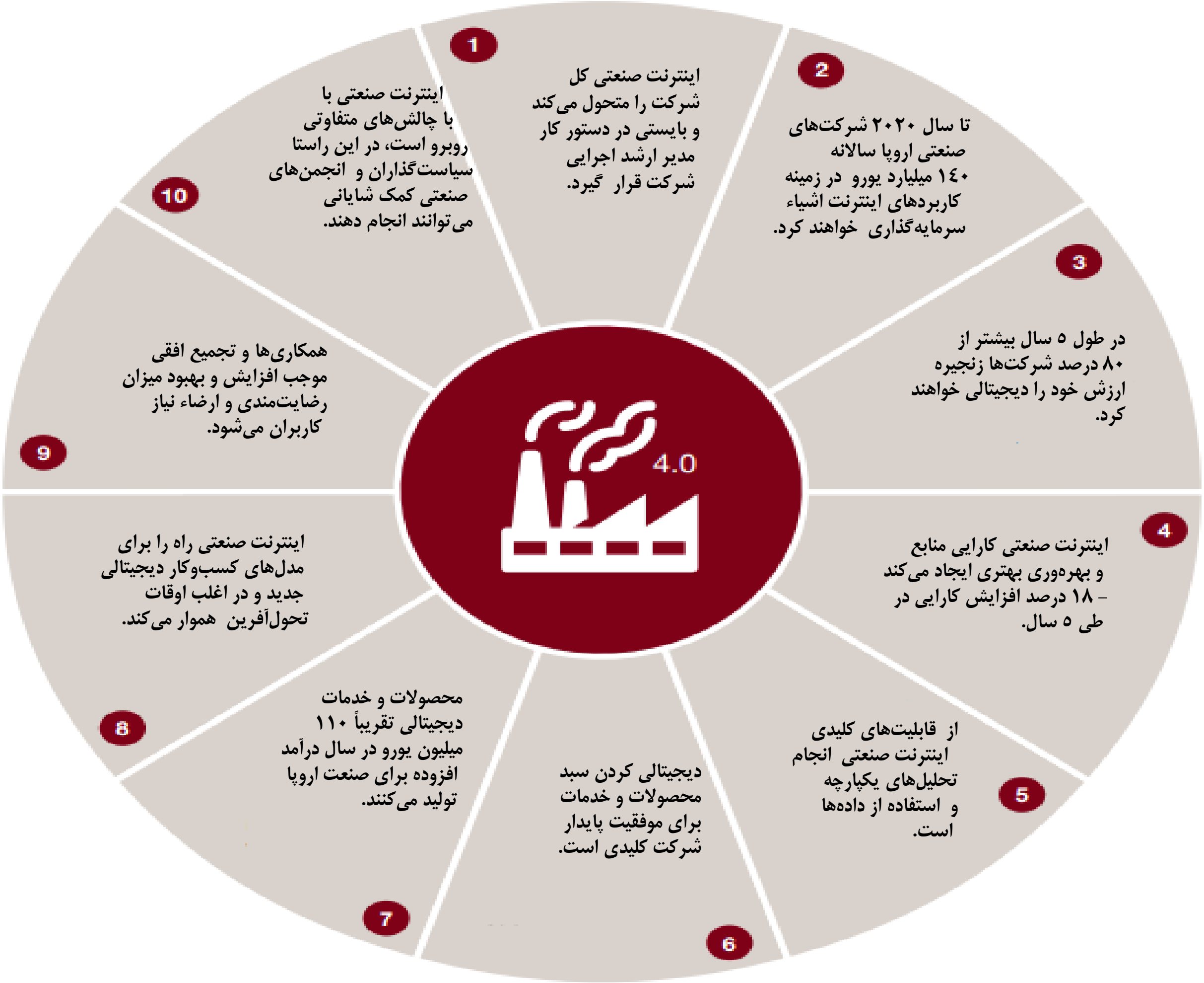
کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

کشور	میزان سرمایه گذاری در حوزه هوشمند سازی زیرساختی
چین	۷۷۴ میلیون دلار طی ۵ سال
هند	۷.۴ میلیارد دلار طی ۵ سال
آلمان	۲۲۱ میلیون دلار طی سال ۲۰۱۷
کره جنوبی	۵ میلیارد دلار طی ۵ سال
آمریکا	۲۰۰ میلیون دلار طی سال ۲۰۱۶
سنگاپور	۶.۱ میلیارد دلار طی ۵ سال

کاربردهای اینترنت اشیاء

اینترنت اشیاء صنعتی در کشور آلمان



کاربردهای اینترنت اشیاء

زیرساخت های صنعتی (IIOT)

- شرکت هایی نظیر زیمنس و GE فراتر از منافع مفهومی اینترنت اشیا و فرآیندهای خودکار سازی در حال حرکت هستند و در حال حاضر شروع به دریافت داده های غنی تر کرده و به دنبال بهره وری عملیاتی بیشتری هستند. (ارائه راهکارهای BI)
- راه اندازی مرکز اینترنت اشیا صنعتی در مونیخ توسط شرکت IBM

تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیا و هوشمندسازی

آسیب پذیری های سایبری حوزه هوشمند سازی

آسیب پذیری ناشی از عملکرد هر عنصر به تنهایی

آسیب پذیری های ناشی از اجزا و فناوری های مورد استفاده در حوزه هوشمند سازی

آسیب پذیری های ناشی از معماری امنیتی نامناسب ناشی از عدم جانمایی مناسب اجزا و فناوری های مختلف

آسیب پذیری های ناشی از عدم وجود مدیریت یکپارچه و برخورداری از سیاست ها و فرایندهای امنیتی مناسب

آسیب پذیریهای IOT و IIOT

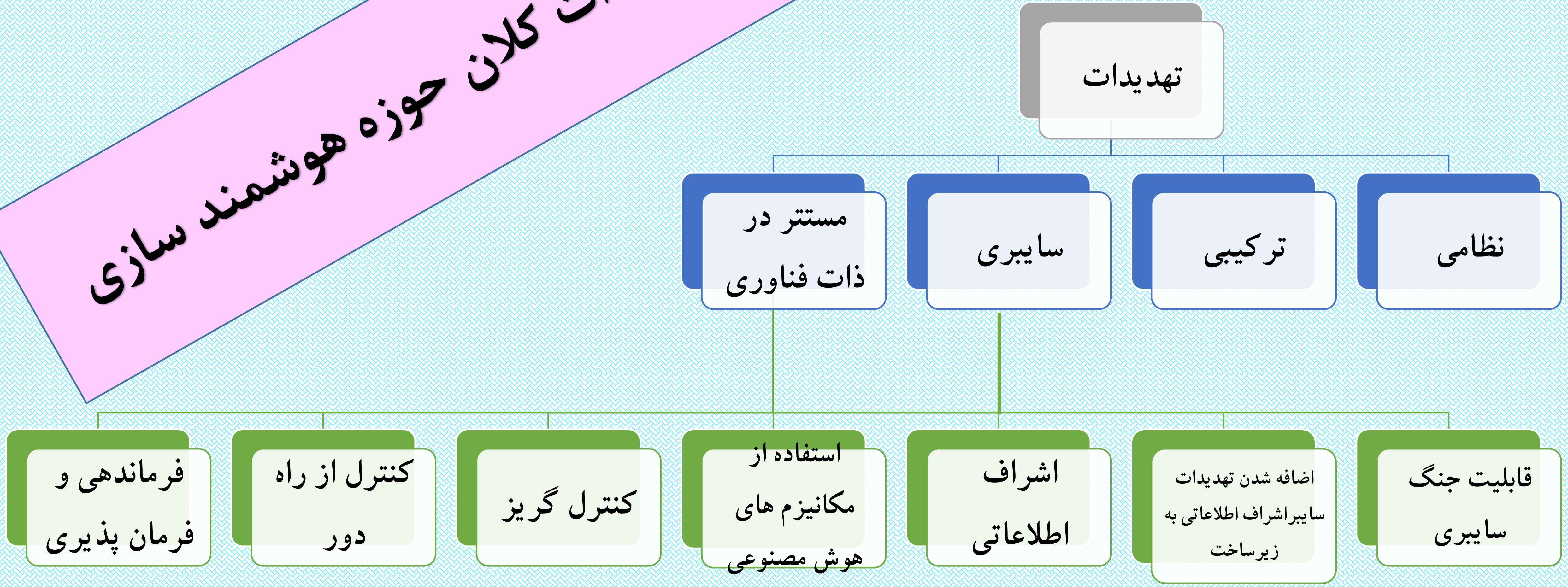
- واسط گرافیکی ناامن
- احراز اصالت و مجوز دهی ناکافی
- سرویس شبکه ناامن
- عدم وجود رمزنگاری در نقل و انتقال
- نگرانی های حریم خصوصی

- رابط ابر ناامن
- رابط موبایل ناامن
- تنظیمات امنیتی ناکافی
- سخت افزار / نرم افزار ناامن
- امنیت فیزیکی ضعیف

چالشهای IOT و IIOT

- نا همگونی و چندگانگی اشیاء، پلتفرمها و شبکه ها
- احراز هویت شبکه های متعدد و ناهمگون
- وجود اشیاء کوچک و ارزان و بدون رعایت نکات امنیتی در ساختار آنها
- زیرساخت کلید خصوصی سبک و قابل استفاده
- مراجع تایید کننده سطح دسترسی، قابلیت اطمینان
- قابلیت پایین برخی الگوریتم های محاسباتی
- انرژی و توان کم حسگرها
- مقیاس پذیری و مدیریت سطح بالا در خصوص پردازش داده های حجیم
- الگوریتم های رمز نیازمند پردازش های قدرتمند و CPU قوی هستند

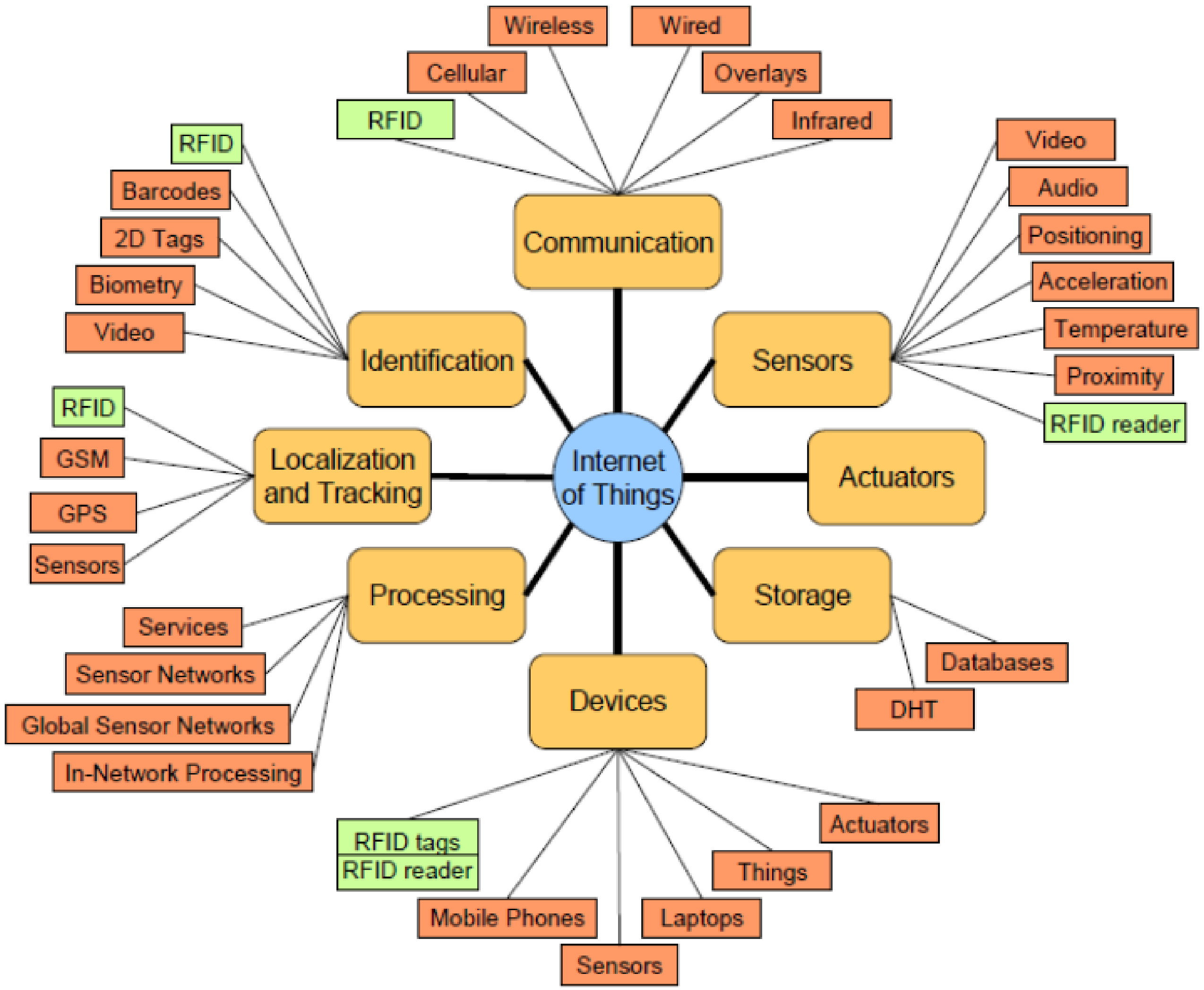
تهدیدات کلان حوزه هوشمند سازی



جنگ سایبری و هوشمند سازی زیرساخت ها

- فضای سایبری پنجمین حوزه نبرد
- استفاده دشمن از قابلیت های نهفته شده در تجهیزات هوشمند بکار رفته در زیرساخت ها
- تسلط دشمن بصورت دومینو وار به تمامی زیرساخت های سایبری و وابسته به سایبر هوشمندسازی شده

طبقه بندی موضوعات و فناوریهای اینترنت اشیاء



تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیای صنعتی

واسط گرافیکی ناامن

موتور تهدید	بردار تهدید	امنیت ضعیف		تاثیر تکنیکی
خاص برنامه‌کاربردی	**بهره‌برداری آسان**	**شیوع معمول**	**آشکارسازی آسان**	**تاثیر شدید**
فرض کنید فردی قصد دسترسی به واسط وبی با خصوصیت کاربر داخلی و خارجی را دارد	مهاجم از اعتبار ضعیف یا اعتبار متن ساده استفاده می‌کند و یا حساب خود را برای دسترسی به واسط وب ارتقاء می‌دهد. حمله می‌تواند از سوی کاربر داخلی یا خارجی صورت گیرد.	واسط گرافیکی ناامن می‌تواند در اثر ارتقاء حساب کاربری، عدم مسدودسازی حساب یا اعتبار ضعیف بوجود آید. واسط ناامن شبکه داخلی را تهدید می‌نماید. هر چند تهدیدات کاربران داخلی به اندازه تهدیدات کاربران خارجی مهم هستند. کشف آسیب‌پذیری واسط وب به‌صورت دستی و همراه ابزار در جهت شناخت حملاتی نظیر cross-site scripting به راحتی امکان‌پذیر است.		از دست دادن داده، خرابی، فقدان مسئولیت، انکار دسترسی از مهمترین عوارض واسط ناامن است و می‌تواند منجر به از کارافتادن سیستم نیز شود.

تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیای صنعتی

احراز اصالت و مجوز دهی ناکافی

موتور تهدید	بردار تهدید	امنیت ضعیف		تاثیر تکنیکی
خاص برنامه‌کاربردی	**بهره‌برداری میانه**	**شیوع معمول**	**آشکارسازی آسان**	**تاثیر شدید**
فرض کنید فردی قصد دسترسی به واسط وب، واسط موبایل یا ابر با خصوصیت کاربر داخلی و خارجی را دارد.	مهاجم از رمزعبور ضعیف، عدم وجود مکانیزم بازیابی رمز عبور، اعتبار حفاظت شده ضعیف یا فقدان سطح بندی دسترسی به واسطها از سوی کابران داخلی یا خارجی، بهره‌برداری می‌نماید.	مجوزدهی ممکن است در هنگام رمز عبور ضعیف و حفاظت نشده، ناکافی باشد. احراز اصالت و مجوزدهی ناکافی در برابر کابران داخل شبکه شایع است. به‌صورت دستی و با استفاده از ابزارهای خودکار می‌توان به راحتی این نوع آسیب‌پذیری را تشخیص داد.		از دست دادن داده، خرابی، عدم مسئولیت، انکار دسترسی از مهمترین عوارض این نوع آسیب‌پذیری است و می‌تواند منجر به از کار افتادن سیستم نیز شود.

تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیای صنعتی

سرویس شبکه ناامن

موتور تهدید	بردار تهدید	امنیت ضعیف		تاثیر تکنیکی
خاص برنامه‌کاربردی	**بهره‌برداری آسان**	**شیوع معمول**	**آشکارسازی آسان**	**تاثیر شدید**
فرض کنید فردی قصد دسترسی به دستگاه از طریق شبکه با خصوصیت کاربر داخلی و خارجی را دارد.	مهاجم از آسیب‌پذیری سرویس شبکه به‌منظور حمله به خود دستگاه استفاده می‌کند.	سرویس شبکه ناامن ممکن است نسبت به حمله سرریز بافر یا انکار سرویس حساس باشد. این نوع تهدید می‌تواند با استفاده از ابزارهای خودکار نظیر پورت اسکنر و fuzzer کشف و شناسایی شود.		از دست دادن داده، خرابی، عدم مسئولیت، انکار سرویس و ... از مهمترین عوارض این نوع آسیب‌پذیری است.

تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیای صنعتی

عدم وجود رمزنگاری در نقل و انتقال

موتور تهدید	بردار تهدید	امنیت ضعیف		تاثیر تکنیکی
خاص برنامه‌کاربردی	**بهره‌برداری میانه**	**شیوع معمول**	**آشکارسازی اسان**	**تاثیر شدید**
فرض کنید فردی از شبکه ای استفاده می‌کند که دستگاهی به آن متصل است. دارای کاربران داخلی و خارجی است.	مهاجم از فقدان رمزنگاری انتقال داده بر روی شبکه استفاده می‌کند. حمله ممکن است از سوی کاربر داخلی یا خارجی باشد.	عدم رمزنگاری باعث نمود داده‌ها در انتقال درون شبکه می‌شود. این موضوع در شبکه‌های محلی و اینترنت به وفور یافت می‌شود. این نوع تهدید به‌آسانی با چک کردن داده‌های آشکار و خواندنی درون شبکه، قابل شناسایی است. علاوه بر آن با استفاده از ابزارهای خودکار می‌توان از پیاده‌سازی مناسب الگوریتم های رمزنگاری نظیر SSL, TLS اطمینان حاصل نمود.		عدم رمزنگاری می‌تواند موجب از دست رفتن اطلاعات شود و بسته به میزان نمایش اطلاعات، می‌تواند منجر به زیان بیشتر به سرویس‌ها و دستگاه‌ها شود.

تهدیدات، آسیب پذیری ها و مخاطرات اجزای اینترنت اشیای صنعتی

رابط ابر ناامن

موتور تهدید	بردار تهدید	امنیت ضعیف		تاثیر تکنیکی
خاص برنامه‌کاربردی	**بهره‌برداری میانه**	**شیوع معمول**	**آشکارسازی اسان**	**تاثیر شدید**
فرض کنید فردی به اینترنت دسترسی دارد.	مهاجم از طریق بردارهای مختلف نظیر احراز اصالت ناکافی، عدم رمزنگاری، ارتقاء سطح دسترسی داده یا کنترل وب سایت ابری و ... عمل می‌نماید. حمله از طریق کاربر داخلی یا خارجی و از طریق اینترنت قابل انجام است.	رابط ابر ناامن زمانی نمود پیدا می‌کند که حدس اعتبارنامه های مورد استفاده، آسان و یا ارتقاء سطح دسترسی امکان‌پذیر باشد. این نوع تهدید به‌آسانی با مرور ارتباطات رابط ابر و SSL مورد استفاده قابل شناسایی است.		رابط ابر نامطمئن می‌تواند منجر به آشکارسازی داده کاربر و کنترل غیرمجاز دستگاه‌ها شود.

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

برخی از ویژگی های معماری امنیتی اینترنت اشیای صنعتی

Autonomous Functionality	Auto-configuration	Scalability
Discoverability	Heterogeneity	Modularity
Unique Identification	Reliability	Security

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

طبقه بندی موضوعات و فناوری های هوشمند سازی و تلاش جهت امن سازی و بومی سازی فناوری ها و تجهیزات حیاتی

لزوم ایجاد معماری امنیتی و پدافندی در تمام سطوح اعم از سطوح کاربری، سطوح هسته شبکه، سطوح محتوا و ... بر اساس معماری امن و لایه به لایه مطابق با سیاست ها و ابلاغیات سازمان پدافند غیرعامل و مبتنی بر متدولوژی دفاع در عمق

لزوم ایجاد مکانیزم های امنیتی و پدافندی مناسب برای مدیریت و حفاظت از پروفایل کاربران در مقابل مکانیزم های داده کاوی و حفظ حریم خصوصی

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

- لزوم لحاظ نمودن موضوع امنیت سایبری در مرحله طراحی، تولید، استقرار، پیاده سازی و ...
- لزوم تعریف دقیق مرز بین حریم خصوصی و امنیت ملی
- لزوم ایجاد مکانیزم های امنیتی و پدافندی مناسب برای مدیریت و حفاظت از پروفایل کاربران در مقابل مکانیزم های داده کاوی و حفظ حریم خصوصی

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

- لزوم راه اندازی مرکزی برای جمع‌آوری، پردازش و مدیریت اطلاعات مربوط به تهدیدات و آسیب-پذیری‌ها و ارائه هشدارهای امنیتی شهر هوشمند (Intelligent Operation Center)
- آموزش، فرهنگ سازی و آگاهی بخشی بهترین روش‌ها و دستورالعمل‌های امنیتی
- لزوم تدوین استانداردهای امنیتی برای اجزای مختلف مورد استفاده در شهر هوشمند جهت استفاده از این فناوری ها در سطوح مختلف شهر هوشمند

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

لزوم بکارگیری وجوه مختلف حفظ محرمانگی مانند محرمانگی اطلاعات، محرمانگی کاربران، محرمانگی پروفایلینگ و ... را مطابق با سیاست ها و ملاحظات ابلاغی

لزوم ارزیابی تجهیزات، شبکه، ارتباطات و پروتکل های مورد استفاده در شهر هوشمند بطور اخص در حوزه زیرساخت های حیاتی و حساس بنا بر الزامات و ملاحظات سازمان پدافند غیرعامل کشور

اصلاح و بروزرسانی قوانین داخلی موجود و پرداختن به خلأهای قانونی

الزامات و ملاحظات کلان پدافند سایبری در حوزه هوشمند سازی

- الزام در نظر گرفتن اصول حریم خصوصی در مرحله طراحی، تولید، استقرار، پیاده سازی و ...

- لزوم لحاظ نمودن موضوعات حقوقی مربوط به طیف فرکانسی، نامبرینگ، سوییچینگ، آدرس دهی و رومینگ

- لزوم ایجاد مکانیزمی برای نگهداری تمامی لاگ ها، رخدادها، هشدارها و ... در سطوح مختلف اعم از کاربری، هسته، محتوا و ... با رعایت اصول پدافندی مانند Signing، Time Stamp، Indexing

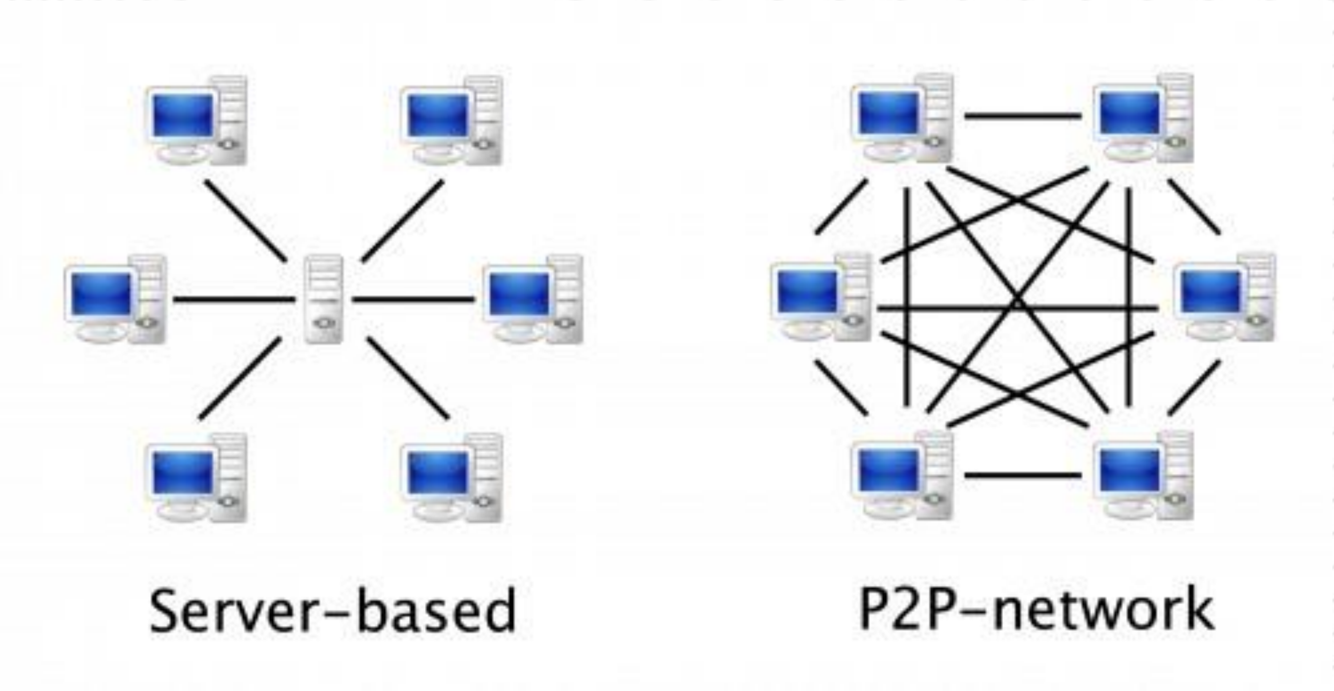
Blockchain & Cryptocurrency

مفاهیم اساسی

Basic Concepts

معماری Peer To Peer (P2P)

- معماری غیر متمرکز دارند
- همه کامپیوترها یا دستگاه‌های عضو این شبکه حجم کاری خود را در شبکه به اشتراک قرار می‌دهند
- کامپیوترهای درون یک شبکه نظیر به نظیر هیچ‌گونه ارجحیتی نسبت به یکدیگر نداشته و همگی و با یکدیگر برابر هستند
- کامپیوترهای درون یک شبکه نظیر به نظیر بدون آن‌که به یک سیستم مدیریت متمرکز نیازی داشته باشند منابع را میان یکدیگری تقسیم می‌کنند
- همگی مجوزها و اختیاراتی یکسان با یگدیگر دارند.
- کامپیوترها می‌توانند در یک زمان در نقش سرور و کلاینت ظاهر می‌شوند
- یک کامپیوتر، از تمام معماری و نقشه شبکه اطلاعی ندارد.


Server-based
P2P-network

ADVANTAGES & DISADVANTAGES OF PEER TO PEER NETWORK

Advantages:

- Use less expensive computer hardware
- Easy to administer
- No NOS required
- More built in redundancy
- Easy setup & low cost

Disadvantages:

- Not very secure
- No central point of storage or file archiving
- Additional load on computer because of resource sharing
- Hard to maintain version control

تابع هش (Hash Function)

- هش یک عملیات یک طرفه ریاضی می باشد که بر روی متن ساده (Plain Text) انجام می شود تا یک متن رمزی با اندازه ثابت را در خروجی به ما بدهد
- اثر انگشت دیجیتالی یک داده
- ویژگی های منحصربفرد هش
  - معکوس ناپذیری
  - هرگز دو ورودی متفاوت به خروجی یکسان منجر نمی شوند
- در صورتیکه متن ساده تغییر پیدا کند حتی یک تغییر بسیار جزئی هش خروجی نیز کاملا تغییر خواهد یافت
- توابع هش دارای قابلیت جلوگیری از تصادم هستند در نتیجه هیچ وقت نبایستی دو ورودی متفاوت هش یکسانی را ایجاد کنند

تابع هش (Hash Function)

مثال : محاسبه هش « هادی »

md2	16	950823270E7DCCE4A430581A2454254F
md4	16	0E412ED2A14553E127CEFC5745BD8155
md5	16	76671D4B83F6E6F953EA2DFB75DED921
sha1	20	F626BFE8A6716F0E60B0F3989B67F5AD2FA9FDA2
sha224	28	7BDD486E467FEB526504134187FD55C27719A90C159933982454D52A
sha256	32	7E7B5941351BFE1E23E37FFB0665A1041A682ECD2C8189054CCC94B16D
sha384	48	DC31357BB4B8C99CB4D6DDA1EE4FD046401275F9F70C6C202CD018C1E
sha512	64	C28E14F8A7661CADF2B53956444823580A941F7B849BE1CF9E793D6535
ripemd128	16	E5E9038FF3C18C627F9D0ED21942CE95

Used For Bitcoin

رمزنگاری (Encryption)

انواع رمزنگاری

رمزنگاری متقارن

* استفاده از یک کلید یکسان برای رمزگذاری و رمزگشایی

❋ Twofish ، Serpent، AES، Blowfish، CAST5، RC4، DES، و IDEA

رمزنگاری نا متقارن

رمزنگاری نامتقارن از کلیدهای متفاوتی برای رمزنگاری و رمزگشایی استفاده میکند. در این نوع رمزنگاری، کاربر نهایی در شبکه عمومی و یا خصوصی، یک جفت کلید در اختیار دارد: یک کلید عمومی برای رمزکردن و یک کلید اختصاصی برای رمزگشایی

❋ Diffie–Hellman, RSA

رمزنگاری نامتقارن

کلید عمومی

(اگر طرف الف بخواهد به طرف ب پیامی ارسال کند،
طرف الف کلید عمومی طرف ب را می‌گیرد و از آن
برای رمزگذاری پیام استفاده می‌کند)

کلید خصوصی

(هنگامی که طرف ب آن را دریافت می‌کند، از کلید
خصوصی خود برای رمزگشایی این پیام استفاده
می‌کند)

امضای دیجیتال

فناوری بلاکچین

مبنای فناوری بلاکچین س[illegible]ی دیگر است که قبل از این وجود داشته اند اما ترکیب هوشمندانه آنها، بلاکچین را خلق کرده است.

- پلتفرم نرم افزاری (پروتکل بلاکچین)
- رمزنگاری و امضای دیجیتال
- شبکه های همتا به همتا یا peer to peer

فناوری بلاکچین

- گذار از عصر Cloud به عصر تمرکززدایی
- دوره ای که کاربران نهایی علاوه بر اینکه مالک و مدیر سخت افزارها به روشی غیرمتمرکز هستند، داده های خود را نیز به روشی غیر متمرکز اداره خواهند کرد
- دفتر کل توزیع شده(DLT) فناوری است که این گذار را ممکن خواهد کرد
- تکنولوژی Block Chainیک پایگاه داده غیر متمرکز است که به صورت ایمن بین چندین سازمان تقسیم شده است و هیچ فرد یا گروهی نمی تواند آن را به صورت انحصاری تحت کنترل داشته باشد و در آن لیست دارایی ها و معاملات بر روی یک شبکه نظیر به نظیر (Peer-to-Peer)نگه‌داری می‌شود.

فناوری بلاکچین

- در واقع یک دفتر ثبت اسناد عمومی است که در آن مشخص می شود هر شخص چه مقدار دارایی دارد و چه معاملاتی را تابحال انجام داده است .
- در این سیستم امنیت مبادلات توسط علم رمزنگاری کامپیوتری تامین می شود و در طول زمان تاریخچه معاملات در بلاک هایی از داده قفل و نگه داری می شوند
- در پایگاه های داده بلاک چین، داده ها بین میلیون ها کامپیوتر توزیع شده اند و هیچ کس قادر به کنترل داده ها نیست و اگر شخصی بخواهد بلاک چین را هک کند باید تمام کامپیوتر های شبکه را که با رمزنگاری پیشرفته حفاظت شده اند را هک کند که غیرممکن است.

فناوری بلاکچین

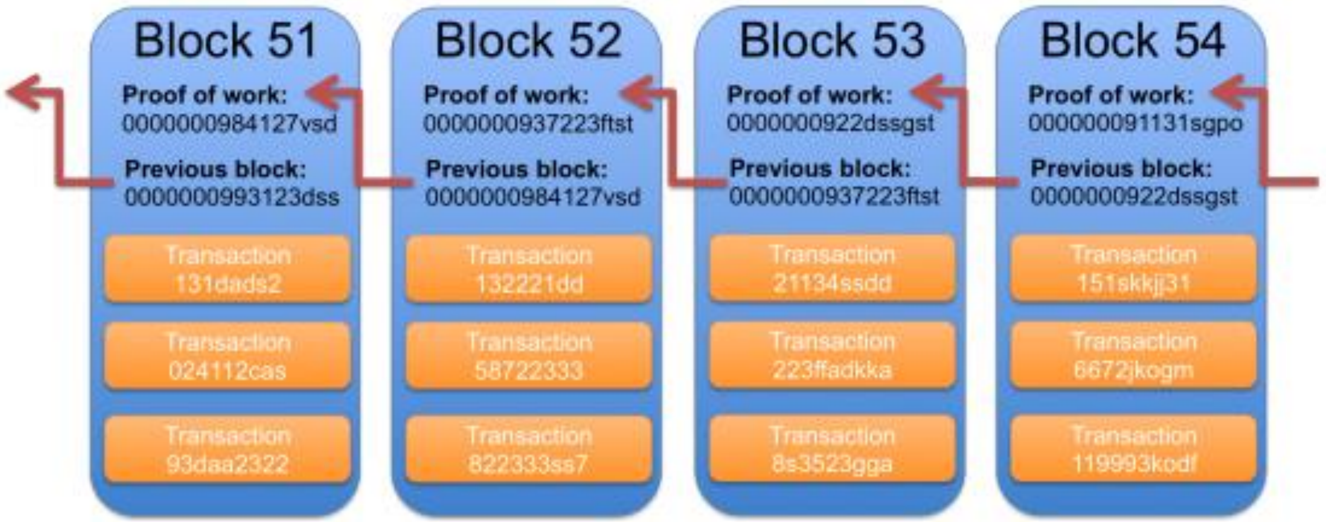
- بلاکچین، رکوردی از رویدادها و متغیرهای موافقت شده است که به شکل رمزنگاری شده از آن محافظت می شود.
- هر بلوک از بلاکچین، شامل اشاره گر هش بلوک قبلی، یک مهر زمانی و داده قابل انتقال است.
- هر یک از بلاک‌های موجود در فناوری مورد بحث با فهرستی از تراکنش‌ها به وجود می‌آیند و دارای یک هِدِر هستند. این هدر خود شامل ۳ نوع داده‌ی زیر می‌شود

از طریق الگوریتم رمزنگاری هش به بلاک والد اشاره می‌کند. منظور از والد در اینجا بلاک قبلی است

برچسب زمانی و اطلاعات مربوط به «الگوریتم اثبات کار» که برای نحوه‌ی استخراج بلاک‌های جدید و تأیید آن‌ها به کار می‌رود.

اطلاعات ساختاری درباره‌ی تراکنش‌های داخل بلاک

فناوری بلاکچین



انواع بلاکچین		
بلاکچین خصوصی (انحصاری)	بلاک چین عمومی انحصاری	بلاکچین عمومی غیر انحصاری

فناوری بلاکچین

انواع بلاکچین

- بلاکچین عمومی غیر انحصاری

بیت کوین، اتریوم، لایت کوین و انواع سیستم های عمومی و آزاد مبتنی بر بلاک چین

انحصار تراکنش‌ها را در اختیار نداریم

از این نوع بلاک چین زمانی استفاده می‌شود که نظر تمام جامعه مورد نظر در آن شبکه مهم باشد، نه فقط چند فرد خاص

در این بلاک چین هر کسی می‌تواند قراردادهای هوشمند ایجاد کند و یا پول و داده‌ها را منتقل کند. اطلاعات مهم در این بلاک چین ها به صورت رمزنگاری شده قابل ذخیره سازی هستند.

فناوری بلاکچین

انواع بلاکچین

- بلاک چین عمومی انحصاری

چند شرکت یا سازمان همسو یا هم هدف

در این بلاک چین افرادی خاص برای تأیید فعالیت‌ها انتخاب می‌شود

داده‌ها قابل مشاهده برای عموم هستند اما می‌توان از یک سری اطلاعات خاص محافظت کرد.

می توان از یک کد QR استفاده نمود و مشتریان می‌توانند با اسکن کد هر محصول از اطلاعات آن آگاه شوند. مشتریان فقط قادر به مشاهده اطلاعات هستند و نمی‌توانند چیزی را کم و زیاد کنند. برای ثبت اطلاعات هر محصول در بلاک چین از روش‌های مختلفی می‌توان کمک گرفت. مثلاًبه تولیدکنندگان و کارمندان بخش بسته بندی، اجازه ثبت اطلاعات در بلاک چین داده می‌شود. اطلاعات ذخیره شده روی بلاک چین قابل تغییر نیستند بنابراین برای شرکت اعتبار بزرگی محسوب می‌شود.

فناوری بلاکچین

انواع بلاکچین

- بلاکچین خصوصی

این نوع بلاک چین می‌تواند برای نهادهای مختلف خصوصی و دولتی مورد استفاده قرارگیرد. در این بلاک چین افرادی خاص برای تایید فعالیت‌ها انتخاب می‌شود و فقط افرادی خاص امکان مشاهده اطلاعات ثبت شده را دارند.

متخصصین امر میگویند که بلاک چین‌های خصوصی اصلاً بلاک چین نیستند. شاید آنها پایگاه‌های داده‌ای به اشتراک‌گذاری شده تحت عنوانی دیگر نباشند، شاید آنها لزوماً توسط فردی با قدرت دسترسی، کنترل شوند. چنین سیستم‌هایی با عنوان تکنولوژی‌های دفتر توزیع‌شده یا DTLشناخته می‌شوند. بدون ماینر، بدون اثبات کار، تنها با مکانیزم اجماعی ساده‌شده که تنها اجازه دسترسی تعدادی خاص نود را می‌دهد. اعتماد برخلاف بی‌نیازی بلاک چین عمومی به اعتماد و اعتمادسازی، در این بلاک چین‌ها به وسیله چند نود خاص انجام می‌گیرد.

فناوری بلاکچین (از منظر دیگر)

انواع بلاکچین

بلاکچین همگن

بلاکچین ناهمگن

فناوری بلاکچین (از منظر دیگر)

بلاکچین همگن

در سیستم های **Multichain**، تمام بلاکچین ها نوع و نقش های یکسان و مشابهی دارند.

مانند : فرمت تراکنش یکسان، استفاده از **VM** مشابه برای اجرای کدهای قرارداد هوشمند، **share** نمودن کریپتوکارنسی مشابه و ...

در بلاکچین همگن، این موارد صراحتا مورد تاکید قرار می گیرد.

داده ها در هر بلاکچین متفاوت می باشند.

بلاکچین ناهمگن

استفاده از بلاکهای متفاوت ---- **Workchain**

برخورداری از نقش های متفاوت

کاربردهای فناوری بلاکچین

تمرکز زدایی جهانی و حذف مراکز سودآور متمرکز

پول دیجیتال (Digital Currency)

قراردادهای هوشمند (Smart Contracts)

اوراق بهادار (Securities)

ثبت و نگهداری سوابق (Record Keeping)

Cryptocurrency

مروری بر تاریخچه پول

دوره اول

مبادله کالا به کالا

دوره دوم

تبادل کالا با
فلزات گرانبها
مانند طلا و نقره

دوره سوم

دوره ظهور پول
به واسطه
ذخایر طلا و یا
اصطلاحا دوره
چاپ اسکناس
با پشتوانه

دوره چهارم

دوره چاپ
اسکناس بدون
پشتوانه یا
پول فیات

رمزارز دیجیتال

Bit coin

- اولین رمزارز دیجیتال
- مقاله ساتوشی ناکاموتو در سال ۲۰۰۸
- استفاده از الگوریتم SHA256
- استفاده از روش proof-of-work
- تعداد ۲۱ میلیون واحد بیت کوین

- پشتوانه بیت کوین
- جلوگیری از مشکل Double Spending
- Mining بیت کوین؛ ASIC
- مشکل سرعت استخراج بلاک جدید
- پذیرش بیت کوین در دنیا

رمزارز دیجیتال

Ethereum

- تفاوت بین بیت کوین و اتریوم
- امکان ایجاد قرارداد هوشمند
- نوآوری مهم اتریوم؛ EVM
- پروتکل بلاکچین؛ Proof-of Work
- مکانیزم HMAC؛ ETHASH
- زمان ایجاد بلاک؛ ۱۰–۱۴ ثانیه
- ابزار ماینینگ؛ GPU/CPU

رمزارز دیجیتال

Ethereum Platform

- تفاوت بین بیت کوین و اتریوم
- امکان ایجاد قرارداد هوشمند
- نوآوری مهم اتریوم؛ EVM
- پروتکل بلاکچین؛ Proof-of Work

- مکانیزم HMAC؛ ETHASH
- زمان ایجاد بلاک؛ ۱۰–۱۴ ثانیه
- ابزار ماینینگ؛ GPU/CPU

رمزارز دیجیتال

Ripple

- ایجاد در سال ۲۰۱۲
- ریپل نت به بانک ها و موسسات بزرگ متصل می شود و انتقال پول یا سایر دارایی ها را می توان در بستر شبکه انجام داد
- ریپل به منظور تسهیل پرداخت های آنلاین به وجود آمد
- زمان ایجاد بلاک؛ ۴ ثانیه

رمزارز دیجیتال

کشورهای استفاده کننده از رمزارز دیجیتال

- بانک مرکزی هند در حال تنظیم مقررات بیت‌کوین است
- بانک مرکزی مالزی در اوایل سال ۲۰۱۸ مقررات ارزهای رمز نگاری شده را صادر می‌کند
- کی‌بانک (KBank) تایلند قصد دارد با استفاده از بلاک‌چین، قراردادهای خود را تا سال ۲۰۱۸ دیجیتالی کند
- اوکراین قصد دارد تا پایان سال ۲۰۱۷، صدو پنجاه ATM بیت‌کوین در این کشور نصب کند
- تشکیل کارگروهی در بانک مرکزی کره جنوبی برای مطالعه تأثیر ارزهای رمزنگاری و تصویب مقررات مربوطه
- شرکت IBM قصد دارد با همکاری بانک‌های بزرگ و به وسیله‌ی بلاک‌چین، معاملات مالی را متحول کند
- شرکت Alibaba از بلاک‌چین برای ایمن‌سازی داده‌های حوزه‌ی سلامت کشور چین استفاده می‌کند

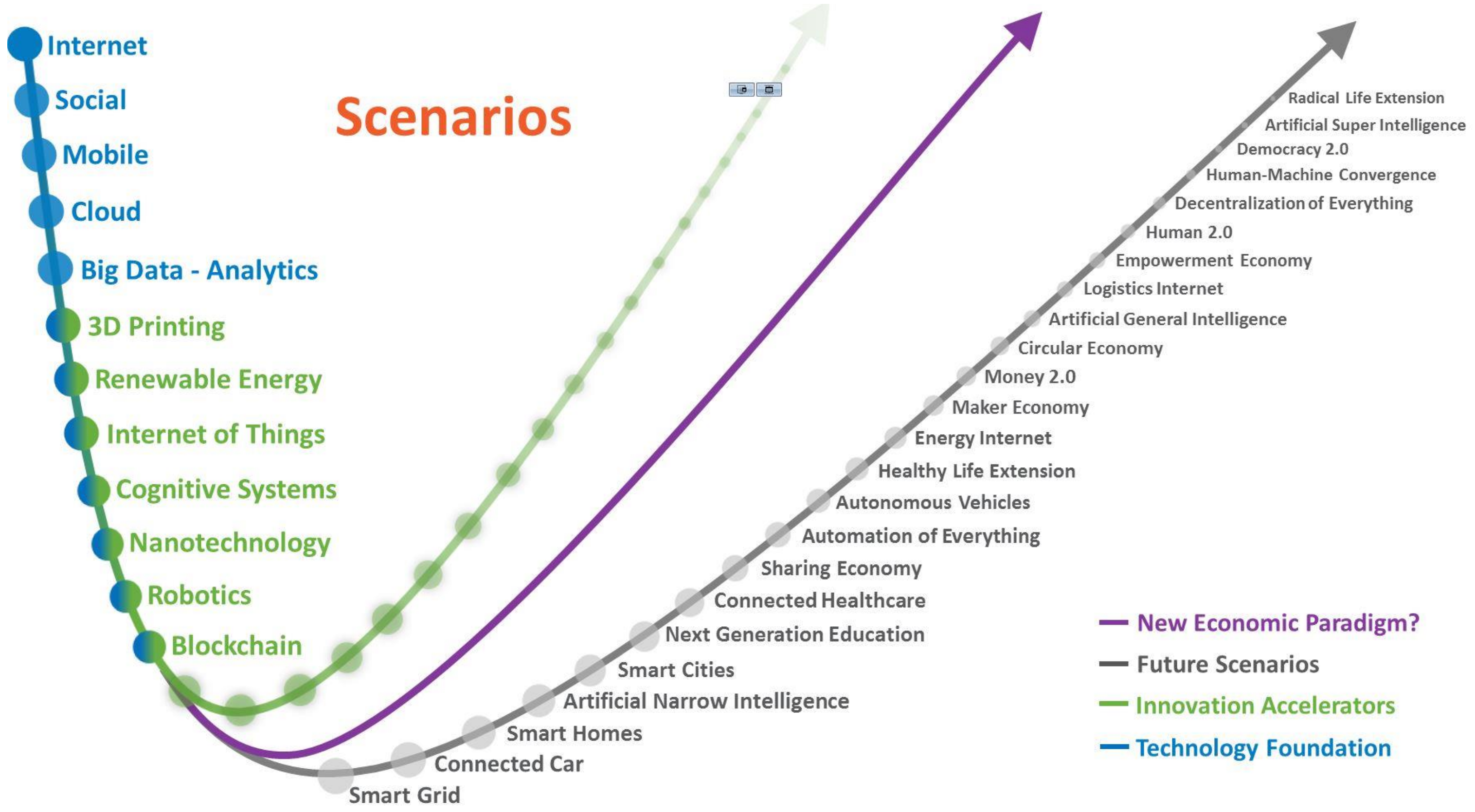
شهر هوشمند

Smart City

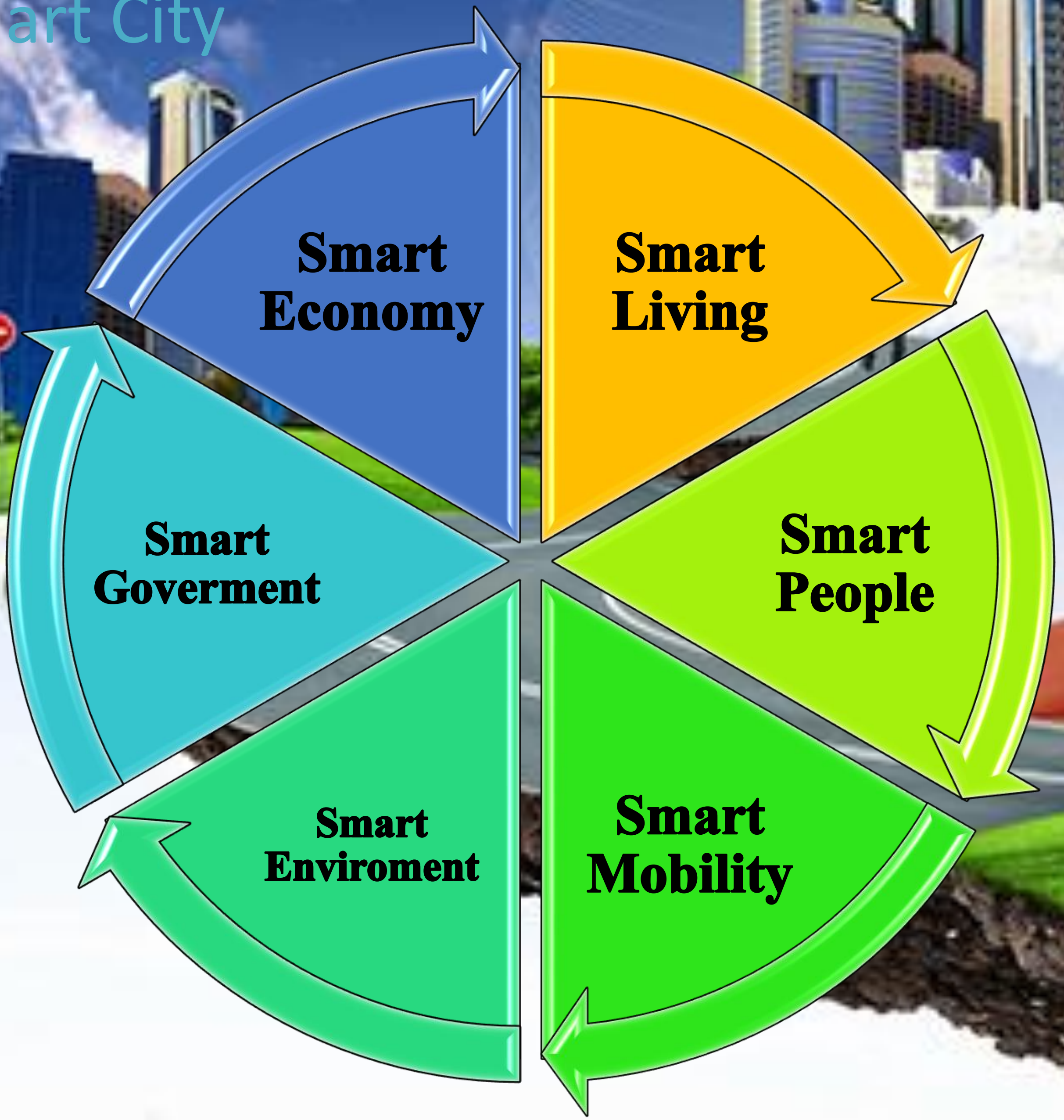
شهر هوشمند

شهر هوشمند، شهری نوآور است که از فناوری اطلاعات و ارتباطات (ICT) و وسایل دیگر استفاده بهینه می کند تا کیفیت زندگی، کارایی عملیات شهری و خدمات، به علاوه رقابت پذیری را ارتقا دهد درحالی که سازگاری و مطابقت با نیازهای نسل های کنونی و آتی را با توجه به جنبه های اقتصادی، اجتماعی و زیست محیطی تضمین می کند. (UNECE and ITU, October 2015)

سناریوهای جدید



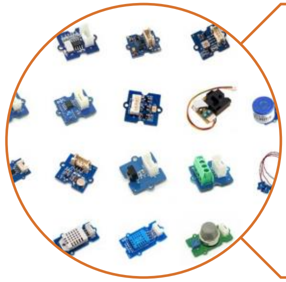
Smart City



Smart Economy
Smart Living
Smart People
Smart Mobility
Smart Enviroment
Smart Goverment

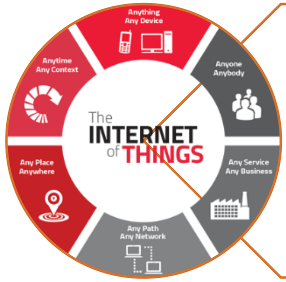
فناوری ها و اجزای کلان سایبری مورد استفاده در شهر هوشمند

فناوری ها و اجزای کلان سایبری
مورد استفاده در
شهر هوشمند



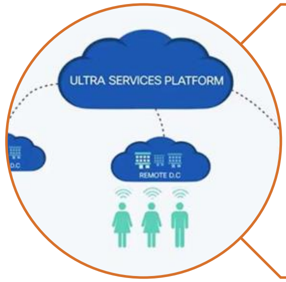
سخت افزار

(شامل سنسورها، عملگرها و دروازه‌های اتصال به شبکه)



شبکه مخابراتی ارتباطی

(شامل شبکه انتقال مبتنی بر IP و شبکه دسترسی)

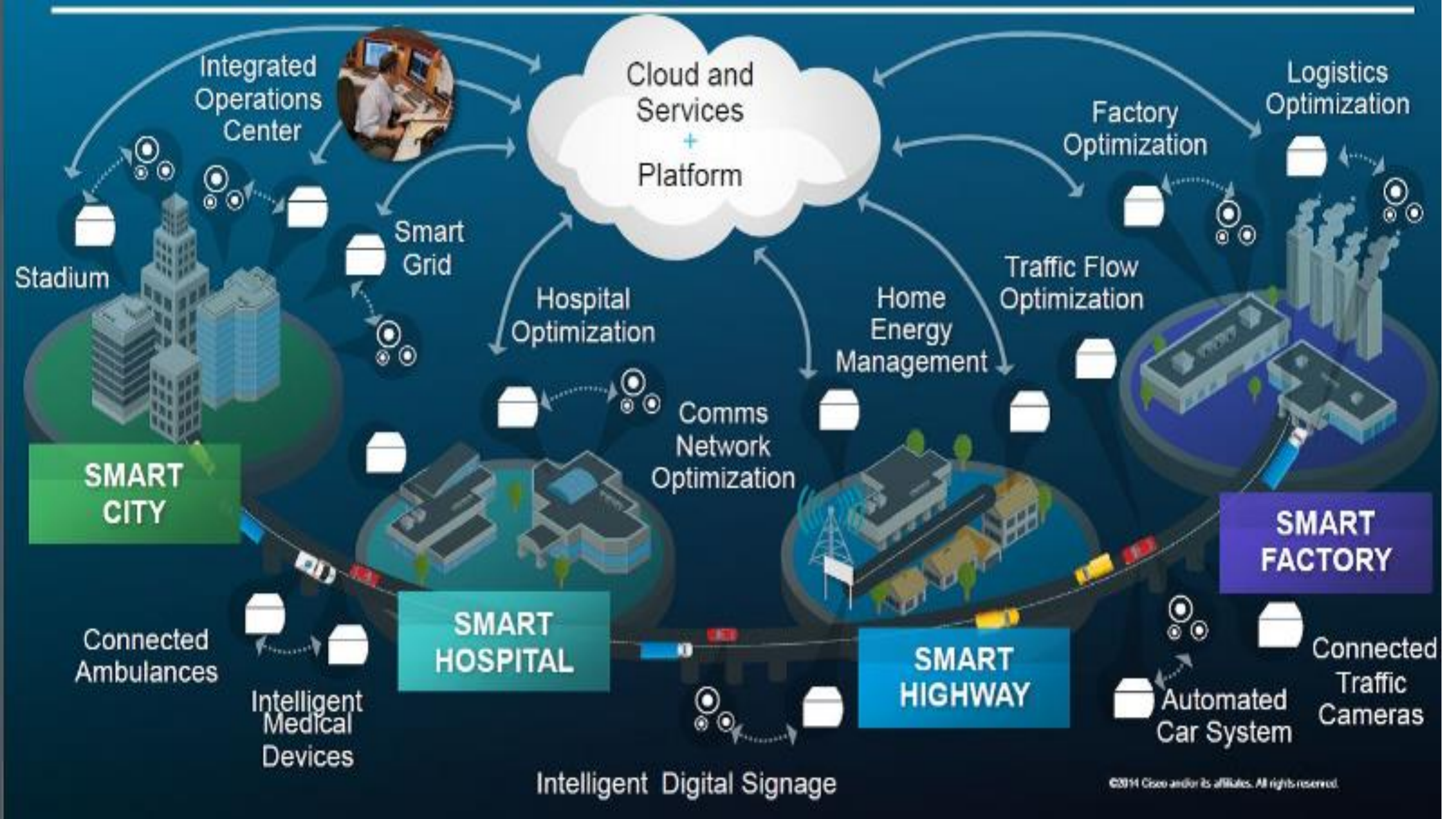


بستر ابری

(مرکز داده، پلتفرم تحلیل کلان داده و میان افزار ارایه سرویس)

برنامه‌های کاربردی

(شامل توسعه‌دهندگان سرویس و سرویس‌گیرندگان)


Cloud and Services + Platform
Integrated Operations Center
Stadium
Smart Grid
Hospital Optimization
Comms Network Optimization
Home Energy Management
Traffic Flow Optimization
Factory Optimization
Logistics Optimization
SMART CITY
SMART HOSPITAL
SMART HIGHWAY
SMART FACTORY
Connected Ambulances
Intelligent Medical Devices
Intelligent Digital Signage
Automated Car System
Connected Traffic Cameras

فناوری‌های مورد استفاده در شهر هوشمند

دیدگاه اول: فناوری‌های پیشران

- اینترنت اشیا
- ابر داده
- پردازش ابری
- سامانه فیزیکی سایبری

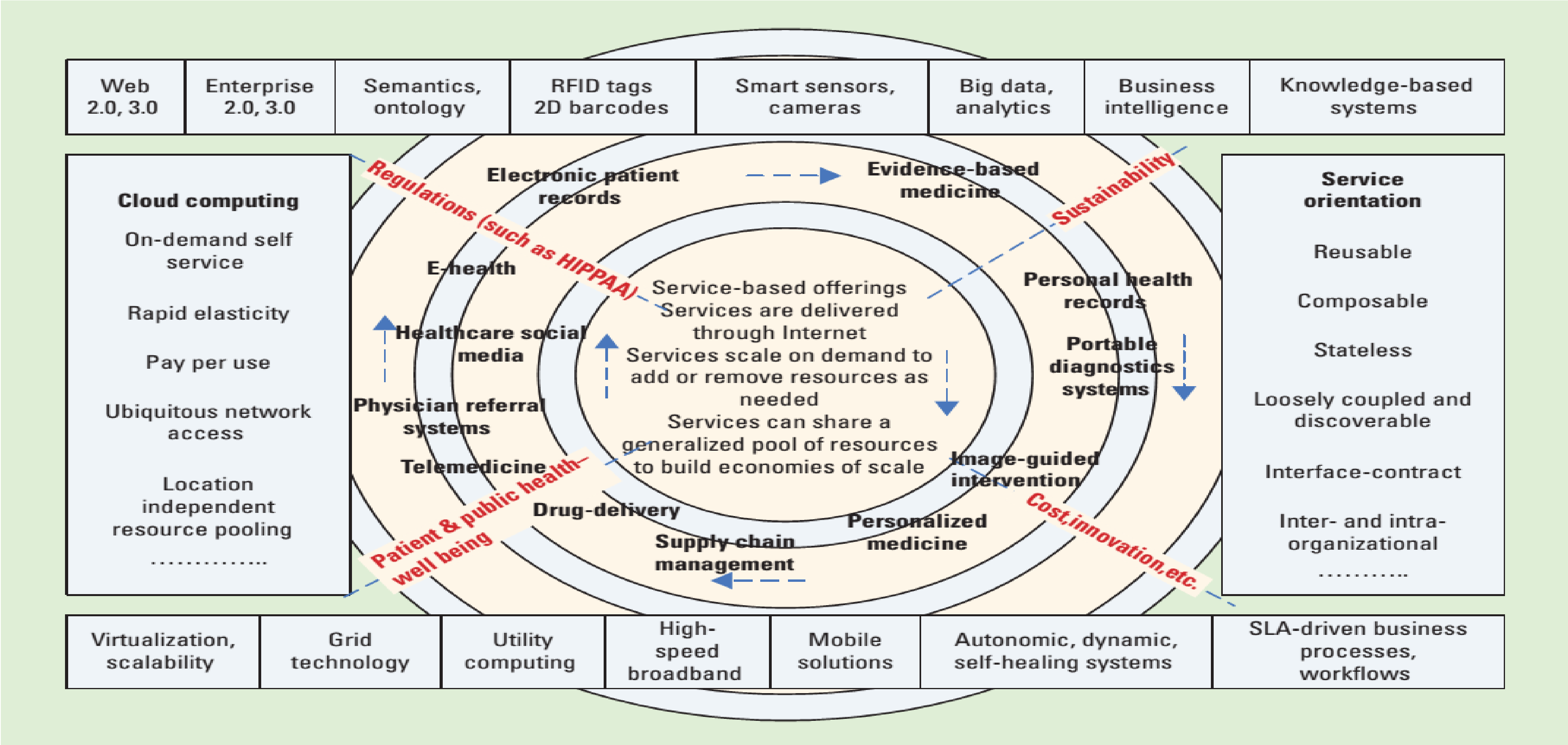
دیدگاه دوم: پشتیبانی فناورانه

- شبکه‌های ناهمگن
- سنجش به عنوان یک سرویس
- پردازش ابری
- ماندگاری اطلاعات
- تجزیه تحلیل اطلاعات

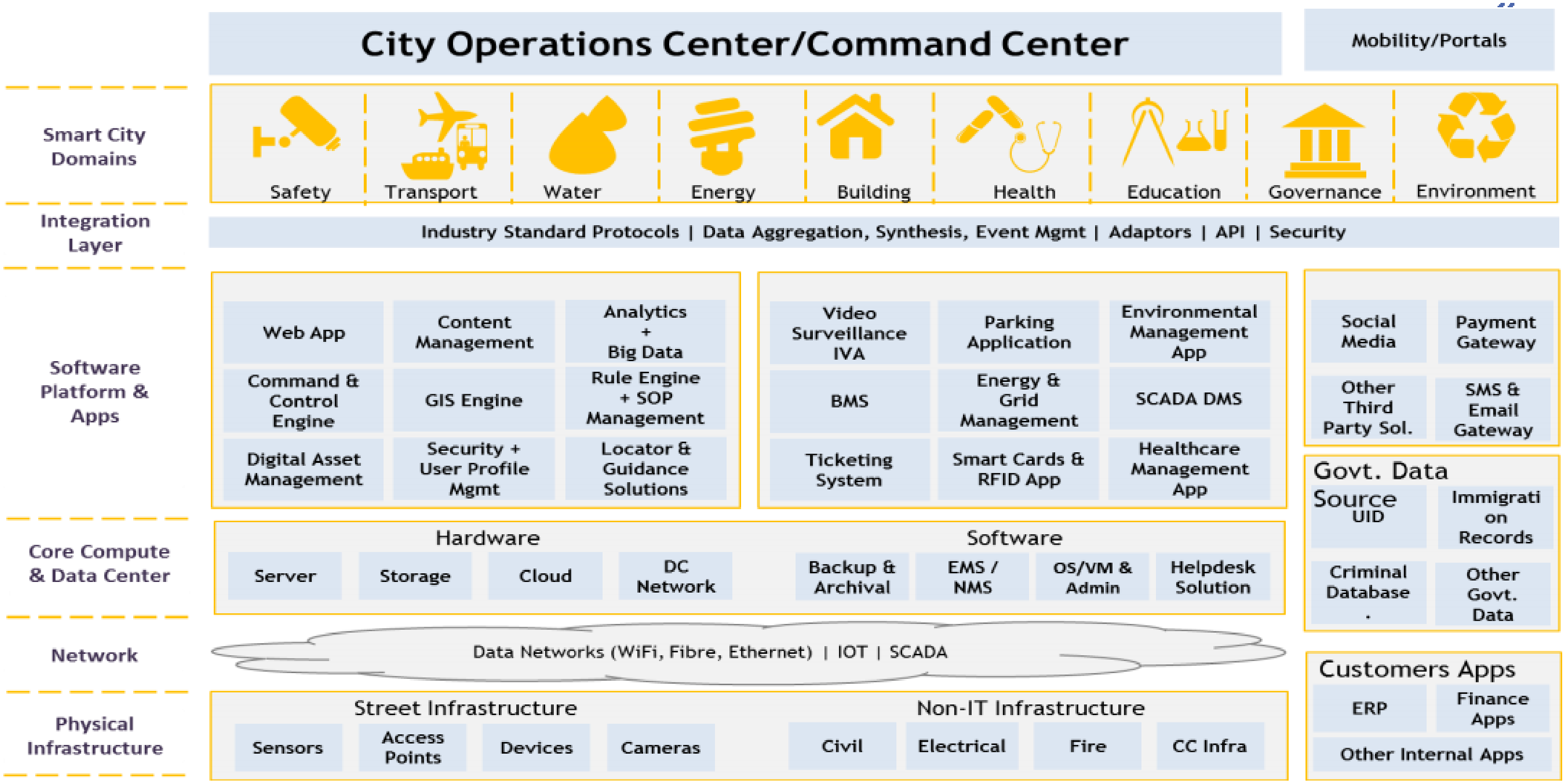
دیدگاه سوم: نوع ارائه خدمت

- مبتنی بر وب
- با نظارت هوش مصنوعی
- ماژول‌های ارتباطی
- روشنایی هوشمند

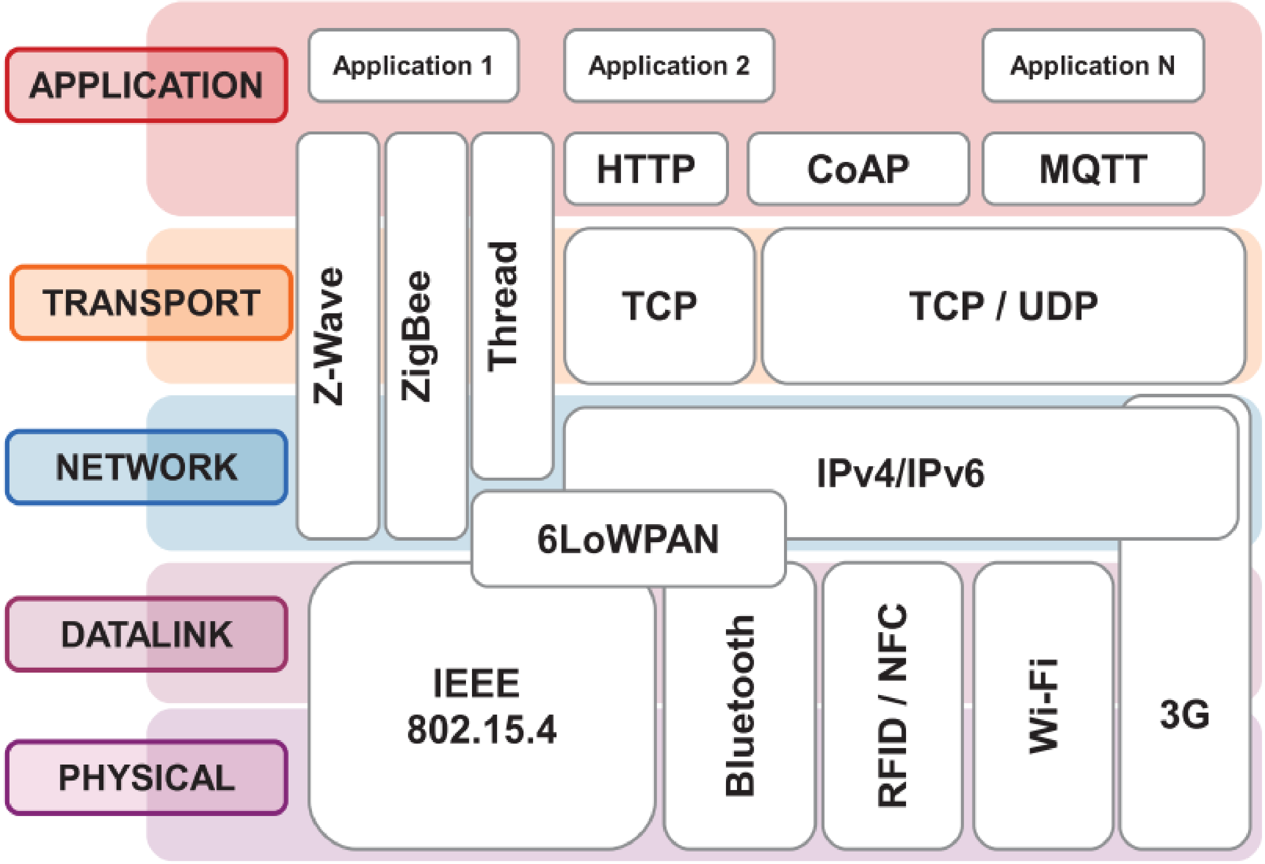
فناوری‌های مورد استفاده در شهر هوشمند



معماری و اجزای شهر هوشمند از دید bsi



پروتکل های ارتباطی در لایه های معماری شبکه شهر هوشمند

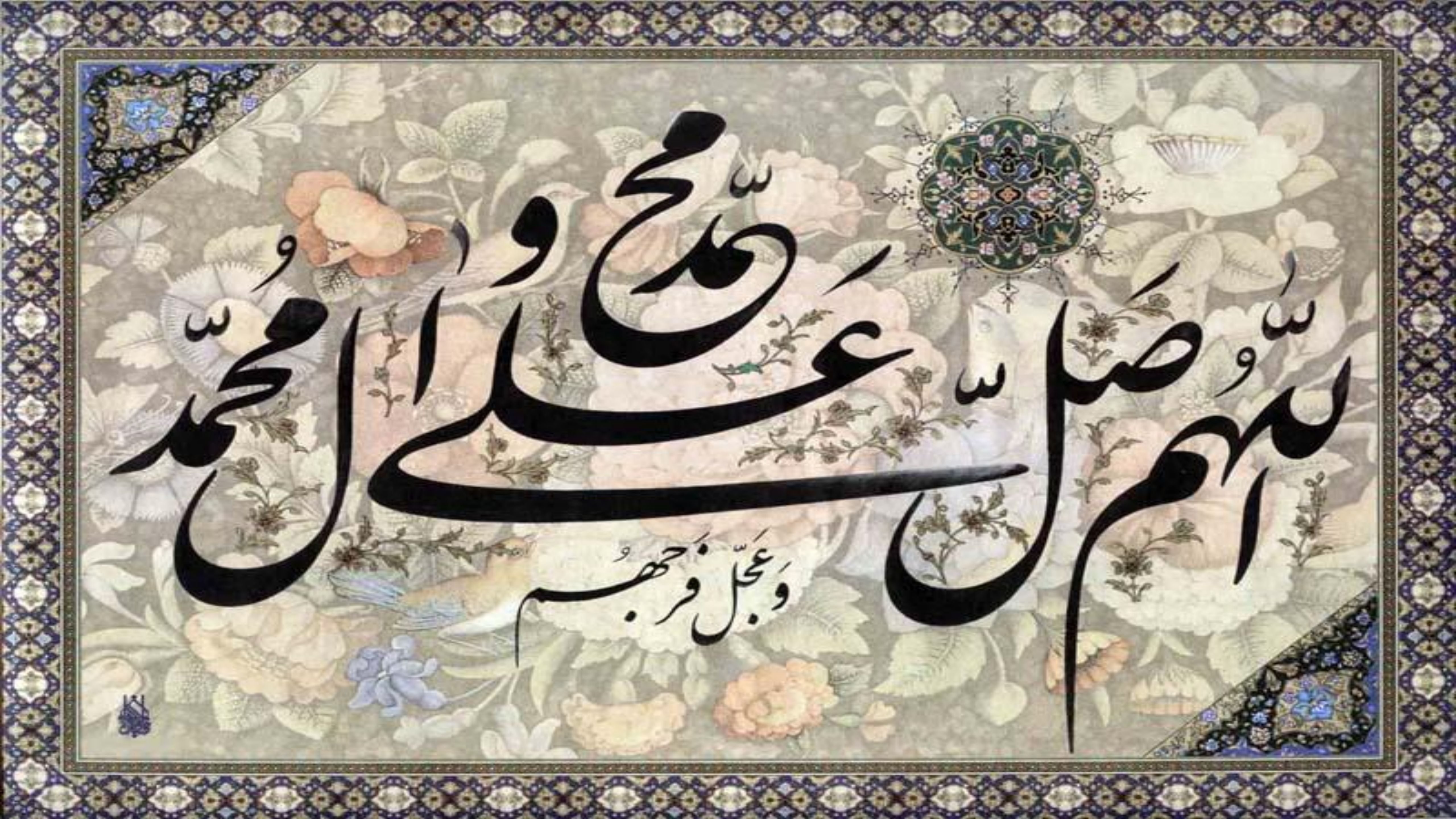


استانداردهای رایج در شهر هوشمند

شماره استاندارد	موضوع	سال ارائه	دامنه کاربرد
ISO 37101	توسعه جوامع پایدار و تاب‌آور – راهکارهای عمومی	2016	
ISO 37102	توسعه جوامع پایدار و تاب‌آور – مفاهیم	2016	
BS 8904	چارچوب توسعه جوامع پایدار	2011	راهبردهای توسعه پایدار
ISO/IEC AWI 30145	فناوری‌های شهرهای هوشمند– چارچوب مرجع فناوری	درحال توسعه	فناوری ها
ISO/IEC AWI 30146	فناوری‌های شهرهای هوشمند– شاخص‌های فناوری	درحال توسعه	فناوری ها
IEEE P2413	چارچوب معماری اینترنت اشیا برای شهرهای هوشمند	۲۰۱۵	اینترنت اشیا
ISO/IEC JTC1	شهرهای هوشمند دیدگاه فناوری	۲۰۱۴	فناوری‌ها

استانداردهای رایج در شهر هوشمند

شماره استاندارد	موضوع	سال ارائه	دامنه کاربرد
PAS 182	مدل مفهومی شهرهای هوشمند– راهنمای پیاده‌سازی مدل برای تبادل اطلاعات	2014	تبادل اطلاعات
PAS 181	چارچوب شهر هوشمند– راهنمای پیاده‌سازی استراتژی‌های شهر هوشمند	2014	چارچوب جامع Tتدوین راهبرد برای هوشمندسازی شهرها
PAS 180	مفاهیم شهر هوشمند	2014	مفاهیم
PD 8100	راهنمای شهرهای هوشمند	2015	مفاهیم و راهنمای عمومی
PAS 185	رهاهکار پیاده‌سازی شهر هوشمند امن	2017	امنیت
PAS 184	تدوین پروپزالهای پروژه برای هوشمندسازی شهرها	2017	مدیریت
PD 8101	نقش برنامه‌ریزی در توسعه شهرهای هوشمند	2014	برنامه‌ریزی
PAS 183	چارچوب تصمیم‌گیری برای اشتراک‌گذاری اطلاعات	2017	اشتراک‌گذاری اطلاعات
ISO 37120	توسعه پایدار جوامع	2018	راهبردهای توسعه پایدار


اللهم صل علی محمد و آل محمد
وعجل فرجهم

بسم الله الرحمن الرحیم

تاب آوری سایبری

علی محمد امین زاده -
am.aminzadeh@sndu.ac.ir

تاب آوری

تاب آوری موضوعی مهمی است که طی سال های اخیر در علوم مختلف کاربرد فرآوانی پیدا کرده است .

در علم مکانیک ، تاب آوری به حدی از تحمل فشار یا کششی است که جسم سخت می تواند آن را بدون تغییر شکل بپذیرد. در این صورت پس از نقطه حد تاب آوری مرحله له شدگی و یا شکنندگی رخ می دهد که در آن جسم سخت اگر چکش خوار و انعطاف پذیر باشد ، دچار تغییر شکل می دهد و در غیر اینصورت دچار شکستگی می شود

در علوم انسانی تاب آوری حدی از تحمل انسان ، مجموعه انسانی و یا سازمانی از نیروی انسانی در مقابل مشکلات است که در جریان آن واکنشی که غیر طبیعی جلوه کند ، رخ ندهد و بتواند به صورت عادی تداوم یابد .

تاب آوری

تاب آوری خاصیت فیزیکی ماده ای را گویند که به واسطه خاصیت ، چنانچه ماده در معرض تغییر شکل قرار گیرد ، بتواند به شکل یا وضعیت اولیه خود برگردد ، مشروط بر اینکه از حد کشسانی خود عدول نکند.

در سازمان ها ، نیروی کار سازمان زمانی تاب آور تلقی می شود که در مقابل مسائل نامطلوب استقامت داشته باشد .

اگر سازمان ها این توانایی را داشته باشند که در مواجهه با مشکلات و سختی ها ، تغییرات پی در پی محیطی و ریسک به اهداف خود برسند ، از ویژگی تاب آوری برخوردار خواهند بود .

علی محمد امین زاده -
am.aminzadeh@sndu.ac.ir

تاب آوری

- برای توصیف یک شی ء یا یک شخص یا یک سازمان دارای ظرفیت تاب آوری ، چند شرط اساسی باید برورده شود :
- در مرحله اول باید عامل مورد نظر در مقابل هر نوع تهدید سخت افزاری یا نرم افزاری ، حد اقل تا مدتی کارکردش را حفظ نماید .
- دوم اینکه بعد از تاثیر پذیری ، شیء یا فرد مورد نظر باید قابلیت و توانایی ادامه هدف یا ماموریت کارکردی خود را حفظ نماید .
- سوم اینکه شی یا فرد یا سازمان مورد نظر باید طی یک مدت زمان منطقی و قابل قبول به وضعیت طبیعی خود بازگردد.

تاب آوری سایبری

به مفهوم تاب آور نمودن افراد، اشیاء ویا سازمان های هدف در مقابل تهدیدات سایبری می باشد به نحوی که عامل مورد نظر بتواند در مقابل هر نوع تهدید سخت افزاری یا نرم افزاری سایبری ، حد اقل تا مدتی کارکردش را حفظ نماید .

اگر تهدید سایبری به مرحله عمل رسید و عامل مورد نظر مورد حمله سایبری قرار گرفته اینکه بعد از تاثیر پذیری ، شیء یا فرد یا سازمان مورد نظر باید قابلیت و توانایی ادامه هدف یا ماموریت کارکردی خود را حفظ نماید .

در نهایت اینکه شی یا فرد یا سازمان مورد نظر باید طی یک مدت زمان منطقی و قابل قبول به وضعیت طبیعی خود به قبل از حمله سایبری بازگردد.

اهمیت تاب آوری سایبری

- در تحقیق انجام شده توسط موسسه اکونومیست برروی ۱۸۱ مدیر اجرایی از سراسر جهان ، ۴۷ درصد از افراد اعلان نموده اند که بیش از یک روز خرابی سیستم های سایبری نمی توانند تحمل کنند و این اختلال بقای شرکت را در معرض ریسک قرار می دهد . (اکونومیست ، ۲۰۰۷)
- در یک تحقیق دیگر مشخص شده است که ۲۵ درصد از سازمان هایی که در معرض قطع سیستم قرار گرفته اند بلافاصله تقاضای اعلام ورشکستگی کرده اند (اکونومیست ، ۲۰۰۷)

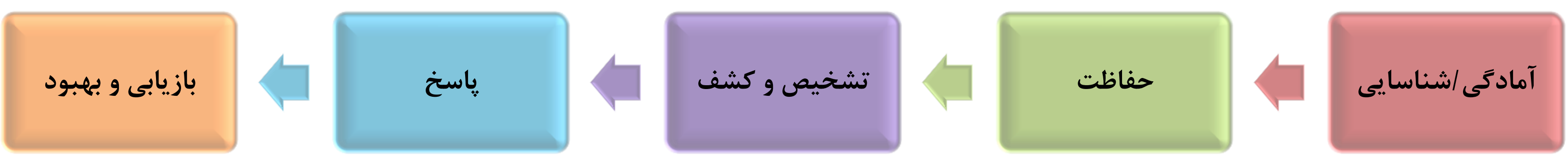
اهمیت تاب آوری سایبری

- در یک تحقیق دیگر در سطح جهان ، حدود ۹۳ درصد از شرکت هایی که دسترسی به مرکز داده هایشان برای ده روز یابیشتر قطع شده بود در عرض یک سال تقاضای ورشکستگی خود را به مراجع قانونی اعلام کردند .
- در گزارش سال ۲۰۰۷ منتشر شده در آمریکا به نام " تاب آوری اقتصادی : تلفیق رقابت پذیری و امنیت بنگاه " اعلان شده است که در قرن ۲۱ ، توانایی یک سازمان برای مدیریت فعال تاب آوری باید به یک اهرم بسیار جدی مشوق رقابت تبدیل شود .
- موارد فوق نشان از اهمیت ارتقاء قابلیت های تاب آوری عملیاتی برای سازمان ها و نهاد های مختلف می باشد .

تاب آوری سایبری

تاب آوری سایبری بر روی کنترل های پیشگیرانه، شناسایی و واکنشی در یک محیط فناوری اطلاعات برای ارزیابی شکاف ها و پیشرفت های محرک برای وضعیت امنیتی کلی سازمان تمرکز دارد.

تاب آوری سایبری سازمانی یک چارچوبی برای ارزیابی تاب آوری سازمان ها است که توسط وزارت امنیت داخلی ایجاد گردیده است. چارچوب دیگری که توسط سیمانتک ایجاد شده است بر پایه ۵ ستون است: آمادگی/ شناسایی، حفاظت، تشخیص و کشف، پاسخ، و بازیابی و بهبود (سمانتک ، ۲۰۱۶).



پنج ستون معرفی شده توسط سیمانتک برای ارزیابی تاب آوری سایبری سازمان(سمانیک ، ۲۰۱۶)

تفاوت امنیت و تاب آوری سایبری

- امنیت سایبری شامل تکنولوژی ها، فرآیندها و اقداماتی است که برای حفاظت از سیستم ها، شبکه ها و داده ها از حمله های سایبری طراحی شده اند.
- امنیت سایبری مؤثر، خطر ابتلا به حمله سایبری را کاهش میدهد و نهادها، سازمان ها و افراد را از سوء استفاده عمدی از سیستم ها، شبکه ها و فناوری ها محافظت میکنند.
- تاب آوری سایبری در ابعاد وسیع تری نگریسته میشود به گونه ای که شامل امنیت سایبری و تاب آوری کسب و کار میشود.
- امنیت سایبری بدون اینکه از قابلیت بهره‌گیری از سیستم ها برخوردار باشد مؤثر است و اگر حمله سایبری موفقیت آمیز باشد، برنامه ی تجاری پیوسته پایدار برای بازگرداندن عملیات وجود دارد.

تفاوت امنیت و تاب آوری سایبری

- تاب آوری سایبری به کسب و کارها کمک میکند تا متوجه شوند که هکرها از ابزار نوآورانه ، عناصر و اهداف تعجب برانگیز برخوردار شوند و میتوانند در تلاش خود موفق شوند.
- این مفهوم به کسب و کار کمک میکند تا فرآیند آمادگی، پیشگیری، واکنش و بازیابی و بهبود موفقیت آمیزی بصورت امنی را پیاده سازی کنند.
- این یک تغییر فرهنگی است بطوری که سازمان، امنیت را به عنوان یک کار تمام وقت و تعبیه بهترین شیوه های امنیتی در عملیات روزمره را میبینند .
- در مقایسه با امنیت سایبری، تاب آوری سایبری نیازمند تفکر متفاوت کسب و کار و چابک تر در برخورد با حملات است.

مدیریت تاب آوری عملیاتی

- کیفیت یک سیستم یا محصول تا حد زیادی تحت تاثیر کیفیت فرآیند استفاده شده در تولید و تداوم آن است .
- مدل مدیریت تاب آوری عملیاتی سه مفهوم نوآورانه و سود مند را ارائه می نماید :

1. بهبود ریسک و مدیریت تاب آوری از طریق همگرایی هدفمند و کاربردی مدیریت امنیت ، تداوم کسب و کار و مدیریت عملیات IT
2. تبدیل کاربردی مدیریت امنیت ، تداوم کسب و کار و مدیریت عملیات IT به رویکرد فرآیند محور و امکان بهبود فرآیند و سنجش و اندازه گیری
3. نهادینه سازی فرآیند و پیشرفت فرآیند سازمانی با بهره گیری از مزیت بلوغ

تفاوت امنیت و تاب آوری سایبری

جنبه	امنیت سایبری	تاب آوری سایبری	توضیحات
هدف	حفظ سیستم های فناوری اطلاعات	تضمین ارائه نتایج مطلوب سیستم	هدف تاب آوری سیستم دارای سطح بالاتری از هدف امنیت سایبری است.
تصمیم (قصد)	شکست ناپذیری	ایمن در برابر خرابی	تصمیم، مرتبط با ویژگی های مطلوب سیستم است. از دید سازمانی، شکست ناپذیری به طراحی و حفظ سیستم برمیگردد درحالیکه ایمن در برابر خرابی اشاره به خرابی بصورت کنترل شده دارد.
روش	اعمال امنیت از بیرون	ایجاد امنیت از درون	نوع روش از دید امنیت، اعمال کردن امنیت بر روی سیستم است به عنوان مثال رمزگذاری بر روی ارتباطات بین سیستم و کاربران آن. اما نوع روش از دید تاب آوری، باید اثر بسیار عمیق تری داشته باشد. بنابراین اعمال امنیت در درون خود سیستم رخ میدهد.

تفاوت امنیت و تاب آوری سایبری

جنبه	امنیت سایبری	تاب آوری سایبری	توضیحات
معماری	حفاظت تک لایه ای	حفاظت چندلایه ای	معماری بیانگر ساختار درونی، ماژول های تشکیل دهنده سیستم ها و روابط آنها است. این حفاظت چندلایه ای برای سیستم های تاب آور، به منظور شکست جزئی میباشد که این ساختار بهتر حفاظت تک لایه ای با پوسته سخت است. همچنین هر لایه بایست براساس اصل *ایمن در برابر خرابی* طراحی گردند.

تفاوت امنیت و تاب آوری سایبری

جنبه	امنیت سایبری	تاب آوری سایبری	توضیحات
محدوده	جزء لایتجزی، یک سازمان یا سیستم	جامع، شبکه ای از سازمان ها یا سیستم ها	دلیل گسترده بودن محدوده تاب آوری سایبری دو مورد میباشد، ۱- تهدید میتواند از هر نوع ارتباط درونی که سیستم برقرار کرده است، باشد. ۲- ارتباطات درونی بین سیستم ها میتواند نقطه قوتی برای زمانی باشد که سیستم ها در برابر رویدادهای مضر مقاومت و بهبود میبابند.

ویژگی های امنیت سایبری در مقابل تاب آوری سایبری (بیورک و همکاران ، ۲۰۱۵)

جنبه های تاب آوری سایبری و اصول آنها

جنبه	اصول تاب آوری سایبری
هدف	تضمین ارائه نتایج مطلوب سیستم طی روادید آسیب های سایبری، تمرکز تاب آوری بر روی حفظ بی عیب و کامل اهداف کسب و کار بجای سیستم های فناوری اطلاعات باشد. بنابراین تحلیل تاب آوری نیازمند یک کسب و کار به عنوان نقطه شروع است تا سیستم های فناوری اطلاعات .
تصمیم (قصد)	ایمن در برابر خرابی: سیستم های تاب آور بایست طوری طراحی گردند که با شکست بصورت کنترل شده مواجه گردند تا اینکه تنها در مقابل شکست حفظ شوند.
روش	ایجاد امنیت از درون: تاب آوری درون سازمان ها و سیستم های فناوری اطلاعات ساخته میشوند تا اینکه بصورت عملکردهای جداگانه به سیستم اضافه گردند.

جنبه های تاب آوری سایبری و اصول آنها

اصول تاب آوری سایبری	جنبه
حفاظت چندلایه ای: یک ساختار تاب آور شامل چندین لایه است که هر کدام قادر به حفاظت و بهبود هستند که بهتر از این است که تنها یک لایه از حفاظت وجود داشته باشد.	**معماری**
جامع، شبکه از سازمان ها: برای مدیریت تاب آوری، کسب و کار و سیستم های فناوری اطلاعات بایست بصورت یک شبکه مرتبط به هم در نظر گرفته شوند، تا اینکه هرکدام بصورت جداگانه همراه با محیط خود تحلیل گردند. تاب آوری، ارتباط شبکه ای بین سازمان ها و سیستم ها را بصورت نقاط قوت و ضعف مینگرد تا اینکه بصورت تنها یک منبع از تهدیدات را در نظر بگیرد.	**محدوده**

جنبه های تاب آوری سایبری و اصول آنها (لینکو و همکاران ۲۰۱۳)

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۱- طبقه بندی	در هر سازمان برای حفاظت از دارایی های آن ها، بایست دارایی ها شناسایی و کدبندی شوند و در یک خط مبنای پایه ای از اهداف قرار گیرند، تا سازمان ها بتوانند هر زیرمجموعه از عمل حفاظت را پیاده سازی کنند. بنابراین مهمترین اصل در ایجاد تاب آوری سایبری سازمان ها است. این اصل با فاز "طبقه بندی" چارچوب مدیریت ریسک NIST قابل مقایسه است (NIST, 2014a).

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۲- ریسک	تاب آوری مستلزم هوشیاری موقعیتی مناسب است. به همین دلیل بایست طیف گسترده ای از ارزیابی ریسک صورت گیرد. این ارزیابی تمامی سناریوهای تهدیدآمیز شناخته شده را شناسایی میکند. همچنین این مرحله، شیوه های هوشیاری موقعیتی را به منظور هدایت بهترین تصمیمات برای تضمین ادامه فعالیت مطلوب اجزا و دارایی های حیاتی بکار میگیرد. خروجی این مرحله، توصیف دقیق تهدیدات و آسیب ها است که مکفی برای حمایت تصمیم گیری ها بر اساس اولویت های سازمانی میباشد. این اصل با فاز "ارزیابی امنیت" NIST 800-53a مطابقت دارد (NIST, 2014c).

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۳-رتبه بندی	این مرحله دارایی هایی را که سازمان بطور قطع نمیتواند از دست بدهد، انتخاب، ارزیابی و یک واکنش موثر برای هر یک از آنها اعمال میکند. دارایی ها شامل تمامی افراد، فرآیندها، فناوری ها و تسهیلات مورد نیاز برای دستیابی به اهداف سازمان میباشند. این اصل با فاز "انتخاب" NIST قابل مقایسه است (NIST, 2014a).

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۴- طراحی/ توسعه	تاب آوری بایست با معماری سازمان منطبق شود به گونه ای که عملکردهای حیاتی از حملات موفقیت آمیز حفاظت شوند. این طراحی کنترل های مورد نیاز برای تضمین کارکرد دارایی های حیاتی را توسعه می دهد. این فاز، اهداف صریح کنترل برای هریک از دارایی های حیاتی را شناسایی می کند. آن اهداف را اولویت بندی می کند و اقدامات هدفمند کنترل را به منظور دستیابی حداکثری به اهداف اولویتی پیاده سازی می کند. سپس مجموعه کنترل توسعه یافته را تحلیل می کند تا این اطمینان حاصل گردد که زیرساخت منتج اهداف اولویتی را حاصل گردد. این اصل با فاز "پیاده سازی" NIST انطباق دارد (NIST, 2014a).

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۵- تست و آزمون	تاب آوری سیستم بایست ارزیابی گردد. این یک کار برنامه ریزی شده است که عملکرد حیاتی کنترل را در برابر اهداف مشخص ماموریت شناسایی می کند. از جمله روش های مورد استفاده در این فاز می توان به "تست نفوذ پذیری" اشاره کرد. این فاز را نیز می توان با فاز "ارزیابی" در NIST انطباق داد (NIST, 2014a).

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۶- بهبود و ترمیم	تعاریف مناسب و خوب فرآیندها و پردازش ها بایست مستند شوند و در مکان هایی قرار داده شوند که تمامی توابع سازمان بطور کامل درون پارامترهای مطلوب مجدد ذخیره شوند. این مرحله قابل قیاس با توصیه های "برنامه- هدف- مرز- ارتباط" در NIST SP 800–34 می باشد.

هفت اصل کلی در تاب آوری سایبری

اصل	توضیحات
۷- تکامل	دراین مرحه برای شناسایی و توسعه عکس العمل ها و بهبود های فرآیند و فناوری ها در سازمان می باشد همچنین سازمان بصورت پویا ، معماری تاب آوری سایبری خود را براساس درسهای آموخته شده تنظیم می کند . این درسهای آموخته شده معمولا شامل ارزیابی عملکرد فرآیندهای توسعه یافته در برابر برنامه ها ، اهداف، استانداردها و روندها و همچنین نتایج نوآوری سازمانی و توسعه فرآیند است . این اصل با پیاده سازی فرآیند چارچوب امنیت سایبری NIST مطابقت دارد

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

مدل ارزیابی و توسعه تاب آوری یک روش ارزیابی نسبتا ساده است ، که توسط موسسه مهندسی نرم افزار دانشگاه کارنگی ملون در سال ۲۰۱۶ که وابسته به وزارت امنیت داخلی آمریکا میباشد به منظور ارزیابی تاب آوری سایبری و عملکردهای تداوم خدمات صاحبان و فعالان حوزه های زیربنای و حیاتی ارایه شده است.

- Carnegie Mellon
- DHS

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

- در روش مدل ارزیابی و توسعه تاب آوری ، بر اساس شاخصهای از قبل معین شده ، در مدت زمان محدود ارزیابی را انجام میشود .
- در این بسته مدل ارزیابی و توسعه تاب آوری این اجازه میدهد که سازمان ها بدون مشارکت تسهیل کنندگان خارجی وضعیت تاب آور بودن سازمان متبوع خود را بسنجند .

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

- با بهر گیری از سؤال های معین و مشخص در یک قالب ساختار یافته ، مکانیسم های را برای به نتیجه رساندن تاب آوری و گزینه هایی برای بهبود آن به همراه خواهد دارد .
- مدل ارزیابی و توسعه تاب آوری یک ارزیابی مبتنی بر مصاحبه است که بعنوان بخشی از یک برنامه مدیریت امنیت سایبری سازمان است.

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

- در این روش تلاش برای درک مدیریت امنیت سایبر سرویس ها و دارایی های مرتبط با آن است که برای موفقیت مأموریت سازمان ضروری است.
- مدل ارزیابی و توسعه تاب آوری تمرکز بر شیوه های حفاظت و نگهداری در حوزه های کلیدی است که معمولا به تاب آوری کامل یک سازمان کمک میکند.

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

- مدل ارزیابی و توسعه تاب آوری اقدامات لازم و ضروری برای امنیت سایبری را برای ارائه شاخص های معنی داری از قابلیت تاب آوری سازمان در حین عملیات عادی و در زمان استرس عملیاتی اندازه گیری می کند. .
- این مدل یک مدل بلوغ متمرکز بر توانایی برای بهبود فرآیند است و این نشان دهنده بهترین شیوه های صنعت و دولت برای مدیریت تاب آوری عملیات در رشته های مدیریت امنیت، مدیریت تداوم کسب و کار و مدیریت عملیات فناوری اطلاعات است.

مدل ارزیابی و توسعه تاب آوری در مقابل تهدیدات سایبری

- در این مدل ۱۰ دامنه اصلی و برای هر دامنه تعدادی هدف و شیوه اجرا در نظر گرفته شده است .

	دامنه
۱	مدیریت دارایی
۲	مدیریت کنترل
۳	پیکره بندی و مدیریت تغییر
۴	مدیریت آسیب پذیری
۵	مدیریت رخداد
۶	مدیریت تداوم خدمات
۷	مدیریت ریسک
۸	مدیریت وابستگی خارجی
۹	آموزش و آگاهی
۱۰	آگاهی وضعیتی

(هاملند سکیوریتی ، ۲۰۱۶)

دامنه ۱: مدیریت دارایی

- هدف مدیریت دارایی شناسایی، مستند سازی و مدیریت دارایی ها در طول چرخه زندگی خود برای اطمینان از بهره وری پایدار برای پشتیبانی از سرویس های حیاتی سازمان می باشد .

- در دامنه مدیریت دارایی سازمان یک روش برای برنامه ریزی، شناسایی، مستند سازی و مدیریت دارایی های خود را ایجاد می کند.

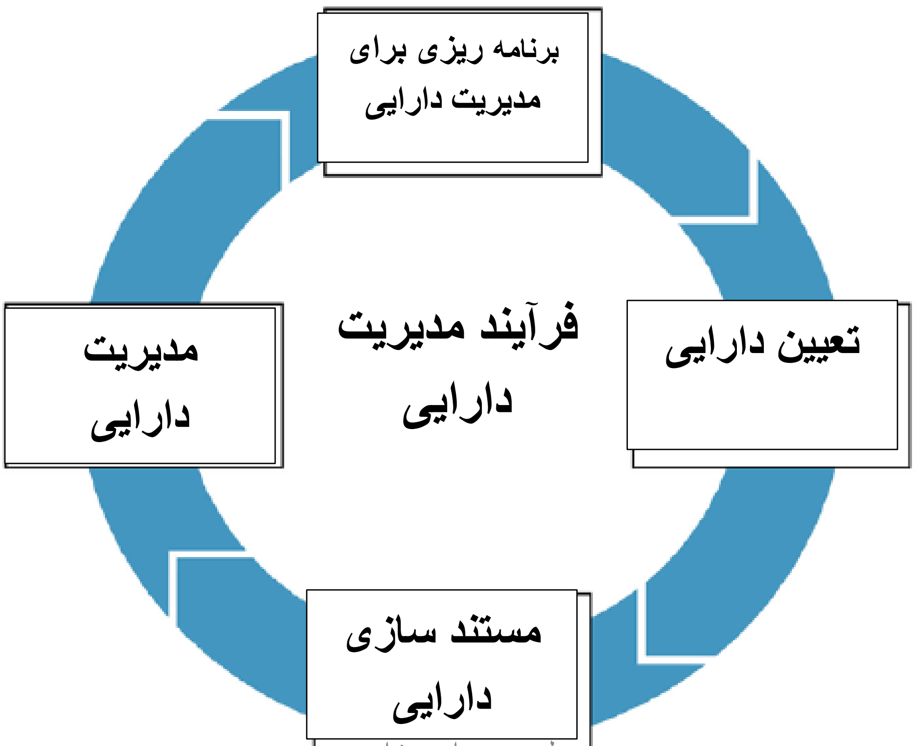
دامنه ۱: مدیریت دارایی

- دارایی ها مواد خامی است که برای انجام خدمات نیاز می شوند . مدل ارزیابی و توسعه تاب آوری دارایی ها را به دسته های زیر دسته بندی می کنند

درایی	هدف
افراد	برای کار و نظارت بر خدمات
اطلاعات و داده ها	برای تغذیه فرایند و تولید توسط سرویس
فناوری	برای اتوماسیون و پشتیبانی از سرویس
تجهیزات	قابلیت ها برای انجام خدمات

دامنه ۱: مدیریت دارایی

- مدل مدیریت دارایی را انجام می دهد مدیریت دارایی در چهار گام اصلی همانگونه که در شکل زیر نشان داده انجام می پذیرد (راهنمای مدیریت منابع سی.ار.ار ، ۲۰۱۶)



اهداف و شیوه مدیریت دارایی

۱- شناسایی و اولویت بندی خدمات .

۱. خدمات سازمان شناسایی شوند.

۲. خدمات سازمان بر اساس نگرش تاثیر بالقوه در صورت اختلال خدمات اولویت بندی شوند.

۳. مأموریت، چشم انداز، ارزش ها و هدف سازمان، از جمله سازمان ها در زیر ساخت های حیاتی شناسایی شده و و اطلاع رسانی شود

۴. مأموریت سازمان، اهداف و فعالیت ها در اولویت قرار گیرد .

اهداف و شیوه مدیریت دارایی

۲. دسته بندی دارایی ها و تعیین مسئولیت این دارایی ها

۱. مشخص نمودن دارایی هایی که مستقیما از سرویس حیاتی پشتیبانی می کنند، (تکنولوژی شامل سخت افزار، نرم افزار و سیستم های اطلاعاتی خارجی).

۲. مشخص نمودن الزامات حفاظت و نگهداری در شرح دارایی ها

۳. مستند سازی صاحبان و نگهبانان دارایی در توضیحات دارایی

۴. مستند سازی مکان های فیزیکی دارایی (در داخل و خارج از سازمان) در موجودی دارایی

۵. مستند سازی و نقشه بندی ارتباطات سازمانی و جریان داده ها در موجودی دارایی ها

اهداف و شیوه مدیریت دارایی

۳. تعیین ارتباط بین دارایی ها و خدماتی که آنها پشتیبانی می کنند

۱. تعیین ارتباط بین دارایی ها و سرویس های مهمی که آنها را پشتیبانی می کند.

۲. الزامات محرمانه بودن، یکپارچگی و در دسترس بودن برای هر یک از دارایی های خدماتی مشخص شده

اهداف و شیوه مدیریت دارایی

۴. مدیریت موجودی دارایی

۱. تعیین معیارهای تغییر برای توصیف دارایی ها

۲. توضیحات دارایی هنگامی که تغییرات در دارایی رخ می دهد به روز می شود.

اهداف و شیوه مدیریت دارایی

۵. مدیریت دسترسی به دارایی ها

۱. دسترسی (از جمله هویت ها و اعتبارنامه ها) به دارایی ها بر اساس الزامات حفاظتی آنها اعطا می شود.

۲. دسترسی درخواست (شامل هویت ها و اعتبارنامه ها) توسط مالک دارایی مورد بررسی و تایید قرار می گیرد.

۳. امتیازات دسترسی برای شناسایی امتیازات بیش از حد یا نامناسب بررسی می شود.

۴. میزان و سطح دسترسی براساس بررسی انجام شده معین و تغییر یافته باشد .

۵. مجوزهای دسترسی مدیریت می شود که شامل اصل حداقل امتیاز است.

۶. مجوزهای دسترسی اداره می شوند که شامل اصل تفکیک وظایف می شود.

اهداف و شیوه مدیریت دارایی

۶. طبقه بندی و مدیریت دارایی های اطلاعاتی جهت حصول اطمینان و حفظ خدمات حیاتی.

۱. دارایی های اطلاعاتی براساس حساسیت و تاثیر بالقوه خدمات حیاتی (مانند عمومی، استفاده داخلی یا محرمانه) طبقه بندی شده اند.

۲. طبقه بندی دارایی های اطلاعاتی نظارت و اجرا می شود.

۳. سیاست ها و رویه ها برای برچسب گذاری مناسب و مدیریت دارایی های اطلاعاتی ایجاد می شود.

۴. همه اعضای کارکنانی که دارایی های اطلاعاتی را شامل می شوند (از جمله کسانی که خارج از سازمان هستند، مانند پیمانکاران) در استفاده از دسته های اطلاعاتی آموزش دیده اند.

۵. دارایی های اطلاعاتی ارزشمند پشتیبانی و حفظ می شوند.

۶. دستورالعمل های مناسب برای مدیریت دارایی های اطلاعاتی ایجاد می شود.

۷. پیروی از دستورالعمل های مدیریت دارایی اطلاعاتی نظارت و اجرا می شود.

اهداف و شیوه مدیریت دارایی

۷. اولویت بندی و مدیریت دارایی ها و تسهیلاتی که از خدمات حیاتی حمایت می کنند

۱. امکانات بر اساس تاثیر بالقوه آنها برای خدمات حیاتی، اولویت بندی می شوند تا شناسایی آن ها که باید تمرکز فعالیت های حفاظت و نگهداری باشد.

۲. اولویت بندی تسهیلات بررسی و تایید می شود.

۳. الزامات حفاظت و نگهداری خدمات حیاتی در هنگام انتخاب امکانات در نظر گرفته می شود.

برگزاری کارگاه مدیریت دارایی سایبری

دامنه ۲: مدیریت کنترل

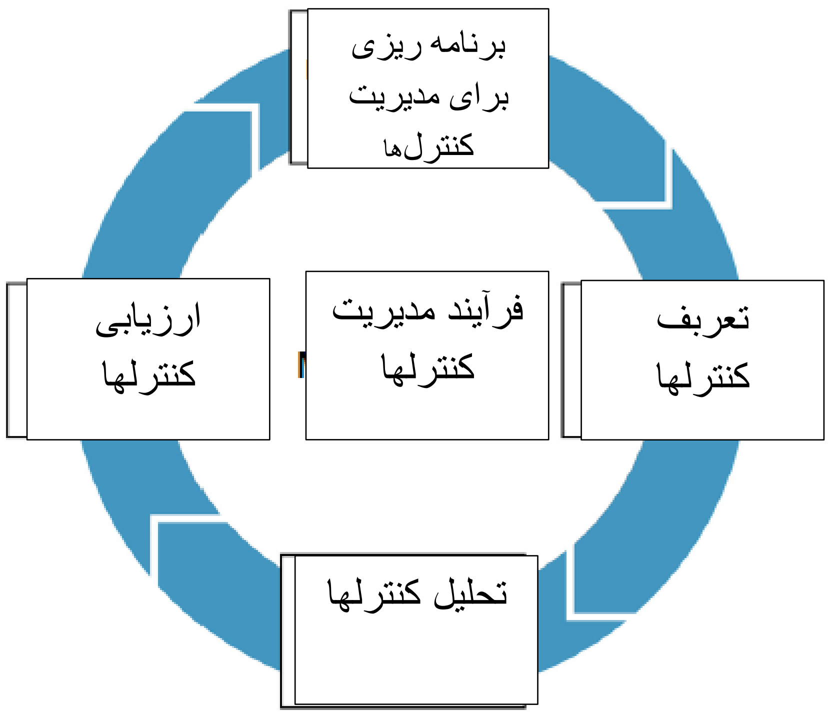
- هدف مدیریت کنترل شناسایی، تجزیه و تحلیل و مدیریت کنترل در یک محیط عملیاتی خدمات حیاتی می باشد .
- کنترل داخلی یک فرآیند نظارتی است که توسط یک سازمان برای اطمینان از دستیابی موثر و کارآمد به اهداف سازمانی و ارائه ضمانت معقول موفقیت انجام می شود.

دامنه ۲: مدیریت کنترل

- دامنه مدیریت کنترل، که در مدل ارزیابی و توسعه تاب آوری مشخص شده است، یک راه برای سازمان برای شناسایی اهداف کنترل و ایجاد کنترل برای رسیدن به این اهداف است.
- دامنه مدیریت کنترل همچنین اهمیت تجزیه و تحلیل و ارزیابی این کنترل ها را مورد بررسی قرار می دهد تا اطمینان حاصل شود که روند در حال بهبود است. (راهنمای مدیریت کنترل سی . ار. ار ۲۰۱۶)
- - CRR Supplemental Resource Guide- Controls Management

فرآیند مدیریت کنترل

- مدیریت کنترل در چهار گام اصلی همانگونه که در شکل زیر نشان داده انجام می پذیرد



اهداف و شیوه مدیریت کنترل

۱-تعیین اهداف کنترل

۱. اهداف کنترل برای دارایی های مورد نیاز برای تحویل خدمات حیاتی تعیین شده است.

۲. اهداف کنترل با توجه به توان بالقوه آنها برای تأمین خدمات بحرانی اولویت بندی می شوند.

انواع کنترل

۱-کنترلهای اداری (مدیریت)

- از هماهنگی با اهداف مدیریت اطمینان پیدا می کند
- اقداماتی نظیر : حاکمیت – سیاست گذاری – حسابرسی – تفکیک وظایف و تدوین و اجرای تداوم خدمات
- برای پیاده سازی الزامات تاب آوری محرمانه بودن ، یکپارچگی و در دسترس بودن

انواع کنترل

۲- کنترل های فنی (عملیاتی)

- از طریق ابزار های فناوری اجرایی می شوند
- کنترل های دسترسی الکترونیکی ، فایروال ها ، رمزگذاری ، سیستم های کشف ورود و خروج
- در فرایند های خودکار حضور دارند
- کاربرد : زیر ساخت نرم افزار ، سیستم ها ، سخت افزار ، شبکه ، ارتباطات از راه دور

علی محمد امین زاده -
am.aminzadeh@sndu.ac.ir

انواع کنترل

۲- کنترل های فیزکی

- موانع فیزیکی را برای دسترسی ایجاد می کنند
- کاربرد : افراد (از نظر ایمنی) ، فناوری ، دارائی های ملموس مانند تاسیسات
- نمونه ها : شناسه تصویری ، کارت خوان ها ، قفل های روی ورودی اتاق های اطلاعات
- این کنترل علاوه بر یکپارچگی و در دسترس بودن برای اطمینان از محرمانه ماندن اطلاعات استفاده می شود

انواع کنترل

۱. پیشگیرانه

- برای بازداری یا جلوگیری از وقوع وادث نامطلوب
- معمولا ماهیت فیزیکی یا فنی دارند

۲. کشف کننده

- کشف اقدامات نامطلوب
- وقوع یک حادثه را نشان می دهد

۳. جبران کننده

- نظارت بیشتر
- کاهش ریسک تاثیر گذاری حوادث نامطلوب

۴. اصلاح کننده

- کمک به حل مشکلات شناسایی شده

اهداف و شیوه مدیریت کنترل

۲. اجرا کنترل

۱. کنترل برای رسیدن به اهداف کنترل شده برای خدمات اساسی انجام می شود.

۲. کنترل برای اجرای حفاظت از شبکه انجام می شود، در صورت لزوم، جداسازی شبکه را شامل می شود.

۳. کنترل برای حفاظت داده ها در حالت استراحت انجام می شود.

۴. کنترل برای حفاظت از اطلاعات در حمل و نقل اجرا می شود.

۵. کنترل برای محافظت در برابر نشت داده ها اجرا می شود.

اهداف و شیوه مدیریت کنترل

۲. اجرا کنترل

۶. گزارش های حسابرسی / ثبت نام، مستند شده، اجرا و بررسی شده با توجه به سیاستهای سازمان .

۷. کنترل برای حفاظت و محدود کردن استفاده از رسانه های قابل جابجایی مطابق با سیاست اجرا می شود.

۸. برای حفاظت از شبکه های ارتباطی و کنترل، کنترل ها اجرا می شوند.

۹. شیوه های منابع انسانی امنیت سایبری برای خدمات حیاتی (مانند برنامه ریزی، بازرسی پرسنل) اجرا می شود.

۱۰. دسترسی به سیستم ها و دارایی ها با ترکیب اصل کمترین قابلیت (به عنوان مثال لیست سفید، فهرست سیاه و غیره) کنترل می شود.

اهداف و شیوه مدیریت کنترل

۳. تحلیل طرح های کنترل برای اطمینان از برآورده شدن اهداف کنترل

۱. طرح های کنترل برای شناسایی شکاف هایی که اهداف کنترل به طور کامل رضایت ندارند، مورد تجزیه و تحلیل قرار می گیرد.

۲. به عنوان یک نتیجه از تجزیه و تحلیل کنترل، کنترل های جدید معرفی شده و یا کنترل های موجود برای رفع شکاف تغییر یافته است.

اهداف و شیوه مدیریت کنترل

۴. رعایت سیستم کنترل داخلی برای اطمینان از اهداف کنترل

۱. عملکرد کنترل ها براساس یک برنامه مشخص می شود تا تأیید شود که آنها همچنان به اهداف کنترل برسند.

۲. در نتیجه ارزیابی های برنامه ریزی شده، کنترل های جدید معرفی می شوند یا کنترل های موجود برای حل مسائل مشکل تغییر می کنند.

برگزاری کارگاه مدیریت کنترل سایبری

دامنه ۳: پیکربندی و مدیریت تغییر

- هدف: برای ایجاد فرآیندهای اجرایی مناسب برای اطمینان از یکپارچگی دارایی ها، با استفاده از کنترل تغییر و حسابرسی کنترل تغییر می باشد.
- زیرساخت سایبری براساس تغییرات تکنولوژی، اطلاعات به روز شده و استخدام پرسنل جدید به طور مداوم در حال تغییر می باشد .

دامنه ۳: پیکربندی و مدیریت تغییر

- دامنه پیکربندی و مدیریت تغییر تعیین می کند سازمان چگونه می تواند فرایندها و رویه های مدیریت دارایی ها را اجرا   کند،   و اطمینان حاصل کند که تغییراتی که به این دارایی ها انجام می شود، برای سازمان مضر نیست .دامنه پیکربندی و مدیریت تغییر شامل سه هدف و ۲۳ شیوه است

اهداف و شیوه پیکربندی و مدیریت تغییر

۱. مدیریت چرخه زندگی دارایی

۱. فرایند مدیریت تغییر برای مدیریت تغییرات در دارایی استفاده می شود.

۲. الزامات تاب آوری به عنوان یک نتیجه از تغییرات در دارایی ها ارزیابی می شود.

۳. مدیریت و برنامه ریزی ظرفیت برای دارایی ها انجام می شود.

۴. درخواست های تغییرات در دارایی ردیابی می شود.

۵. صاحبان سهام هنگامی که تحت تاثیر تغییرات دارایی هستند مطلع می شوند.

۶. یک چرخه زندگی توسعه سیستم برای مدیریت سیستم های پشتیبانی از بحران اجرا می شود

اهداف و شیوه پیکربندی و مدیریت تغییر

۲. مدیریت تمامیت دارایی فناوری و اطلاعات

۱. مدیریت پیکربندی برای دارایی های تکنولوژی انجام می شود.

۲. تکنیک ها برای تشخیص تغییرات در دارایی های تکنولوژیکی استفاده می شود.

۳. تغییرات در دارایی های تکنولوژی بررسی می شود.

۴. الزامات یکپارچگی برای تعیین اینکه چه کارکنان مجاز به تغییر دارایی های اطلاعاتی هستند .

۵. یکپارچگی دارایی های اطلاعاتی نظارت می شود.

۶. اصلاحات غیر مجاز یا غیرقابل توضیح به دارایی های تکنولوژی اعمال می شود.

اهداف و شیوه پیکربندی و مدیریت تغییر

۲. مدیریت تمامیت دارایی فناوری و اطلاعات

۷. تغییرات در دارایی های سیستم های تکنولوژیک قبل از اینکه به تولید وابسته شوند، آزمایش می شوند

۸. فرآیند مدیریت دسترسی به دارایی های تکنولوژیکی پیاده سازی شده است.

۹. نگهداری و تعمیر دارایی ها به موقع انجام می شود و وارد سیستم می شود.

۱۰. نگهداری و تعمیر دارایی ها با ابزارهای تایید شده و کنترل شده انجام می شود

۱۱. تعمیر و نگهداری راه دور و تعمیر دارایی ها مورد تایید، ورود و خروج قرار می گیرد

۱۲. شیوه ای که از دسترسی غیرمجاز جلوگیری می کند وجود دارد .

اهداف و شیوه پیکربندی و مدیریت تغییر

۳. تعیین پایه پیکربندی دارایی

۱. مستندات پیکربندی دارایی های تکنولوژی ایجاد می شوند.

۲. برای تغییرات پیشنهاد شده ، بررسی کاملی انجام می شود .

۳. خط مبنا و پایه ایی(baseline) برای عملیات شبکه ایجاد شده است.

۴. خط مبنا عملیات شبکه مدیریت می شود.

۵. مبنای جریان داده مورد انتظار برای کاربران و سیستم ها ایجاد شده است.

۶. جریان داده مورد انتظار برای کاربران و سیستم ها مدیریت می شود

برگزاری کارگاه پیکربندی و مدیریت تغییر

دامنه ۴: مدیریت آسیب پذیری

- هدف اصلی از مدیریت آسیب پذیری دارایی ها شناسایی، تجزیه و تحلیل و مدیریت آسیب پذیری ها در محیط عملیاتی ارائه خدمات حیاتی می باشد . آسیب پذیری یکی از حساسیتهای مهم در عملکرد صحیح تجهیزات و ارائه خدمات حیاتی مربوطه در زمان اختلال می باشد .

دامنه ۴: مدیریت آسیب پذیری

- از آنجایکه آسیب پذیری ها می توانند به خطرات عملیاتی منجر شوند باید شناسایی و مدیریت شوند تا از وقوع اختلال در محیط عملیاتی خدمات حیاتی جلوگیری شود.

- یک فرآیند مدیریت آسیب پذیری باید قبل از بهره برداری از آسیب پذیری ها شناسایی و تحلیل شود و سیستم را در فرآیند مدیریت ریسک تحلیل و آگاه نماید تا مشخص شود که آیا بر اساس میزان تحمل پذیری سازمان در مقابل این آیا سازمان به خطر می افتد یا خیر .*دامنه مدیریت آسیب پذیری شامل چهار هدف و ۱۵ شیوه است*

اهداف و شیوه مدیریت آسیب پذیری

۱. آماده سازی برای تجزیه و تحلیل آسیب پذیری ها و فعالیت های لازم برای حل و فصل آنها

۱. تجزیه و تحلیل آسیب پذیری و راهبرد های حل و فصل توسعه یافته است.

۲. مجموعه ای از ابزار و / یا روش های استاندارد برای شناسایی آسیب پذیری در دارایی ها وجود دارد.

۳. یک مجموعه استاندارد ابزار و / یا روش ها برای تشخیص کد مخرب در دارایی ها استفاده می شود.

۴. مجموعه ای از ابزارها و / یا روش های استاندارد برای تشخیص کد های غیر مجاز در دارایی استفاده می شود.

۵. یک مجموعه استاندارد ابزار و / یا روش ها برای نظارت بر دارایی ها برای پرسنل غیر مجاز، اتصالات، دستگاه ها و نرم افزار استفاده می شود.

اهداف و شیوه مدیریت آسیب پذیری

۲. ایجاد و حفظ روند شناسایی و تجزیه و تحلیل آسیب پذیری ها

۱. منابع اطلاعات آسیب پذیر شناسایی شده اند.

۲. اطلاعات از این منابع در جریان است.

۳. آسیب پذیری ها فعالانه کشف می شوند.

۴. آسیب پذیری ها دسته بندی شده و اولویت بندی می شوند.

۵. آسیب پذیری ها برای تعیین ارتباط با سازمان تجزیه و تحلیل می شوند.

۶. مخزن برای ضبط اطلاعات در مورد آسیب پذیری ها و حل و فصل آنها استفاده می شود.

اهداف و شیوه مدیریت آسیب پذیری

۳. اقدامات لازم برای مدیریت مواجهه آسیب پذیری های شناسایی شده

۱. اقدامات لازم برای مدیریت مواجهه با آسیب پذیری های شناسایی شده انجام می شود.

۲. اثربخشی کاهش آسیب پذیری بررسی شده است.

۳. وضعیت آسیب پذیری های حل نشده تحت نظارت است.

۴. توجه به علل ریشه ای آسیب پذیری ها

علل اصلی آسیب پذیری ها (از طریق تجزیه و تحلیل علل ریشه یا روش های دیگر) شناسایی شده و مورد توجه قرار می گیرند.

برگزاری کارگاه مدیریت آسیب پذیری

دامنه ۵: مدیریت حوادث

- هدف اصلی از مدیریت رخداد ها ایجاد مراحل شناسایی و تجزیه و تحلیل رویدادها، تشخیص حوادث و تعیین پاسخ مناسب سازمانی می باشد .
- اختلال در محیط عملیاتی سازمان به طور مرتب رخ می دهد و لازم است دامنه مدیریت حوادث، قابلیت سازمان را برای تشخیص اختلالات بالقوه، تجزیه و تحلیل آنها و تعیین نحوه و زمان پاسخگویی بررسی کند.
- حوزه مدیریت حوادث شامل پنج هدف و ۲۳ شیوه است

اهداف و شیوه مدیریت حوادث

۱. ایجاد فرایند شناسایی، تحلیل، پاسخ دادن و یادگیری از حوادث

۱. سازمان برنامه ای برای مدیریت حوادث دارد.

۲. طرح مدیریت حادثه بررسی و به روز می شود.

۳. نقش ها و مسئولیت ها در طرح در شرح شغل گنجانده شده است.

۴. در برنامه مدیریتی به کارکنان نقش و مسئولیت های مشخص شده در حادثه اختصاص داده شده است

اهداف و شیوه مدیریت حوادث

۵. رویدادها اولویت بندی می شوند.

۶. وضعیت رویدادها ردیابی می شود.

۷. رویدادها قابل حل هستند.

۸. الزامات (قوانین، قوانین، مقررات، سیاست ها و غیره) برای شناسایی شواهد رویداد برای اهداف قانونی شناسایی می شوند.

۹. فرایند برای اطمینان از حصول اطمینان در مورد رویدادهای مورد نیاز توسط قانون انجام می شود یا سایر تعهدات پیگیری می شود.

اهداف و شیوه مدیریت حوادث

۲. فرآیند شناسایی، گزارش دهی، ردیابی و تجزیه و تحلیل رویدادها .

۱. رویدادها شناسایی و گزارش می شوند (شامل رویدادهای مربوط به امنیت سایبری مربوط به پرسنل فعالیت، فعالیت شبکه، محیط فیزیکی و اطلاعات).

۲. داده های رویداد در یک پایگاه اطلاعاتی حادثه یا مکانیزم مشابه وارد شده است.

۳. رویدادها طبقه بندی شده اند.

۴. رویدادها برای تعیین اینکه آیا آنها مربوط به رویدادهای دیگر هستند، تجزیه و تحلیل می شوند.

۳. اعلام حوادث

۱. حوادث اعلام شده است.

۲. معیارهای اعلام حادثه تعیین می شود.

۳. حوادث برای تعیین یک پاسخ بررسی می شوند.

اهداف و شیوه مدیریت حوادث

۴. فرایند پاسخگویی و بهبود حوادث مشخص شده

۱. حوادث برای ورود و تفکیک به سهامداران اعلان می شود .

۲. پاسخ به حوادث اعلام شده، مطابق با رویه های پیش تعریف شده، طراحی شده و اجرا می شود.

۳. وضعیت حوادث و واکنش به طرف احزاب آسیب دیده (از جمله کارکنان روابط عمومی و رسانه های خارجی) اطلاع داده می شود.

۴. حوادث ردیابی می شوند.

اهداف و شیوه مدیریت حوادث

۵. تبدیل درسهای آموخته شده پس از حادثه به برنامه های بهبود

۱. برای تعیین علل ریشه های حوادث، تجزیه و تحلیل انجام شده است.

۲. ارتباط بین پروسه مدیریت رویداد و سایر فرایندهای مرتبط (مدیریت آسیب پذیری ها ، مدیریت ریسک، مدیریت تغییر، و غیره) ایجاد شده است.

برگزاری کارگاه مدیریت حوادث

دامنه ۶: مدیریت تداوم خدمات

- هدف مدیریت تداوم خدمات برای اطمینان از تداوم عملیات ضروری خدمات و دارایی های مرتبط با آن، اگر یک وقفه ناشی از حادثه، فاجعه یا رویداد دیگر رخ دهد.فرآیند ارزیابی، اولویت بندی، برنامه ریزی و پاسخ به برنامه های مربوط به وقوع حوادث ناگوار و بهبود آن ها به عنوان تداوم خدمات شناخته می شود.

دامنه ۶: مدیریت تداوم خدمات

- هدف از تداوم خدمات، کاهش اثرات حوادث ناگوار با استفاده از برنامه های آزمایش شده یا انجام شده است که تداوم قابل پیش بینی و تداوم خدمات بحرانی را تسهیل می کند.
- دامنه مدیریت تداوم سرویس شامل چهار هدف و ۱۵ شیوه است:

اهداف و شیوه مدیریت تداوم خدمات

۱. توسعه برنامه های تداوم خدمات برای خدمات ارزشمند

۱. برنامه های تداوم خدمات برای دارایی ها (مردم، اطلاعات، فن آوری و امکانات) که برای تحویل خدمات حیاتی ارائه می شوند، توسعه یافته و مستند می شوند.

۲- درسهای آموخته شده از مدیریت حوادث برای بهبود حفاظت از دارایی ها و اصلاح راهبرد و برنامه ها

۳- برنامه های تداوم خدمات با استفاده از استانداردها، دستورالعمل ها و قالب های ایجاد شده توسعه یافته است.

اهداف و شیوه مدیریت تداوم خدمات

۲. بررسی برنامه های تداوم خدمات برای حل اختلاف بین برنامه ها

۱. برنامه ها برای شناسایی و حل و فصل اختلافات بررسی می شوند.

۳. آزمایش برنامه های تداوم خدمات در جهت ایجاد اطمینان از برآورده شدن اهداف اعلام شده

۱. استانداردهای تست برنامه های تداوم خدمات پیاده سازی شده است.

۲. برنامه ای برای تست برنامه های تداوم خدمات ایجاد شده است.

۳. برنامه تداوم خدمات تست شده است.

۴. روش پشتیبان گیری و ذخیره سازی برای دارایی های اطلاعات ارزشمندی مورد آزمایش قرار می گیرد.

۵. نتایج تست با اهداف تست مقایسه می شود تا شناسایی بهبود های مورد نیاز در سرویس برنامه های تداوم

اهداف و شیوه مدیریت تداوم خدمات

۴. برنامه ریزی و بررسی برنامه های تداوم خدمات

۱. شرایط شناسایی شده است که باعث اجرای طرح تداوم خدمات می شود.

۲. اجرای برنامه های تداوم خدمات بررسی می شود.

۳. بهبود در نتیجه اجرای برنامه های تداوم خدمات شناسایی می شود. تداوم خدمات استفاده می شود.

برگزاری کارگاه مدیریت تداوم خدمات

دامنه ۷: مدیریت ریسک

- هدف اصلی از مدیریت ریسک شناسایی، تجزیه و تحلیل و کاهش ریسک ها برای دارایی های خدمات بحرانی که می تواند بر عملکرد و ارائه خدمات تأثیر منفی داشته باشد.

- مدیریت ریسک یک فعالیت پایه ای برای هر سازمان است و در همه سطوح، از مدیران تا افراد درون واحد های کاری، را درگیر می کند.

- مدل ارزیابی و توسعه تاب آوری بر ریسک های مربوط به عملیات وابسته به سایبر متمرکز است که امکان وقوع تحویل سرویس حیاتی در بر می گیرد .

- در حالی که مدل ارزیابی و توسعه تاب آوری بر ریسک عملیاتی تمرکز دارد، مهم است که توجه داشته باشید که مدیریت ریسک عملیاتی نیازمند یک رویکرد جامع برای موثر بودن است.

- دامنه مدیریت ریسک شامل پنج هدف و ۱۳ شیوه است

اهداف و شیوه مدیریت ریسک

۱. توسعه راهبرد برای شناسایی، تحلیل و رفع خطرات .

۱. منابع خطراتی که می توانند بر عملیات تأثیر بگذارند شناسایی شده است.

۲. دسته بندی هایی برای خطرات ایجاد شده اند.

۳. برنامه ریزی برای مدیریت ریسک عملیاتی ایجاد شده است.

۴. طرح مدیریت ریسک عملیاتی به ذینفعان داده شده است.

اهداف و شیوه مدیریت ریسک

۲. شناسایی تحمل خطر و تمرکز فعالیت های مدیریت ریسک

۱. مناطق تاثیرگذار مانند شهرت، سلامت مالی و انطباق قانونی شناسایی شده است.

۲. مناطق تاثیرگذاری برای تعیین اهمیت نسبی آنها اولویت بندی شده اند.

۳. پارامترهای تحمل ریسک برای هر منطقه تاثیرگذاری تعیین شده است.

۴. آستانه تحمل ریسک، که باعث اقدام، برای هر دسته از خطرات تعریف می شود.

اهداف و شیوه مدیریت ریسک

۳. شناسایی ریسک ها

۱. خطرات عملیاتی که می تواند بر تحویل سرویس اساسی تأثیر بگذارد شناسایی می شود.

۴. تجزیه و تحلیل ریسک ها

۱. خطرات برای تعیین تاثیر بالقوه بر سرویس اساسی مورد تجزیه و تحلیل قرار می گیرند.

۲. وضعیت (پذیرش، انتقال، کاهش، و غیره) به خطرات شناخته شده اختصاص یافته است.

۵. کنترل و کاهش ریسک ها برای دارایی ها و خدمات

۱. برنامه ریزی برای ریسک هایی است که سازمان تصمیم می گیرد تا آن را کاهش دهد.

۲. خطرات شناسایی شده برای بستن ردیابی می شوند.

برگزاری کارگاه مدیریت ریسک

دامنه ۸: مدیریت وابستگی خارجی

- هدف مدیریت وابستگی خارجی برای ایجاد فرآیندهای برای مدیریت سطح مناسب کنترل برای اطمینان از پایداری و حفاظت از خدمات و دارایی هایی که وابسته به اقدامات نهادهای خارجی هستند.
- برون سپاری خدمات، توسعه و تولید، بخش عادی و معمولی عملیات برای بسیاری از سازمان ها شده است، زیرا برون سپاری می تواند مهارت ها و تجهیزات تخصصی را با صرفه جویی در هزینه ها بر روی گزینه های داخلی درگیر کند.
- دامنه مدیریت وابستگی خارجی مدل ارزیابی و توسعه تاب آوری یک روش برای یک سازمان برای شناسایی و اولویت بندی وابستگی های خارجی ارائه می دهد و سپس بر مدیریت و حفظ این وابستگی ها تمرکز می کند.
- دامنه مدیریت وابستگان خارجی شامل پنج هدف و ۱۴ شیوه است:

اهداف و شیوه مدیریت وابستگی خارجی

۱. شناسایی و اولویت بندی وابستگی های خارجی برای اطمینان از کارایی با ارزش بالا خدمات.

۱. وابستگی به روابط خارجی که برای سرویس مهم هستند شناسایی می شوند.

۲. یک پروسه برای ایجاد و نگهداری فهرست وابستگی های خارجی ایجاد شده است.

۳. وابستگی های خارجی اولویت بندی می شوند.

۲. خطرات ناشی از وابستگی های خارجی شناسایی و مدیریت می شوند.

۱. خطرات ناشی از وابستگی های خارجی شناسایی و مدیریت می شوند.

اهداف و شیوه مدیریت وابستگی خارجی

۳. تأسیس و نگهداری روابط با نهادهای خارجی بطور رسمی

۱. الزامات تاب آوری سرویس انتقادی ایجاد شده است که به طور خاص به هر وابستگی خارجی اعمال می شود.

۲. این الزامات بررسی و به روز می شود.

۳. توانایی اشخاص خارجی برای برآوردن نیازهای انعطاف پذیر خدمات حیاتی در فرایند انتخاب در نظر گرفته می شود.

۴. الزامات تاب آوری در موافقت نامه های رسمی با نهادهای خارجی گنجانده شده است.

اهداف و شیوه مدیریت وابستگی خارجی

۴. مدیریت عملکرد نهادهای خارجی

۱. عملکرد ارگان های خارجی در برابر الزامات تاب آوری نظارت می شود.

۲. مسئولیت نظارت بر عملکرد اجرایی خارجی (به عنوان مورد نیاز برای تاب آوری) تعیین می شود.

۳. برای مقابله با مسائل با عملکرد بیرونی خارجی (همانطور که مربوط به الزامات تاب آوری)، اقدامات اصلاحی لازم است.

۴. اقدامات اصلاحی ارزیابی می شود تا مشکلات حل شوند

۵. شناسایی وابستگی به خدمات عمومی و ارائه دهندگان خدمات زیرساخت

۱. خدمات عمومی که خدمات حیاتی آن بستگی دارد (پاسخ های آتش نشانی و خدمات نجات، اجرای قانون و غیره) شناسایی می شوند.

۲. ارائه دهندگان زیرساخت که خدمات حیاتی بستگی دارد (خدمات مخابراتی و تلفن، منابع انرژی و ...) شناسایی می شوند.

برگزاری کارگاه مدیریت وابستگی خارجی

دامنه ۹: آموزش و آگاهی

- هدف آموزش و آگاهی هدف آموزش و آگاه سازی، توسعه مهارت ها و ارتقاء آگاهی برای افرادی است که از نقش هایی که از خدمات حیاتی حمایت می کنند، حمایت می کند.
- آموزش و آگاهی بر روی فرایندهایی است که سازمان آن را برنامه ریزی، شناسایی نیازها، انجام و بهبود آموزش و آگاهی می کند تا اطمینان حاصل شود که الزامات و اهداف عملکرد انعطاف پذیر سایبری سازمان شناخته شده و ملاقات می شود.
- سازمان برنامه ای برای فعالیت های آموزشی و اطلاع رسانی است که اعضای کارکنان از نقش خود در نگرانی ها و سیاست های تاب آوری سایبری آگاه هستند.
- اعضای ستاد همچنین آموزش های ویژه ای را برای آنها فراهم می کند تا نقش خود را در مدیریت تاب آوری سایبری سازمانی بازی کنند.دامنه آموزش و آگاهی شامل دو هدف و ۱۱ شیوه است

اهداف و شیوه آموزش و آگاهی

۱. ایجاد برنامه آگاهی رسانی و برنامه های آموزشی سایبری

۱. نیازهای آگاهی رسانی در مورد امنیت سایبر برای خدمات حیاتی شناسایی شده است.

۲. مهارت های مورد نیاز برای نقش های خاص (مدیران، تکنسین ها، و غیره) برای سرویس انتقادی

۳. شکاف های موجود در پرسنل مسئول امنیت سایبری مشخص می شود.

۴. نیازهای آموزشی شناسایی شده است.

اهداف و شیوه آموزش و آگاهی

۲. فعالیت های آگاهی و آموزش در حال انجام است.

۱. فعالیت های آگاهی رسانی در مورد امنیت سایبری برای خدمات انتقادی انجام می شود.

۲. فعالیت های آموزشی در زمینه امنیت سایبری برای خدمات حیاتی انجام می شود.

۳. اثربخشی برنامه های آگاهی و آموزش، ارزیابی می شود.

اهداف و شیوه آموزش و آگاهی

۴. فعالیت های آگاهی و آموزش در صورت نیاز مورد تجدید نظر قرار می گیرد.

۵. کاربران مجاز در حمایت از خدمات انتقادی در نقش ها و مسئولیت های خاص خود آموزش دیده اند.

۶. مدیران ارشد در زمینه نقش وظیفه و مسئولیت های خاص خود در حمایت از خدمات حیاتی آموزش دیده اند.

۷. پرسنل امنیتی فیزیکی و اطلاعاتی در نقش های خاص و مسئولیت های خود در حمایت از خدمات حیاتی آموزش دیده اند.

برگزاری کارگاه آموزش و آگاهی

دامنه ۱۰: آگاهی وضعیتی

- هدف آگاهی وضعیتی فعالانه آشکار سازی و تجزیه و تحلیل اطلاعات مربوط به ثبات و امنیت فوری عملیاتی و هماهنگ کردن چنین اطلاعاتی را در سراسر شرکت برای اطمینان از اینکه تمام واحد های سازمانی تحت یک تصویر عملیاتی انجام می شوند.
- فعالیت های آگاهانه وضعیتی در سراسر سازمان برای ارائه اطلاعات به موقع و دقیق در مورد وضعیت فعلی فرایندهای عملیاتی انجام می شود. فعالیت ها باید از ارتباط با انواع ذینفعان داخلی و خارجی حمایت کنند تا از الزامات تاب آوری خدمات انتقادی پشتیبانی کنند. دامنه آگاهی وضعیتی شامل سه هدف و هشت روش است

اهداف و شیوه آگاهی وضعیتی

۱. نظارت بر تهدید

۱. مسئولیت نظارت بر منابع اطلاعات تهدید مشخص شده است.

۲. مراحل نظارت بر تهدید اجرا شده است.

۳. برای نظارت بر تهدید، منابع اختصاص یافته و آموزش دیده اند.

اهداف و شیوه آگاهی وضعیتی

۲. الزامات برقراری ارتباط اطلاعات تهدید

۱. ذینفعان داخلی (مانند صاحب خدمات مهم و کارکنان مدیریت حوادث) که اطلاعات تهدید را باید در اختیار آنها گذاشته شود شناسایی شده است.

۲. ذینفعان خارجی (مانند پرسنل مدیریت اورژانس، تنظیم کننده ها، وسازمان های به اشتراک گذاری اطلاعات) که اطلاعات مربوط به تهدید را باید در اختیار آنها گذاشته شود شناسایی شده است.

۳. انتقال اطلاعات تهدید

۱. اطلاعات تهدید به ذینفعان داده می شود.

۲. منابع برای تأیید اطلاعات تهدید و مسئولیت پذیری اختصاص یافته است.

۳. منابع با توجه به نقش خاص خود در برقراری ارتباط اطلاعات تهدید شده آموزش دیده اند.

برگزاری کارگاه آگاهی وضعیتی


و عجل فرجهم
اللهم صل علی محمد و آل محمد

تمرین/مانور سایبری

ارائه دهنده : خالق گرجی

فهرست مطالب

تمرین/رزمایش سایبری:

- عبارت است از مجموعه اتفاقات طرح ریزی شده به منظور ایجاد و ارتقاء توانمندیها و آمادگی‌ها و ارزیابی آنها در یک سازمان که به منظور پیشگیری از حملات سایبری،کشف و کاهش تاثیرات و واکنش به آن، اجرا می‌شود.
- یک رویداد برنامه‌ریزی شده که طی آن یک سازمان یک اختلال سایبری را برای توسعه یا آزمایش قابلیت هایی مانند جلوگیری ، شناسایی ، کاهش ، پاسخ یا بهبودی از اختلال شبیه سازی می کند.[۱]
- از تمرین‌های سایبر برای شبیه سازی محیط های حادثه سایبر برای ارزیابی دانش و مهارت پرسنل امنیت اطلاعات استفاده می شود. استفاده از تمرین سایبر برای ارزیابی آمادگی جامعه در برابر بحران سایبری و حوادث مهم زیرساخت اطلاعاتی گسترش یافته است.

1. *Source: NICCS™ Portal Cybersecurity Lexicon, National Initiative for Cybersecurity Careers and Studies (https://niccs.us-cert.gov/glossary) as of 11 November 2015*
2. **A Cyber Exercise Post Assessment: Adoption of the Kirkpatrick Model**: *Arniyati Ahmad, Christopher Johnson, Timothy Storer*

اهداف اجرای تمرین/رزمایش سایبری

- آزمودن میزان آمادگی خودی در برابر تهدیدات و حملات
- استخراج نقاط ضعف و قوت در برابر تهدیدات
- استخراج آسیب‌پذیری‌های موجود در سامانه‌های عملیاتی
- آموزش متخصصین سایبری
- ایجاد فرصتی جهت بکارگیری تجربیات
- ایجاد زیرساخت‌های فنی
- افزایش سطح همکاری بین تیم‌های شرکت کننده در برابر رخدادها و حوادث سایبری

- *Locked Shields*,

بزرگترین ، پیچیده ترین پیشرفته‌ترین تمرین دفاع سایبری است که توسط مرکز تعالی دفاع سایبری مشارکتی ناتو "*CCD COE*" در " تالین" پایتخت "استونی" برگزار می‌شود. این تمرین سایبری در سال ۲۰۱۷ با حضور بیش از ۹۰۰ متخصص امنیت سایبری از سراسر جهان و و تیم‌های مدافع سایبری ۲۰ کشور برگزار شد. در این تمرین که در آن بیش از ۳۰۰۰ سیستم مجازی درگیر بودند، بیش از ۲۵۰۰حمله به تیم های مدافع انجام شد. در این تمرین/مانور سیستم های شبکه هوشمند ، سیستم های سوخت رسانی هوا به هوا و سیستم های کنترل هواپیماهای بدون سرنشین در سال ۲۰۱۷ به محیط تمرین و مانور سایبری اضافه شدند.

- *Cyber Coalition*

ائتلاف سایبری یک تمرین جمعی بین اعضای ناتو است که جنبه رقابتی ندارد و برای حل مشکلات و تمرین انجام وظایف مشخص ، برای رسیدن به یک هدف خاص کار می کنند.

ائتلاف سایبری سه هدف اساسی را دنبال می کند:

- برای **تعامل بین ناتو** ، متحدان و شرکا برای بهبود همکاری در حوزه فضای مجازی با مکانیزم های موجود
- **افزایش توانایی اتحاد** در انجام عملیات فضای مجازی برای نهادهای نظامی و غیرنظامی با استفاده از **توسعه آگاهی وضعیتی** ، به **اشتراک گذاری اطلاعات** فضای مجازی و **مدیریت حوادث** سایبری ،
- شناسایی ضعف توانایی ، جهت احصاء نیازهای آموزشی.

این ائتلاف سایبر همه ساله توسط ناتو سازماندهی می شود. این یک رویداد سه روزه است و مشارکت اعضای ناتو و کشورهای متحد است.

Cyber Europe

این برنامه توسط ENISA[1] (آژانس اتحادیه اروپا برای شبکه و امنیت اطلاعات) ، هر دو سال یکبار برای اعضای اتحادیه اروپا برگزار می شود. بر خلاف تمرین های مستقر در ارتش مانند Lock Shields و ائتلاف سایبر ، این تمرین توسط یک مقام غیرنظامی برگزار می شود. این رزمایش که در سال ۲۰۱۶ برگزار شد ، شامل ۲۸ کشور عضو اتحادیه اروپا و ۲ کشور عضو " اتحادیه تجارت آزاد اروپا" (EFTA)[2] بود ، گرچه این کشورها عضو اتحادیه اروپا نیستند.

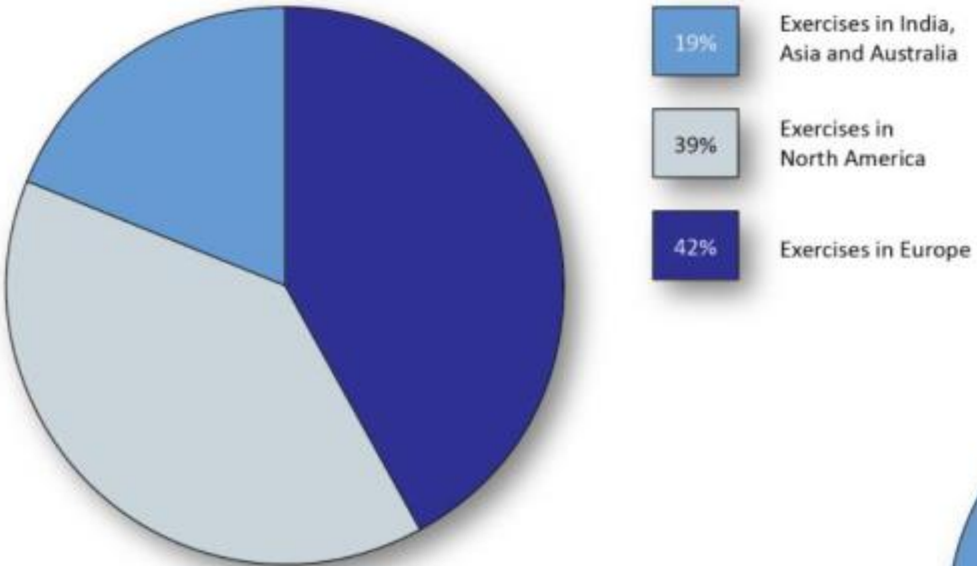
Cyber Defence Exercise(CDX)

یک رقابت سالانه است که توسط اداره تضمین اطلاعات متعلق به آژانس امنیت ملی ایالات متحده برگزار و پشتیبانی می‌شود و تعدادی ازکارشناسان موسسات آموزشی را برای طراحی ، پیاده سازی و دفاع از یک شبکه رایانه ای در برابر حمله رقابت می‌کنند. NSA شبکه تمرینی را ایجاد می کند و زیرساخت های امتیازدهی را فراهم می‌نماید و به عنوان داور مسابقه عمل می کند و یک تیم قرمز را با هدف به خطر انداختنِ محرمانگی، صحت و در دسترس بودن شبکه های رقبا ، آماده کرده و به کار می‌گیرد.شرکت کنندگان در این تمرین به شرح زیر هستند.

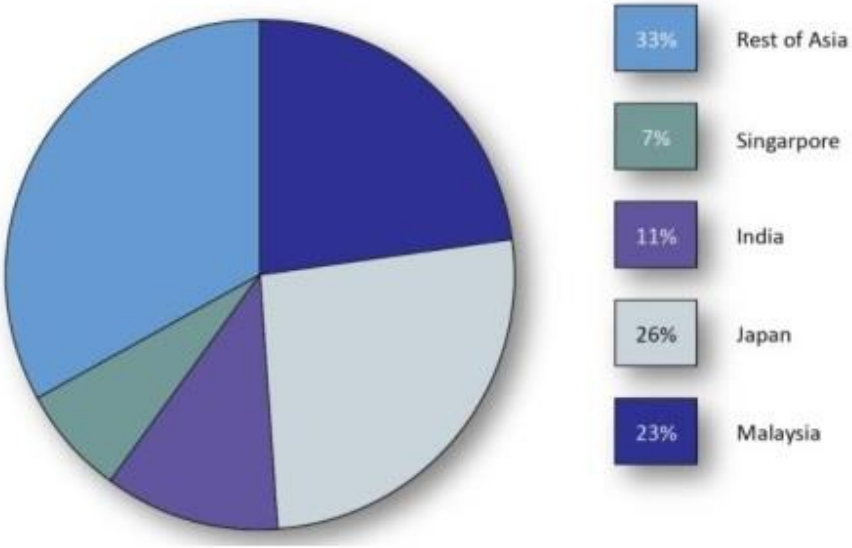
- United States Merchant Marine Academy
- United States Military Academy
- Air Force Institute of Technology
- Royal Military College of Canada

1. European Union Agency for Network and Information Security
2. European Free Trade Association

آمار تمرین‌های سایبری در دنیا

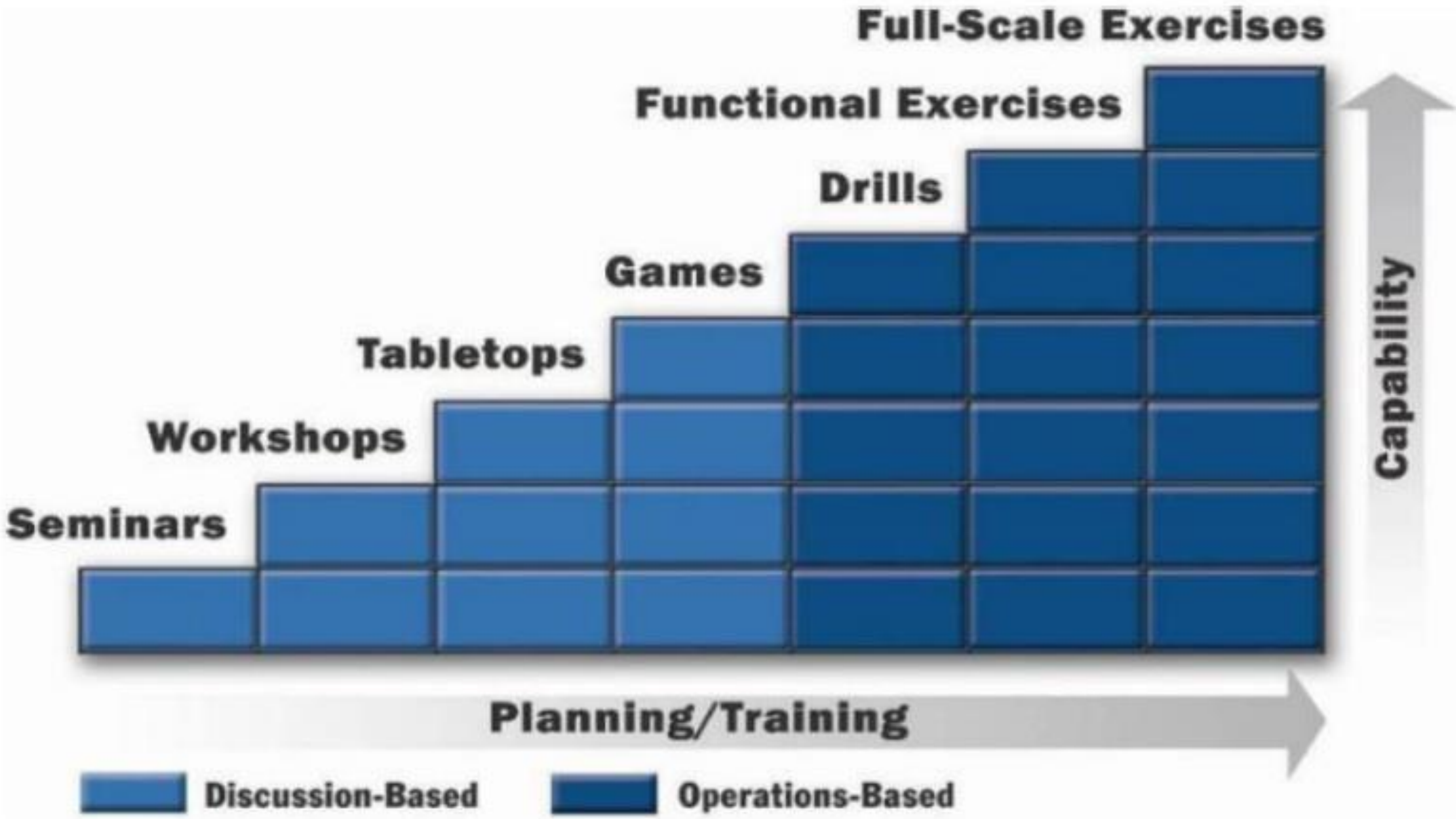


Cyber Defence Exercises (Worldwide Distribution)



Cyber Defence Exercises (Asia Distribution)

دسته بندی انواع تمرین‌های دفاع سایبری



Cyber Defence ExercisesTaxonomy

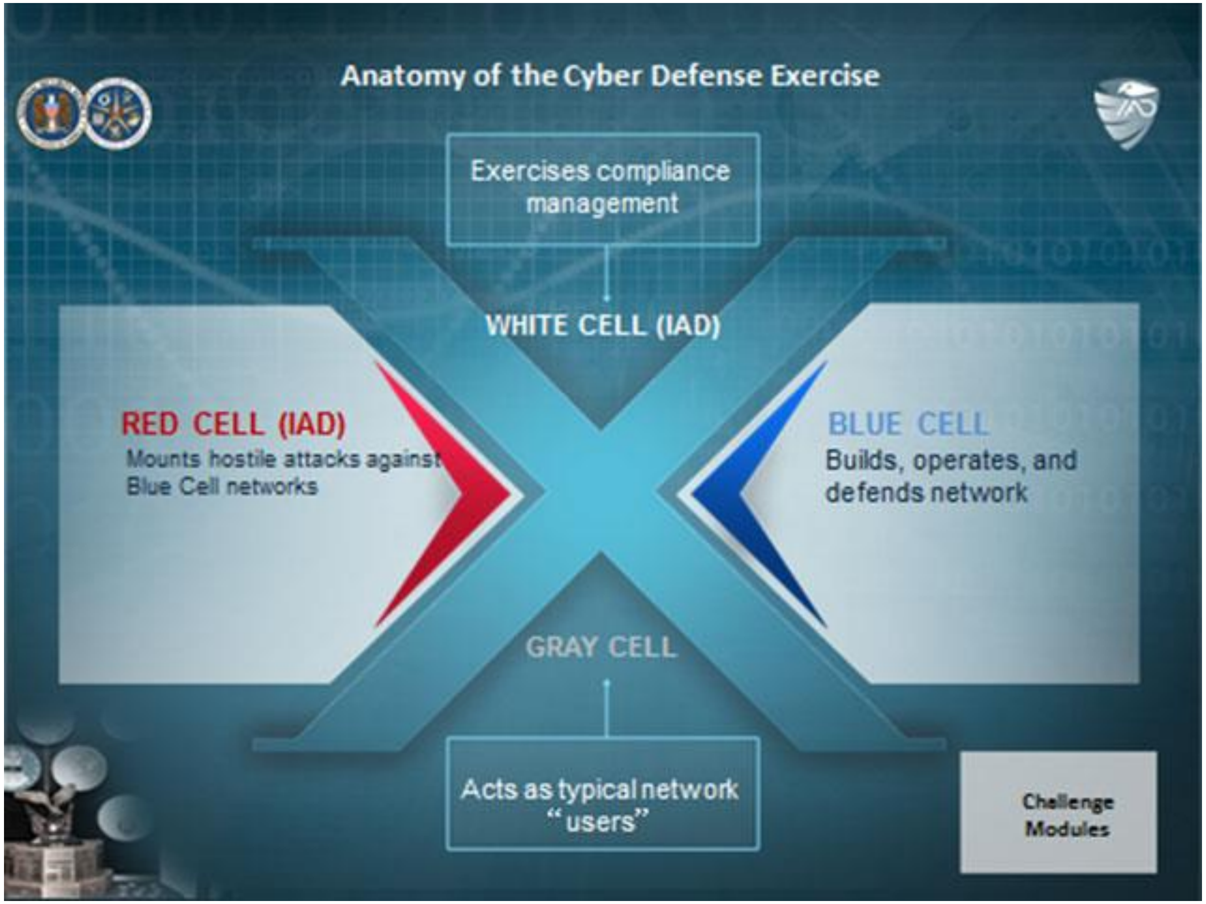
رزمایش مبتنی بر مذاکره

- در این نوع رزمایش، اعضای تیم‌های رزمایش درخصوص اهداف رزمایش و نحوه آمادگی تجهیزات و تیم‌های عمل کننده به بحث و بررسی و تحلیل وضعیت می‌پردازند. و با تهیه یک یا چند سناریو و انجام هماهنگیهای گروهی و سازمانی،اقدامات متناسب با آن را بررسی کرده و میزان آمادگی در برابر حوادث سایبری مورد ارزیابی قرار می‌گیرد.
- سمینار آموزشی
- کارگاه آموزشی
- دورمیزی
- بازی رزمایش (رزمایش شبیه‌سازی شده)

در این نوع رزمایش، تمامی اجزای رزمایش یا بخشی از آن در یک محیط شبیه‌سازی می‌شود و سپس با مشارکت تیم‌های شرکت کننده، رزمایش اجرا می‌شود.

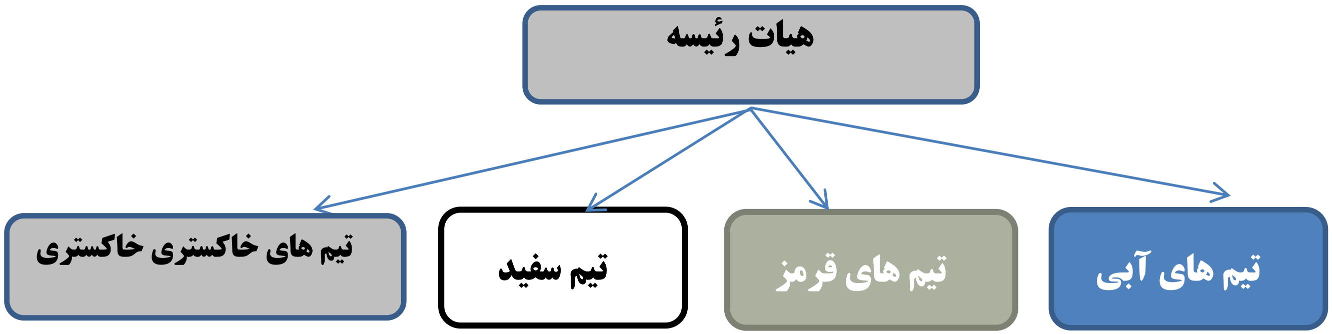
رزمایش عملیاتی

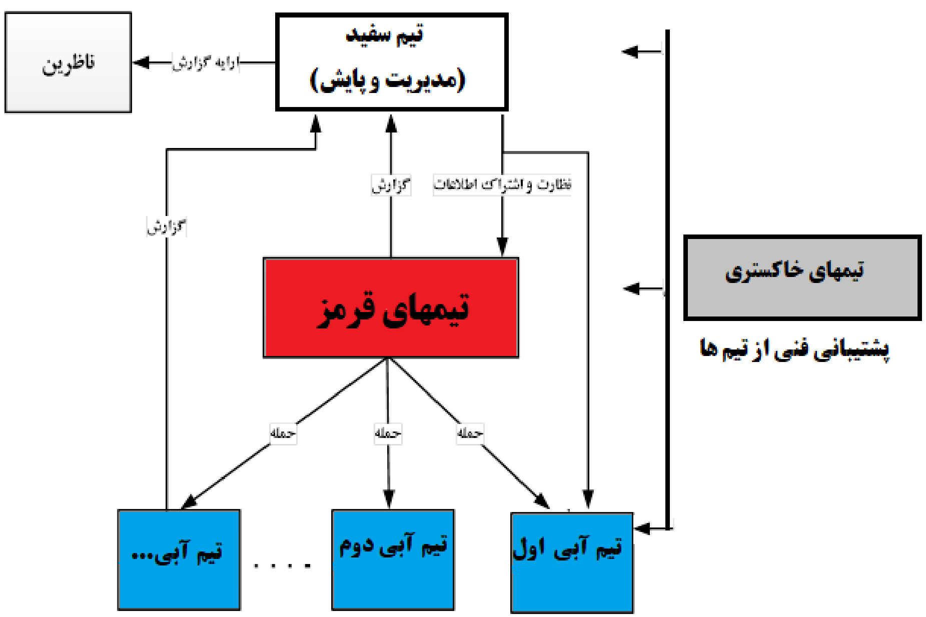
- در این روش تیم‌های شرکت‌کننده در رزمایش در محیط‌های واقعی مطابق با اصول و سناریو تهیه شده و رزمایش انجام می‌دهند.
- شبیه سازی با اقدام اجرایی تیم آبی
- عملیاتی محدود
- عملیاتی کامل



Cyber Defense Exercise (CDX)
In US

ساختار و سازمان تمرین سایبری





هیئت رئیسه

- هدایت و راهبری رزمایش
- تصویب زمان شروع و پایان رزمایش.
- تصویب و ابلاغ سناریوی رزمایش.
- سیاست‌گذاری و تعیین رویکرد رزمایش.
- تحلیل گزارشات پایانی و ابلاغ نتایج و دستاوردهای رزمایش پس از برگزاری آن.
- دریافت گزارشات از تیم سفید و بررسی آن و کنترل چهارچوب اجرای رزمایش مطابق با سناریوی ابلاغی

تیم سفید

- تهیه و تدوین سناریو رزمایش و اخذ تاییدیه از هیئت رئیسه
- کنترل نحوه اجرای رزمایش (تعیین زمان شروع، پایان و تقدم و تاخر انجام وظایف تیم ها)
- رصد و پایش اقدامات تیم‌های آبی و قرمز
- تهیه چک لیست برابر سناریو رزمایش با کمک تیم های شرکت کننده
- ارزیابی اقدامات تیم های آبی و قرمز
- تجزیه و تحلیل و تهیه گزارش اقدامات تیم‌ها
- تهیه گزارش ارزیابی نهایی رزمایش و ارائه به هیئت رئیسه
- نظارت بر آماده‌سازی زیرساختهای مورد نیاز جهت انجام رزمایش توسط زیرساخت مربوطه

تیم‌های آبی

تیم‌های آبی مخاطبان اصلی مانور هستند. این تیم‌ها باید در زمان اجرای مانور به مجموعه‌ای از وظایف عمل کند. وظایف کلی این تیم عبارتند از:

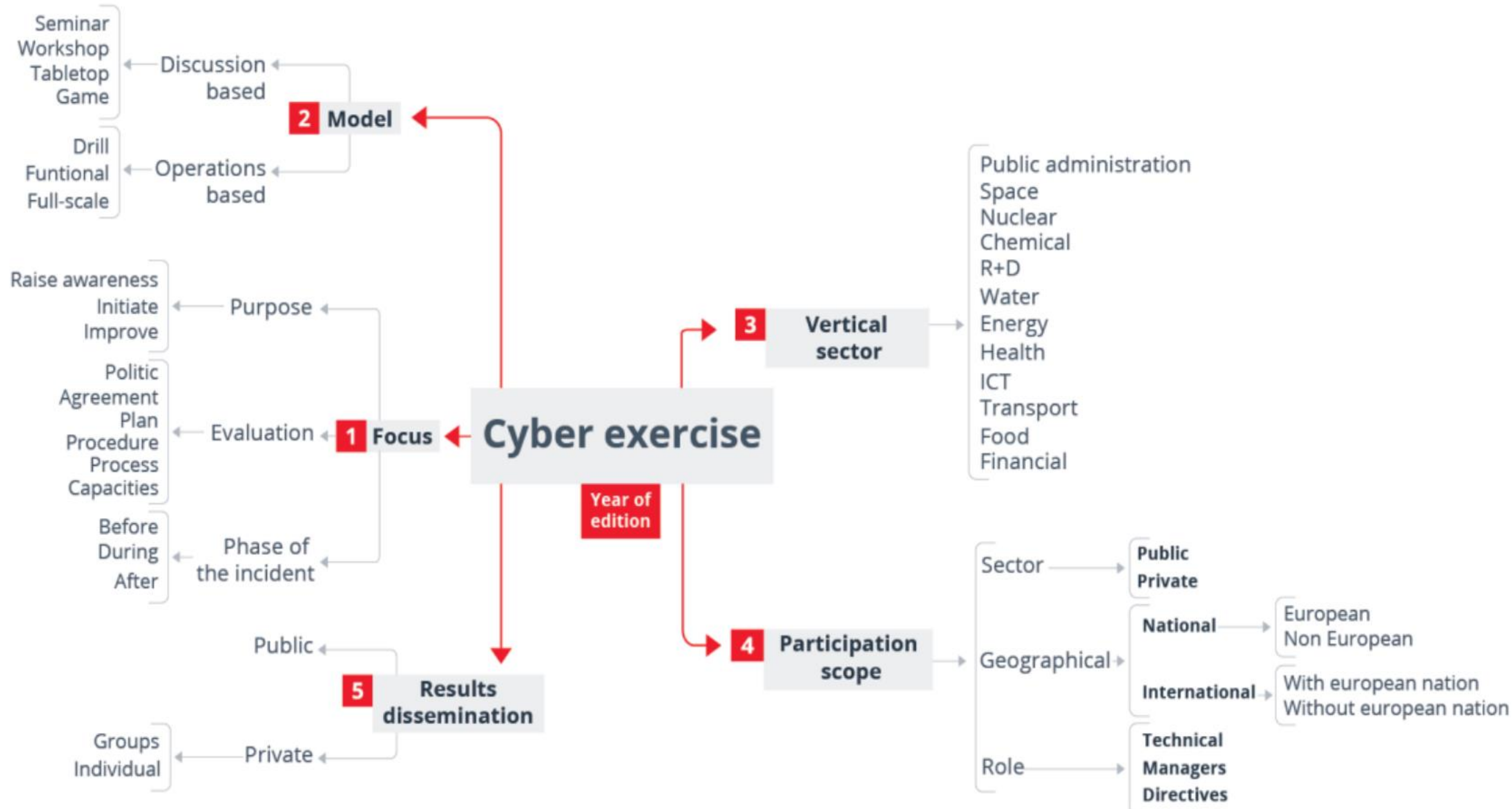
- تضمین امنیت سیستم‌های ناامن و دفاع در مقابل حملات تیم قرمز
- مصون‌سازی، امن‌سازی و پایدارسازی سیستم‌ها
- شناسایی حوادث رخ داده در ارایه گزارش از هر یک از آن‌ها
- ارایه گزارشی از مجموعه عملکرد گروه آبی به تیم سفید

تیم قرمز

تیم قرمز نقش مهاجم و یا مختل کننده در زیرساخت را دارد از نمایندگان و تیم‌های تحت کنترل و مدیریت دستگاه‌های مرتبط تمرین/رزمایش می‌باشند که عهده دار وظایف زیر هستند:

- تیم قرمز سعی در نفوذ، اختلال و یا از کاراندازی سیستم‌ها را بر عهده دارد.
- حمله به نقاط آسیب‌پذیر سیستم‌های تحت حفاظت تیم آبی
- گردآوری اطلاعات مورد نیاز در مورد هدف‌های مورد نظر و تصویب شده.
- تعیین فرایندهای هجوم به تیم آبی و تعیین روش‌های نفوذ.
- ارایه گزارشی از مجموعه عملکردهای گروه به تیم سفید
- تهیه و تدوین سناریوی تهاجم

Cyber Exercise Taxonomy



- سه فاز اصلی تمرین دفاع سایبری
- طراحی (*planning*)
- اجرا(*Execution*)
- ارزیابی (*Evalution*)

Cyber Defence Exercises (CDX)
Planning

- *A. Determination of Objectives*
- *B. Planning Process*

Planning Process

A. Determination of Objectives

The exercise planning process begins with the determination of the purpose of the exercise and its desired outcome. Without explicit targets, planners cannot design a meaningful exercise. These goals allow participants to clearly configure scenarios in practice to determine whether they have the necessary skills in a cyber-environment against cyber threats.

- *B. Planning Process*

Planning Process

- *B. Planning Process*

1) Initial Planning Meeting/Conference;

Covers topics such as;

- *Determination of requirements and conditions,*
- *Determination of scenario variables and draft scenario proposals,*
- *Collection of required information and distribution of tasks between execution planners,*

It takes place approximately 6, 7 months before the exercises.

- *B. Planning Process*

II) Main Planning Meeting/Conference;

overs topics such as;

 Reconciliation of logistical and organizational problems such as personnel, scenario and time schedule development and administrative requirements,

 Examining, evaluating and finalizing all the draft documents to be used in the exercise,

 Examination and development of the injections prior to the final planning stage,

 Reviewing of the duties, conditions, and standards determined for the purpose of the exercise,

It takes place approximately 3, 4 months before the exercise.

B. Planning Process

III) Final Planning Meeting/Conference;

The final planning conference is the final meeting to versee the implementation processes and procedures. After this meeting, no major changes should be made to the design or coverage of the exercise or its supporting documentation. It takes place approximately 3, 4 weeks before the exercise.

- *B. Planning Process*

IV) Test-Run;

Test-Run is the final preparation phase for testing and evaluating the technical infrastructure of the cyber defense exercises. In test-run, it is aimed to establish all the substructures to be used for the exercise in the selected place for the exercise and to test these sub-structures as if the exercise process is working normally and to observe the possible problems before the exercise. Participation from all teams except the blue teams takes place in test-run. Thus, all teams will have the chance to review their final situation and practice process before the exercise. Test-run takes place approximately one week before the exercise.

Execution

- A. Teams
- B. Scenario
- C. Scoring
- D. Monitoring
- ....

Cyber Defence Exercises (CDX)
Evaluation

One of the most important outputs of the cyber defense exercises is the After Action Report. At this report, it is mentioned the detailed performance of each blue team after the exercise. Addition to that the scenario and sub-scenarios, injections, exercise purposes, participants, scoring, technical infrastructure, red team attacks (client-side, web, network), defences made by the blue team, defects in these defences, general mistakes made, observations from all teams and subteams, Recommendations and evaluations Are Also covered.