شرکت ملی نفت ایران

سومین کنفرانس

امنیت اطلاعات و ارتباطات

در صنعت نفت

عنوان:

راهکارهای امنیت در جهان و تطبیق آن با وضعیت ایران

AUT Industerial Cyber Security Team

تیم امنیت سایبری سیستم های صنعتی دانشگاه صنعتی امیرکبیر


مقابله با بدافزارها در سیستم های
کنترل صنعتی و زیرساخت های حیاتی
پژوهشکده بدافند غیر عامل
دانشگاه صنعتی امیر کبیر
دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)
آسیب پذیری های
سیستم کنترل
پژوهشکده بدافند غیر عامل
دانشگاه صنعتی امیر کبیر

فهرست مطالب

- مقدمه
- مروری بر راهکارهای امنیت در سیستم های کنترل صنعتی و SCADA
- ایزوله کردن واحد صنعتی، راهبرد رایج در ایران
- روش ها و ابزارهای ارزیابی امنیت در شبکه های صنعتی اسکادا
- معرفی ابزار ارزیاب ICSAT، طراحی شده و پیاده سازی شده در تیم امنیت سایبری پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر

این ارائه برگرفته از نتایج طرح

"طراحی و پیاده سازی سامانه جامع مقابله با بدافزارها در سیستم های کنترل صنعتی و زیر ساخت های حیاتی"

در قالب

طرح کلان ملی مصوب شورای عالی عتف

"طرح معماری و راه‌اندازی مرکز ملی دفاع سایبری و سامانه‌های زیرساختی فضای سایبری"

می باشد.

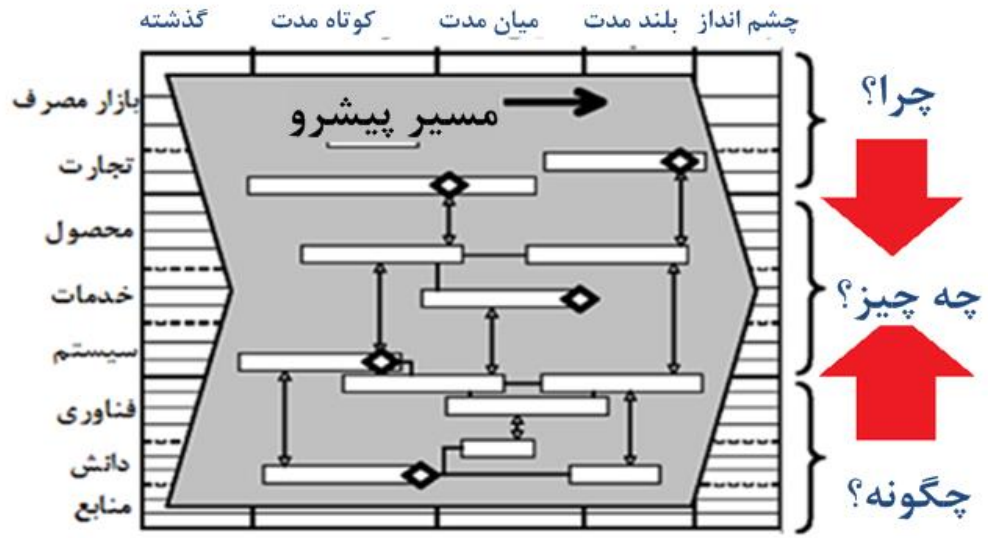
فاز صفر طرح: تهیه ره نگاشت

نوع دانش

دیدگاه های اساسی

نقطه نظرات متداول

- استراتژیک و تجاری
- خلاقیت و تولیدی
- پژوهش و فناوری



سوالات کلیدی

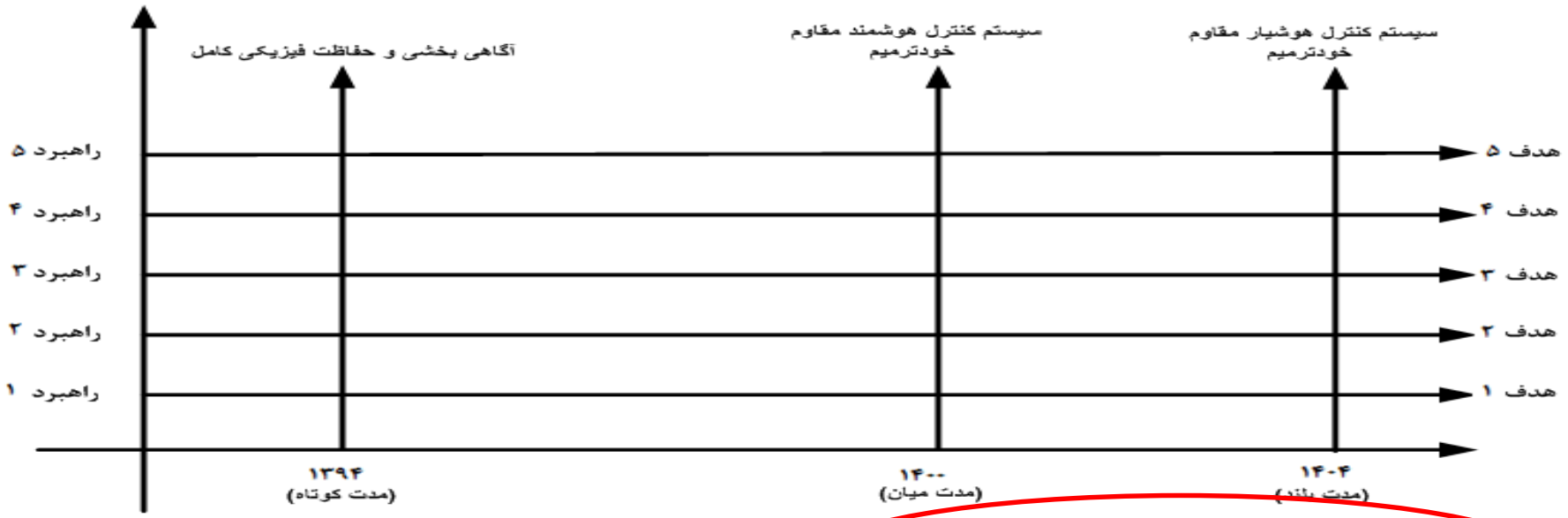
۱)- در حال حاضر کجا هستیم؟

۲)- به کجا می خواهیم برویم؟

۳)- چطور می توانیم برسیم؟

چشم انداز

در افق ۱۴۰۴، سیستم های کنترل ای در واحدهای صنعتی و زیر ساخت های حیاتی طراحی، نصب و نگهداری خواهند شد که در مواجه با تهاجم بدافزاری عملکرد حیاتی خود را از دست نمی دهند و قابلیت بازیابی خودکار دارند.



راهبرد ۱ حساس سازی و آگاهی بخشی کامل کارشناسان فنی و دست اندرکاران بخش های مختلف سیستم های کنترل صنعتی و زیرساخت های حیاتی

راهبرد ۲ ارزیابی و پایش پیوسته ریسک به منظور اطلاع دقیق و به روز ازعملکرد و امنیت سیستم های کنترل صنعتی و زیرساخت های حیاتی کشور در تمامی سطوح

راهبرد ۳ اجرای دقیق قوانین و مقررات امنیتی و به روزرسانی آنها ،حفاظت فیزیکی کامل سیستم های کنترل صنعتی و زیرساخت های حیاتی

راهبرد ۴ نصب ،راه اندازی و نگهداری سیستم های کنترل صنعتی و زیرساخت های حیاتی با قابلیت بازیابی خودکار در زمان حملات بدافزاری و توانایی حفظ عملکرد در مواجه با حمله

راهبرد ۵ ایجاد هماهنگی در بین نهادها و شرکتهای خصوصی و دولتی فعال در زمینه مقابله با حملات بدافزاری در سیستم های کنترل صنعتی و زیرساخت های حیاتی و در جهت هم افزایی و کاهش هزینه ها

هدف ۱ حساس سازی ،ایجاد فرهنگ امنیتی و نهادینه کردن آن.

هدف ۲ آگاهی دائمی نسبت به وضعیت امنیتی سیستم کنترل.

هدف ۳ تبیین نظام حقوقی ،تدوین قوانین ،تنظیم مقررات و اتخاذ تدابیر ویژه به منظور کاهش ریسک .

هدف ۴ مدیریت پیشگیری ،مقابله و بازیابی سیستم کنترل ،دربرابر حمله بدافزاری و انباشت دانش مربوطه.

هدف ۵ مدیریت یکپارچگی.

پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

فازدوم طرح:

- با توجه به نیاز کارف
- هدف اول ره نگاشت
  - برگزاری کارگاه های
  - انتشار ماهانه بولتن
    ساخت های حیاتی
  - ...
- هدف دوم ره نگ
  سیستم کنترل صنع
  - طراحی و پیاده ساز
  - طراحی و پیاده س
    سیستم‌های کنترل
  - طراحی آزمایشگاه

دانشگاه صنعتی امیرکبیر

بولتن خبری (داخلی)
"مقابله با بدافزارها در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی"
سال دوم، شماره ۱۲
دی ۱۳۹۳

بولتن خبری مقابله با بدافزار در زیرساخت‌های حیاتی و سیستم‌های صنعتی با هدف اطلاع‌رسانی در مورد لزوم، چالش‌ها و راهکارهای حفاظت از زیرساخت‌های حیاتی و سیستم‌های صنعتی در برابر حملات بدافزاری و با حمایت شورای عالی علوم، تحقیقات و فناوری در پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر تهیه شده است.

مطالب این شماره:

- ✓ راهکارهای مقابله با بدافزار در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی
- ✓ بررسی راهکارهای امنیتی پیشنهادی شرکت‌های صنعتی برای شبکه SCADA
- ✓ دوره‌های آموزشی، کنفرانس‌ها و گردهمایی‌های مرتبط

راهکارهای مقابله با بدافزار در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی

در شماره‌های پیش اشاره شد که شبکه‌های کنترل نظارتی و اکتساب داده (SCADA) نقش اساسی در کنترل و نظارت زیرساخت‌های حیاتی و سیستم‌های صنعتی دارند و امنیت آن‌ها در برابر حملات سایبری حائز اهمیت می‌باشد.

سیستم SCADA طی سال‌ها از یک سیستم پیچیده به سیستمی ساده شامل یک رایانه شخصی استاندارد، سیستم عامل

آن و شبکه ارتباطی استاندارد مبتنی بر TCP/IP با قابلیت دسترسی به اینترنت تبدیل شده است. شبکه‌های کنترل صنعتی و زیرساخت‌های حیاتی که در گذشته به صورت مجزا به کار خود می‌پرداختند، امروزه به واسطه سیستم SCADA، شبکه‌ای یکپارچه را تشکیل داده‌اند. ویژگی نظیر قابلیت دسترسی بالا، آن‌ها را در معرض تهدیدهای سایبری و حمله بدافزارها قرار داده است.

با توجه به آسیب‌پذیری‌های جدی در اکثر شبکه‌های SCADA، برخی از شرکت‌های صنعتی راهکارهای حفاظتی را جهت امنیت آن‌ها ارائه داده‌اند. در سه شماره‌ی پیش، راهکارهای حفاظتی شرکت‌هایی نظیر Tofino، Siemens، ABB و ... بیان شد. در این شماره راهکارها و محصولات امنیتی شرکت‌های Rockwell Automation و Honeywell معرفی می‌گردند.

بررسی راهکارهای امنیتی پیشنهادی شرکت‌های صنعتی برای شبکه SCADA

- **شرکت Rockwell Automation**

جهت اتصال امن، مطمئن و بدون مشکل سیستم کنترل صنعتی به شبکه مالی و تجاری، شرکت‌های Rockwell و Cisco با یکدیگر تلفیق شده‌اند. همکاری آن‌ها شامل موارد زیر می‌باشد:

- دیدگاه فناوری مشترک: حمایت از استفاده از استانداردهای در دسترس و ویژگی‌های شبکه‌بندی هوشمند در شبکه‌های اتوماسیون
- همکاری برای ارائه شبکه مرجع: ارائه توصیه‌های دقیق در مورد معماری و ساختار شبکه مرجع
- بهینه‌سازی فرآیندها و نیروهای کار: ارائه راهنمایی‌های مفید در زمینه آموزش کارکنان و افزایش درک نیروهای IT و کنترلی
- تولید محصولات مشترک: تولید سوئیچ اترنت صنعتی که در تهیه آن از فناوری هر دو شرکت استفاده شود.

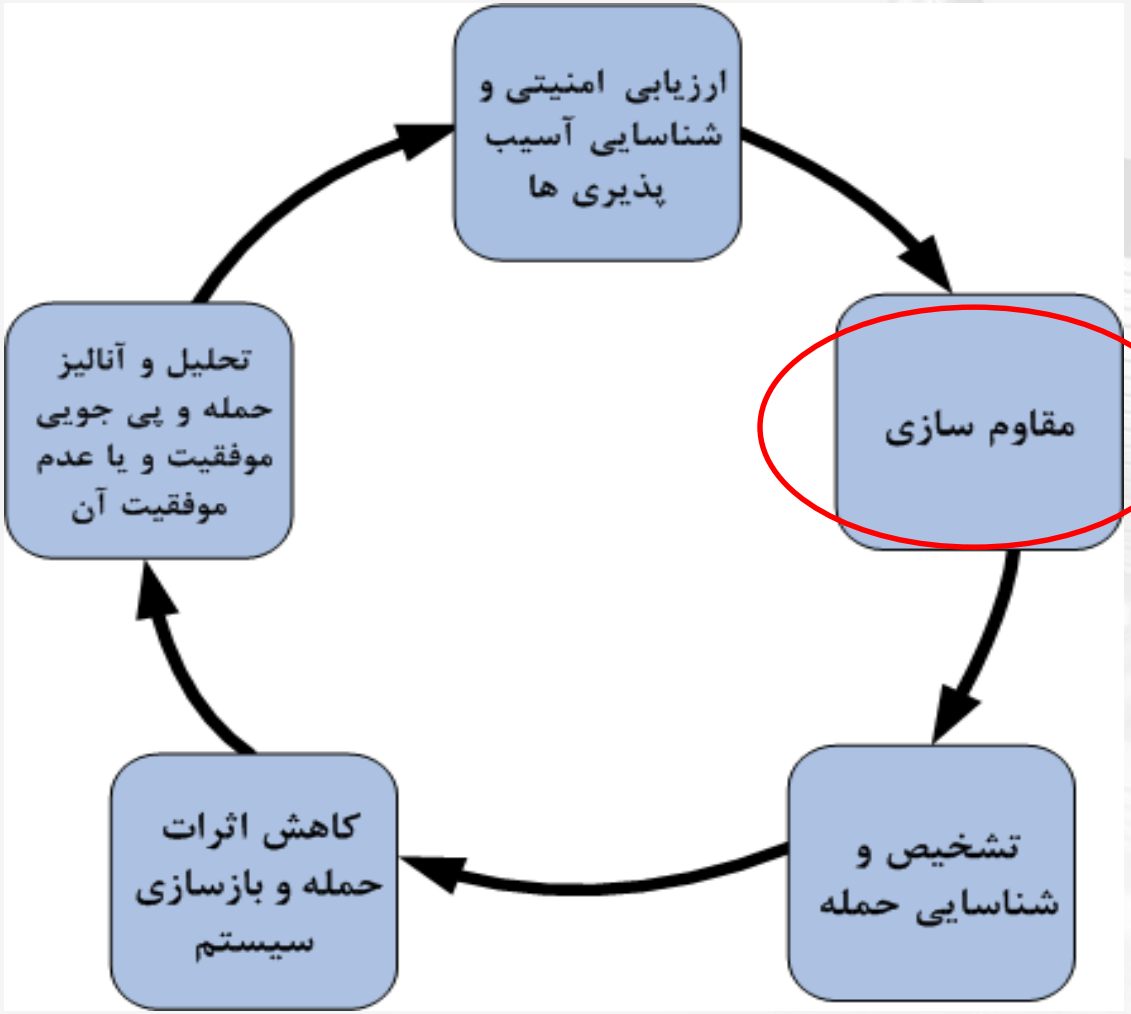
۱

طرح کلان ملی معماری و راه‌اندازی مرکز ملی دفاع سایبری
و سامانه‌های زیرساختی فضای سایبری

پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

مروری بر راهکارهای امنیت در سیستم های کنترل صنعتی و SCADA

چرخه امنیت


ارزیابی امنیتی و شناسایی آسیب پذیری ها
مقاوم سازی
تشخیص و شناسایی حمله
کاهش اثرات حمله و بازسازی سیستم
تحلیل و آنالیز حمله و پی جویی موفقیت و یا عدم موفقیت آن

هدف راهکارهای مقاوم سازی

هدف راهکارهای مقاوم سازی، کاهش و یا رفع آسیب پذیری

- تبیین سیاست گذاری های امنیتی مناسب
- طراحی ساختار امن
- اعمال وصله
- تغییر در پیکربندی
- حذف سرویس یا سیستم آسیب پذیر
- ایزوله کردن سیستم یا سرویس آسیب پذیری و حفاظت قوی از آن

انواع آسیب پذیری در سیستم های کنترل و SCADA

- آسیب پذیری های سیاست ها و رویه های امنیتی
  - نامناسب بودن راهبرد امنیتی
  - نبود برنامه های مناسب به منظور مدیریت تغییرات
  - نبود برنامه های آموزشی مناسب
- آسیب پذیری های ساختاری شبکه کنترل
  - ساختار امنیتی ضعیف شبکه
  - اتصال غیرضروری شبکه به شبکه های نا امن
  - الگوریتم های نا امن کنترلی
- آسیب پذیری های تجهیزات و ارتباطات سیستم کنترل
  - آسیب پذیری های سخت افزاری
  - آسیب پذیری های نرم افزاری
  - آسیب پذیری های پیکربندی
  - آسیب پذیری های پروتکل های ارتباطی

آسیب پذیری تجهیزات و ارتباطات سیستم کنترل

- با توجه مدل لایه ای سیستم کنترل، آسیب پذیری های دسته سوم، به ۶ دسته تقسیم می شوند:

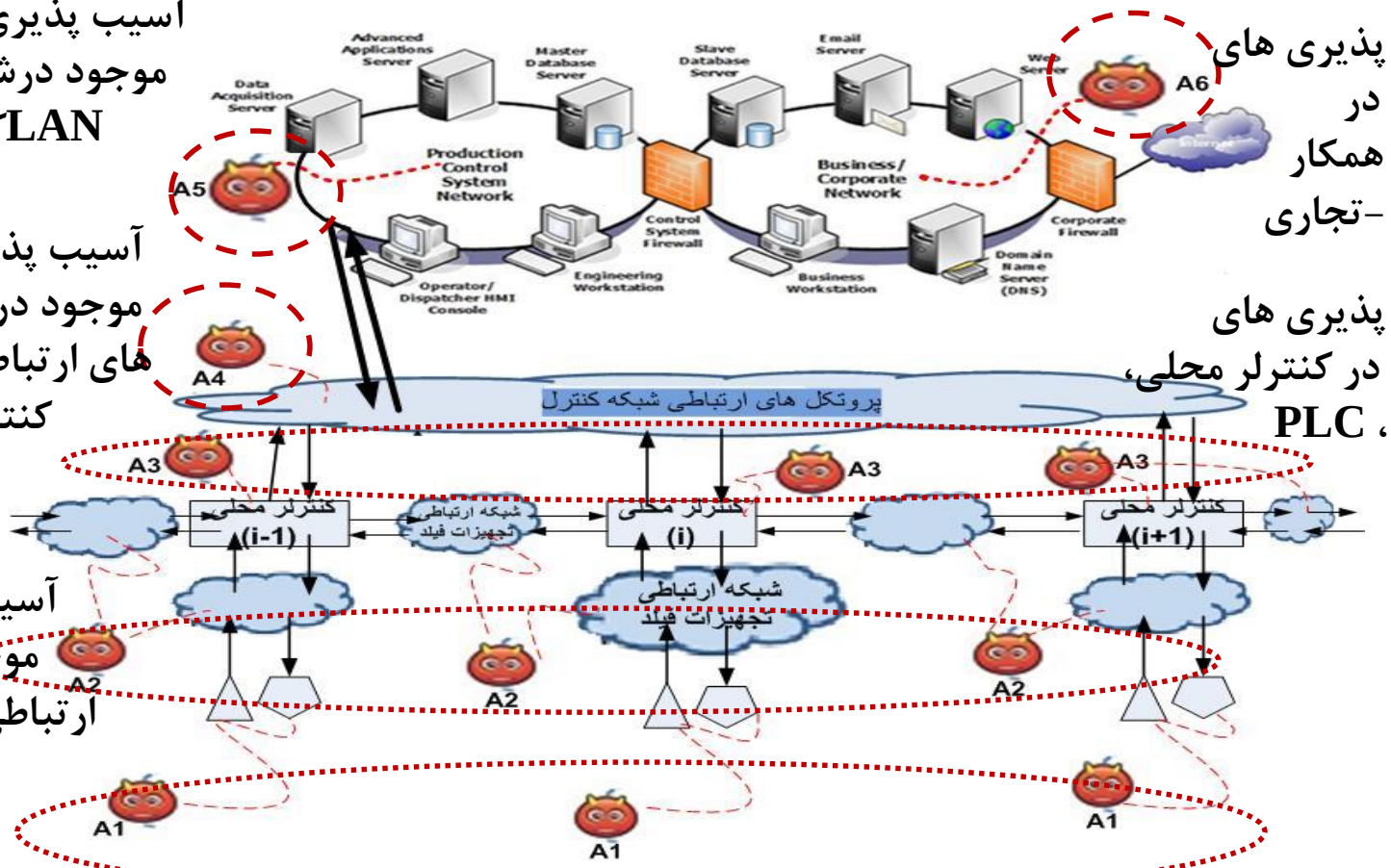
آسیب پذیری های موجود درشبکه LANکنترلی

آسیب پذیری های موجود در شبکه همکار و مالی -تجاری

آسیب پذیری های موجود در پروتکل های ارتباطی شبکه کنترل

آسیب پذیری های موجود در کنترلر محلی، PLC ، RTU

آسیب پذیری های موجود درشبکه ارتباطی تجهیزات فیلد



آسیب پذیری های موجود در تجهیزات فیلد

دسته بندی راهکارهای امنیت در سیستم کنترل و SCADA

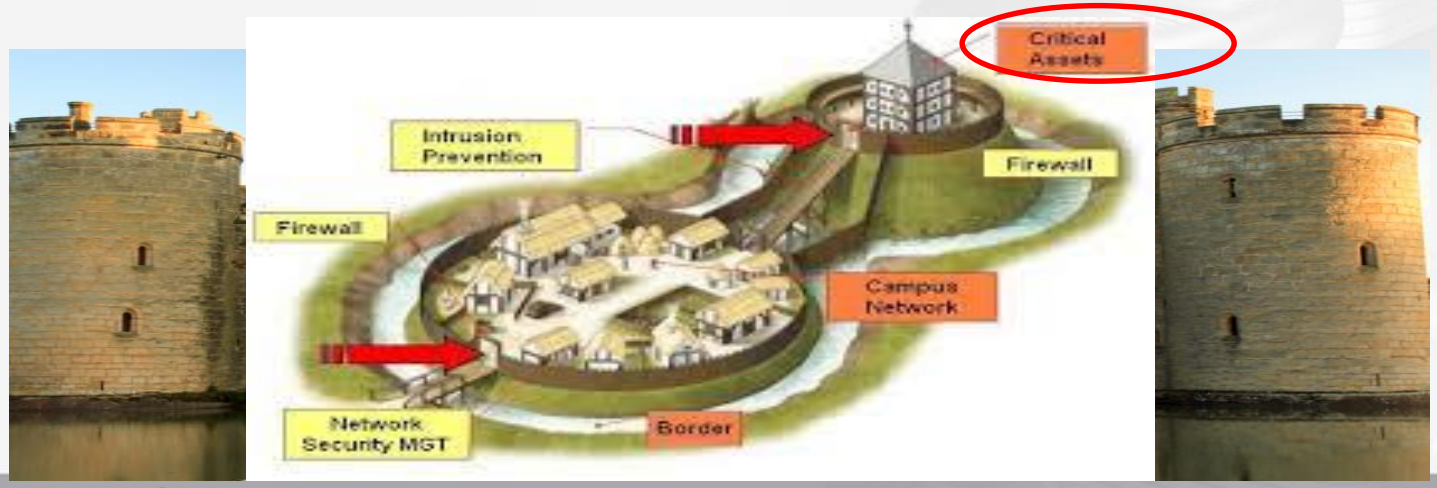
- تدوین برنامه ها وسیاست های امنیتی
- طراحی ساختار امن شبکه کنترل
- امن سازی تجهیزات و ارتباطات سیستم کنترل

گام اول: تدوین برنامه ها و سیاست های امنیتی

- تبیین راهبرد امنیتی
- تعریف سیاست ها و رویه های امنیتی
- تعریف نقش ها و مسئولیت ها
- تعریف فعالیت ها و فرآیندهای مجاز و غیرمجاز
- برنامه ریزی ارزیابی امنیتی، شناسایی آسیب پذیری ها، تحلیل ریسک
- آموزش و آگاهی رسانی

راهبرد کلان دفاع در عمق

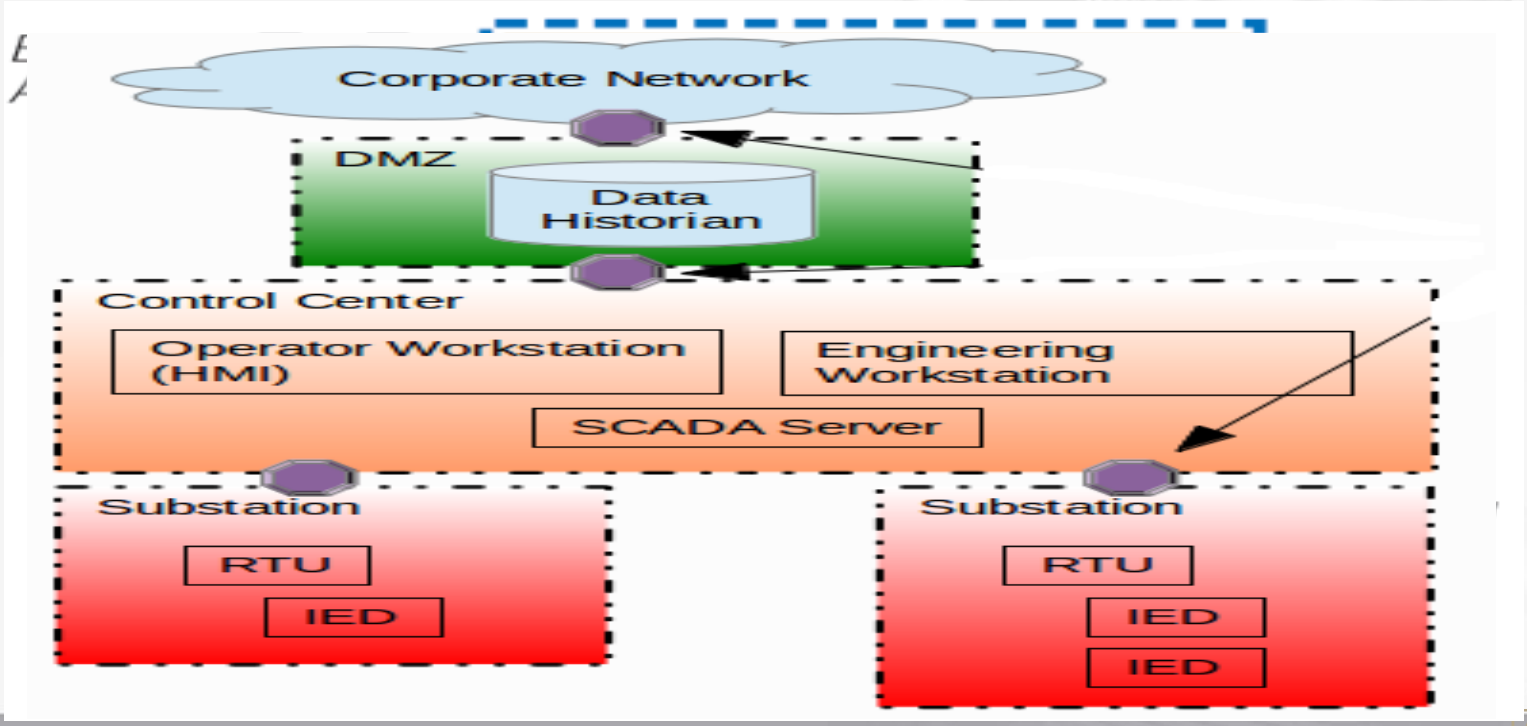
- **دفاع در عمق راهبرد کلانی است که در اکثر استانداردهای امنیتی سیستم های صنعتی، توصیه شده است.**
- **دفاع در عمق**: فراهم نمودن محافظت چندگانه، به خصوص به شکل لایه ای، با هدف جلوگیری یا حداقل به تاخیر انداختن یک حمله.
- ضعف موجود در یک لایه می تواند به وسیله قابلیت های لایه های دیگر جبران شود.
- برای سیستم های حیاتی تر امکان بکارگیری لایه های حفاظتی بیشتر فراهم می شود.



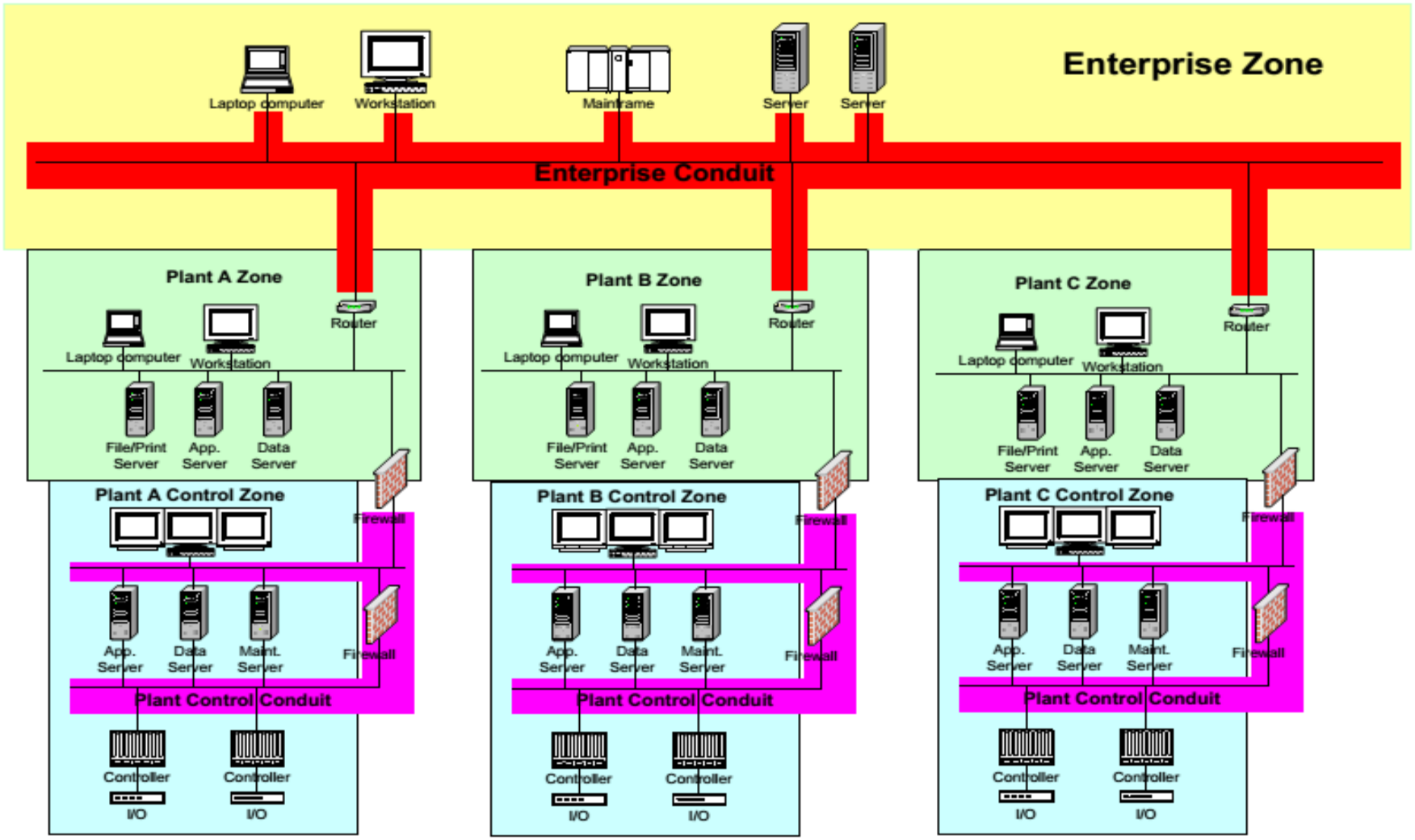
گام دوم: امن سازی ساختار شبکه کنترل بر پایه راهبرد تبیین شده

طراحی امن ساختار شبکه

- استاندارد NERC: تعریف ESPها و PSPهای چندگانه (اولیه، ثانویه و ثالثیه)
- استاندارد ISA99: تعریف zone و conduit (مناطق و مجراهای امنیتی)



مدل مناطق امنیتی و مجراها(ISA99):



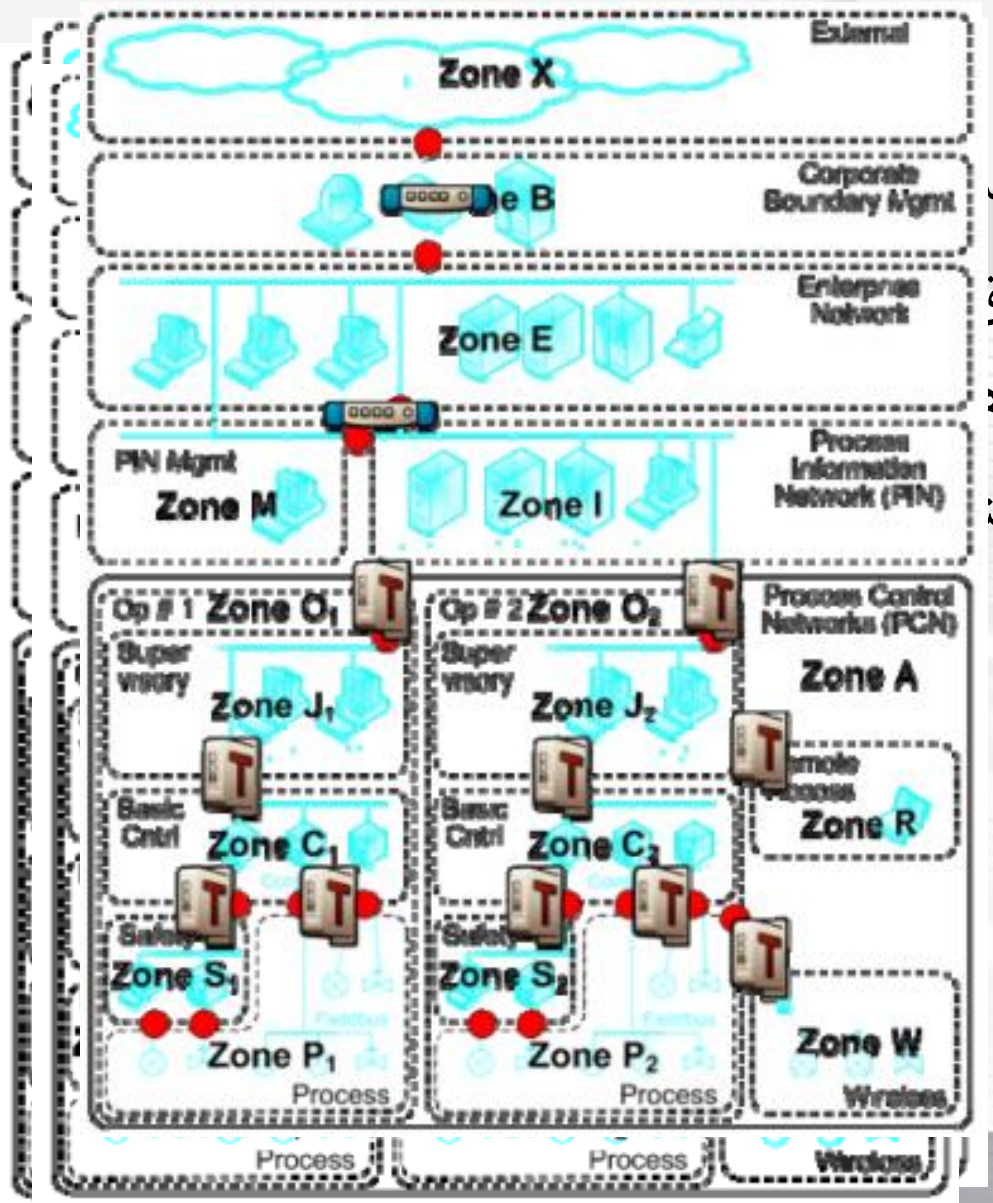
تعریف مناطق(محدوده های) امنیتی:

- تعریف مناطق امنیتی با ارزیابی واحد صنعتی و عملیات آن و شناسایی گروه هایی از دارایی ها که **عملکرد** و **الزامات امنیتی مشترک** دارند آغاز می شود.
- شناسایی گروه های عملکردی
  - گروه های عملکردی می توانند بر اساس معیارهای مختلفی تعریف شوند. برای مثال حلقه های کنترلی، سرویس ها، پروتکل ها، میزان حیاتی بودن و ....
- تعریف مناطق امنیتی بر اساس گروه های عملکردی
  - ترکیب گروه های عملکردی که با هم اشتراک دارند برای دستیابی به تعدادی منطقه امنیتی قابل مدیریت

گام سوم: امن کردن تجهیزات و ارتباطات سیستم کنترل بر پایه ساختار امن طراحی شده

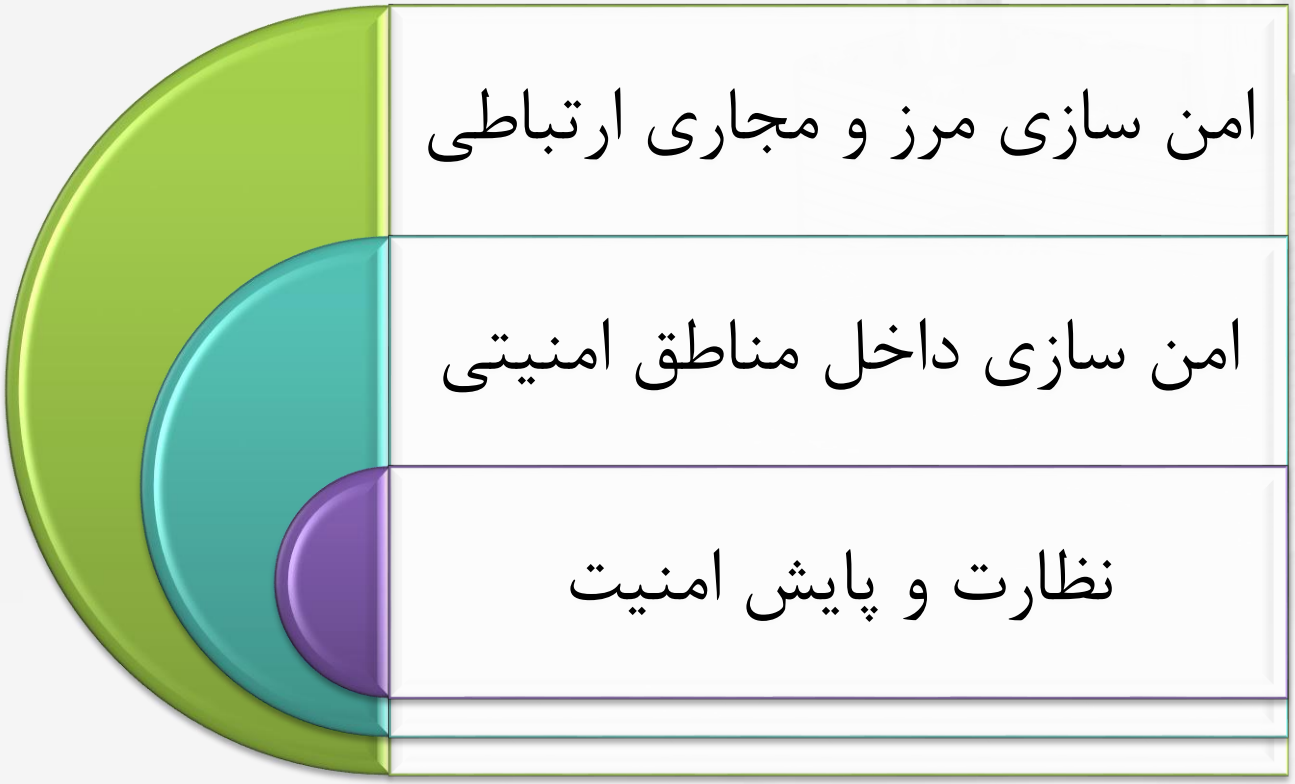
- امن کردن مرزهای مناطق امنیتی و حفاظت از مجراها
  - جلوگیری از حملات خارجی
  - جلوگیری از نفوذ یا گسترش حملات در مناطق
  - رفع آسیب پذیری های پروتکل های ارتباطی
  - استفاده از ابزارهای امنیتی مانند دیواره آتش، رمزنگاری و UTM
- امن کردن داخل مناطق امنیتی
  - جلوگیری از حملات داخلی یا حملات خارجی که دفاع مرزی را به نوعی پشت سر گذاشته اند.
  - استفاده از وصله ها به منظور رفع آسیب پذیری تجهیزات
  - استفاده از ابزارهای امنیتی مانند آنتی ویروس، IDPS
- نظارت و پایش امنیت
  - استفاده از تجهیزاتی مانند SIEM

مثال پالایشگاه نفت(Tofino)

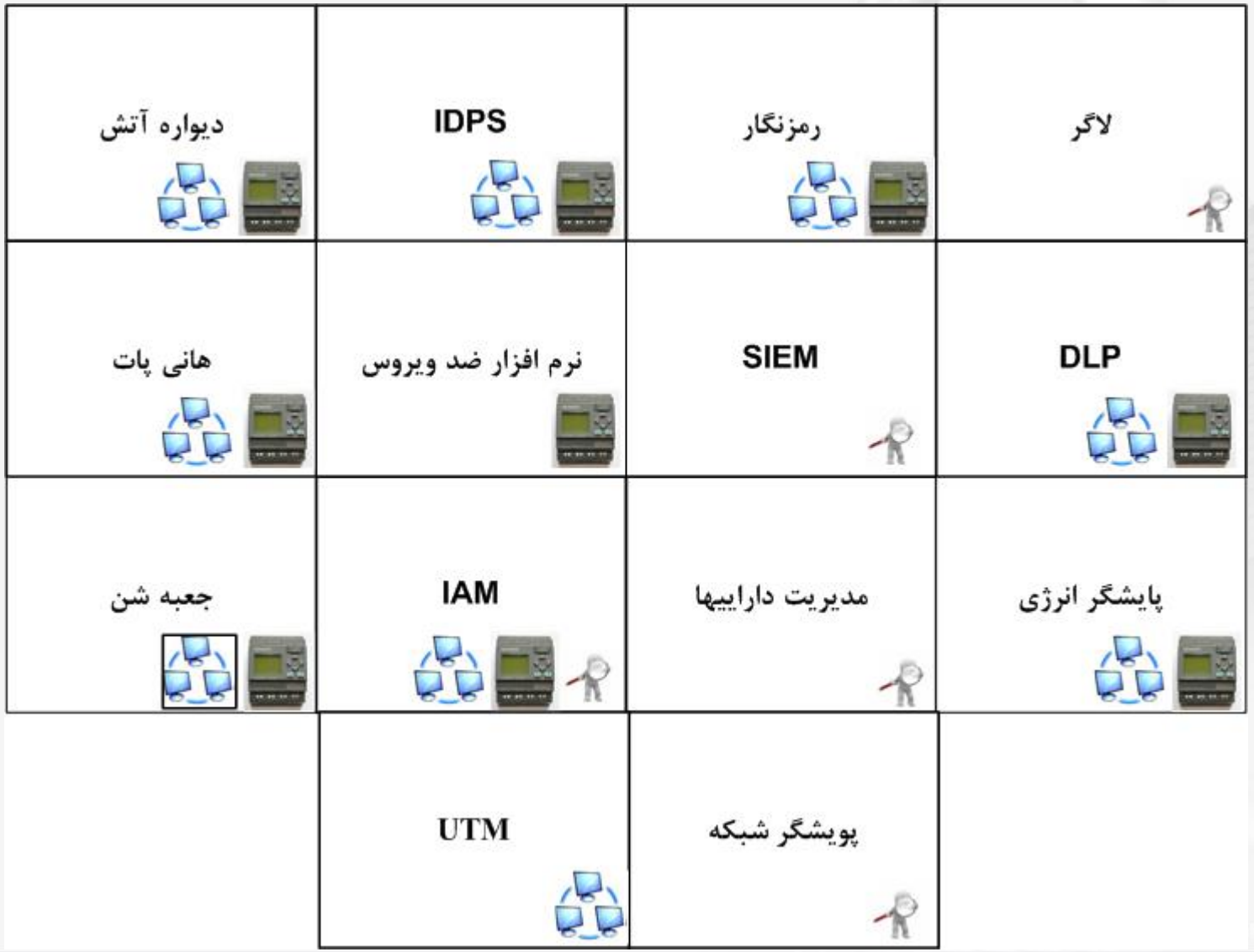


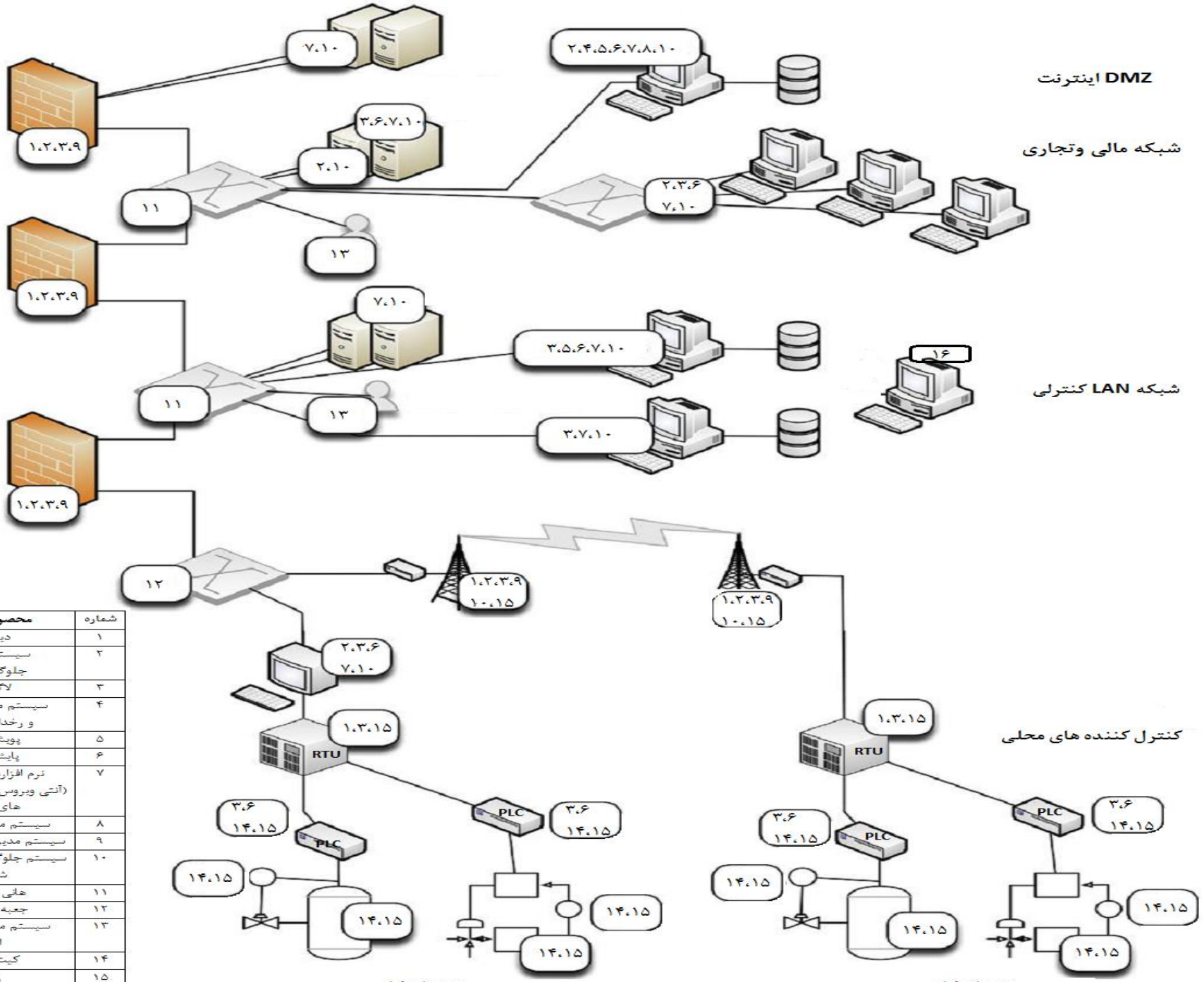
- عملیات اساس
- تعریف مناطق
- تعریف مجراه
- امن کردن من

اهداف ابزارهای امنیتی به منظور مقاوم سازی:



ابزارهای امنیتی به منظور مقاوم سازی:

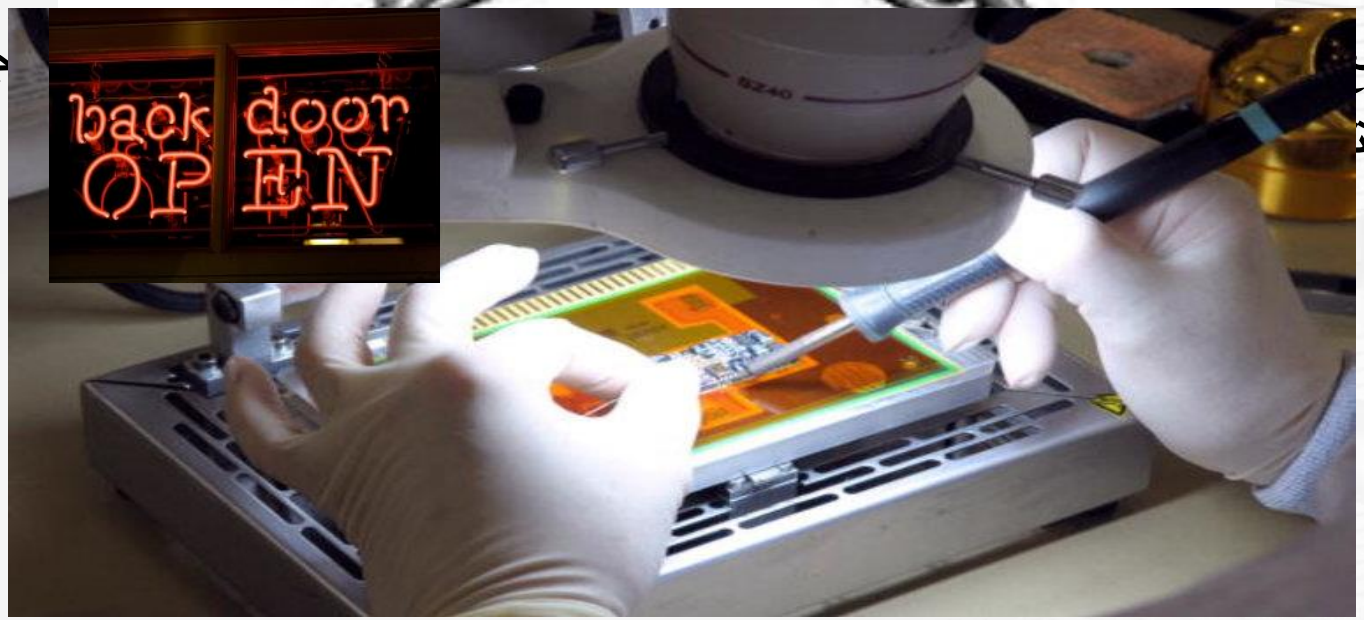




شماره	محصولات امنیتی
۱	دیواره آتش
۲	سیستم تشخیص / جلوگیری از نفوذ
۳	لاگر امنیتی
۴	سیستم مدیریت اطلاعات و رخدادهای امنیتی
۵	پویشگر امنیتی
۶	پایشگر امنیتی
۷	نرم افزارهای ضد بدافزار (آنتی ویروس، لیست سفید برنامه های کاربردی)
۸	سیستم مدیریت دارایی ها
۹	سیستم مدیریت یکپارچه تهدید
۱۰	سیستم جلوگیری از نابودی/فاش شدن داده
۱۱	هاب پات صنعتی
۱۲	جعبه شن صنعتی
۱۳	سیستم مدیریت دسترسی اشخاص
۱۴	کیت شناساگر
۱۵	رمزگذار
۱۶	شبیه ساز حمله/ابزار تست نفوذ

ایزوله کردن واحد صنعتی راهبرد رایج در ایران

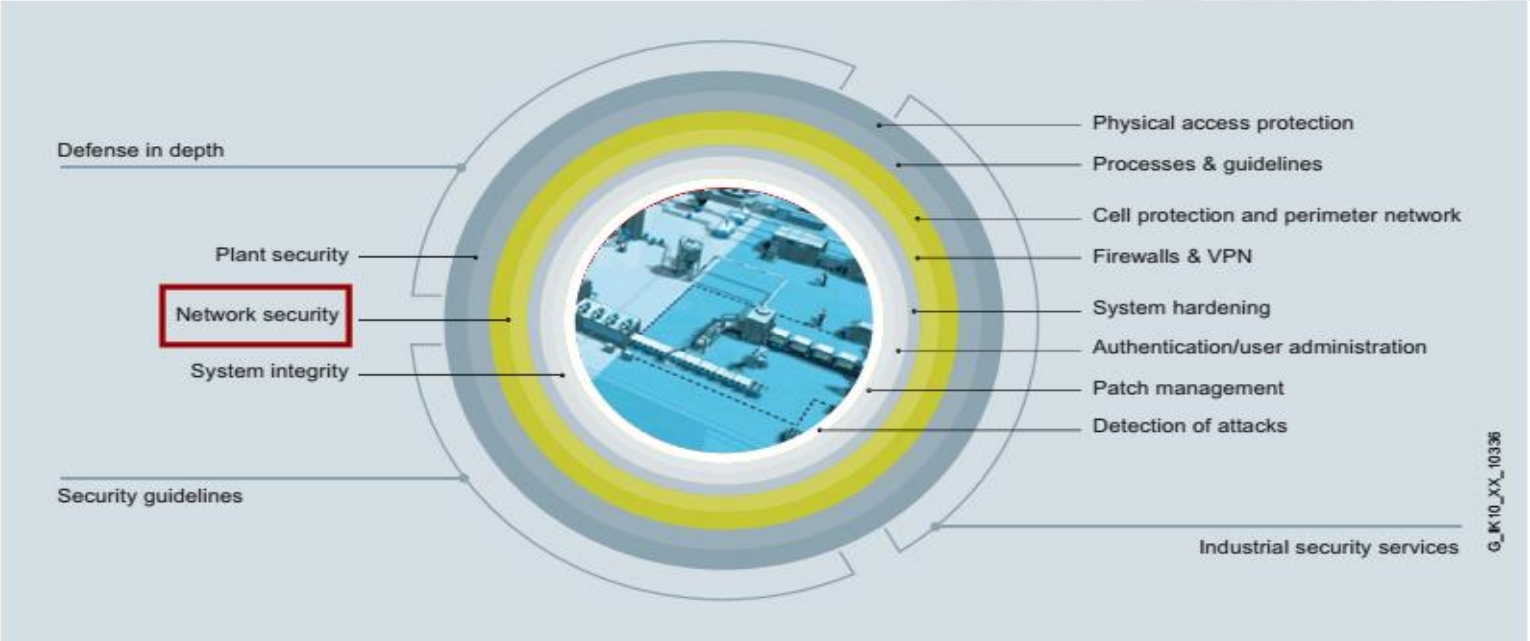
- **معایب:**
  - میزان امنیت یک سیستم برابر با میزان امنیت ضعیف ترین حلقه است.
  - این راهکار به طرق مختلف از جمله اشتباه عمدی یا غیر عمدی یک کارمند ممکن است به خطر بیافتد.
  - این راه ی کاملا ناکارآه
  - قطع جر به اخت

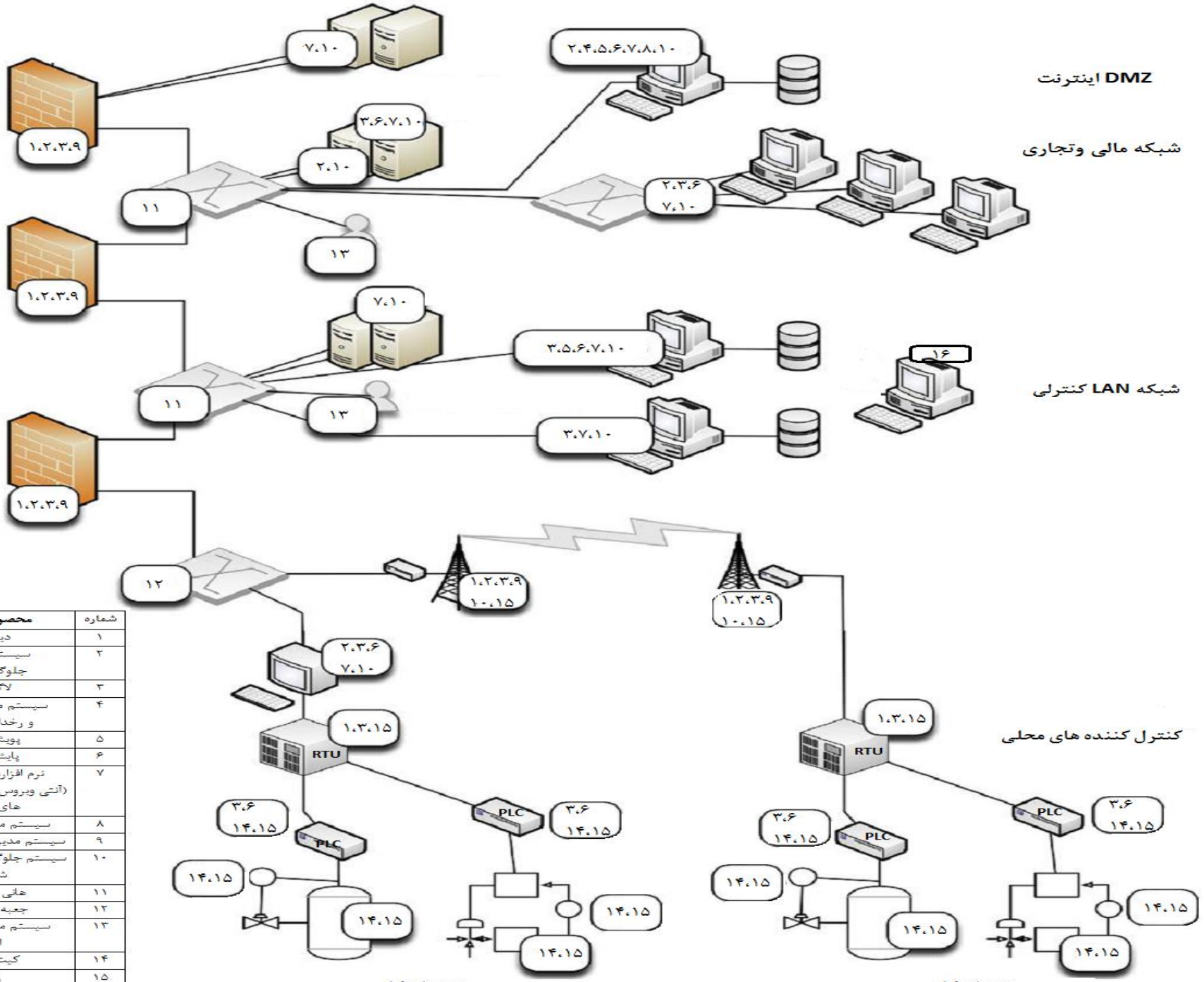


راهبرد پیشنهادی علاوه بر ایزوله کردن مناسب واحدها

راهبرد پیشنهاد شده در تمام اسناد امنیت سایبری در سیستم های صنعتی **دفاع در عمق** می باشد.

فراهم نمودن محافظت چندگانه، به خصوص به شکل لایه ای





شماره	محصولات امنیتی
۱	دیواره آتش
۲	سیستم تشخیص / جلوگیری از نفوذ
۳	لاگر امنیتی
۴	سیستم مدیریت اطلاعات و رخدادهای امنیتی
۵	پویشگر امنیتی
۶	پایشگر امنیتی
۷	نرم افزارهای ضد بدافزار (آنتی ویروس، لیست سفید برنامه های کاربردی)
۸	سیستم مدیریت دارایی ها
۹	سیستم مدیریت یکپارچه تهدید
۱۰	سیستم جلوگیری از نابودی/فاش شدن داده
۱۱	هاب پات صنعتی
۱۲	جعبه شن صنعتی
۱۳	سیستم مدیریت دسترسی اشخاص
۱۴	کیت شناساگر
۱۵	رمزگذار
۱۶	شبیه ساز حمله/ابزار تست نفوذ

شرکت ملی نفت ایران

سومین کنفرانس

امنیت اطلاعات و ارتباطات

در صنعت نفت

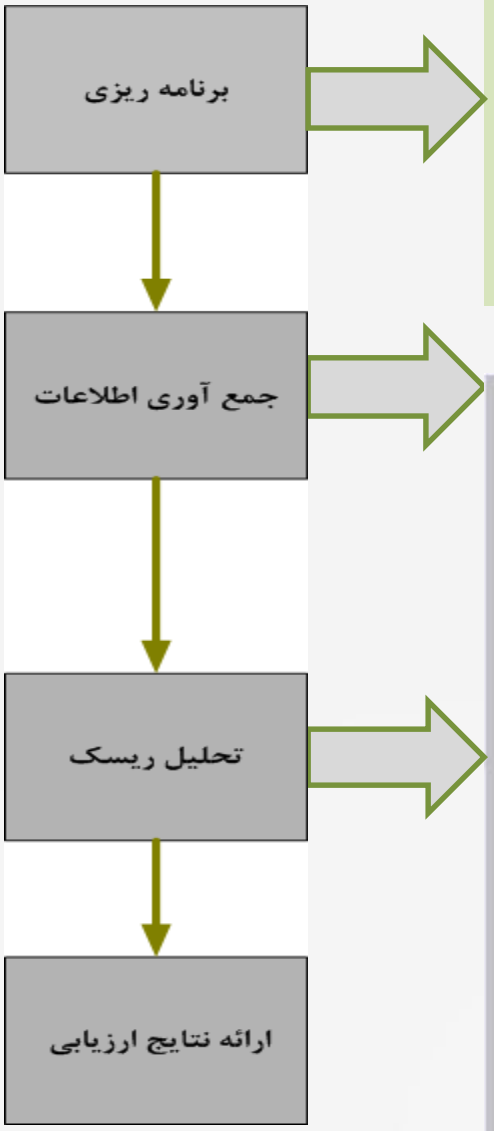
عنوان:

روش ها و ابزارهای ارزیابی امنیت در شبکه های صنعتی اسکادا

ارزیابی امنیتی سیستم های کنترل صنعتی

- **هدف ارزیابی امنیتی ICS** :
  - آگاهی از وضعیت امنیتی موجود و شناسایی آسیب پذیری های سیستم در برابر حملات می باشد.
- **ویژگی ها**:
  - وجود تفاوت های زیادی میان ارزیابی امنیتی سیستم ICS و IT
  - لزوم اجرای ارزیابی امنیتی به شکل دوره ای(فرآیند نه پروژه)
- **ویژگی های گروه ارزیاب**:
  - آشنایی به محدودیت ها و چالش های انجام تست در یک محیط صنعتی
  - ضرورت شناخت گروه ارزیابی از سیستم ICS، خطرات سنجش و عواقب احتمالی ایجاد اختلال در عملکرد سیستم
  - ضرورت وجود آمادگی برای بروز مشکلات در هنگام انجام هر نوع ارزیابی روی سیستم ICS ، کنترل دستی و ...
  - آشنا با پروتکل ها، زبان های برنامه نویسی، برنامه های کاربردی و سیستم عامل مورد استفاده در ICS
  - برخورداری از تجربه ارزیابی سیستم های ICS

گام های عمومی در ارزیابی امنیتی



- انتخاب تیم ارزیاب
- مشخص کردن روش های ارزیابی و

- تست نفوذ
- ارزیابی آزمایشگاهی
- ارزیابی امنیتی در محل
- ارزیابی نفوذپذیری نقطه به نقطه
- سنجش اجزای سیستم
- مرور مستندات فنی
- مرور پیکربندی و عملکرد
- مصاحبه با کارکنان

برای انجام یک ارزیابی جامع و موثر، لازم است از ترکیبی از روش ها و ابزارهای مختلف استفاده شود.

لزوم تحلیل ریسک

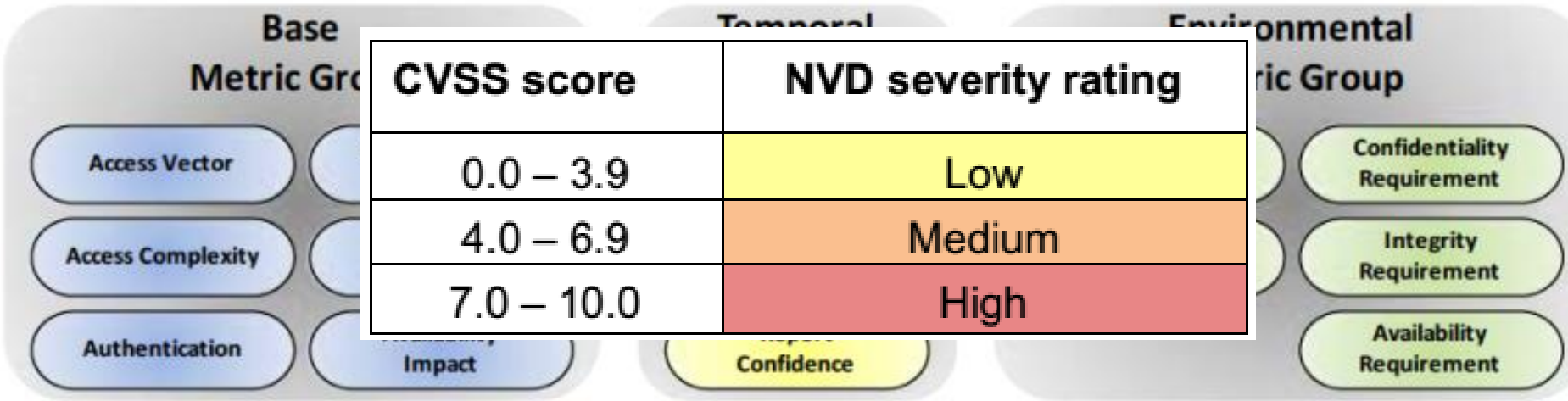
با توجه به محدود بودن منابع هر سازمان ارزیابی ریسک جهت اولویت بندی دارایی ها و سیستم ها ضروری می باشد.

نتایج ارزیابی

- گزارش ارزیابی
  - آسیب پذیری ها
  - اثرات آسیب پذیری ها(از طریق تولید exploits)
  - شاخص ها: برای مشخص کردن اهمیت آسیب پذیری ها و ریسک ناشی از آن ها
    - CVSS v2(Common Vulnerability Scoring System)
  - ارائه پیشنهادات و راهکارهایی جهت رفع یا کاهش آسیب پذیری ها

Common Vulnerability Scoring System

- معیارها:
  - Base: ویژگی های ذاتی و اساسی یک آسیب پذیری که نسبت به زمان و محیط تغییر نمی کنند.
  - Temporal: ویژگی های متغیر با زمان و نه با محیط کاربر
  - Environmental: ویژگی های مربوط و منحصر به محیط کاربر



CVSS score	NVD severity rating
0.0 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 10.0	High

نتایج ارزیابی

هزینه سواستفاده موفقیت آمیز> هزینه مقاوم سازی

مقاوم سازی و رفع آسیب پذیری ها بر اساس تحلیل ریسک

ابزارهای ارزیابی امنیتی

- ابزارهایی هستند که می توان از آن ها در فرآیند ارزیابی امنیتی بهره برد.
- با استفاده از این ابزارها می توان بخشی از فرآیند ارزیابی را به شکل خودکار انجام داد.
- نمونه هایی از قابلیت هایی که ابزارهای ارزیابی ارائه می دهند:
  - نگاشت شبکه(Network Mapping)
  - پویش آسیب پذیری ها
  - بررسی تطابق با استانداردهای امنیتی
  - بررسی پیکربندی های امنیتی
  - مدیریت دارایی ها

ابزارهای ارزیابی امنیتی

- ابزارهای ارزیابی را می توان به دو دسته فعال و غیرفعال تقسیم کرد:
  - ابزارهای فعال: تغییری را در سیستم به وجود می آورند، برای مثال ترافیک به شبکه اضافه می کنند و می توانند بر عملکرد سیستم تاثیرگذار باشند.
  - ابزارهای غیرفعال: تغییری را در شبکه به وجود نمی آورند، و تاثیری بر عملکرد شبکه ندارند.
- تعدادی از ابزارهایی که در فرآیند ارزیابی سیستم های صنعتی کاربرد دارند:
  - پویشگر Nessus
  - پویشگر Nmap
  - ابزار ارزیابی CSET
  - ابزار ارزیابی ICSAT

ابزار پویشگر Nmap (فعال)

- ابزار پویشگر Nmap، پویشگری فعال با قابلیت نگاشت شبکه:
  - شناسایی میزبان های شبکه
  - شناسایی سیستم های عامل
  - پویش پورت ها
  - شناسایی برنامه های کاربردی و نسخه آن ها
  - شناسایی آسیب پذیری های شناخته شده

- قابلیت پویش شبکه و آسیب پذیری های برخی از شبکه های SCADA با استفاده از قابلیت NSE(Nmap Scripting Engine) به این ابزار اضافه شده است.
  - برای مثال اسکریپت Modbus-discover است که برای سرشماری دستگاه های فرمانبر Modbus در سیستم SCADA و جمع آوری اطلاعات آن ها شامل سازنده و سفت افزار، نوشته شده است

ابزار پویشگر Nessus(فعال)

- ابزار پویشگر Nessus، **پویشگر فعال** با قابلیت:
  - پویش آسیب پذیری با کمترین تاثیر
  - شناسایی دارایی های شبکه
  - شناسایی آسیب پذیری ها
  - بررسی پیکربندی امنیتی

- Nessus در بر گیرنده دانش خاص سیستم کنترلی به شکل:
  - فایل های بازرسی امنیتی Bandolier: فایل های بازرسی امنیتی Nessus برای کاربردهای سیستم کنترلی تهیه شده و با استفاده از پلاگین های تطبیق سیاست Nessus گزارش می دهند که سرور یا ایستگاه کاری در یک پیکربنی امنیتی بهینه قرار دارد یا خیر.
  - خانواده پلاگین های SCADA که نمونه ای از پویش های آسیب پذیری هستند که به طور خاص برای برنامه های کاربردی و پروتکلهای سیستم کنترل تولید شده اند.
  - Tenable در سال ۲۰۰۸ اعلام کرد که بیش از ۲۰۰۰۰ پلاگین منحصر به فرد SCADA تولید کرده است.

مخاطرات پویشگرهای فعال

طول عمر بالای سیستم های ICS و فاصله با فناوری روز

این سیستم ها می توانند به راحتی با ترافیک ایجاد شده به وسیله ابزارهای فعال دچار مشکل شوند بنابراین پویشگرهای فعال باید با احتیاط در مورد سیستم ICS به کار گرفته شوند.

- مثال(NIST SP 800-82):
  - قفل شدن سیستم SCADA در یک واحد تولید گاز طبیعی در اثر انجام تست نفوذ روی بخشی از شبکه مالی تجاری که مستقیما به سیستم SCADA متصل بود. این اتفاق باعث شد این واحد قادر نباشد به مدت **۴ ساعت** گاز را داخل خطوط لوله خود بفرستد.
  - سیستم کنترل یک واحد تولید IC در اثر اجرای ping sweep در شبکه ICS قفل شد. این پویش برای شناسایی تمامی میزبان های شبکه انجام شده بود، این اتفاق به خسارتی معادل ۵۰۰۰۰ دلار منجر شد.
  - چرخش ۱۸۰ درجه ای یک بازوی ربات ۹ فیتی در اثر اجرای ping sweep روی سیستم SCADA کنترل کننده آن بوجود آمد.

ابزار CSET (غیرفعال)

Homeland Security

- نرم افزاری برای ارزیابی امنیت ICS بر اساس استانداردها، دستورالعمل ها و بهترین شیوه ها
- خروجی آن لیستی از توصیه ها جهت بهبود امنیت و دست یافتن به سطح امنیت مطلوب(SAL)

انتخاب استانداردها	• سوالات استانداردها
ایجاد دیاگرام	• سوالات اجزا
تعیین سطح امنیت	• بررسی آماری پاسخ ها
پاسخ به سوالات	• گزارش

ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی ICSAT (غیر فعال)

پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

قابلیت های ابزار ارزیاب

- ✓ شناسایی دارایی های سیستم
- ✓ شناسایی آسیب پذیری های شناخته شده تجهیزات
- ✓ تشخیص تهدیدات متناظر با آسیب پذیری ها
- ✓ تحلیل ریسک
- ✓ ارائه راهکارها و پیشنهادهایی برای رفع آسیب پذیری ها و کاهش ریسک

فرآیند کاری ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی

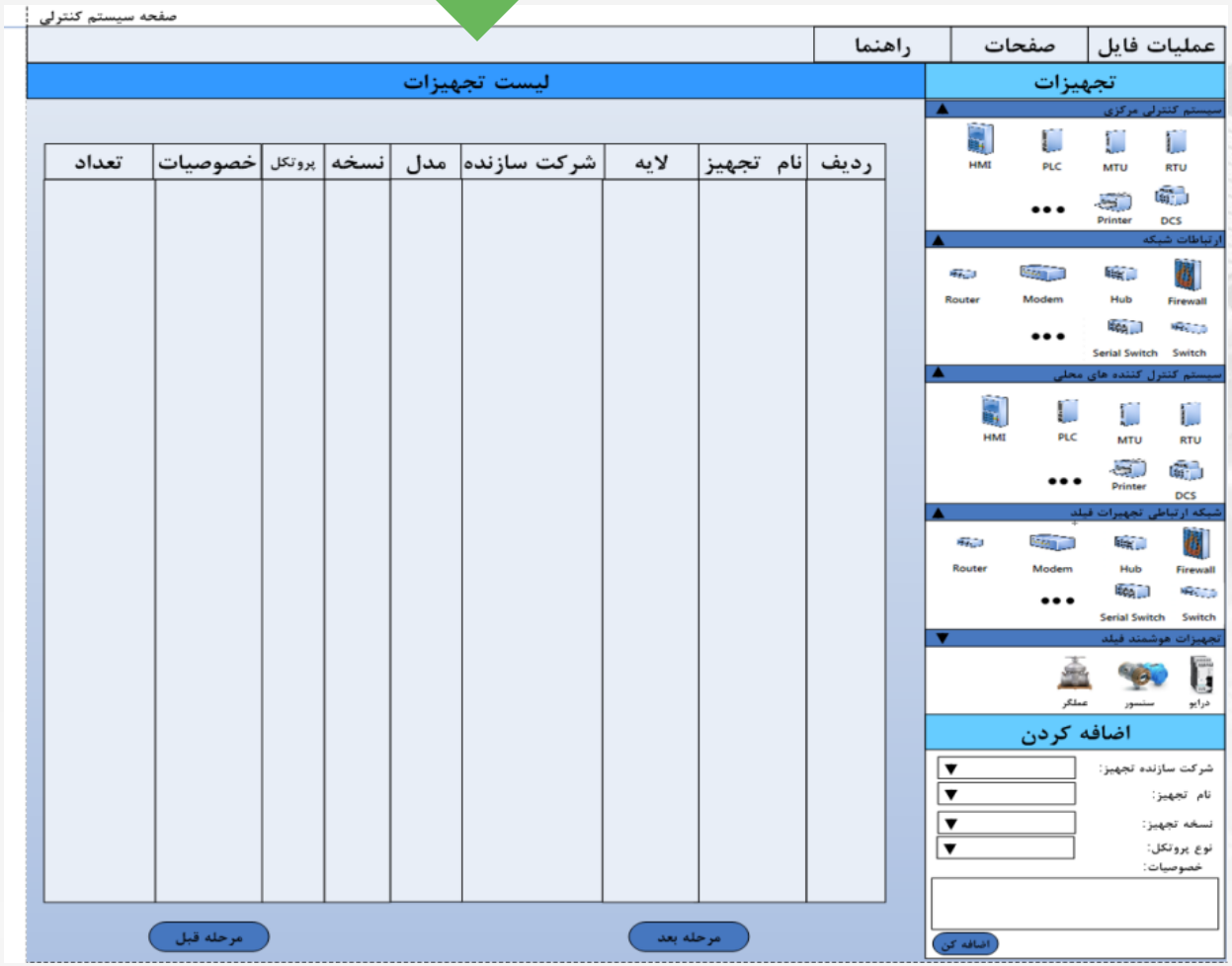
- تعیین مشخصات واحد صنعتی
- پاسخ به سوالات و انتخاب تجهیزات توسط کاربر
- شناسایی آسیب پذیری ها و تهدیدات تجهیزات بر اساس پایگاه داده
- تطابق پاسخ های کاربران به سوالات با الگوی امن مرجع
- تحلیل ریسک
- نمایش نتایج ارزیابی در غالب نمودارها و جداول
- تولید گزارشات خروجی شامل نتایج ارزیابی، راهکارها و پیشنهادات و ...

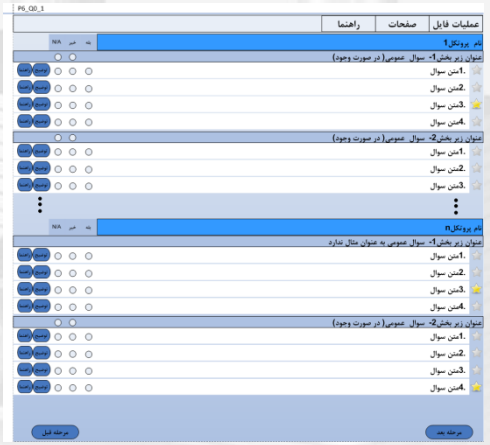
معماری ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی(ادامه)

- تعیین مشخصات واحد صنعتی

معماری ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی(ادامه)

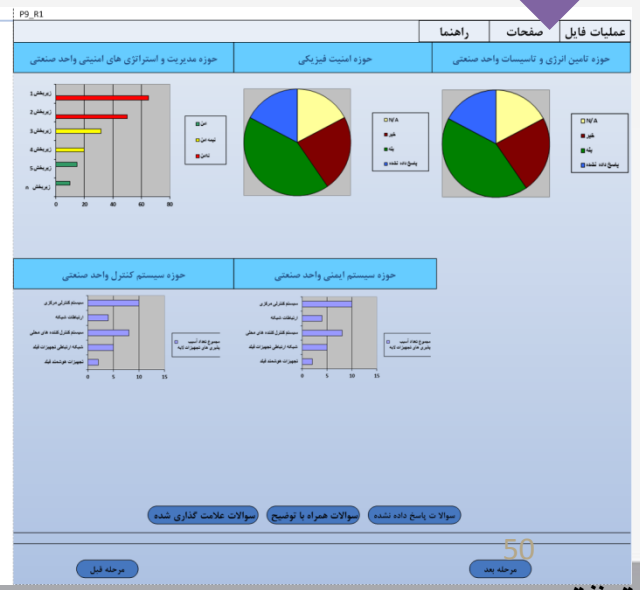
- انتخاب تجهیزات توسط کاربر و پاسخ به سوالات مبتنی بر استانداردهای امنیتی



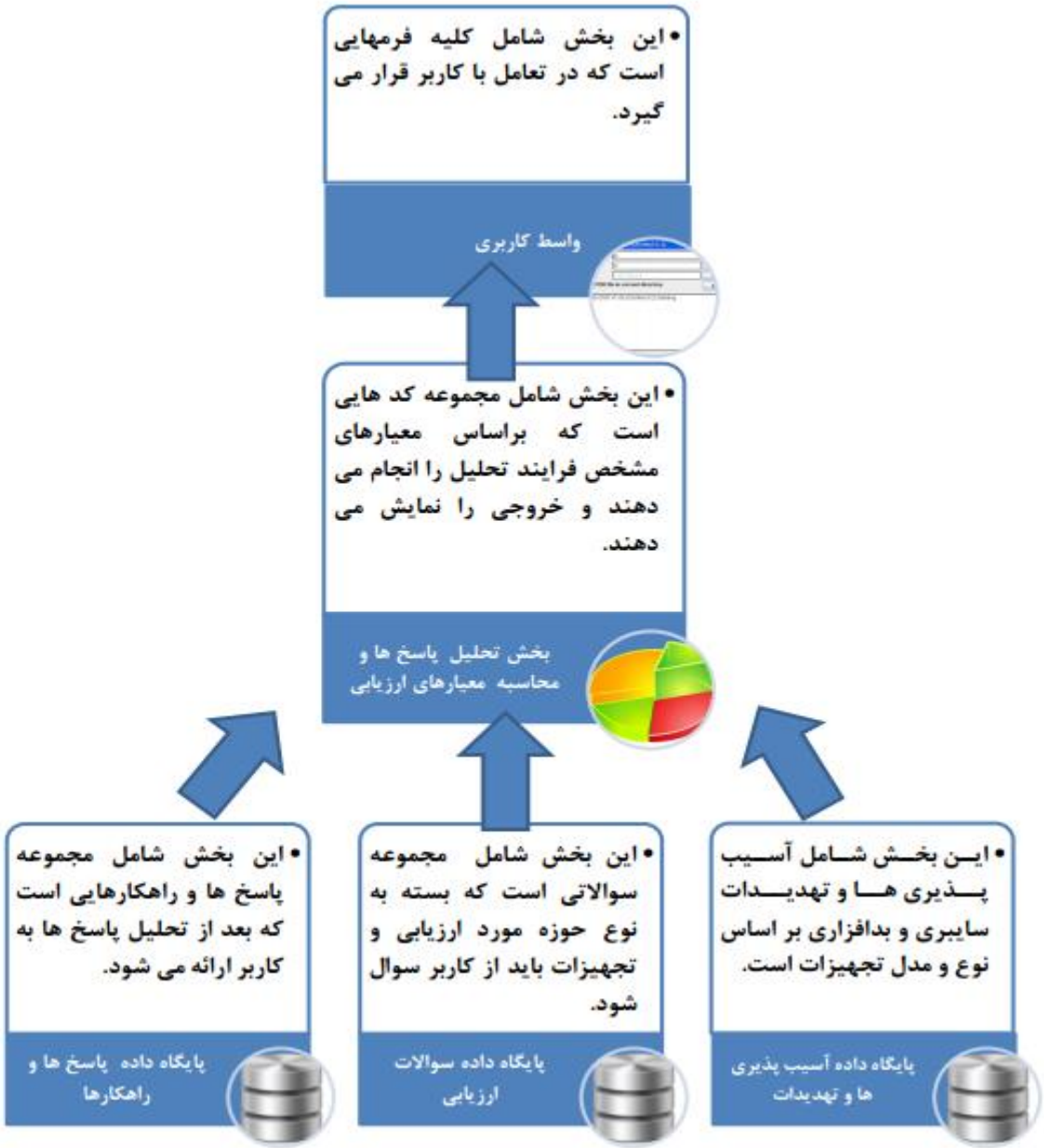


معماری ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی(ادامه)

- شناسایی آسیب پذیری ها و تهدیدات تجهیزات بر اساس پایگاه داده
- تطابق پاسخ های کاربران به سوالات با الگوی امن مرجع
- تحلیل ریسک
- نمایش نتایج ارزیابی در غالب نمودارها و جداول
- تولید گزارشات خروجی شامل نتایج ارزیابی، راهکارها و پیشنهادات و ...



معماری ابزار ارزیاب وضعیت امنیت سایبری سیستم های صنعتی

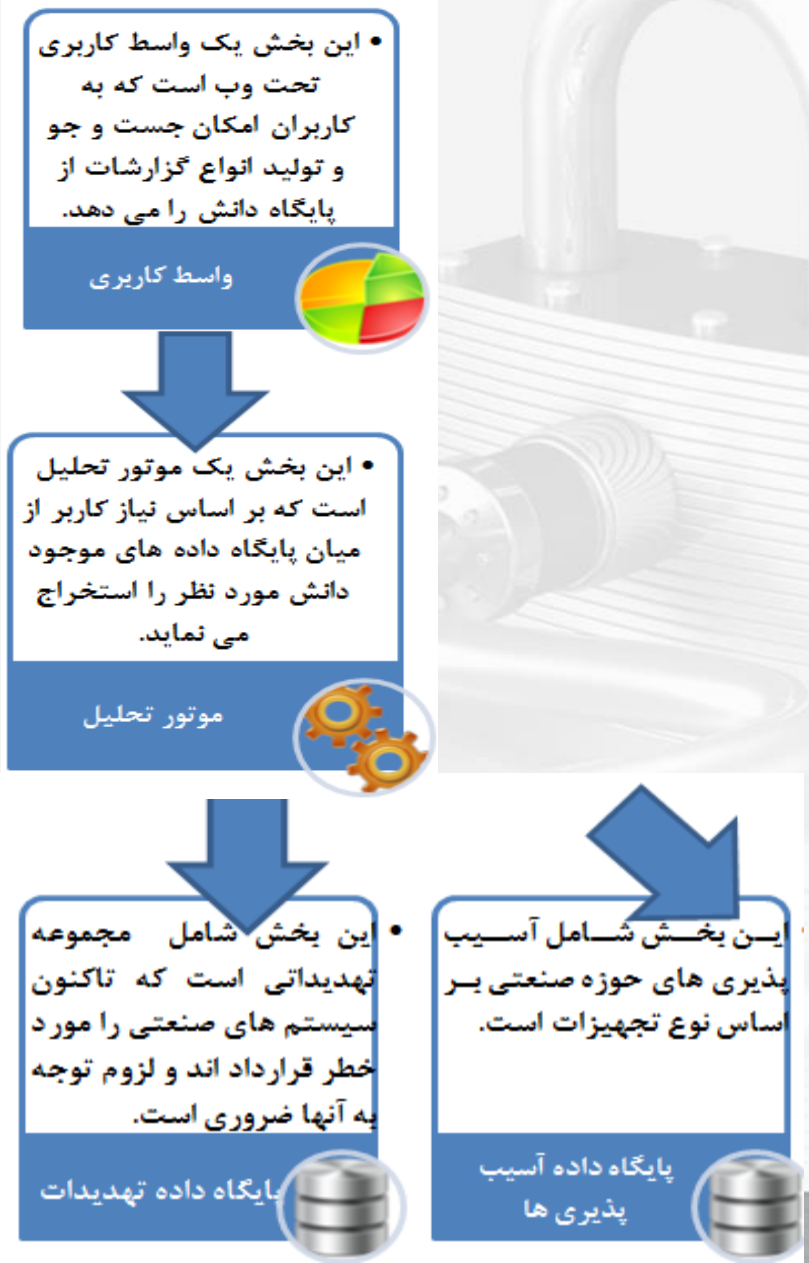


پایگاه دانش آسیب‌پذیری‌ها، بدافزارها، حملات حوزه سیستم‌های صنعتی

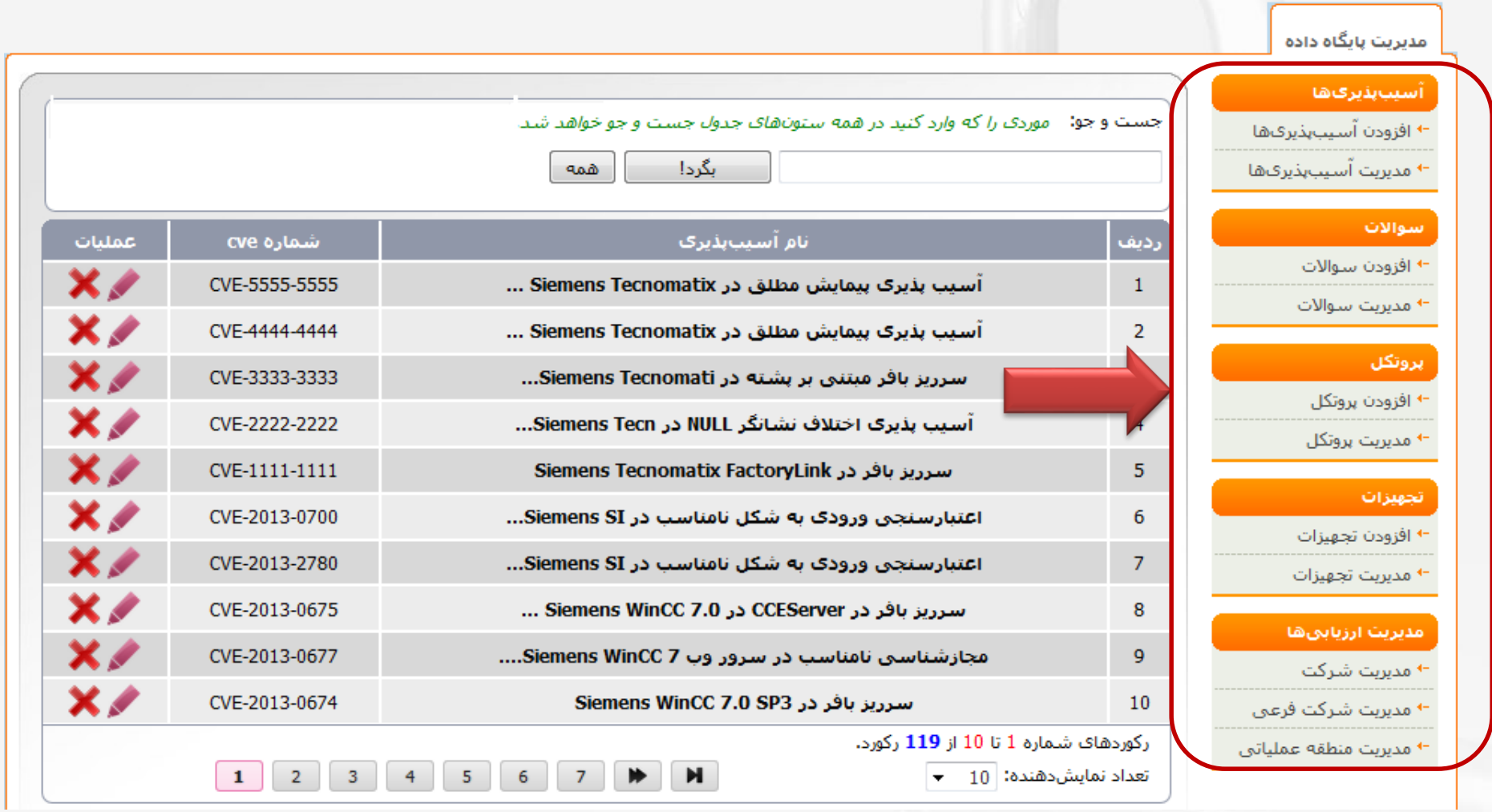
قابلیت های پایگاه

- ✓ دسترسی کاربر به اطلاعات آسیب‌پذیری‌های حوزه تجهیزات سیستم‌های صنعتی(بر اساس نقش و سطوح دسترسی)
  - امکان آشنایی کاربر با تجهیز آسیب پذیر و کاربرد آن در صنایع مختلف
- ✓ امکان آشنایی کاربر با تهدیدات ناشی از هر آسیب پذیری
- ✓ دسترسی کاربر به اطلاعات بدافزارها و حملات حوزه سیستم‌های کنترل صنعتی
- ✓ امکان گزارش

معماری پایگاه دانش



ساختار پویای تغذیه پایگاه دانش



پایگاه دانش آسیب پذیری ها، تهدیدات و بدافزارهای سیستم های صنعتی

اولین پایگاه دانش تخصص در زمینه امنیت سامانه های صنعتی

ده آسیب‌پذیری اخیر

1) ICS-Vul-14-323-01:
Advantech EKI-6340 Command Injection

2) ICS-Vul-14-323-02:
Advantech AdamView Buffer Overflows

3) ICS-Vul-14-281-01A:
Ongoing Sophisticated Malware Campaign

4) ICS-Vul-14-176-02A:
ICS Focused Malware (Update A)

5) ICS-Vul-14-155-01A:
Daktronics Vanguard Default

6) ICS-Vul-14-099-01E:
Ecava IntegraXor Buffer Overflow Vulnerabili

7) ICS-Vul-14-015-01:
Nordex NC2 - Cross-Site Scripting

8) ICS-Vul-13-304-01:
Advantech EKI-6340 Command Injection

9) ICS-Vul-13-259-01:
Mitsubishi Electric Automation MC-WorX

10) ICS-Vul-13-256-01:
WellinTech KingView ActiveX Vulnerabilities

« آرشیو »

ده تهدید اخیر

1) BOF:
Buffer Over Flow on Seimens ...

2) Online attacks via office / enterprise networ
Advantech AdamView Buffer Overflow

3) Attacks on used standard components in the
OpenSSL CVE-2014-3566 Man In The Middle Info

4) (D)DoS attacks:
Advantech EKI-6340 Command Injection

5) Human misbehaviour and sabotage:
Advantech AdamView Buffer Overflow

6) IRKB-2012-0722-B:
Introduction of malicious code via removable

7) Unauthorised access to resources:

8)Attacks to network components:

9) ICS-Vul-14-323-02:
Advantech AdamView Buffer Overflow

10) attacks via office / enterprise networks:

« آرشیو »

ده بدافزار جدید

1) Cookie.Weborama:
Weborama and other malware removal made easy

2) Win32.Generic:
Trojan.Win32.Generic File C:\Documents and S

3) Trojan.Generic.:
Technical Details. Named after the Trojan Ho

4) Trojan.Script:
A detection name that uses the format "troja

5) Protecc:
The IP Code, International Protection Markin

6) Trojan:
Description Trojan Remover aids in the remov

7) Cookie.Rub:
Tracking Cookie/Rub Signature Details: The f

8) Trojan.Sality.A:
Sality is the classification for a family of

9) Protecc.v2:

10) Trojan.SS.:
Trojan SS. STI announces the design of our f

« آرشیو »

ده آسیب‌پذیری اخیر
1) ICS-Vul-14-323-01:
Advantech EKI-6340 Command Injection

ده تهدید اخیر
1) BOF:
Buffer Over Flow on Seimens ...

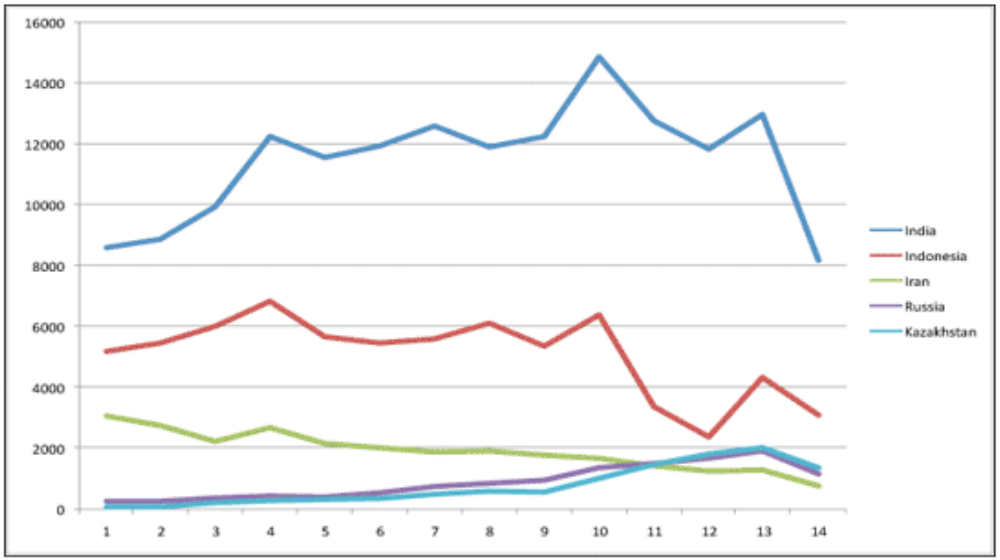
ده بدافزار جدید
1) Cookie.Weborama:
Cookie.Weborama is malware that...

خصیصه مورد تحلیل: انتخاب خصیصه تحلیلی

بازه زمانی: از: ۱۳ / / تا: ۱۳ / /

نوع نمودار: خطی دایره‌ای

رسم نمودار



پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

مقایسه ابزار ICSAT و CSET

ویژگی / عنوان	دیاگرام	سوالات مبتنی بر استانداردهای امنیتی و تجهیزات	شناسایی دارایی های سیستم	شناسایی آسیب پذیری های شناخته شده تجهیزات	تشخیص تهدیدات متناظر با آسیب پذیری ها	تحلیل ریسک	تبیین سطح امنیت	ارائه راهکارها و پیشنهادها مبتنی بر استانداردها	ارائه راهکارها برای رفع آسیب پذیری های تجهیزات و کاهش ریسک
CSET (DHS)	✓	✓	✗	✗	✗	✗	تحلیل آماری پاسخ ها	✓	✗
ICSAT (AUT) 1st ver.	✓	✓	✓	✓	✓	✓	تحلیل ریسک و سوالات وزن دار	✓	✓

پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

با تشکر از توجه شما

پژوهشکده پدافند غیر عامل
دانشگاه صنعتی امیرکبیر

از حضور گرمتان
کمال تشکر را داریم

مرکز آموزش شرکت ملی نفت ایران – محمودآباد