دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر

آزمایشگاه امنیت داده و شبکه
http://dnsl.ce.sharif.edu

درس ۱۳: سیستم تشخیص نفوذ (IDS)

محمد صادق دوستی

فهرست مطالب

- **مقدمه و تعاریف اولیه**
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

سیستم تشخیص نفوذ

- تشخیص نفوذ (ID): فرآیند نظارت بر وقایع رخ داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست‌های امنیتی.
- سیستم تشخیص نفوذ (IDS): یک نرم‌افزار با قابلیت تشخیص، آشکارسازی و پاسخ (واکنش) به فعالیت‌های غیرمجاز یا ناهنجار در رابطه با سیستم.
- تحقیقات و توسعه آن از سال ۱۹۸۰ به بعد

وظایف عمومی یک IDS

- نظارت و تحلیل فعالیت‌های شبکه، سیستم و کاربر
- تشخیص الگوهای منطبق با حملات شناخته شده
- تحلیل الگوهای فعالیت ناهنجار

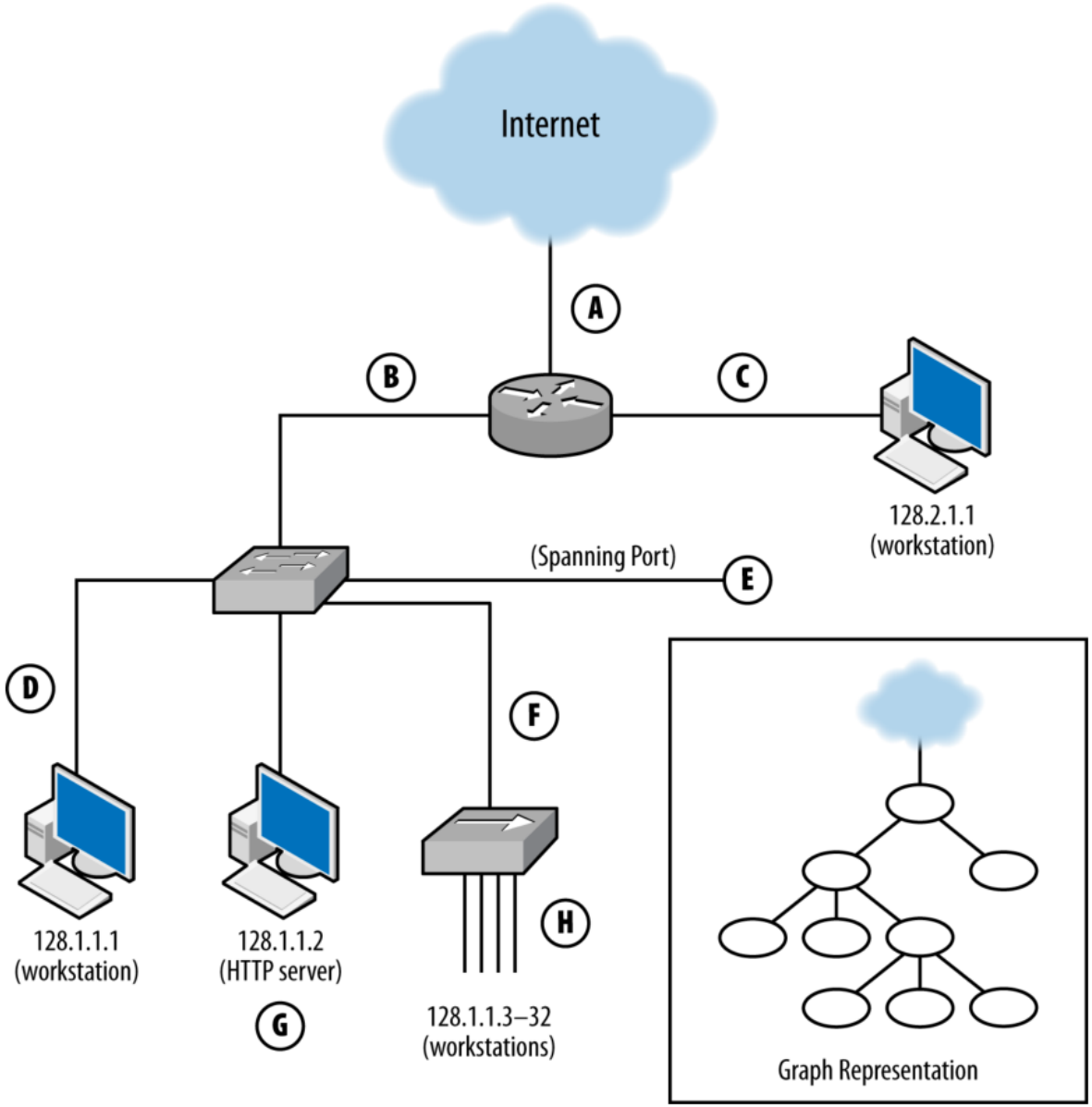
دلایل استفاده از سیستم‌های تشخیص نفوذ

- تشخیص و ثبت تهدیدات موجود برای یک سازمان
- جلوگیری از کامل شدن حملات با تشخیص در مراحل اولیه
- جلوگیری از تکرار حملات مشابه با آگاهی رسانی در مورد حملات کشف شده
- جمع‌آوری اطلاعات مفید درباره حملات و نفوذهای اتفاق افتاده
- فراهم‌سازی امکان عیب‌یابی (شناخت آسیب‌پذیری‌ها)، کشف، و تصحیح عامل‌های سبب شونده

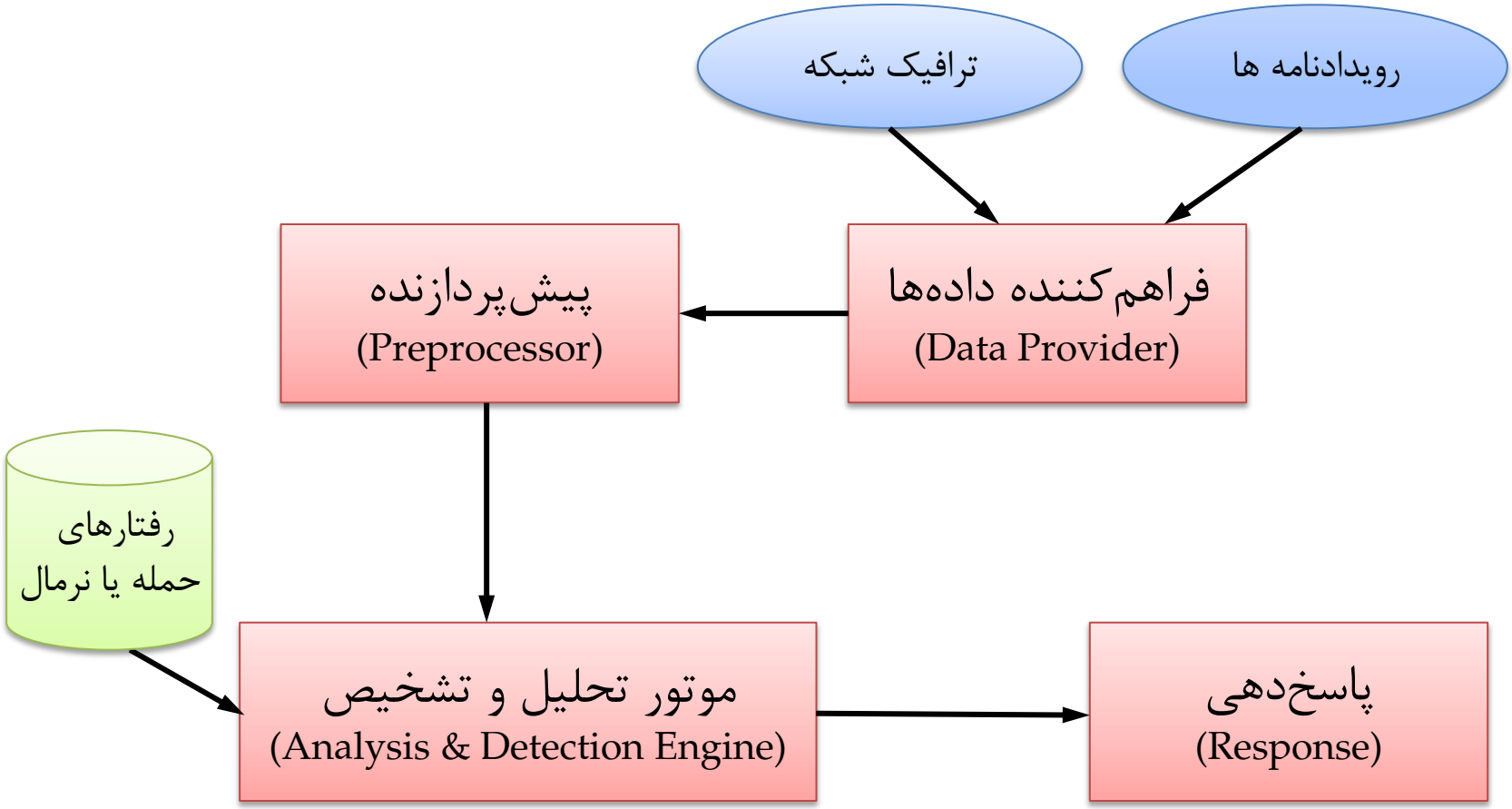
فهرست مطالب

- مقدمه و تعاریف اولیه
- **رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ**
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- مکمل سیستم‌های تشخیص نفوذ

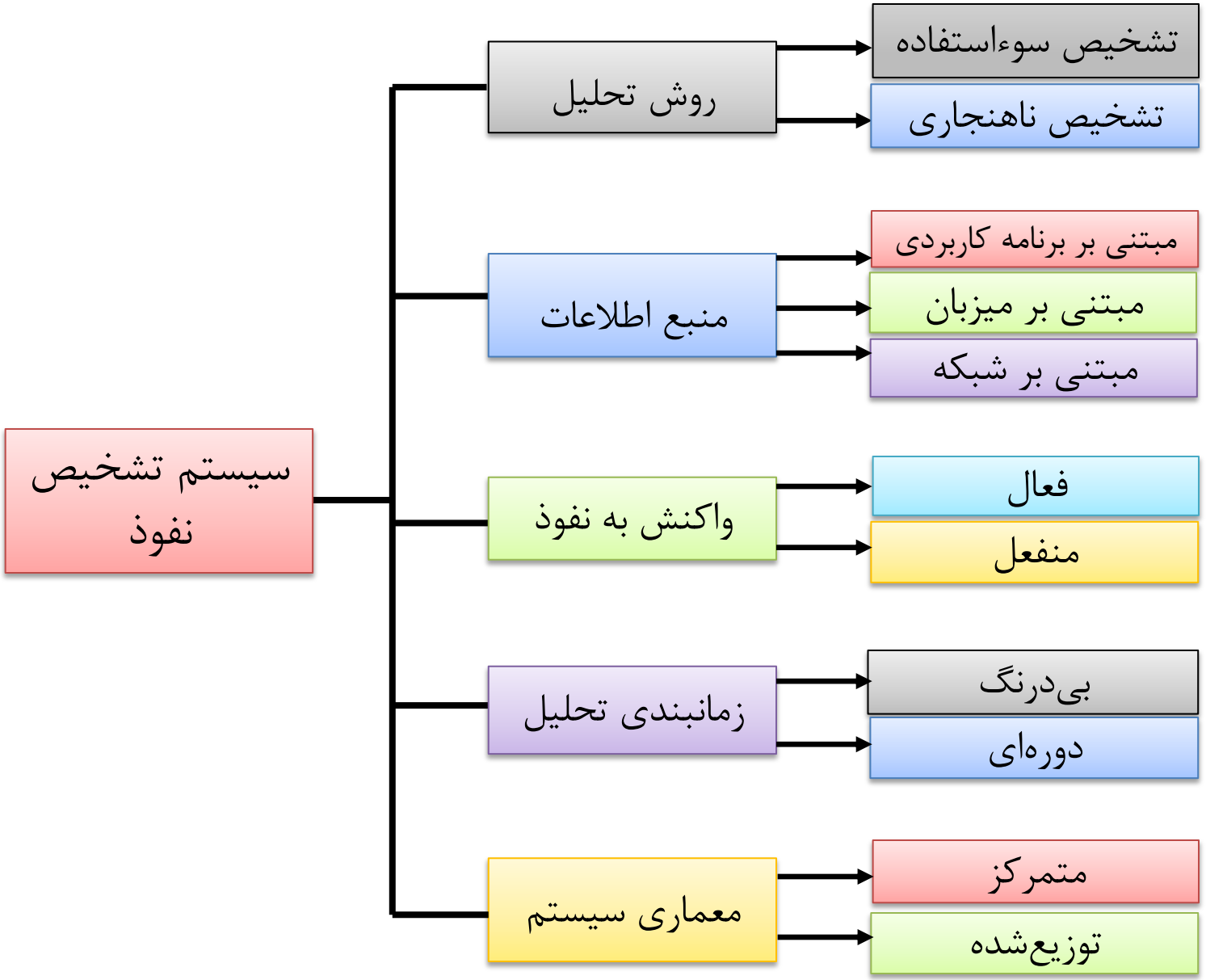
آرایش قرارگیری سنسور IDS در شبکه



معماری یک IDS



رده‌بندی کلی سیستم‌های تشخیص نفوذ



جمع آوری اطلاعات

- عملیات جمع‌آوری داده از یک منبع اطلاعاتی و تحویل آنها به پیش‌پردازنده و موتور تحلیل
- مبتنی بر شبکه (NIDS)
- **مبتنی بر میزبان (HIDS):**
  - دنباله‌های ممیزی سیستم‌عامل (Audit Trail)، رویدادنامه‌ها (Logs)
- مبتنی بر برنامه کاربردی
  - رویدادنامه پایگاه‌داده‌ها، رویدادنامه کارگزار وب

جمع آوری اطلاعات (ادامه)

- تشخیص نفوذ مبتنی بر شبکه
- مزایا:
  - قابلیت نظارت بر یک شبکه بزرگ
  - عدم تداخل با عملکرد معمولی شبکه
  - قابلیت مخفی نگه‌داشته شدن از دید مهاجمان
- معایب:
  - عدم عملکرد صحیح در ترافیک سنگین
  - عدم توانایی در تحلیل اطلاعات رمز شده (مانند VPN)

جمع آوری اطلاعات (ادامه)

- نظارت مبتنی بر میزبان
- مزایا:
  - کشف حملاتی که از طریق شبکه قابل شناسایی نیستند.
  - قابلیت عمل در محیطی که ترافیک شبکه در آن رمز شده
- معایب:
  - امکان غیرفعال شدن سیستم در بخشی از حمله
  - نیاز به انباره زیاد برای ذخیره اطلاعات
  - سربار محاسباتی برای میزبان

زمانبندی تحلیل

- **زمانبندی (Timing)**: فاصله زمانی بین رخداد وقـایع در منبـع اطلاعات تا تحلیل آنها توسط موتور تحلیل
- زمانبندی دسته‌ای یا دوره‌ای (Batch)

☜ کشف نفوذ پس از وقوع، عدم امکان پاسخ‌گویی فعال

- زمان‌بندی بی‌درنگ (Real-time)

☜ تشخیص نفوذ به محض وقوع و یا حتی قبـل از آن، وجـود امکـان پاسخ‌گویی فعال و پیش‌گیری از نفوذ

تحلیل و تشخیص

- تشخیص سوء استفاده (Misuse Detection)
  - علائم حمله (Attack Signatures)
- تشخیص ناهنجاری (Anomaly Detection)
  - رفتار غیرنرمال

تشخیص سوء استفاده

- مشخصات
  - شناخت حملات موجود
  - تعریف الگوی حملات برای موتور تحلیل
  - جستجوی مجموعه‌ای از وقایع که با یک الگوی از پیش تعریف شده مطابقت دارد.
  - نیاز به بروزرسانی الگوهای حمله
- روشهای پیاده‌سازی: سیستم خبره، روشهای مبتنی بر گذار حالات و ...

تشخیص ناهنجاری

- مشخصات
  - شناخت عملکرد نرمال سیستم
  - تهیه نمایه‌هایی از رفتار نرمال سیستم برای موتور تحلیل
  - جستجوی فعالیت غیر نرمال
- آیا هر رفتار غیر نرمال یک حمله است؟
- روشهای پیاده‌سازی: روشهای آماری، شبکه‌های عصبی و ...

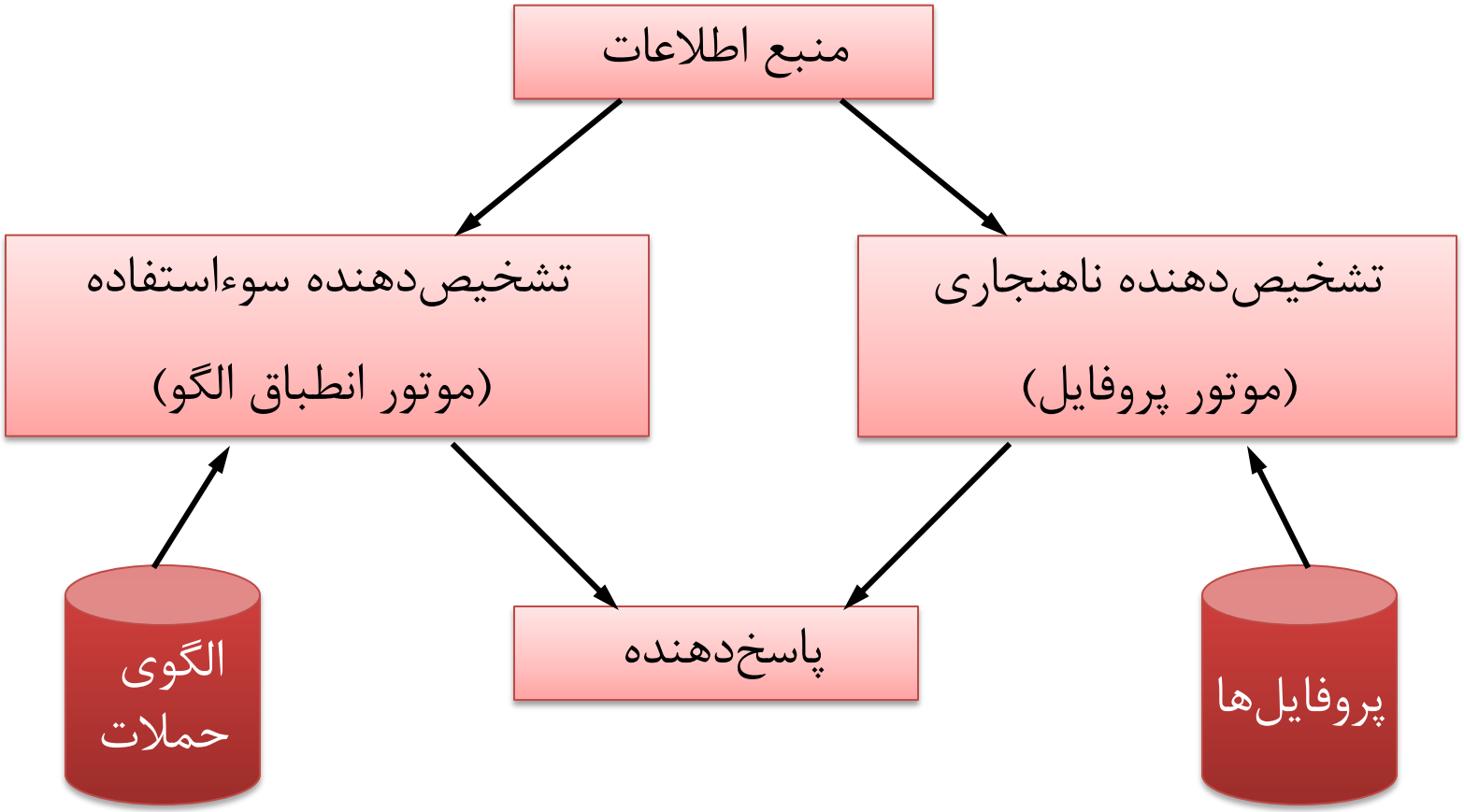
تحلیل و تشخیص (مقایسه)

تشخیص سوءاستفاده Misuse Detection	تشخیص ناهنجاری Anomaly Detection
تشخیص فقط در حد حملات شناخته شده	تشخیص حملات ناشناخته
تشخیص سریع و مطمئن با خطای کمتر	بالابودن درصد خطای مثبت غلط

- مثبت غلط (False Positive): تشخیص نادرست ترافیک خوب به عنوان حمله
- منفی غلط (False Negative): تشخیص نادرست ترافیک حمله به عنوان خوب

ترکیب دو نوع موتور تحلیل

- نمای یک سیستم تشخیص نفوذ ترکیبی



واکنش به نفوذ

- فعال (Active): در صورت تشخیص حمله انجام برخی اعمال واکنشی به صورت خودکار
  - انجام عملی علیه مهاجم (مثلا انسداد دسترسی مهاجم)
  - جمع‌آوری اطلاعات بیشتر

عنوان دیگر IDSهای فعال:
سیستمهای جلوگیری از نفوذ (IPS)

- منفعل (Passive): گزارش به مدیران و واگذاری واکنش به آنها
  - نمایش پیغام بر روی صفحه
  - ارسال پست الکترونیکی / پیامک

فهرست مطالب

روشهای پیاده‌سازی تشخیص سوءاستفاده

- سیستم خبره (Expert System)

☜ سازوکاری برای پردازش حقایق و استنتاج نتایج منطقی از این حقایق با توجه به زنجیره‌ای از قواعد

قواعد ⟵ الگوها یا سناریوهای نفوذ

حقایق ⟵ وقایع رخ‌داده در سیستم

روش‌های پیاده‌سازی تشخیص سوءاستفاده

- مزایا
  - ارائه حملات در قالب قواعد توسط کاربر بدون نیاز به دانستن نحوه عملکرد سیستم خبره
  - امکان اضافه کردن قواعد جدید بدون تغییر قواعد قبلی
- معایب
  - کارآیی پایین، نامناسب برای حجم زیاد داده‌ها
  - نامناسب برای بیان ترتیب در قواعد

روش‌های پیاده‌سازی تشخیص سوءاستفاده

- روش‌های مبتنی بر گذار حالت (State Transition)

☜ استفاده از مفهوم حالت سیستم و گذار (مدلهای گرافیکی نظیر شبکه‌های مارکوف / بیزی)

☜ استفاده از تکنیک‌های انطباق الگو

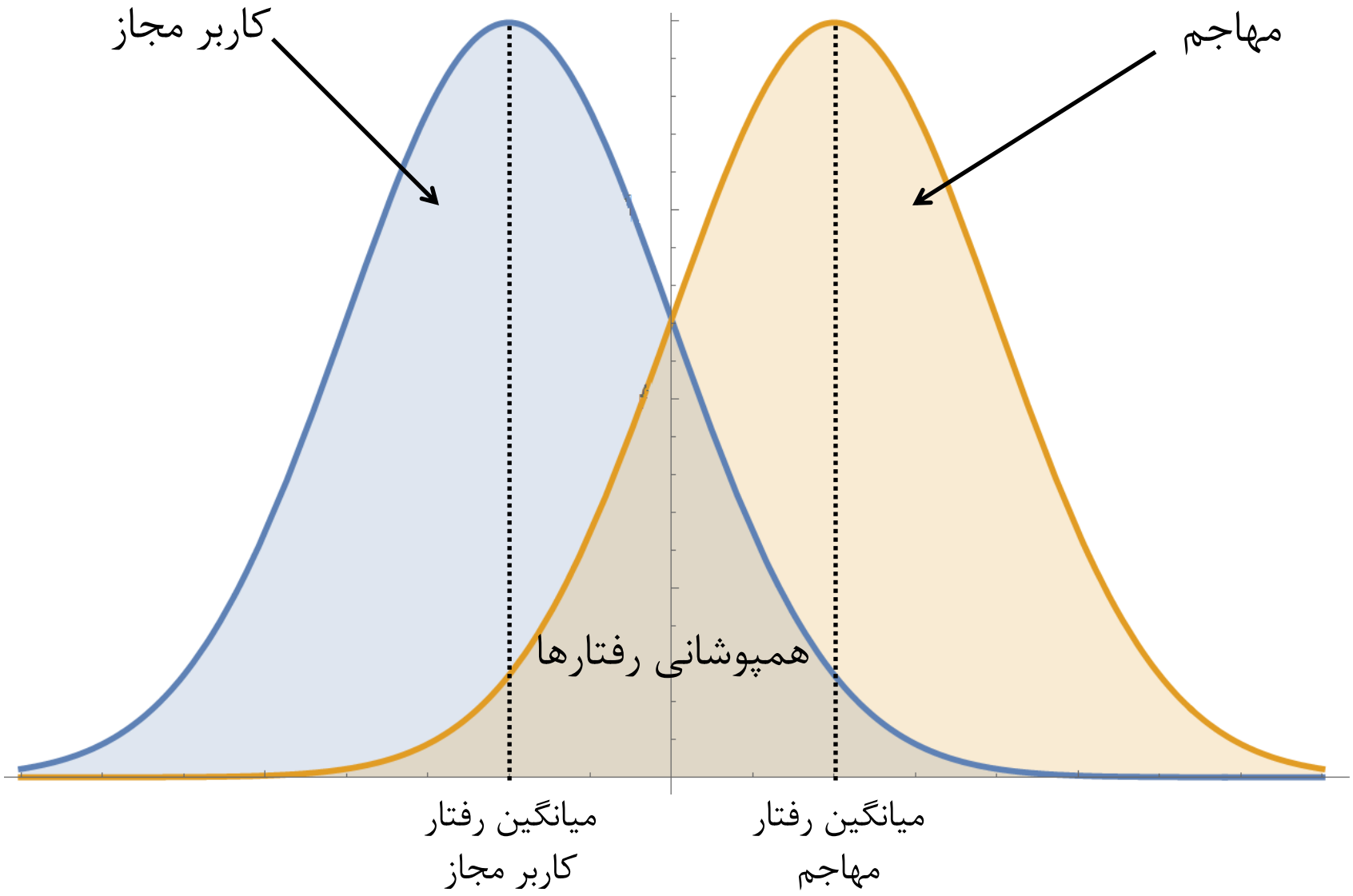
☜ سرعت و قابلیت

الگوی حمله : **حالت امن اولیه** ←(عملیات کلیدی)— **حالت خطرناک نهایی**

روش‌های پیاده‌سازی تشخیص ناهنجاری

- **تحلیل کمّی:** بیان نمایه با معیارهای عددی
  - تعداد مجاز ورود ناموفق برای کاربر A، n است.
- **تحلیل آماری:** بیان نمایه با معیارهای آماری
  - ورودهای ناموفق برای کاربر A از یک توزیع نرمال با میانگین μ و انحراف معیار σ پیروی می‌کند.
  - IDES، NIDES، Haystack
- **داده‌کاوی:** دسته‌بندی (classification) رفتارها بر حسب نرمال و غیرنرمال

مقایسه پروفایل رفتار کاربر مجاز و مهاجم

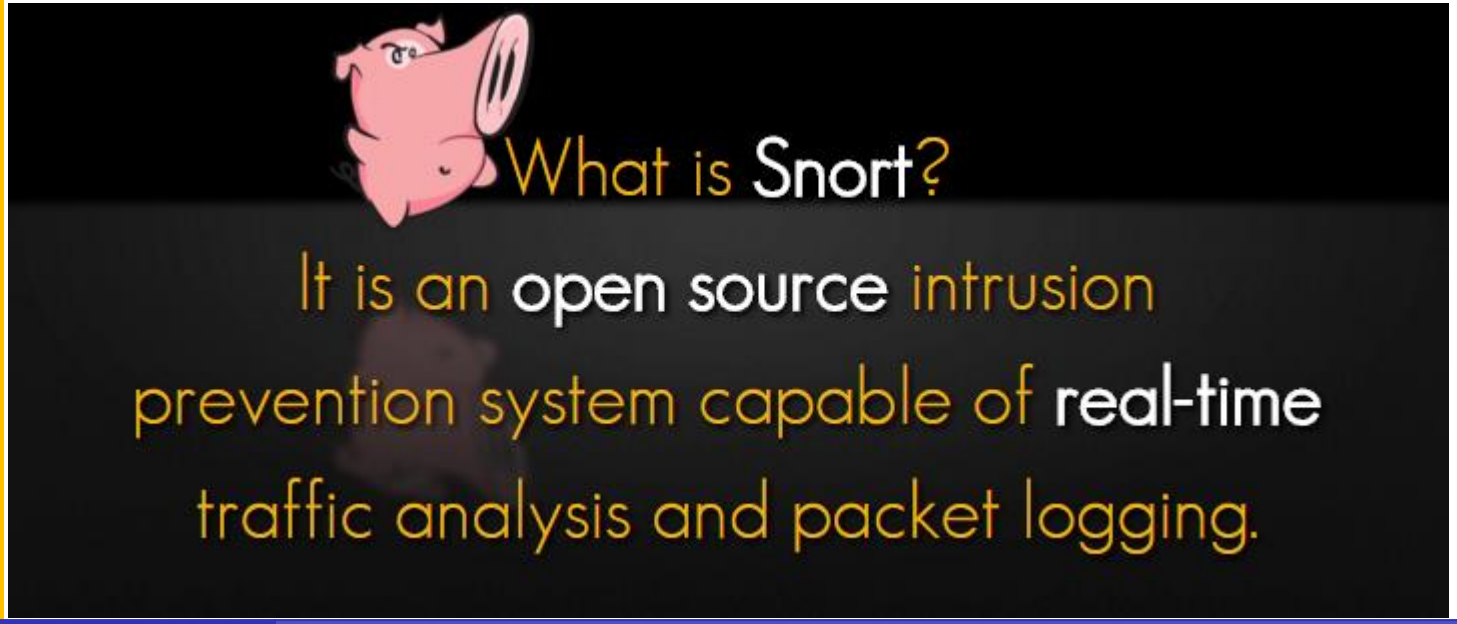


فهرست مطالب

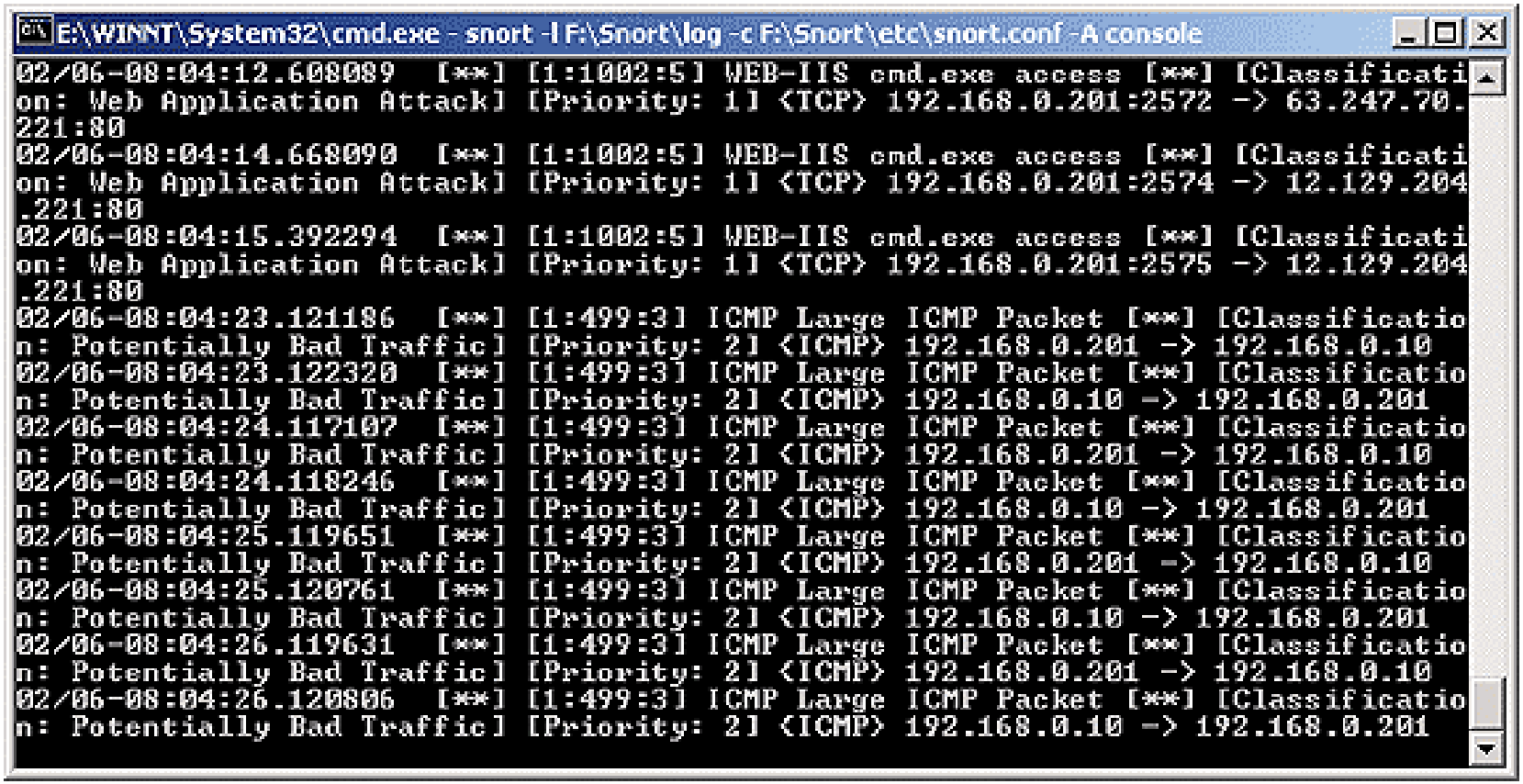
- مقدمه و تعاریف اولیه
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- **معرفی چند سیستم تشخیص نفوذ نمونه**
- مکمل سیستم‌های تشخیص نفوذ

سیستم Snort

- متن‌باز و رایگان
- مبتنی بر شبکه (NIDS)
- تشخیص سوءاستفاده
- حاوی الگوی هزاران نوع حمله



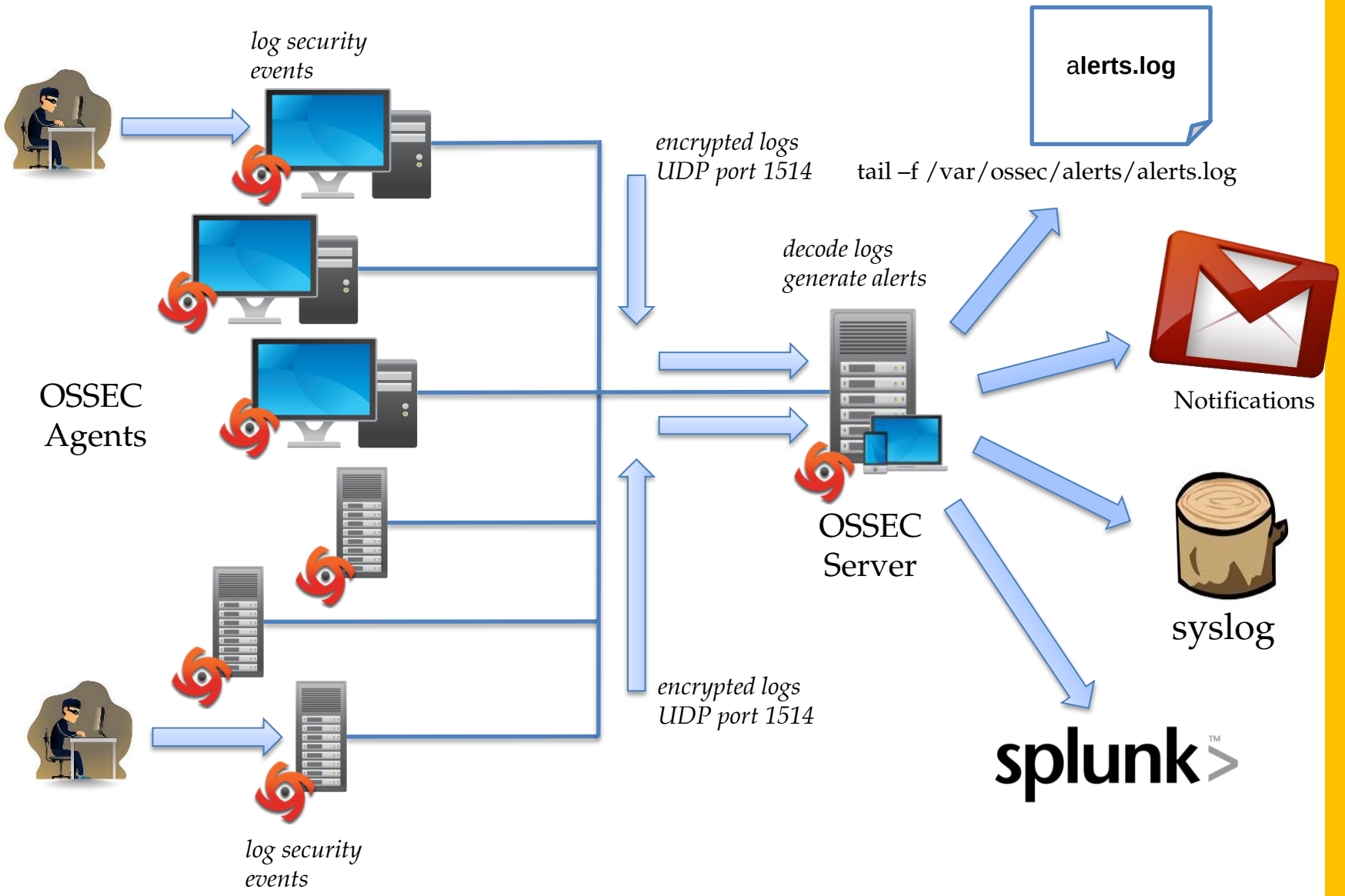
نمونه خروجی Snort



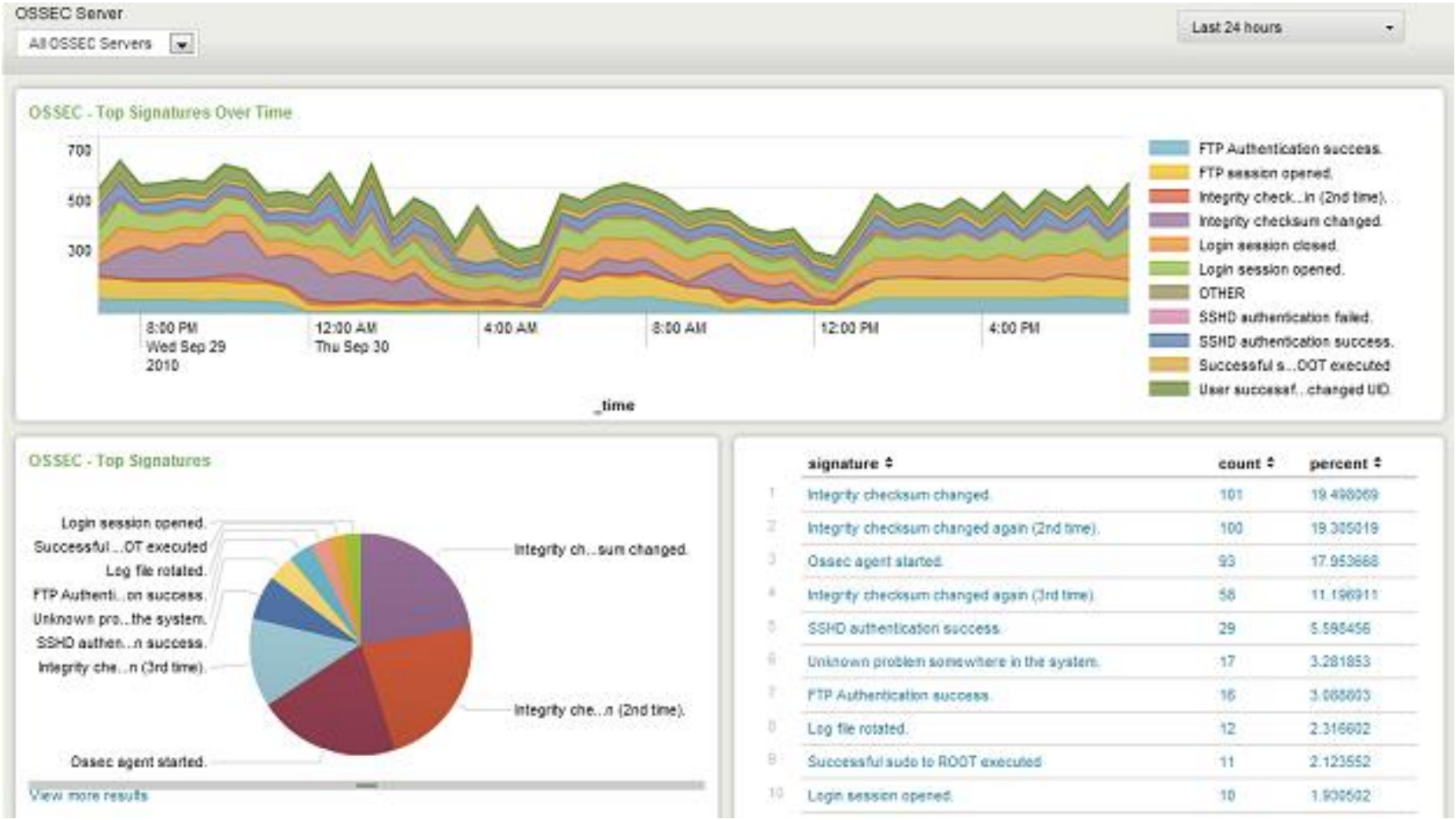
سیستم OSSEC

- متن‌باز و رایگان
- مبتنی بر میزبان (HIDS)
- امکان تحلیل رویدادنامه، کنترل صحت، مانیتورینگ رجیستری (ویندوز)، و تشخیص rootkit
- قابلیت به کارگیری در سیستم‌های عامل‌های مختلف (مانند Linux، FreeBSD، Mac OS، و Windows)

نحوه کار OSSEC



داشبورد Splunk for OSSEC



فهرست مطالب

- مقدمه و تعاریف اولیه
- رده‌بندی و مشخصات سیستم‌های تشخیص نفوذ
- پیاده‌سازی سیستم‌های تشخیص نفوذ
- معرفی چند سیستم تشخیص نفوذ نمونه
- **مکمل سیستم‌های تشخیص نفوذ**

ترکیب با سیستم‌های تله

- **سیستم تله‌عسل (Honeypot)**: اغفال و فریب مهاجم جهت جمع‌آوری اطلاعات بیشتر از نحوهٔ عملکرد آن.

- درحال حاضر بیشتر برای جمع‌آوری بدافزارها استفاده می‌شود.

- امکان استفاده از سیستم‌های تشخیص ناهنجاری برای هدایت ترافیک مشکوک به تله‌ها

تحلیل همبستگی هشدارها

- سیستم همبسته‌ساز هشدارها (Alert Correlation)

  - سیستمی برای تحلیل همبستگی بین رویدادهای ثبت شده (هشدارهای تولید شده) توسط سیستم‌های تشخیص نفوذ

- اهداف:

  - کاهش حجم هشدارها و اعلان‌ها
  - وارسی صحت هشدارها
  - استخراج حملات چند مرحله‌ای

سیستم اخطار زودرس (EWS)

- Early Warning System
  - پیش‌بینی حملات قبل از وقوع
    - بر اساس جمع‌آوری و همبسته‌سازی هشدارها از منابع متعدد
  - مثال: DeepSight (محصول Symantec)
    - جمع‌آوری اطلاعات از شبکه‌های هزاران مشتری
    - هر مشتری می‌تواند اطلاعات شبکه خود را در پورتال DeepSight مشاهده نماید.
    - در صورت حمله به یک مشتری، سایرین به سرعت مطلع می‌شوند.