Intrusion Detection Systems and Security Information and Event Management

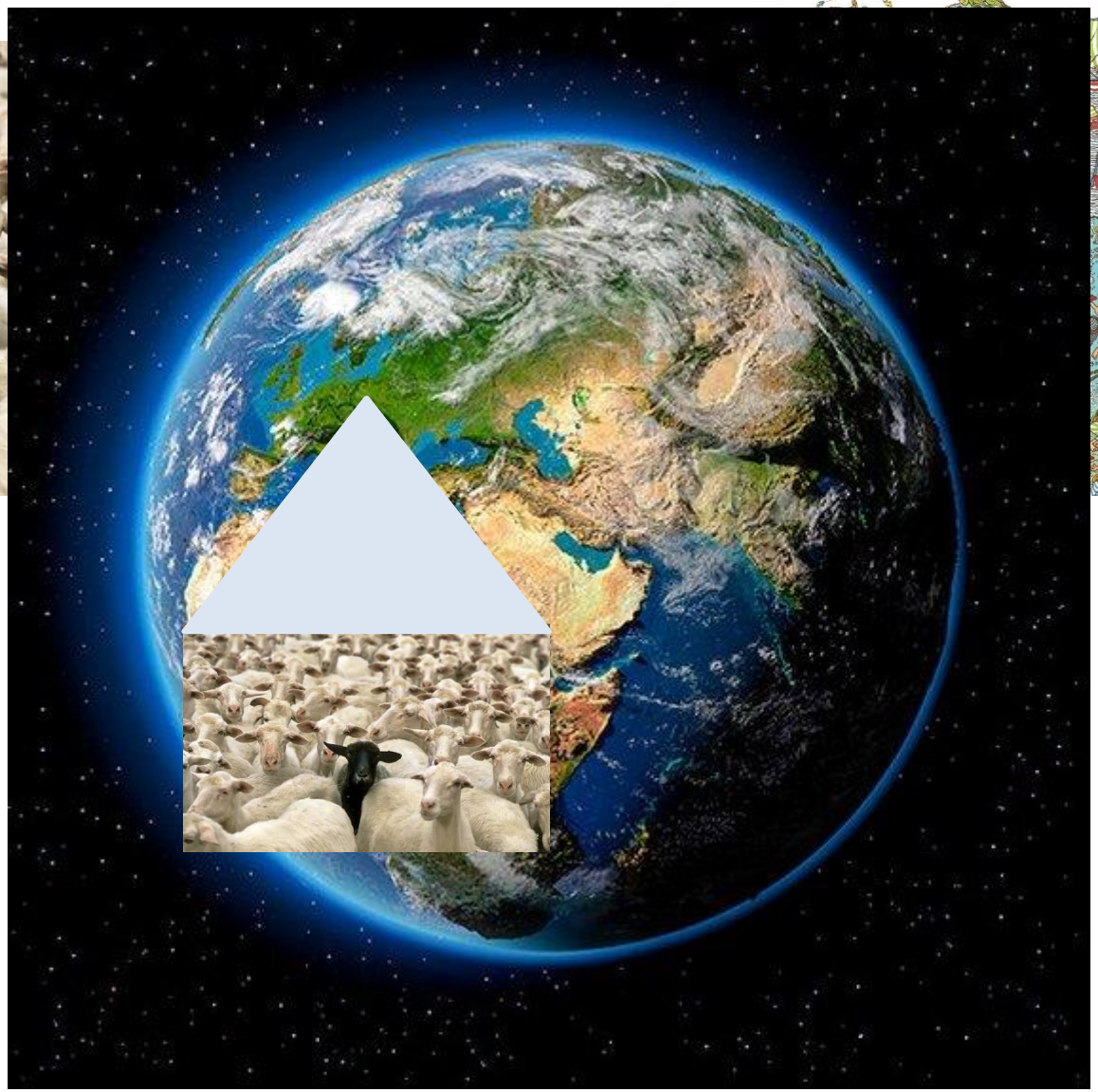
Tamás Holczer
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Holczer@CrySyS.hu

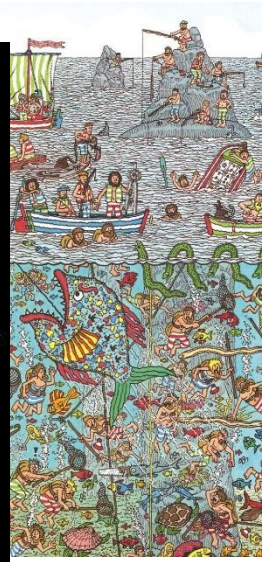
IDS: Definitions

- **intrusion**
  - a security incident (set of events) in which an intruder attempts to gain access to a system (or system resource), or to increase privileges without having authorization to do so
  - often exploit system or software vulnerabilities
  - examples: remote root compromise, web server defacement, password cracking, installing a backdoor, installing a root kit, …

- **intrusion detection**
  - a security service that monitors and analyzes system events for the purpose of detecting intrusions and providing real-time or near real-time warnings

Is it a hard task?





Attacker types

- hackers
  - motivated by becoming famous (in the hacker community, status is determined by level of competence)
  - do not necessary want to cause harm
- criminal organizations
  - objective is to gain financial advantage (e.g., obtaining credit card numbers, phishing e-banking passwords)
  - may have political motivations (penetration into the computer system of foreign governments)
  - have substantial resources and specific target, act quickly and get out
  - may not necessarily divulge that penetration happened
- insider attackers
  - may be motivated by revenge or hired by criminal organizations
  - internal employees have access and system knowledge
  - may have the ability to destroy the evidence of the intrusion
- generally, in network security, it is very important to define the attacker model what we intend to protect against.
- alarm can be raised if one or few attacker steps are detected (false alarms?)
- better if we see the process (see SIEM part of this lecture)

Hacker behavior – an example

Hacking/Cracking is not a single step. It is a process, e.g.:

- select targets using IP lookup tools
- map network for accessible services (collect information)
- identify potentially vulnerable services (analyze situation)
- Use exploits or brute force attacks (e.g. guess passwords) (attack)
- install remote administration tool (backdoor)
- wait for admin to log on and capture password (further attacks)
- use password to access other parts of the network
- control the whole system.

Criminal organization behavior

A criminal organization makes it in a bit different fashion:

- Act quickly and precisely to make their activities harder to detect
- Detailed attack plan
- Identifying vulnerabilities slowly but efficiently
- Attack from multiple sources to avoid identification
- Possibly “employing” internals / ISP staff
- Do not stick around until noticed
- Make few or no mistakes
- Actually use the collected information (e.g. credit cards)

Insider attacker behavior example

- create network accounts for themselves and their friends
- access accounts and applications they wouldn't normally use for their daily jobs
- e-mail former and prospective employers
- visit specific web sites that cater to disgruntled employees
- perform large downloads and file copying
- access the network during off hours.

Motivations for intrusion detection

- need a second (third?) line of defense if attack prevention systems (e.g., firewalls) fail
- IDS/IPS is similar to burglar alarm systems
  - catch intruders before they can do much damage
    - » fast detection of and reaction to intrusions can help to alleviate the effects of the attack
  - intruders may stay out if they think they may be caught
    - » there are much more easier targets around
- firewalls are ineffective against insider attacks (may be a compromised host)
- using an IDS can provide lot of useful information about how intrusions happen → this helps to design more secure systems

“Second line of defense”

- First, server software used to contain access control mechanism (e.g. web server – basic authentication)
- Operating system permissions, access rules are also used

e.g. unix file access permissions

AND role based access control as “second line” defense

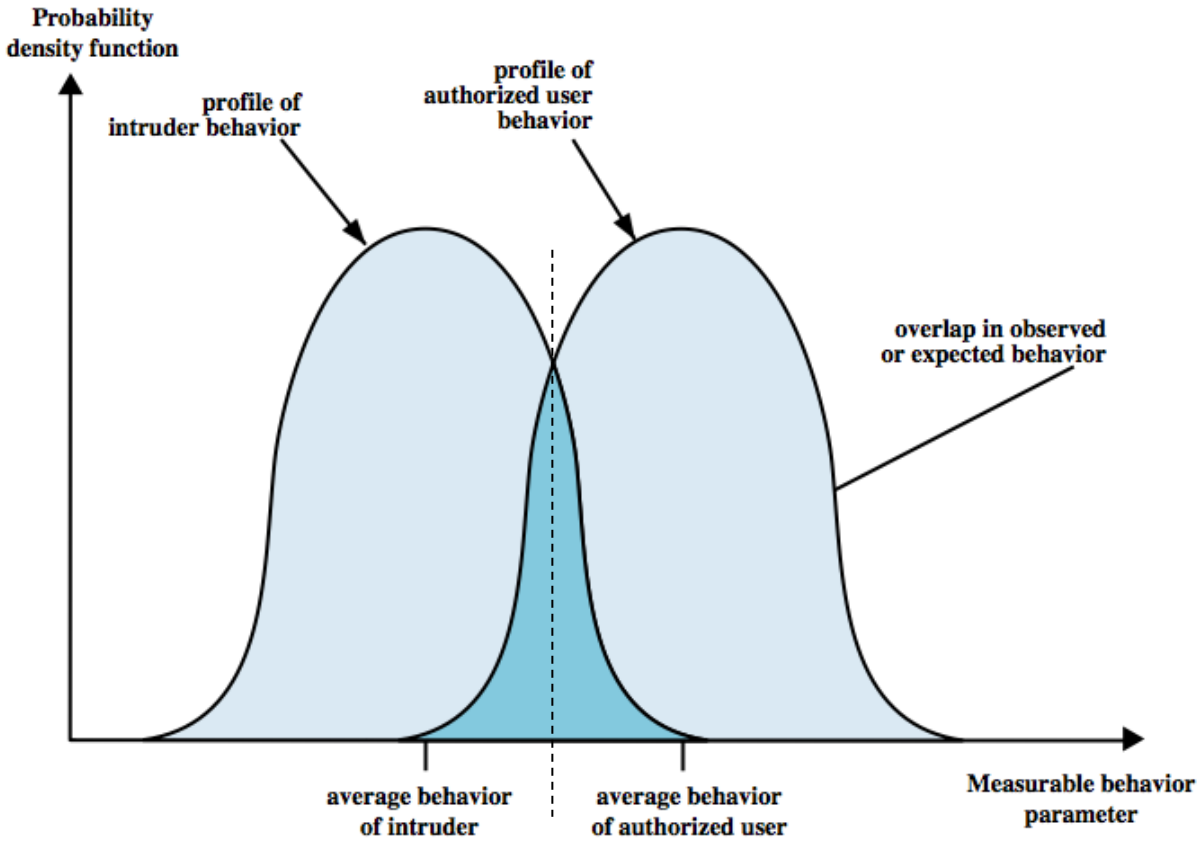
- Firewall and content filtering avoids attacks (e.g. URL exploit prevention)
- Finally, IDS/IPS is used as a “N-th line” defense to at least detect the incident.

- The system protection is a multi-layered approach and each layer should help the others. Some features might overlap, some layers might missing, but altogether security is a system of several components.

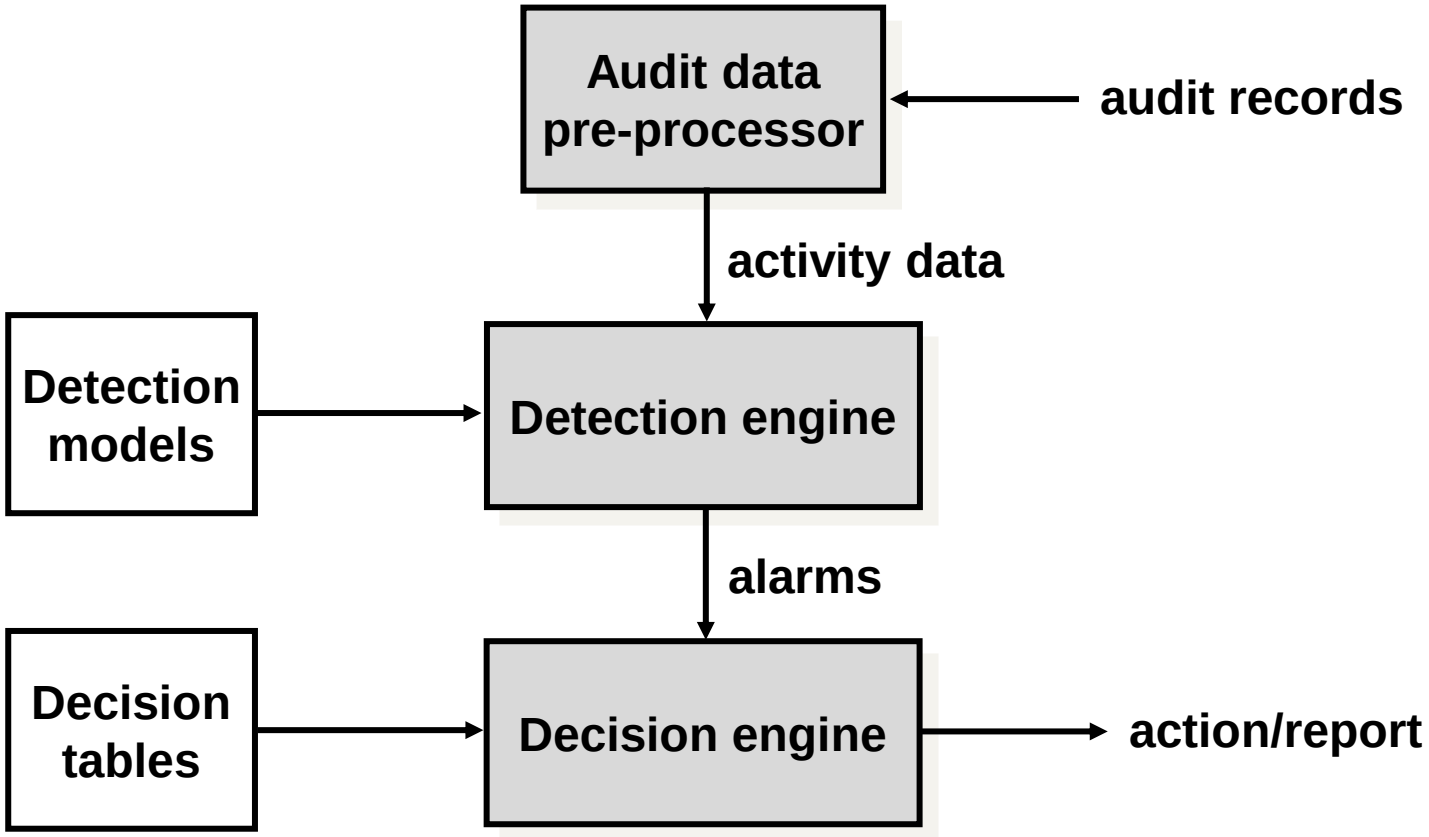
Two basic assumptions of IDS's

1. System activities are observable
2. Normal and abnormal/intrusive activities are distinctive from each other

   - however, expect some overlap
   - problems of false positives and false negatives
   - must find a trade-off



IDS functional architecture



IDS system components

- sensors – collect audit data
- analyzers – process audit data and determine if intrusion has occurred
- user interface – to manage and view the IDS

- components are often organized into a distributed system architecture
  - sensors are deployed at different locations and at different logical layers
  - analyzers collect data from sensors and make local decisions
  - analyzers may cooperate to increase the effectiveness of the detection
  - single console to connect to the other components and configure them

IDS types, detection model

- Signature-based intrusion detection
  - uses a database that contains known attack signatures
  - collected audit data is matched against this database
  - can detect only known attacks
  - efficient
  - useless against unknown attacks
- Anomaly detection
  - maintains a profile of normal system behavior
  - detects deviations from the normal behavior
  - can detect yet unknown attacks, but have a relatively high false positive rate (new normal activities are identified as anomalies)
- Stateful protocol analysis
  - Follow the state of the protocol
  - Allowed next steps and states
  - Can contain reasonableness tests (login name < 20 char)
  - Resource intensive
  - Cannot detect many attacks (e.g. DoS)

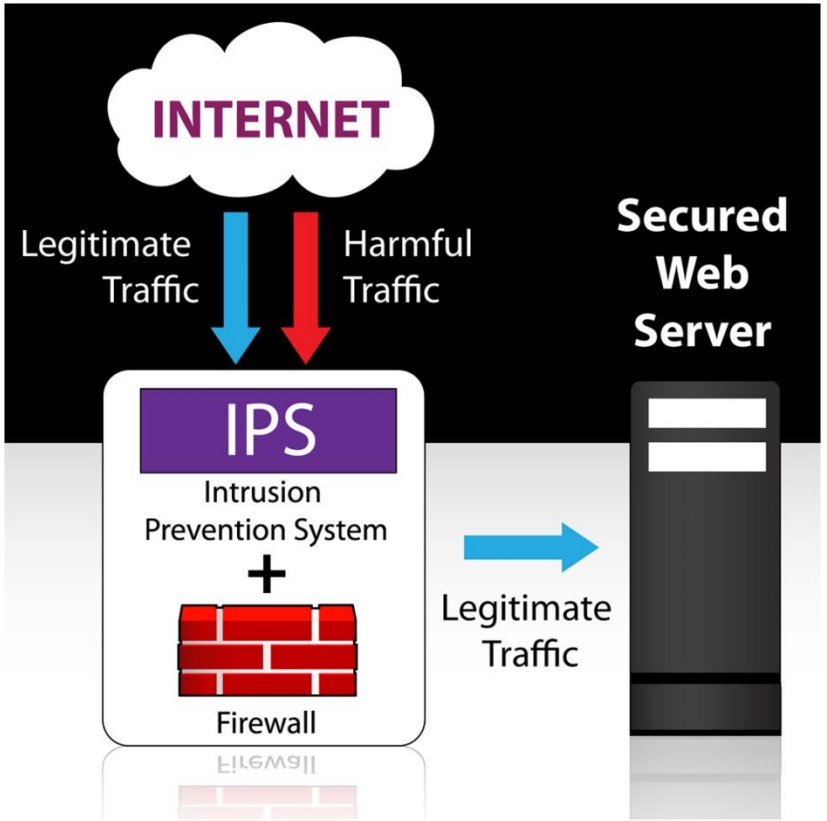
IDS types

Based on detection scope

- host-based IDS
  - detects intrusions that occur on a host
  - uses data from audit logs and system call histories (native OS or special mechanisms)
- network-based IDS
  - not limited to a single host
  - monitors network traffic patterns by using sensors deployed at strategic locations such as routers and switches
  - watches for violations of protocols, unusual patterns, or known intrusive patterns
  - looks into payload of packets for malicious commands and contents

IDS vs IPS

- IPS = Intrusion Prevention System
- Inline appliance
- Can stop the traffic immediately
- Can be a bottleneck
- Can be a single point of failure



- Hardware types
  - PC based (also IDS)
  - Appliance based
    - » Router/switch integrated
    - » Sec appliance (e.g.: ASA)
    - » IPS appliance (e.g.: IPS 4270)

Audit data

- audit data generally comes in several different formats, depending on the tools used to collect it
- the format, granularity, completeness, and source of data all affects the kinds of intrusions which can be detected
- IDS data can be collected at many levels and with many tools
  - some system tools log audit data (login, su)
  - use “sniffers” to observe data “externally” (network probes, filters on commands such as tcp wrappers)
  - add auditing to applications – Web logs, proxy firewall logs

Honeypot

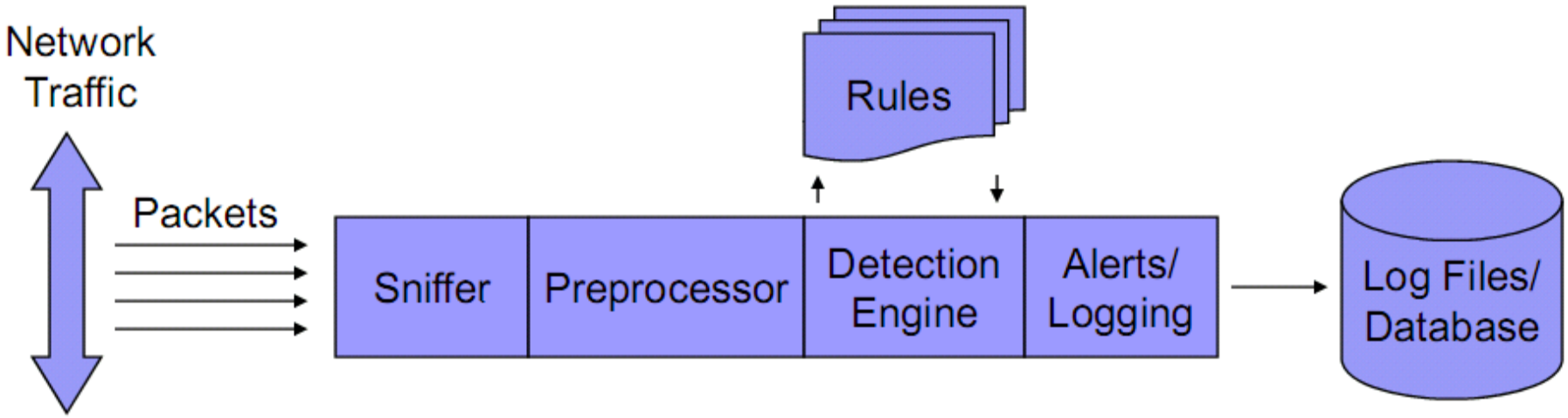
- decoy systems
  - filled with fabricated info
  - instrumented with monitors / event loggers
- divert and hold attacker to collect activity info without exposing production systems
- initially were single systems (e.g. a fake server)
- more recently entire networks are emulated
- Basic example: non-interactive honeypot: Only basic functions are emulated, e.g. first-step protocol answers
- Highly Interactive honeypot: Almost a real computer, attacker can gain shell access, etc.
  - Harder to manage
  - Might mean security risk

IDS Summary

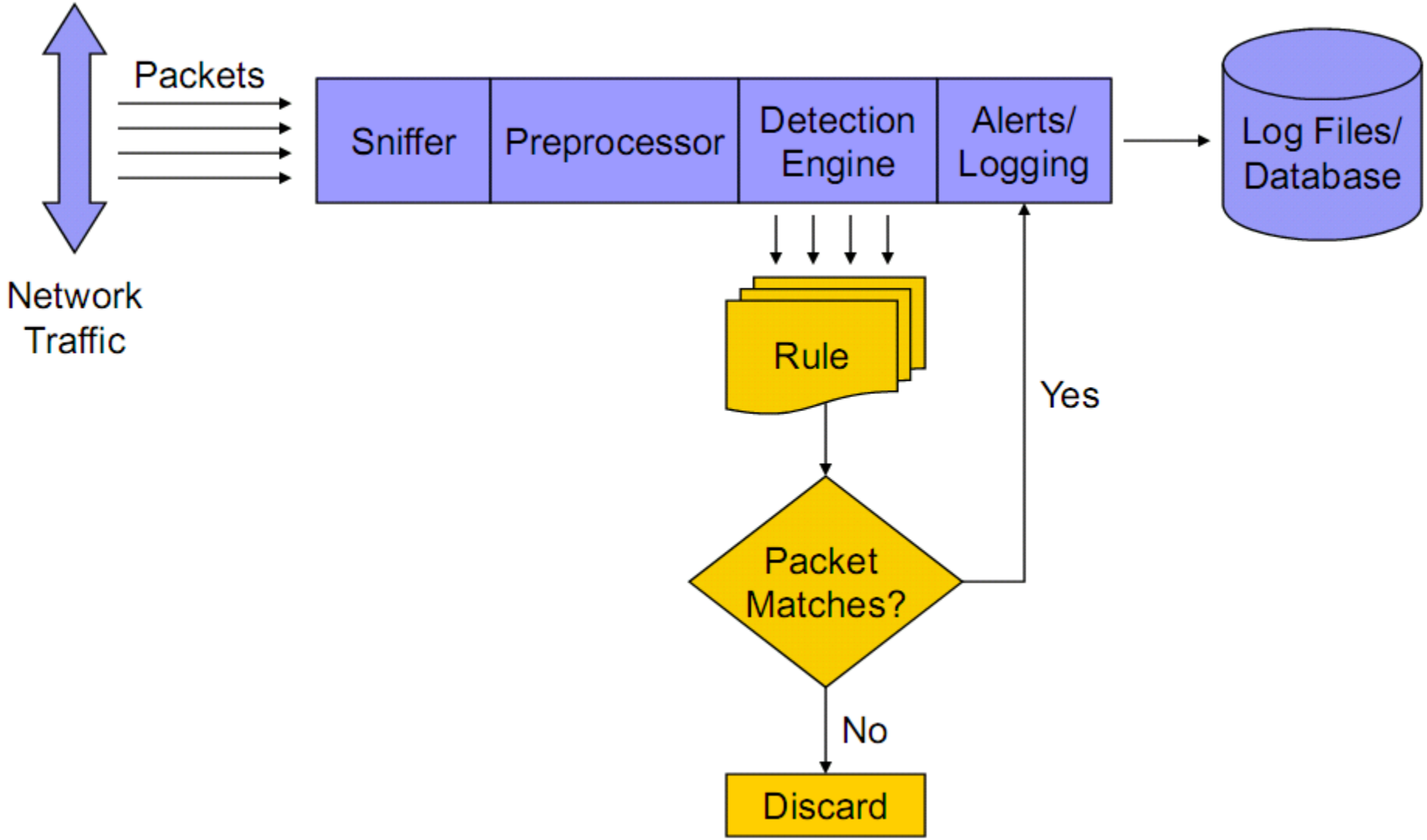
- IDS has potential to catch intruders of your system
- serves as a second line of defense, and acts when other preventive systems have failed
- can be used when really concerned about internal users doing things they shouldn't
- Instant countermeasure is possible
  - e.g., turn off certain ports or ban users from access
- high false positive rates (configure!)
- many useless results (configure!)

Snort basic structure

- Sniffer
- Preprocessor
- Detection Engine
- Alerts and Logging



Snort detection engine



Snort rules

- A simple rule

alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mountd access";)

- Conficker B botnet:

```
alert tcp any any -> $HOME_NET 445 (msg: "conficker.b shellcode"; content:
   "|e8 ff ff ff ff c2|_|8d|O|10 80|1|c4|Af|81|9MSu|f5|8|ae c6 9d a0|O|85
   ea|O|84 c8|O|84 d8|O|c4|O|9c cc|Ise|c4 c4 c4|,|ed c4 c4 c4
   94|&<O8|92|\;|d3|WG|02 c3|,|dc c4 c4 c4 f7 16 96 96|O|08 a2 03 c5 bc ea
   95|\;|b3 c0 96 96 95 92 96|\;|f3|\;|24 |i|95 92|QO|8f f8|O|88 cf bc c7 0f
   f7|2I|d0|w|c7 95 e4|O|d6 c7 17 cb c4 04 cb|{|04 05 04 c3 f6 c6 86|D|fe c4
   b1|1|ff 01 b0 c2 82 ff b5 dc b6 1f|O|95 e0 c7 17 cb|s|d0 b6|O|85 d8 c7
   07|O|c0|T|c7 07 9a 9d 07 a4|fN|b2 e2|Dh|0c b1 b6 a8 a9 ab aa c4|]|e7 99 1d
   ac b0 b0 b4 fe eb eb|"; sid: 2000002; rev: 1;)
```

(mixed binary and ASCII text, simple content matching)

- Regular expressions (PCRE) and other tricks can be used to write efficient and robust rules

- Hard to read/write/understand rules
- Different sources/categories for rules

Cisco IDS

- Signature types
  - Pattern-based detection
  - Anomaly-based detection
  - Policy-based detection
  - Honeypot-based detection

- Anomaly-based
  - learning phase
  - Specific pattern
- Policy
  - Similar to anomaly-based
  - traffic behaviour

- Honeypot: rarely used, mainly by AV vendors and other professionals

Cisco IDS

- Decision:
  - Generate an alert.
  - Log the activity.
  - Drop or prevent the activity.
  - Reset a TCP connection.
  - Block future activity.
  - Allow the activity.

- IPS Global Correlation
  - Real-time update (can be turned off)
  - Automatic information sharing (can be turned off)
    - » Signature ID, Attacker IP address, Attacker port, Maximum segment size, Victim IP address, Victim port, Signature version, TCP options string, Reputation score, Risk rating
  - Mainly based on the reputation of IP addresses

IPS Example

Part of honeypot log:

1420076145, 202.162.197.22X, 1, socknum=7

1420076146, 202.162.197.22X, 8, socknum=7, url=tmUnblock.cgi

1420076146, 202.162.197.22X, 11, socknum=7, error=404

1420076146, 0.0.0.0, 10, socknum=7, requestserved=0

1420232610, 89.46.101.14Y, 1, socknum=7

1420232610, 89.46.101.14Y, 8, socknum=7, url=/phpMyAdmin/scripts/setup.php

1420232610, 89.46.101.14Y, 11, socknum=7, error=404

1420232610, 0.0.0.0, 10, socknum=7, requestserved=0

What to search for (rule):

- *.cgi
- *.php

What to block temporarily (ip):

- 202.162.197.22X
- 89.46.101.14Y
- Timeframe of block?

IDS Summary

Some end notes:

- Useful, but not ultimate solution
- Cannot check encrypted traffic (network based)
- Never enable all signatures
- Check CPU and memory usage
- Update rules regularly
- Disable unused modules
- Enable log and alarm
- Store logs for at least a few days
- CHECK logs/alerts regularly
- Use correlation engine

SIEM systems

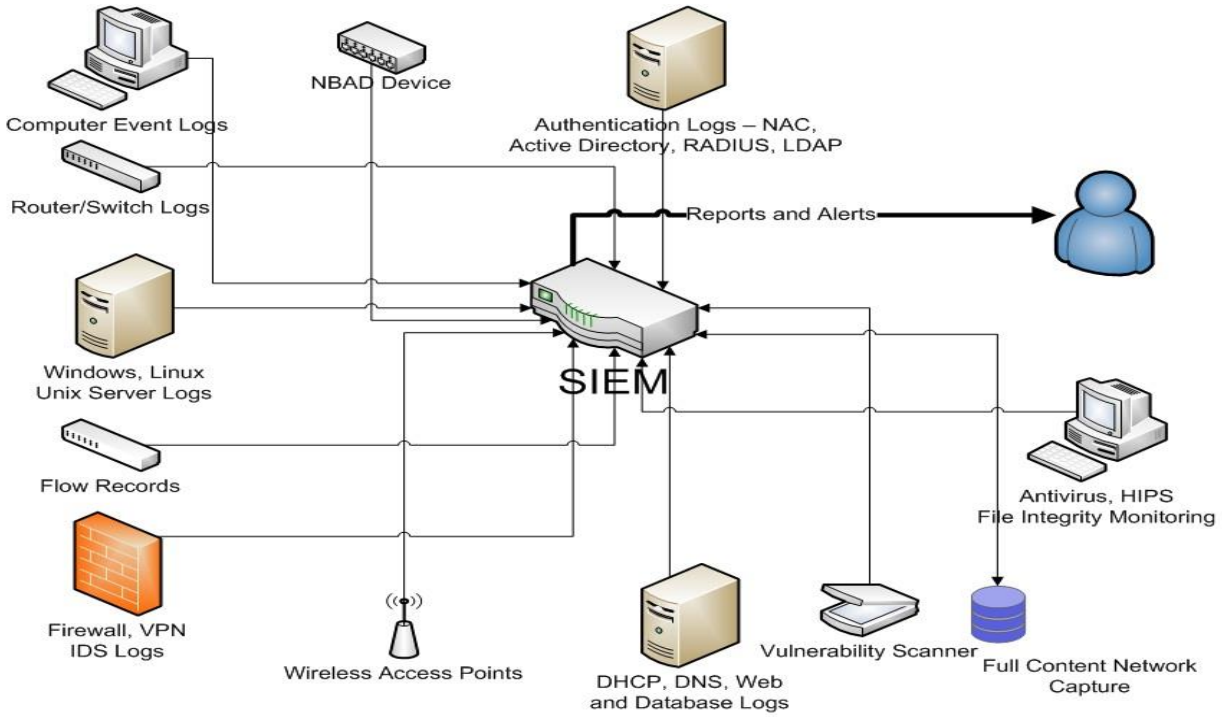
- Problem: extremely lot of logs from several sources
- Event logs are very useful but too many generated
- When to alert the sysadmin?
- Big data problems and solutions
- Correlation between events can be analyzed
- False positives can be largely eliminated

SIEM, Main tasks

- Log consolidation, Log management
- Log normalization
  - When, Who, What, Where, On What, Where from, Where to
- Correlation
  - Statistical approaches
  - Machine learning approaches
- Incident Management
  - Who to alert, what to alert
- Reporting
  - Regular not reported events
- Asset management
  - Know your network

SIEM, What to collect?

- Collect all data, everything is important:
  - From workstations
  - From database servers
  - From webservers
  - From email servers
  - From IPS
  - From IDS
  - From antivirus
  - From firewall
  - From fileserver
  - Wireless access log
  - NAS log
  - VPN log
  - SAP logs
  - …



SIEM, Information (data) collection

- Scalable
- Wide device support
- Robust
- Core system remains intact, SIEM accomodates
- Wide protocol support:
  - Syslog, syslog-ng, SNMP, Windows event logging API, FTP, SCP, ODBC, SDEE…

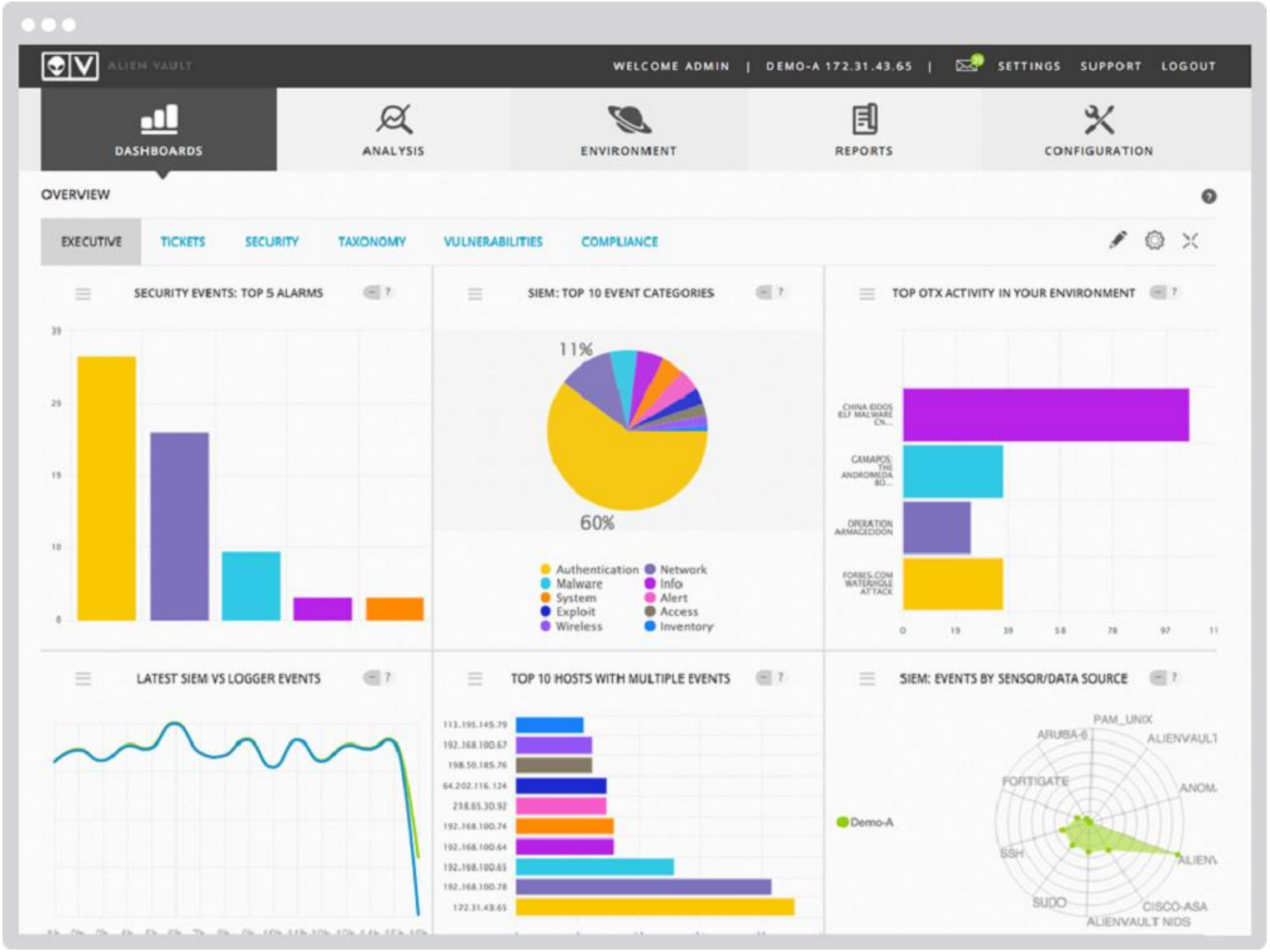
- SIEM makes information from the data

SIEM, Analysis

- Must be in REAL time
- Anomaly based correlation:
  - Automatically computes baseline
  - Baseline for fast and slow patterns
  - Variations from baseline is detected
- Rule based correlation
  - Violations of corporate policy
- Easy to use real time GUI for alerts

- Alert severity automatically computed
- Ranking of alerts to focus on criticals
- Events are classified

SIEM Dashboard



Why correlate

Log Correlation is the difference between:

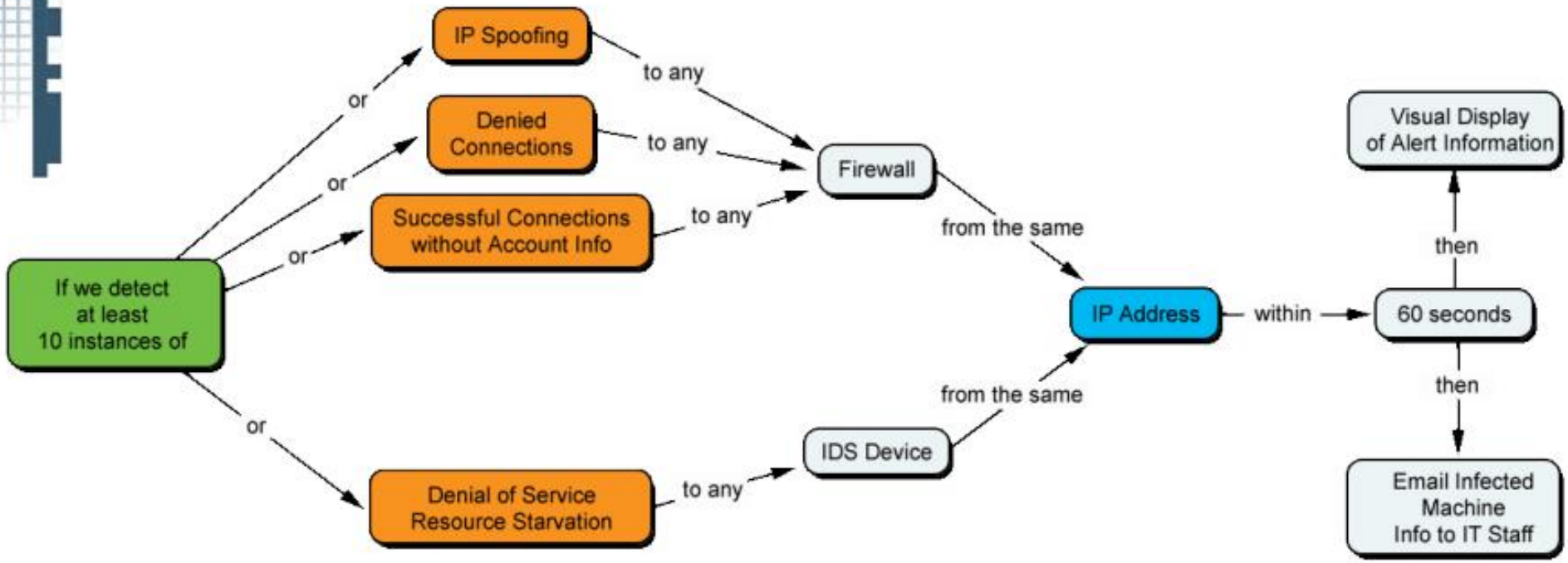
"14:10 7/4/20110 User BRoberts Successful Auth to 10.100.52.105 from 10.10.8.22"

From alienvault.com

Correlation example

Correlation Rule Name: W32.Blaster Worm

The goal of this rule is to detect Blaster worm variants as well as other malicious code by analyzing network traffic patterns.



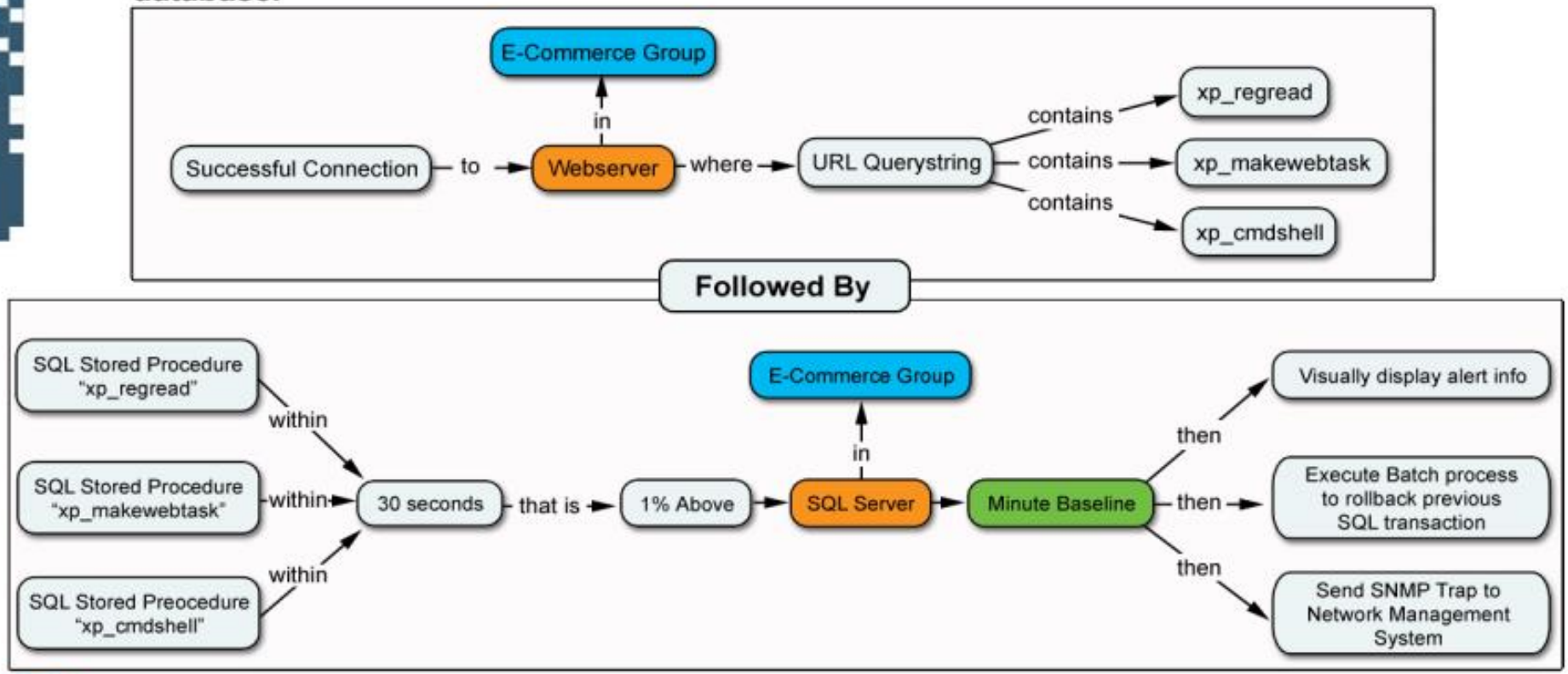
Network Intelligence CORPORATION

From: Network Intelligence Corporation

Correlation example

Correlation Rule Name: SQL Injection Attack

The goal of this rule is to detect information theft from E-Commerce websites through the exploitation of the trusted connection between the web server and the database.



Network Intelligence CORPORATION

14

From: Network Intelligence Corporation

How to buy a SIEM

- Support for your sources (customization?)
- Integration with existing tools (e.g. malware analysis)
- Support for your company size
- In house expertise (courses?)
- Stability
- Support
- Price

https://community.softwaregrp.com/dcvta86296/attachments/dcvta86296/arcsight-discussions/1580/1/InfoSec%20SIEM%20Comparison.pdf

SIEM, Best practices, final thoughts

- Do not filter data at source
- Determine reporting periods
- Archive all data before purging from SIEM
- Synchronise time
- Logs can contain sensitive information (e.g. passwords), secure the system
- Send alert only when it is important
- Fine-tune rule based correlation
- Test your logging system

- Configure your SIEM to your needs
- Check the output of your SIEM (read email, check dashboard etc.)

SOC: Security Operations Center

- Technology
- Processes
  - What to do if
  - Prepared guides with conditions
- People
  - Training
  - Tier 1: Triage, filtering
  - Tier 2: Investigation
  - Tier 3: Threat hunting
- Inhouse vs outsourced solutions
- Goal: prevention, detection, analysis and response to security incidents

Some products

- Commercial SIEM Solutions
  - HP ArcSight (www.arcsight.com)
  - IBM Q1Labs Qradar (www.q1labs.com)
  - RSA Envision (www.rsa.com)
  - …
- Lower Cost/Free Log Search
  - Q1Labs FE (www.q1labs.com)
  - OSSEC (www.ossec.net)
  - Splunk (www.splunk.com)
  - Ossim (www.alienvault.com)
  - …

Control questions

- What is the goal of an IDS?
- What are the main IDS types/detection models?
- What can be a source for an IDS/IPS/SIEM?
- What is the difference between an IDS and an IPS?
- In what problem a SIEM can help us?