Security and Trust in Distributed Systems

Master Degree in New Technologies in Computer Science

2022/23

Security Information and Event Management (SIEM)

Antonio Ruiz Martínez, Pantaleone Nespoli,
Félix Gómez Mármol

UNIVERSIDAD DE MURCIA

Outline

Part I

- Motivation
- What's a SIEM?
- What for?
- SIEM Architecture
- SIEMs Comparison

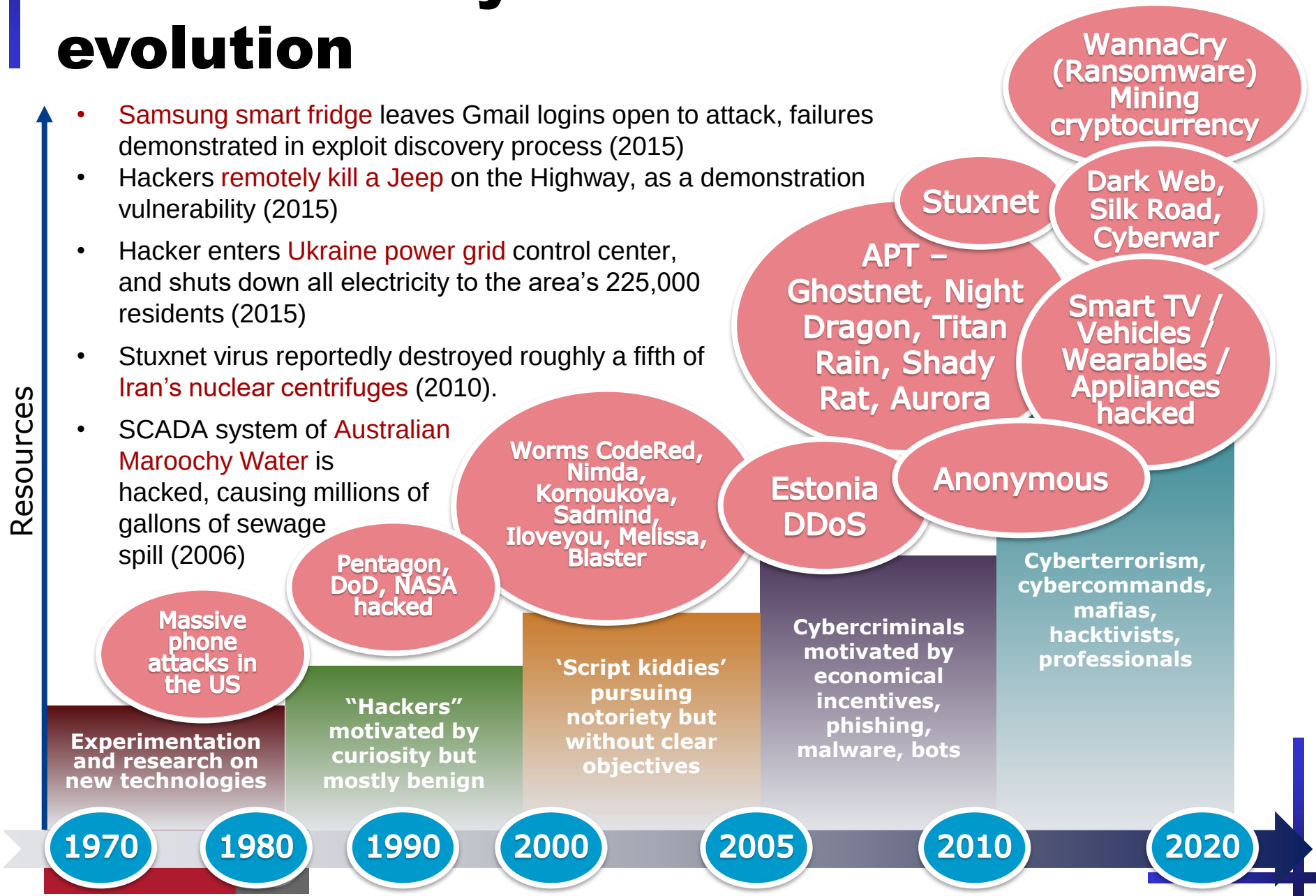
Part II

- OSSIM
  - Installation
  - Configuration
  - Operation

Motivation

Motivation: cyberattacks evolution

- Samsung smart fridge leaves Gmail logins open to attack, failures demonstrated in exploit discovery process (2015)
- Hackers remotely kill a Jeep on the Highway, as a demonstration vulnerability (2015)
- Hacker enters Ukraine power grid control center, and shuts down all electricity to the area's 225,000 residents (2015)
- Stuxnet virus reportedly destroyed roughly a fifth of Iran's nuclear centrifuges (2010).
- SCADA system of Australian Maroochy Water is hacked, causing millions of gallons of sewage spill (2006)

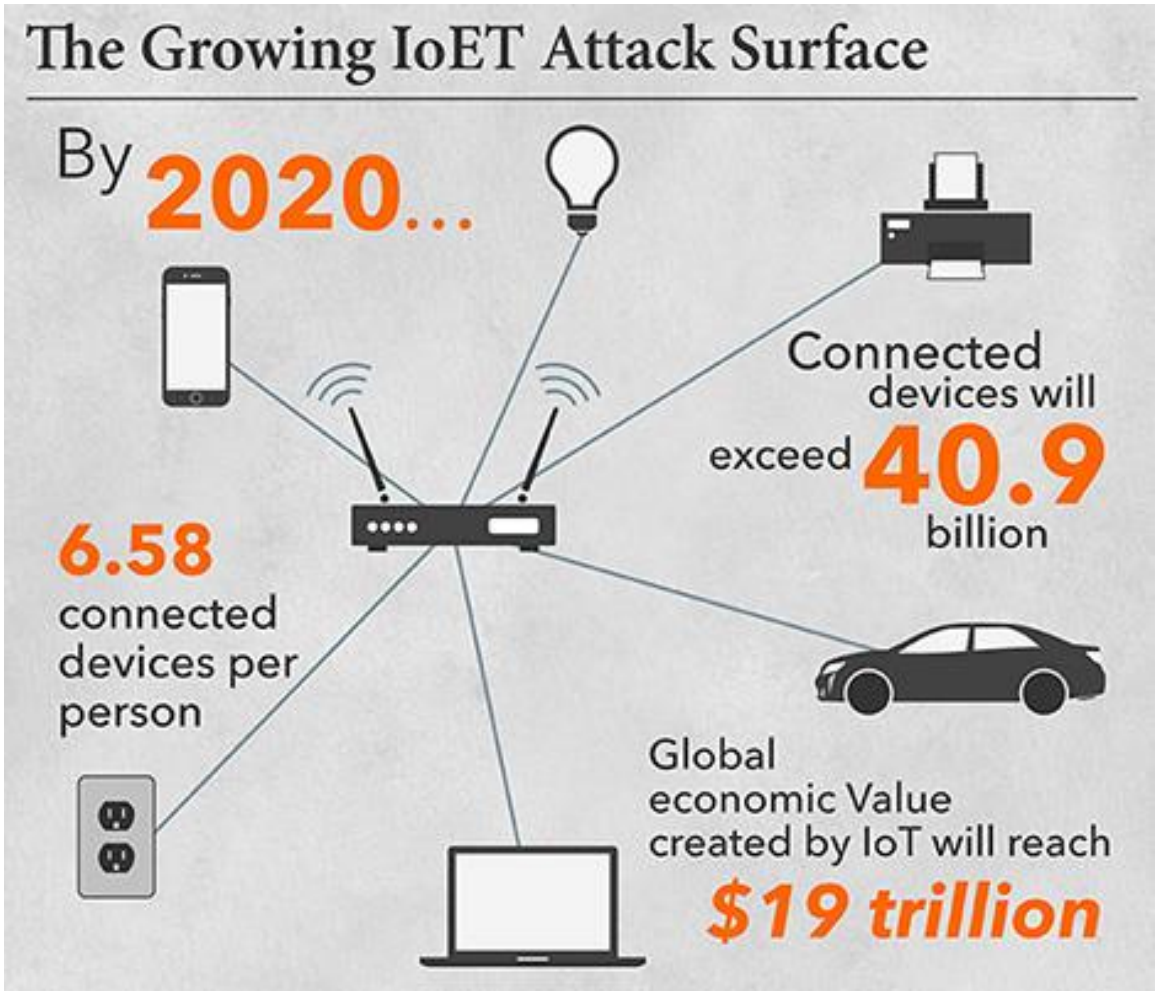


Motivation: Continuously under attack

Motivation: Continuously under attack

Motivation: Continuously under attack

Motivation: Heterogeneity and big data



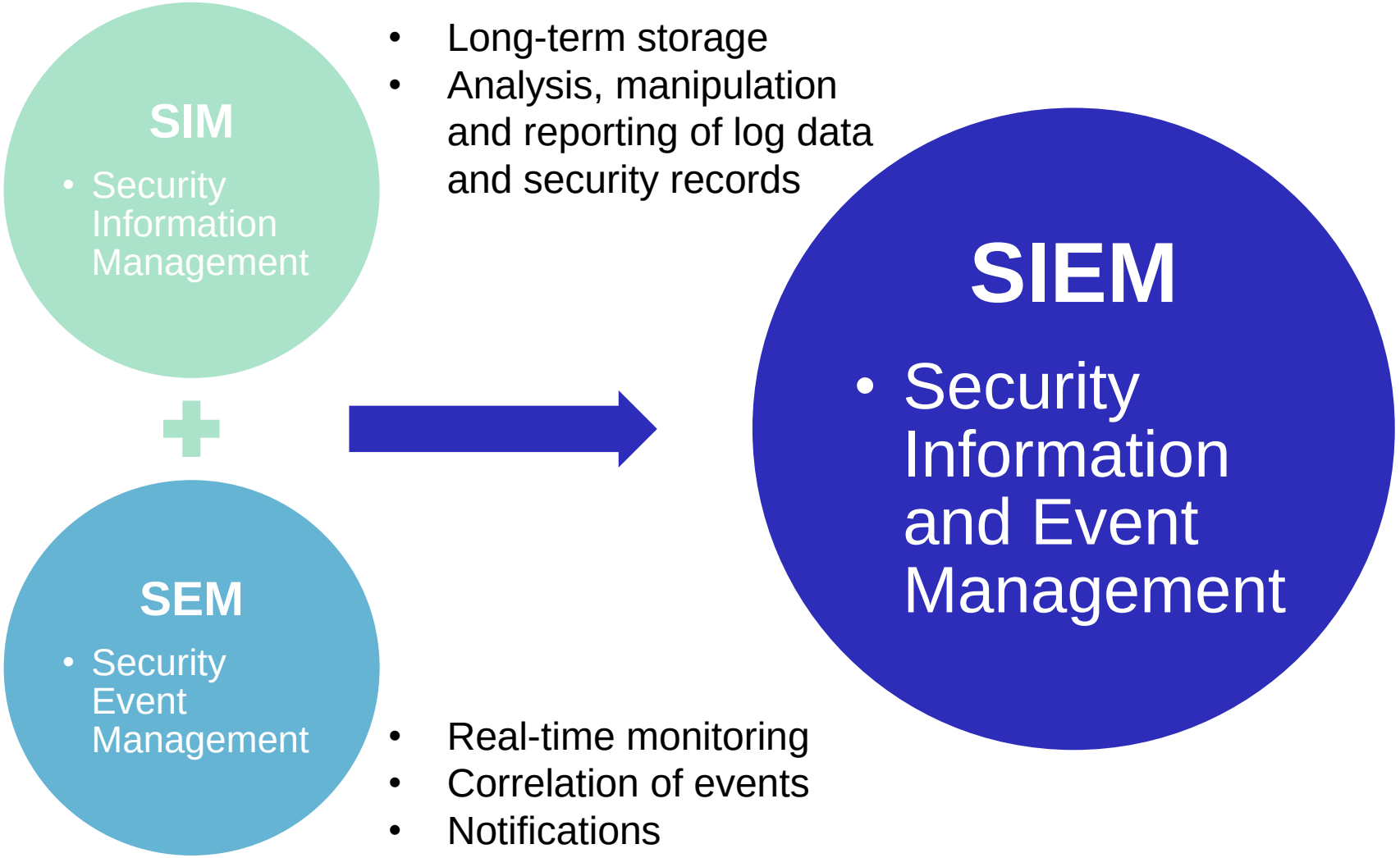
Motivation: Summary

- Need to face and defend against sophisticated attacks
  - Advanced Persistent Threats (APT)
  - Cyber criminals, cyber terrorists, but also script kiddies
- Need for a real-time (or near real-time) response
  - Not feasible for a human administrator to react in real-time to complex attacks
- Need to handle, process and analyse massive amounts of information
  - Not feasible for a human administrator to digest vast amounts of information in a timely manner

- We need SIEM!!

What's a SIEM?

What's a SIEM?



UNIVERSIDAD DE MURCIA

What's a SIEM? Features

Technology supporting threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources

- **Event and Log collection**
  - In real-time from a wide variety of contextual data sources
- **Layered Centric Views** or Heterogeneous
  - In the form of dashboards or "views"

What's a SIEM? Features

- **Normalization**
  - Translating computerized jargon to readable data to be displayed, and mapping data to user- or vendor-defined classifications
- **Correlation**
  - Creation of relationships based on rules, architecture and alerts either historical or real-time
- **Adaptability** (Scalable)
  - Ability to speak the language regardless of source vendor, format, type, change or compliance requirement
- **Reporting and Alerting**
  - Automated verification of continuous monitoring, trends and auditing
- **Log Management**
  - Storing events and logs into a central location

What's a SIEM? Benefits

- Increased awareness over the monitored system
- Quick detection and identification of security events
- Effective and efficient prevention of security breaches
- Reduction of the impact of security events
- Enhanced reporting and alerting
- Log collection, analysis and retention
- IT compliance with business policies, business models and regulation
- Economic costs reduction

What for?

From security event to security incident

- According to NIST, a security event is defined as "*an identifiable occurrence that could theoretically be relevant to information security*"
  - E.g., a spam e-mail
- Whereas a security incident is defined as "*an event that is a viable risk or that causes damage such as lost data or operational disruptions*"
  - E.g., clicking a link within a spam e-mail

- A SIEM system helps the sysadmins to spot security events amid tones of normal events and to know when to escalate them into security incidents

From security event to security incident: Vulnerabilities

- A vulnerability is defined as a flaw in code or design that creates a potential point of security compromise for an endpoint or network
- Vulnerabilities create possible attack vectors, or paths through which an intruder can gain access to a computer to deliver a payload or malicious outcome
- A payload is defined as the eventual effect of a malware within a computer
- Malicious software, or malware, refers to a variety of forms of harmful or intrusive software
- The attack surface of a system is built upon the collection of all its possible attack vectors
- A successful vulnerability exploitation entails a cyberattack

From security event to security incident: Vulnerabilities

- CVE (Common Vulnerabilities and Exposures) is a publicly available repository of vulnerabilities
- It has become the de facto standard to report new discovered vulnerabilities and to gather existing ones
- Format
  - `CVE-YYYY-NNNN`, where `YYYY` refers to the year when the vulnerability was released and `NNNN` is a sequential counter
  - E.g., `CVE-2017-0144`, was one of the vulnerabilities exploited by the ransomware WannaCry
  - https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
- Maintained by Mitre
  - http://cve.mitre.org

From security event to security incident: Vulnerabilities

- NVD (National Vulnerability Database) is a publicly available repository of of standards-based vulnerability management data
- Uses the Security Content Automation Protocol (SCAP), composed by
  - Common Vulnerabilities and Exposures (CVE)
  - Common Configuration Enumeration (CCE)
  - Common Platform Enumeration (CPE)
  - Common Weakness Enumeration (CWE)
  - Common Vulnerability Scoring System (CVSS)
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Open Vulnerability and Assessment Language (OVAL), and more…
- Maintained by NIST (National Institute of Standards and Technology)
  - https://nvd.nist.gov

From security event to security incident: Vulnerabilities

- CVSS (Common Vulnerability Scoring System)
  - https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- **Base Score Metrics**
  - Exploitability Metrics
    - Attack Vector (AV)
      - Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)
    - Attack Complexity (AC)
      - Low (AC:L) | High (AC:H)
    - Privileges Required (PR)
      - None (PR:N) | Low (PR:L) | High (PR:H)
    - User Interaction (UI)
      - None (UI:N) | Required (UI:R)
    - Scope (S)
      - Unchanged (S:U) | Changed (S:C)
  - Impact Metrics
    - Confidentiality Impact (C)
      - None (C:N) | Low (C:L) | High (C:H)
    - Integrity Impact (I)
      - None (I:N) | Low (I:L) | High (I:H)
    - Availability Impact (A)
      - None (A:N) | Low (A:L) | High (A:H)

From security event to security incident: Vulnerabilities

- CVSS (Common Vulnerability Scoring System) (cont'd)
- **Temporal Score Metrics**
  - Exploitability (E)
    - Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)
  - Remediation Level (RL)
    - Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)
  - Report Confidence (RC)
    - Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

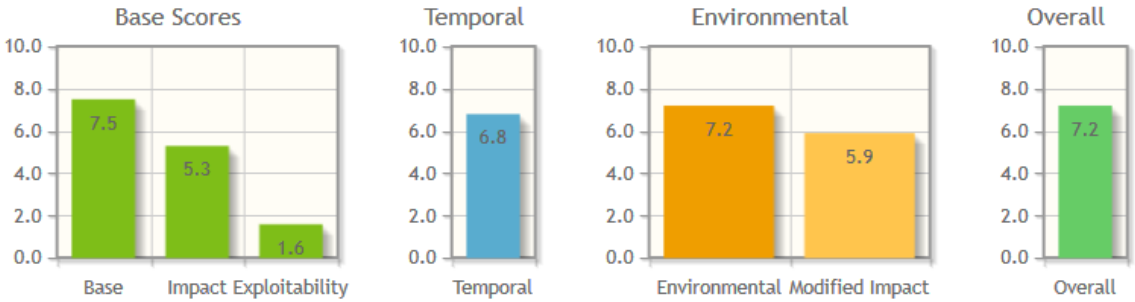
From security event to security incident: Vulnerabilities

- CVSS (Common Vulnerability Scoring System) (cont'd)
- **Environmental Score Metrics**
  - Base Modifiers
    - Attack Vector (MAV)
      - Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)
    - Attack Complexity (MAC)
      - Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)
    - Privileges Required (PR)
      - Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)
    - User Interaction (UI)
      - Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)
    - Scope (S)
      - Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)
  - Impact Metrics
    - Confidentiality Impact (MC)
      - Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)
    - Integrity Impact (MI)
      - Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)
    - Availability Impact (MA)
      - Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)
  - Impact Subscore Modifiers
    - Confidentiality Requirement (CR)
      - Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)
    - Integrity Requirement (IR)
      - Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)
    - Availability Requirement (AR)
      - Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

From security event to security incident: Vulnerabilities

Common Vulnerability Scoring System Calculator Version 3

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 7.5
Impact Subscore: 5.3
Exploitability Subscore: 1.6
CVSS Temporal Score: 6.8
CVSS Environmental Score: 7.2
Modified Impact Subscore: 5.9
Overall CVSS Score: 7.2

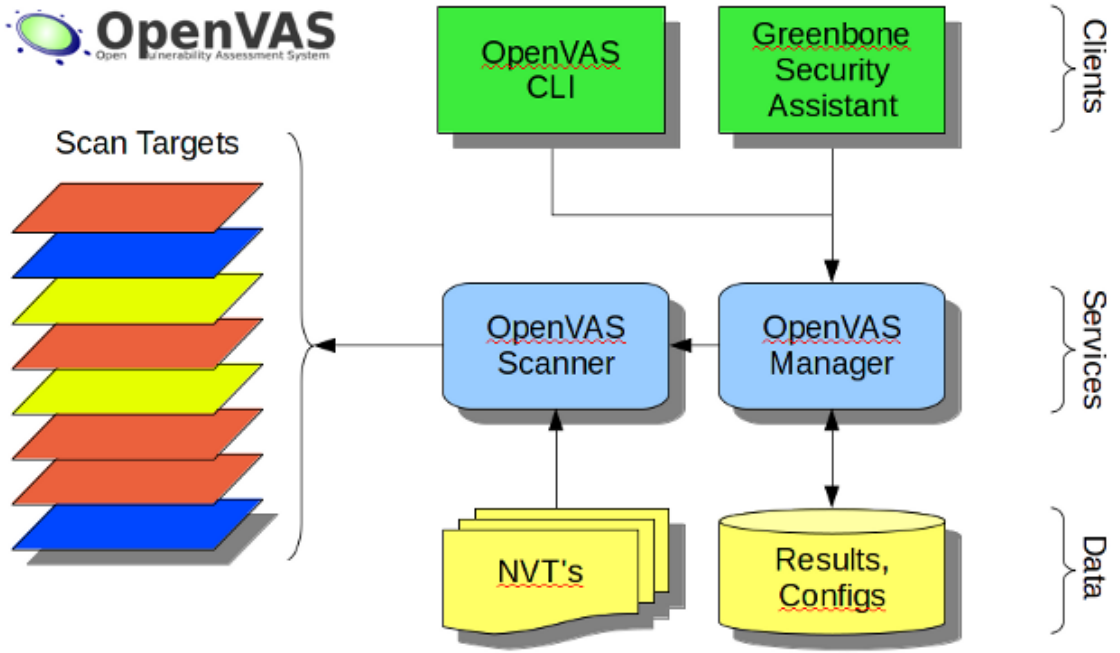
Show Equations

CVSS v3 Vector

AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:L/E:F/RL:T/RC:R/CR:M/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:L/MI:L/MA:H

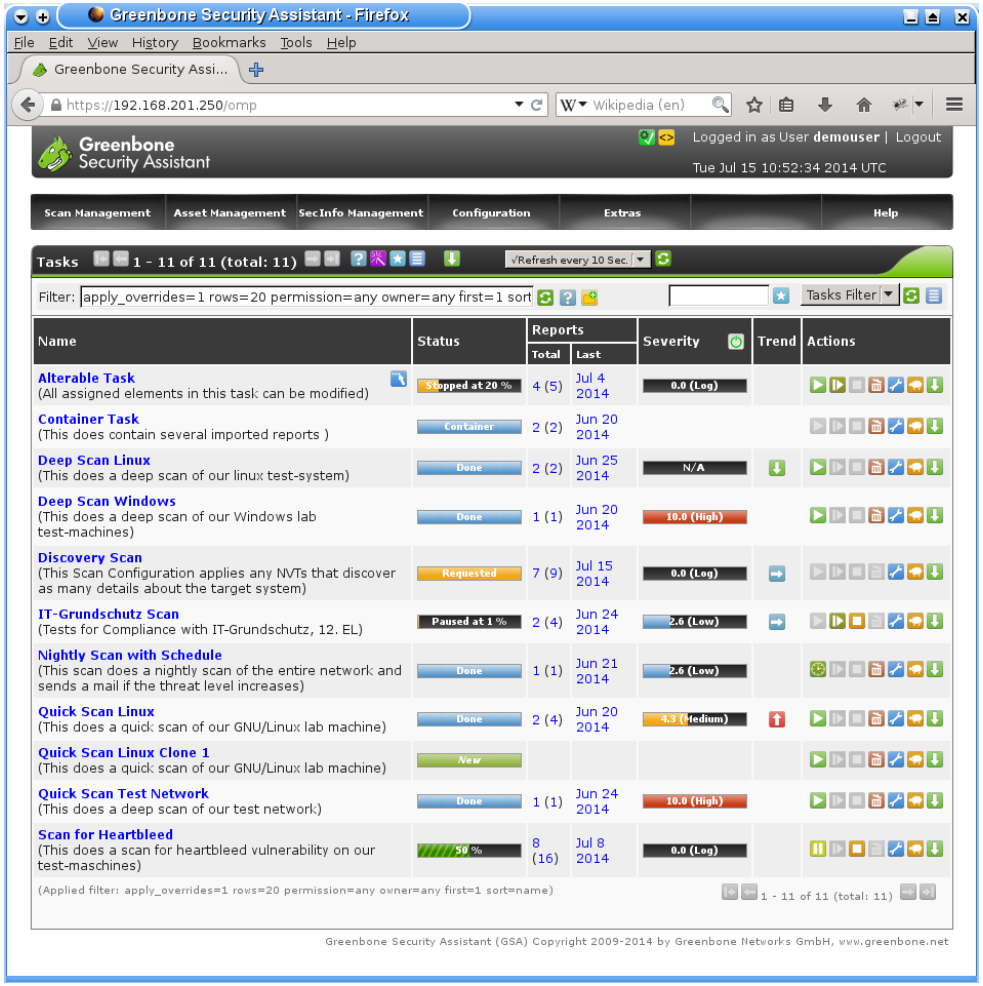
From security event to security incident: Vulnerabilities

- OpenVAS (Open Vulnerability Assessment System)
- Open source vulnerability scanner and manager
  - http://www.openvas.org
- Over 50,000 Network Vulnerability Tests (NVTs)
- Integrated in OSSIM



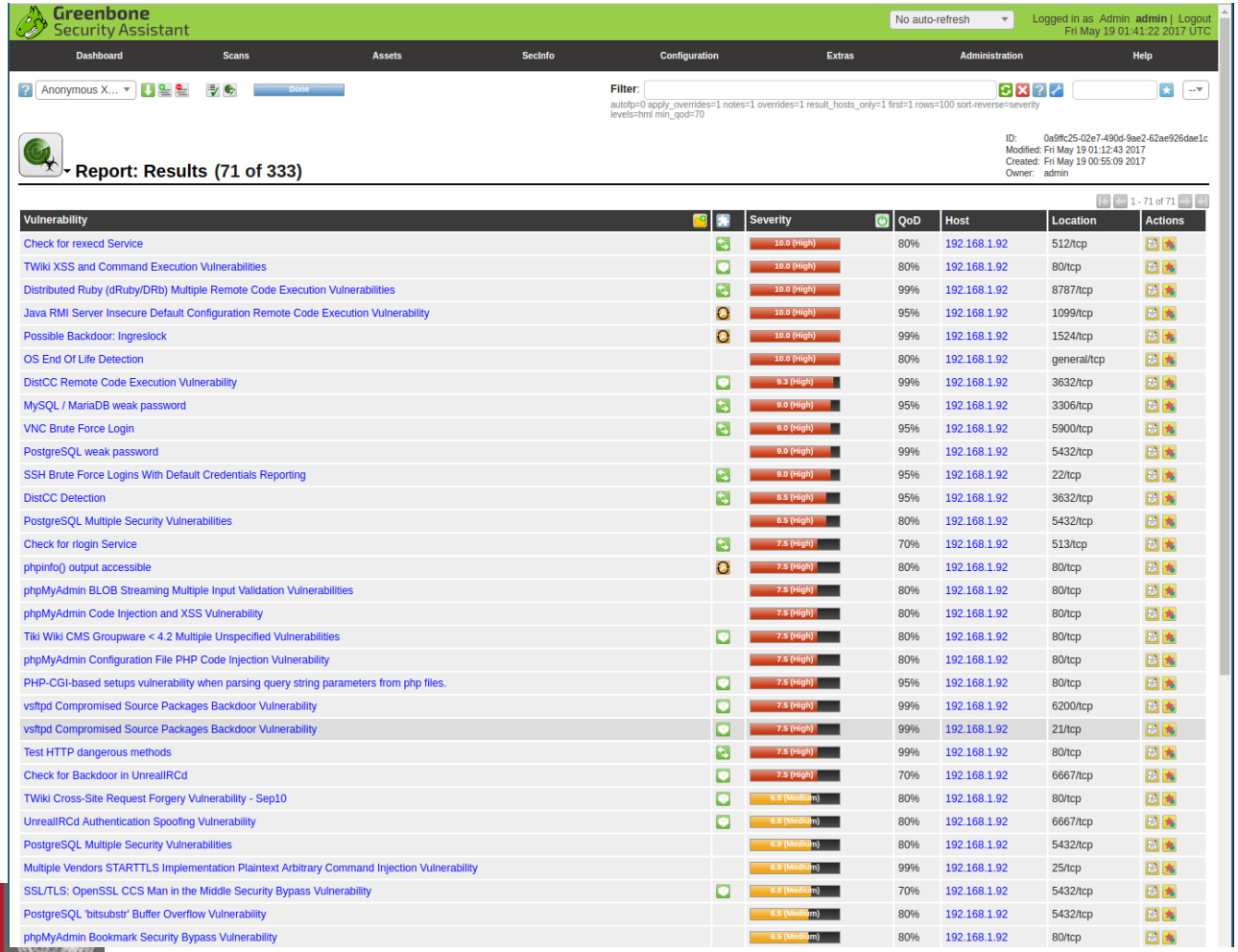
From security event to security incident: Vulnerabilities

- OpenVAS (Open Vulnerability Assessment System)



From security event to security incident: Vulnerabilities

- OpenVAS (Open Vulnerability Assessment System)



From security event to security incident: Cyber Kill Chain

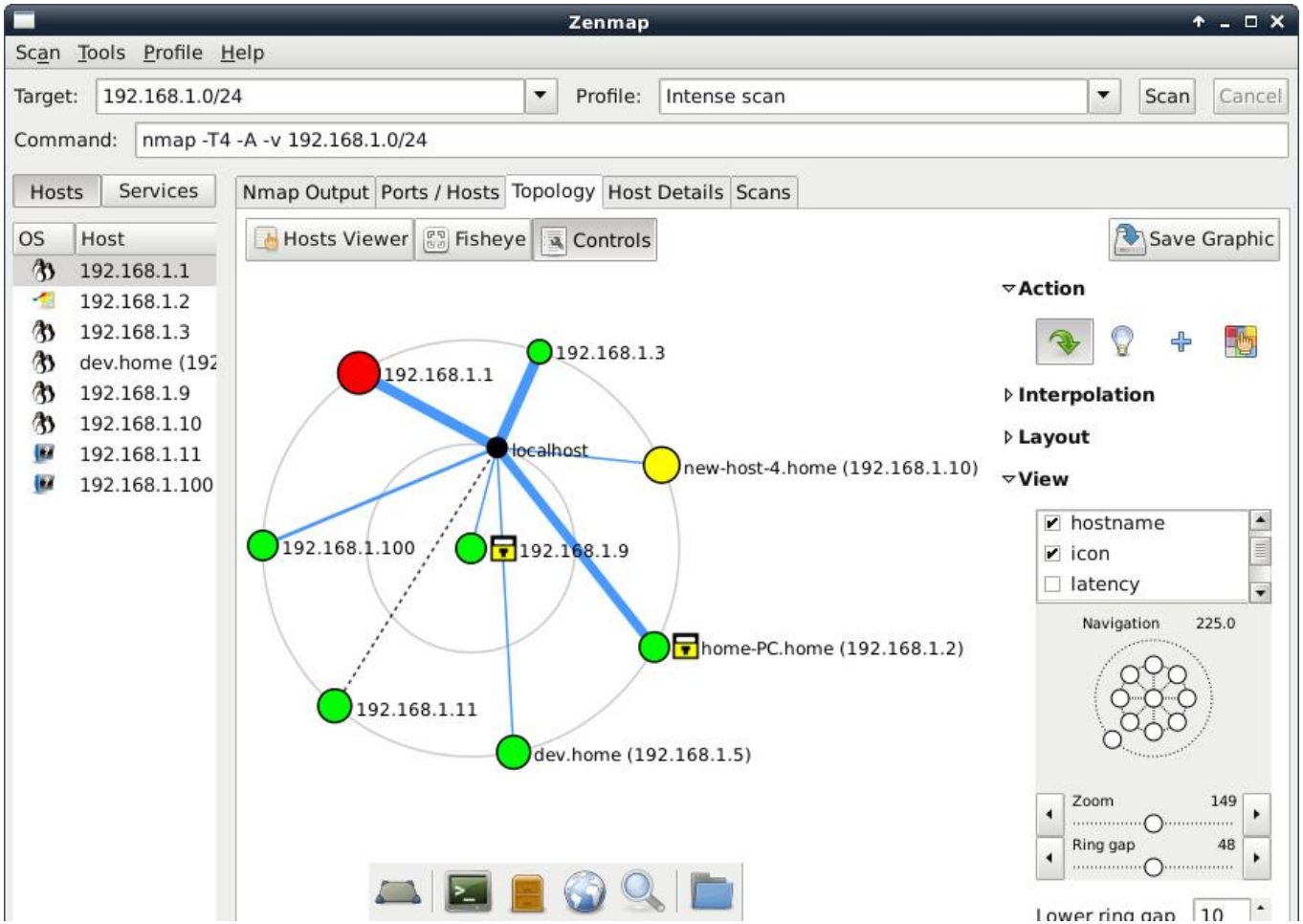
- Models the sequential steps to be conducted in order to achieve a successful cyberattack or advanced persistent threat (APT)
- Helps to identify and prevent cyber intrusions
- Developed by Lockheed-Martin corporation in 2011
  - https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

From security event to security incident: Cyber Kill Chain

- Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network

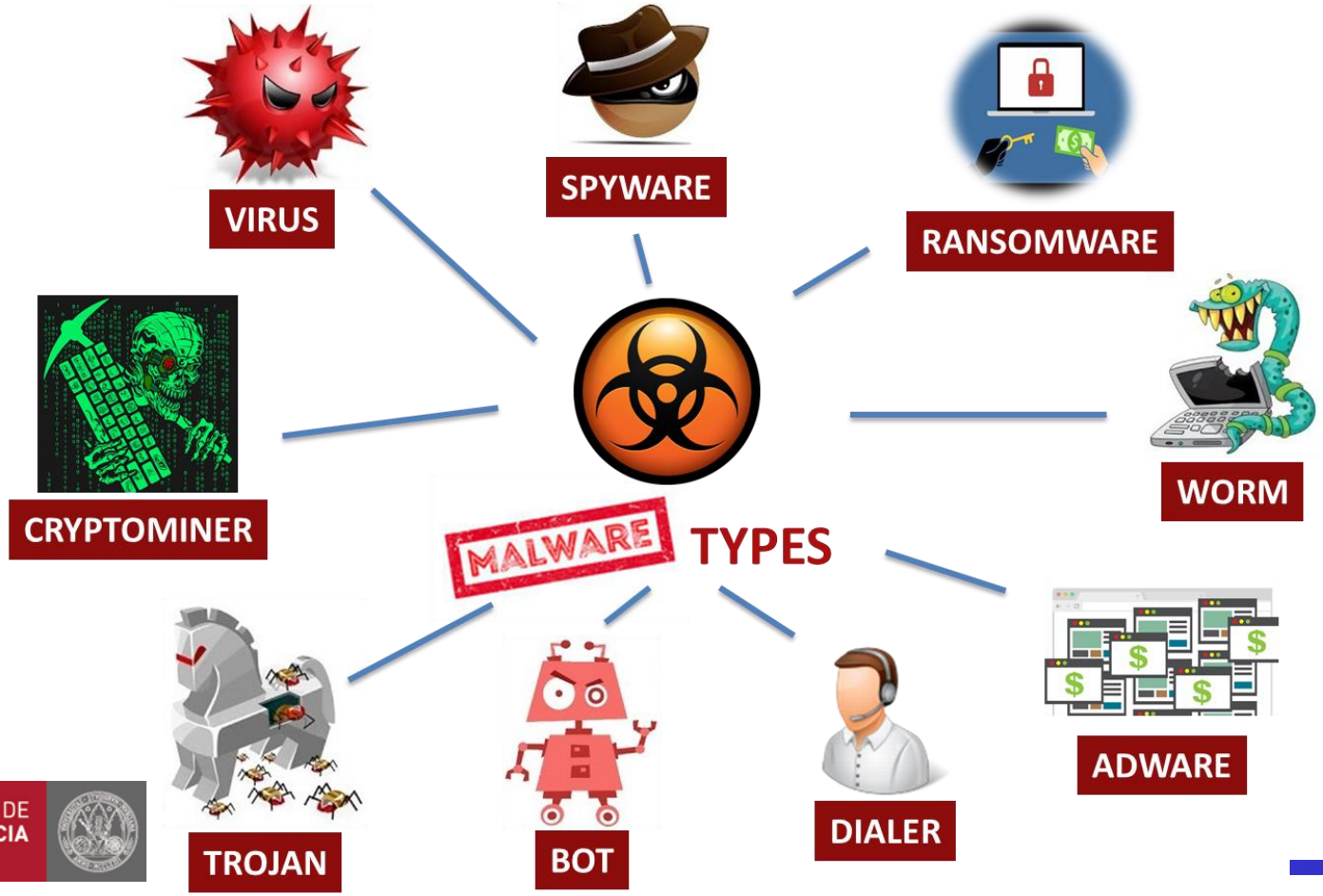
- Footprinting → Building a network map of the victim
  - Scanning IP subnets and systems on those subnets
- Fingerprinting → Identify the nature of a network node within the victim
  - Operating system
  - Open ports
  - Offered services, etc
- Often conducted through automated tools
  - Nmap is a security scanner used to discover hosts and services on a computer network, thus building a network "map“
  - https://nmap.org

From security event to security incident: Cyber Kill Chain



From security event to security incident: Cyber Kill Chain

- Intruder creates remote access malware weapon tailored to one or more vulnerabilities



From security event to security incident: Cyber Kill Chain

VIRUS

- Its main feature is its capacity to replicate itself by infecting other programs or files
- It can also mute (polymorphic) to avoid detection

SPYWARE

- Its main purpose is to gather information (spy) about the victim without their knowledge or consent
  - E.g., keyloggers

From security event to security incident: Cyber Kill Chain

RANSOMWARE

- It threatens to publish the victim's data or perpetually block access to it unless a ransom is paid
- It can lock the system or even encrypt it (totally or partially)
  - E.g., WannaCry

WORM

- Its main feature consists in propagating itself through the network
  - E.g., Conficker, Stuxnet, Blaster, ILOVEYOU

From security event to security incident: Cyber Kill Chain

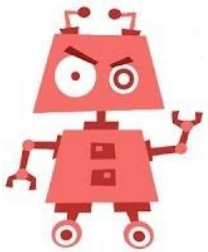
ADWARE

- It generates revenue for its developer by generating online advertisements in the GUI
- Revenue for the display of the advertisement or on a "pay-per-click" basis
  - E.g., a static box display, a banner display, full screen, a video, pop-up ad, etc.

DIALER

- It makes a call to premium-rate numbers or sends SMSs to premium services
- Now also targeting smartphones through infected Apps

From security event to security incident: Cyber Kill Chain



BOT

- It infects the victim to make it belong to a botnet, i.e., a set of devices remotely controlled to conduct a coordinated attack
- Usually created to conduct a Distributed Denial of Service (DDoS) attack
  - E.g., Mirai, Zeus

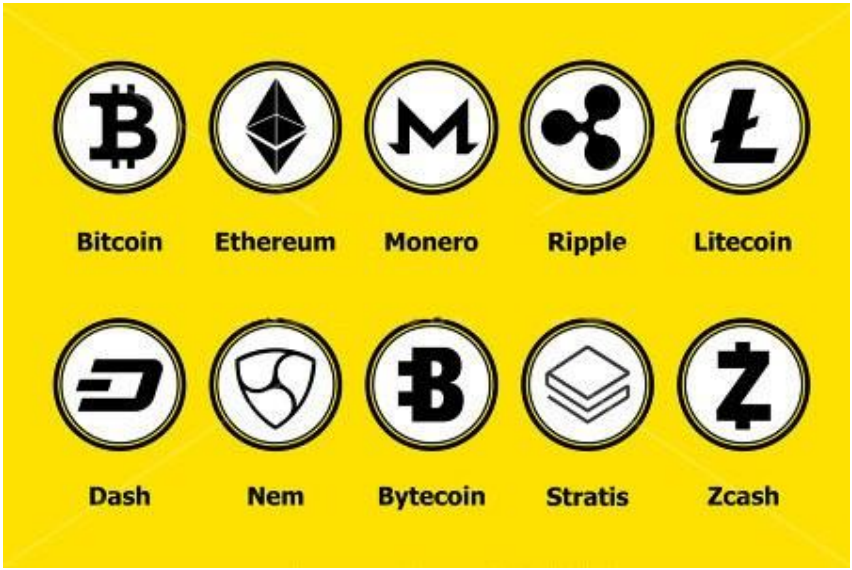
TROJAN

- Its distinctive feature is its capacity to camouflage as harmless software, trying to mislead its victims
- It usually leverages social engineering

From security event to security incident: Cyber Kill Chain

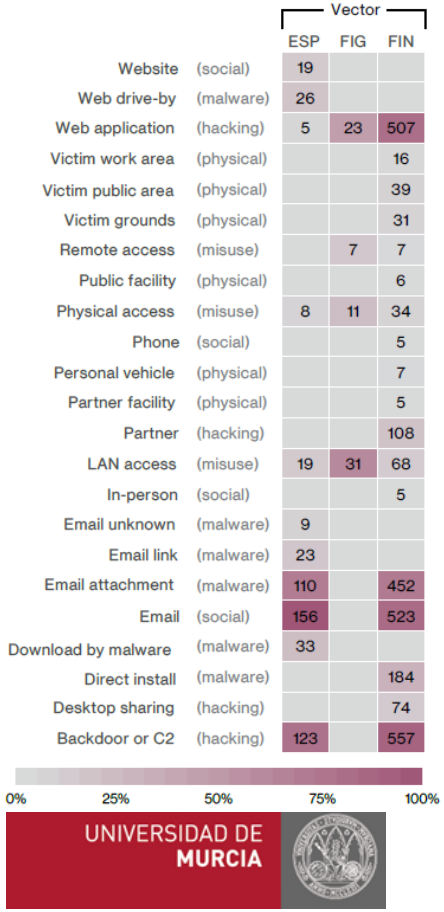
CRYPTOMINER

- It leverages the victim's computing resources to mine cryptocurrencies
- Developed as a desktop program or even using javascript
  - Coinhive (https://coinhive.com)



From security event to security incident: Cyber Kill Chain

- Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)



		Vector		
		ESP	FIG	FIN
Website	(social)	19		
Web drive-by	(malware)	26		
Web application	(hacking)	5	23	507
Victim work area	(physical)			16
Victim public area	(physical)			39
Victim grounds	(physical)			31
Remote access	(misuse)		7	7
Public facility	(physical)			6
Physical access	(misuse)	8	11	34
Phone	(social)			5
Personal vehicle	(physical)			7
Partner facility	(physical)			5
Partner	(hacking)			108
LAN access	(misuse)	19	31	68
In-person	(social)			5
Email unknown	(malware)	9		
Email link	(malware)	23		
Email attachment	(malware)	110		452
Email	(social)	156		523
Download by malware	(malware)	33		
Direct install	(malware)			184
Desktop sharing	(hacking)			74
Backdoor or C2	(hacking)	123		557

- According to 2017 Verizon's DBIR (Data Breach Investigations Report), 66% of malware was installed via malicious e-mails attachments
- After e-mail attachments, websites and backdoors or C2 (command and control) were the next most successful attack vectors
- Yet, do not underestimate USB drives
  - 60% of people who found a random USB drive plugged it to their computer
  - Stuxnet, targeting Iran's nuclear centrifuges

From security event to security incident: Cyber Kill Chain

- Malware weapon's program code triggers, taking action on target network to exploit vulnerability

- Payload within the malware is launched and executed
- Privilege escalation → Gain (unauthorized) elevated access to restricted resources
- Buffer overflow → Overrun the buffer's boundary while writing data on it
- Denial of Service (DoS) → Make a service, asset or network node unavailable to legitimate users
- Spoofing attack → Masquerade as another person or program by falsifying data
  - E.g., IP spoofing, ARP spoofing

From security event to security incident: Cyber Kill Chain

- Malware weapon installs access point (e.g., "backdoor") used by intruder and entrenches itself

- Use of known bad or blacklist IP addresses
  - Many of the servers hosting malware in the Internet are known
  - Their IP addresses are maintained and updated in black lists
- Use of dark IP address space
  - Reserved and unused public IP addresses
  - Intruders can use untraceable addresses within the dark space
- Use of a good destination IP address, but with unusual behavior
  - As soon as the IP address of the intruder is blacklisted, she switches to another IP address
  - Some countries (China, Russia, North Korea..) might be suspicious

From security event to security incident: Cyber Kill Chain

- Some common entrenchment techniques to extend the time the intruder keeps hidden consist in
  - Disabling operating system and application updates
    - So to avoid installing patches
  - Disabling antivirus and antispyware updates
    - So to avoid being detected by these solutions
  - Disabling forwarding logs to syslog or the SIEM system
    - So to avoid storing evidences (logs) of the intrusion for further analysis
  - Making system configuration changes
    - So to ease the presence of the intruder in the victim
  - Installing new service(s) and/or stopping service(s)
    - So to create new backdoors or attack vectors

From security event to security incident: Cyber Kill Chain

- Malware enables intruder to have "hands on the keyboard" persistent access to target network

- Telnet is the simplest way of communicating with the victim
  - Communications are unencrypted and unauthenticated
- IRC is often used to communicate with the victim
  - Commands are sent to the victim as key words or key phrases through chat rooms
- P2P has arisen as an alternative to IRC, since IRC is easily to block
  - Sometimes communications are even encrypted
- Domains controlled by the intruder and visited by the victim
  - Victim downloads the list of controlling commands
  - Easy to maintain and update for the intruder

From security event to security incident: Cyber Kill Chain

- Intruder takes action to achieve their goals, e.g. data exfiltration/destruction or encryption (ransom)

Pattern	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
Denial of Service	4	228	445	3	508	10	617	180				1	2		1	
Privilege Misuse	5	7	48	125	23	13	7,417	9	5	5	26	104	13	8	58	6
Lost and Stolen Assets	5	13	10	92	4	2	5,519	4	4	3	2	42	2	1	7	
Everything Else	8	106	20	40	32	213	88	8	8	14	16	28	24	4	19	3
Point of Sale	182		3	4	1			9	180		3	3				8
Miscellaneous Errors	2	24	14	114	13	3	2,246	16	1	16	10	96	9	2	38	12
Web App Attacks	4	25	376	32	73	4	148	28	3	11	364	15	61		13	24
Crimeware	5	32	30	54	63	261	5,102	14		5	7	12	1	2	5	1
Payment Card Skimmers	6		53			1	1	57	5		44				1	39
Cyber-Espionage		22	5	2	4	115	112	3		19	5	1	4	108	98	1

(left: all security incidents, right: breaches only)

UNIVERSIDAD DE MURCIA

From security event to security incident: Cyber Kill Chain

- Intruder removes any evidence of the attack and leaves

- After completion of the attack, or when the intruder feels jeopardized (being detected), she deletes any evidence of the attack before leaving
  - Deleting those logs proving her activity in the victim
  - Re-enabling normal logging to syslog and SIEM
  - Re-enabling updates for operating system, antivirus, etc
  - Undoing system configuration changes (e.g., restoring registry)
  - Uninstalling created backdoors
- Goal → hinder digital forensics activities afterwards

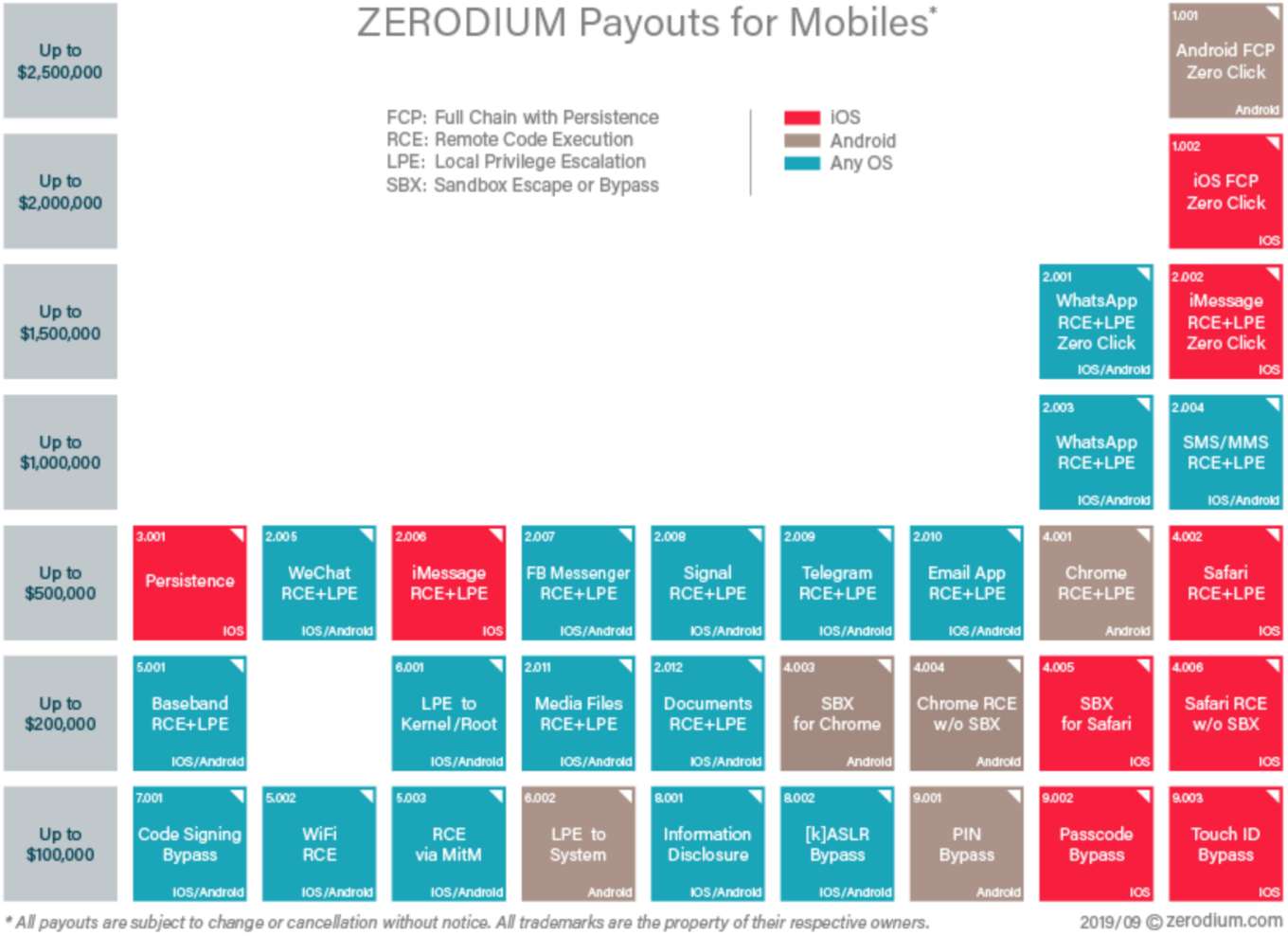
Want to make profit out of this?

- A platform for exploits acquisition
- Big bounties for zero-day high-risk vulnerabilities with fully functional exploits

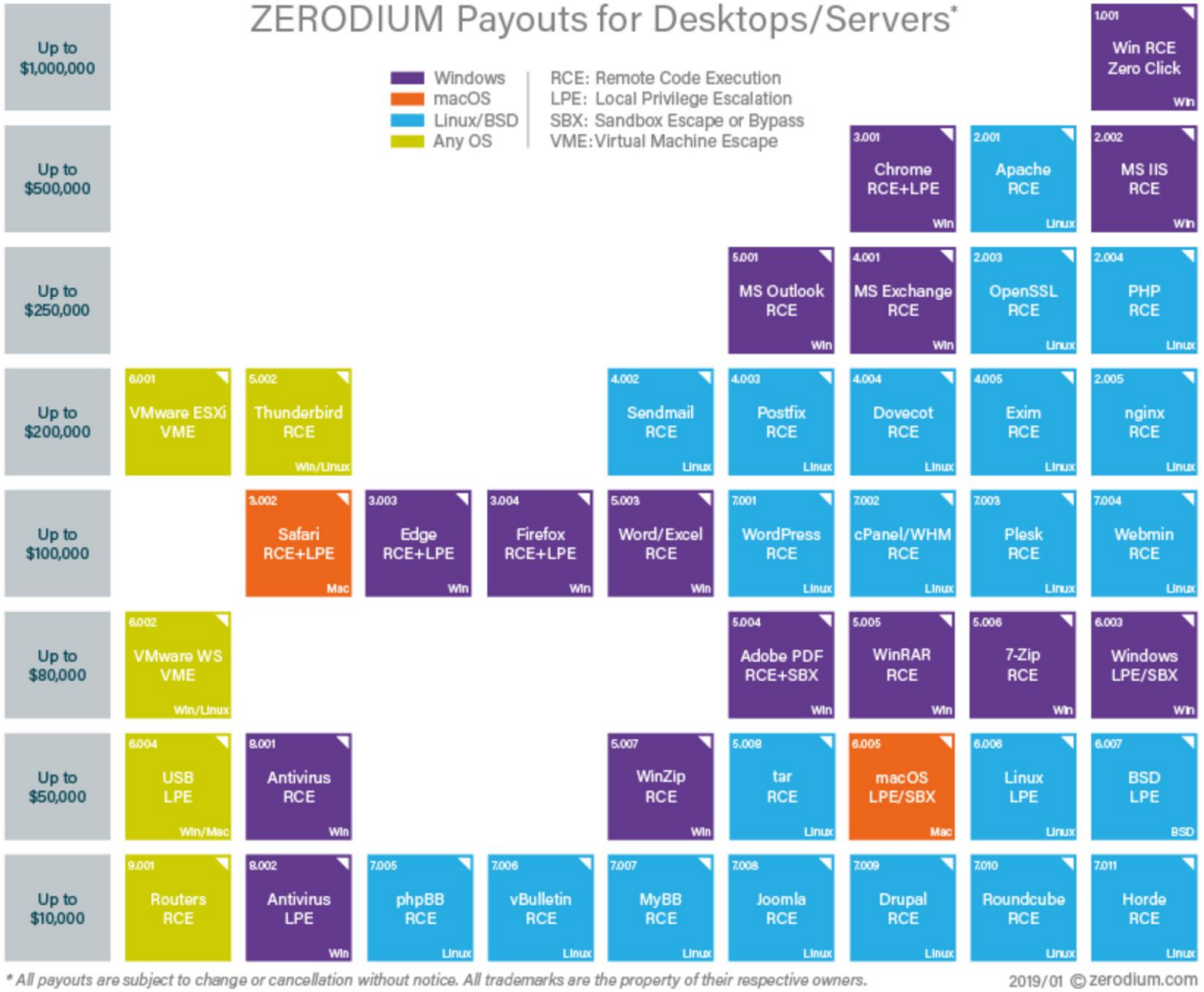
Category	Changes
New Payouts (**Mobiles**)	**$2,500,000** - Android full chain (Zero-Click) with persistence (**New Entry**) **$500,000** - Apple iOS persistence exploits or techniques (**New Entry**)
Increased Payouts (**Mobiles**)	**$1,500,000** - WhatsApp RCE + LPE (Zero-Click) without persistence (previously: **$1,000,000**) **$1,500,000** - iMessage RCE + LPE (Zero-Click) without persistence (previously: **$1,000,000**)
Decreased Payouts (**Mobiles**)	**$1,000,000** - Apple iOS full chain (1-Click) with persistence (previously: **$1,500,000**) **$500,000** - iMessage RCE + LPE (1-Click) without persistence (previously: **$1,000,000**)
Desktops/Servers	No modifications.

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

Want to make profit out of this?

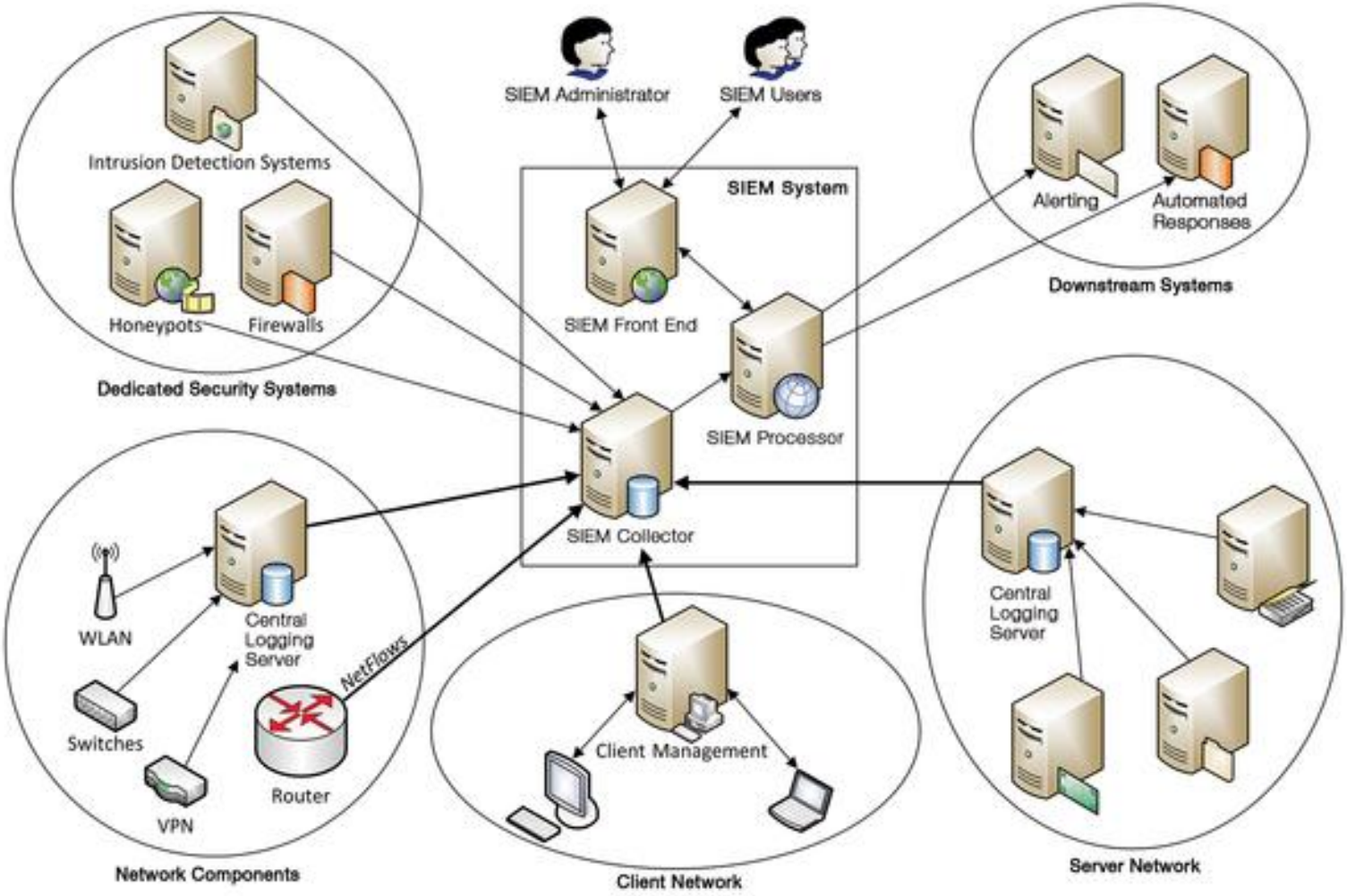


Want to make profit out of this?

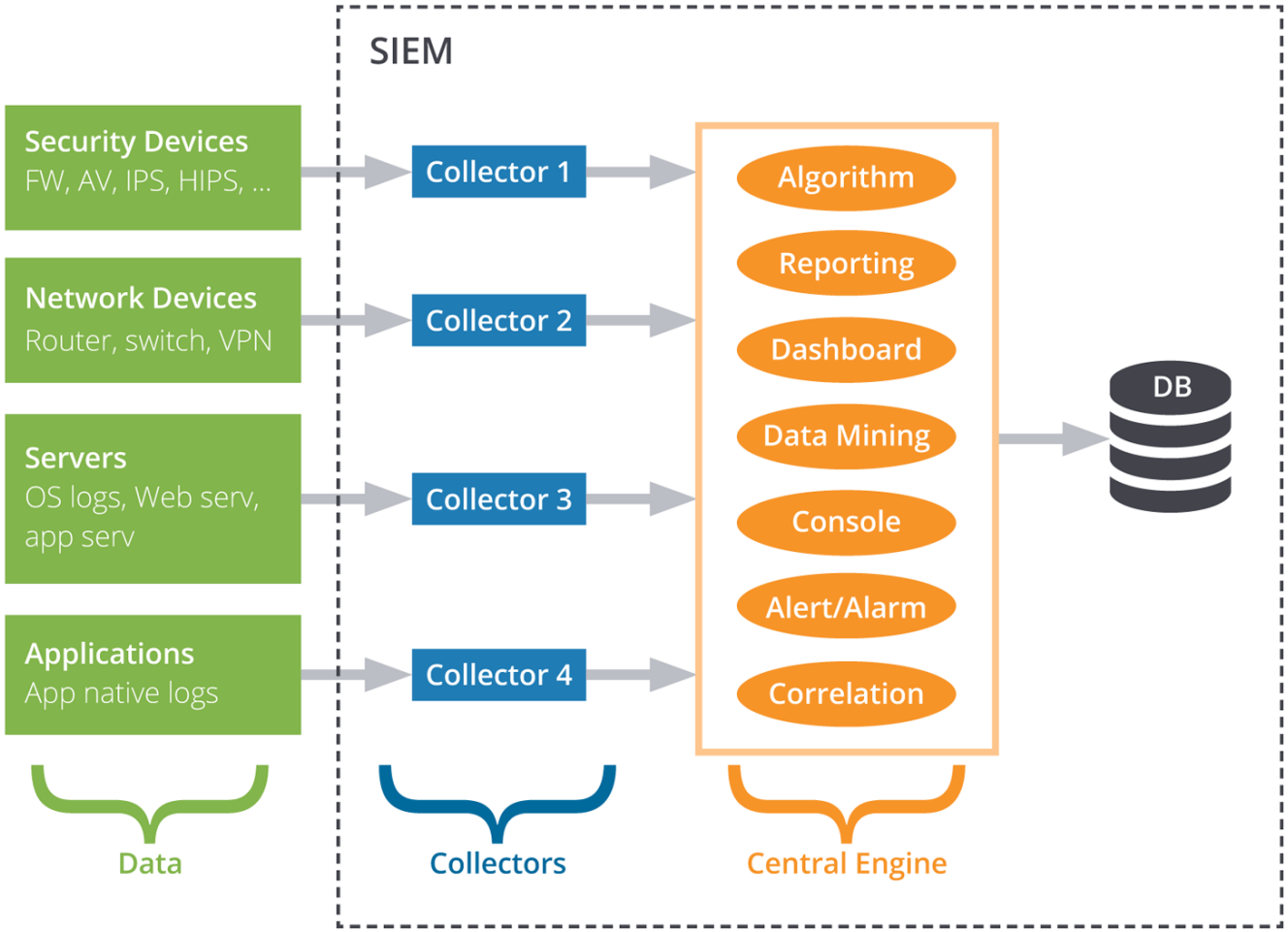


SIEM Architecture

SIEM Architecture



SIEM Architecture

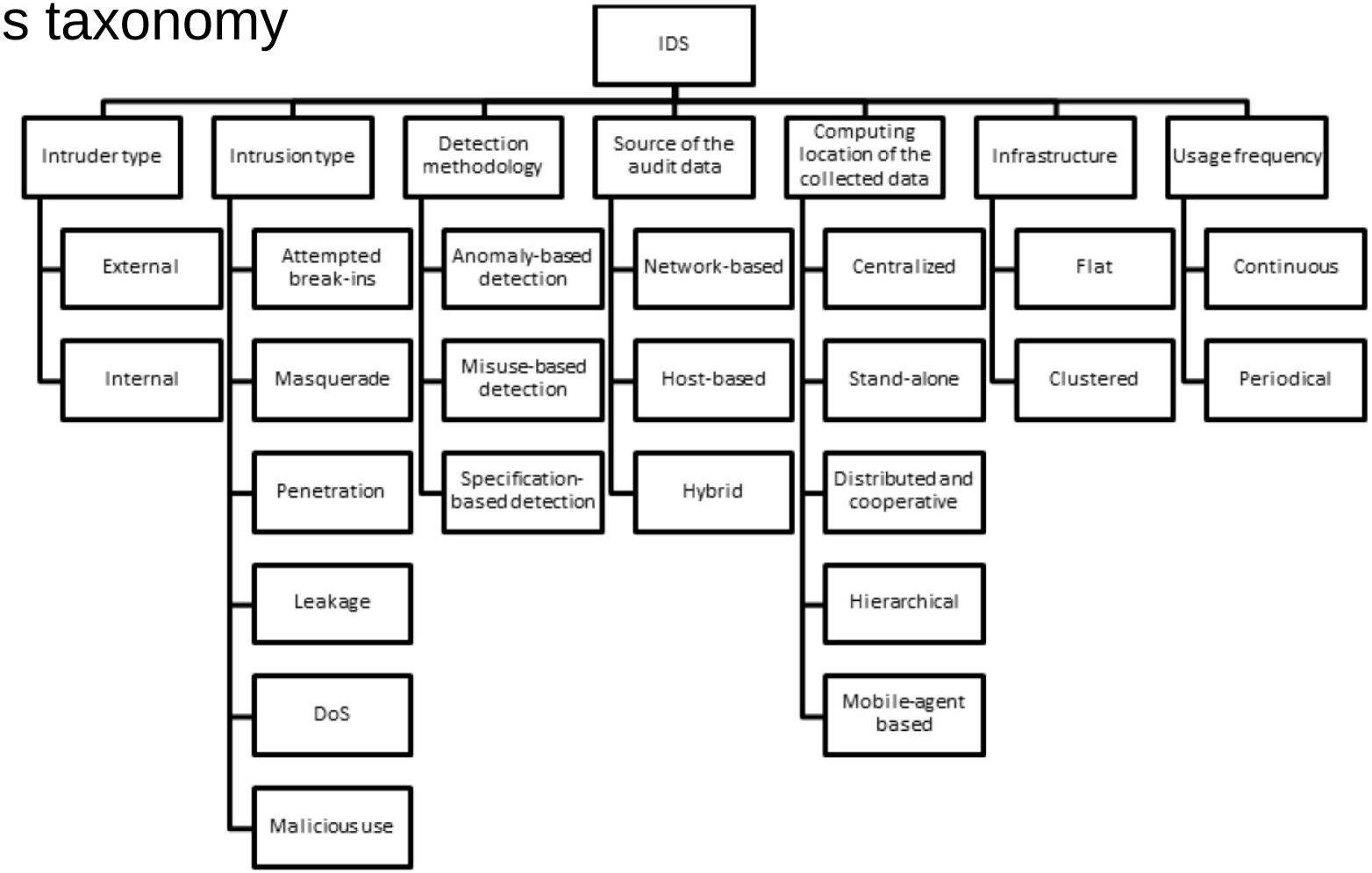


SIEM Architecture: Data Sources

- **Security Devices**
  - Antivirus (AV) and antispyware
    - When some sort of malware is detected, a log is sent to the SIEM
    - When the detected malware has been eradicated, a log is sent to the SIEM too
  - Firewall (FW)
    - A device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port
    - Packets that do not match policy are rejected and a log is sent to the SIEM
  - Intrusion Detection Systems (IDS)
    - A device or application that analyzes whole packets, both header and payload, looking for known intrusions
    - When a known intrusion is detected a log message is sent to the SIEM
  - Intrusion Prevention Systems (IPS)
    - A device or application that analyzes whole packets, both header and payload, looking for known intrusions
    - When a known intrusion is detected the packet is rejected and a log message is sent to the SIEM

SIEM Architecture: Data sources

- IDSs taxonomy

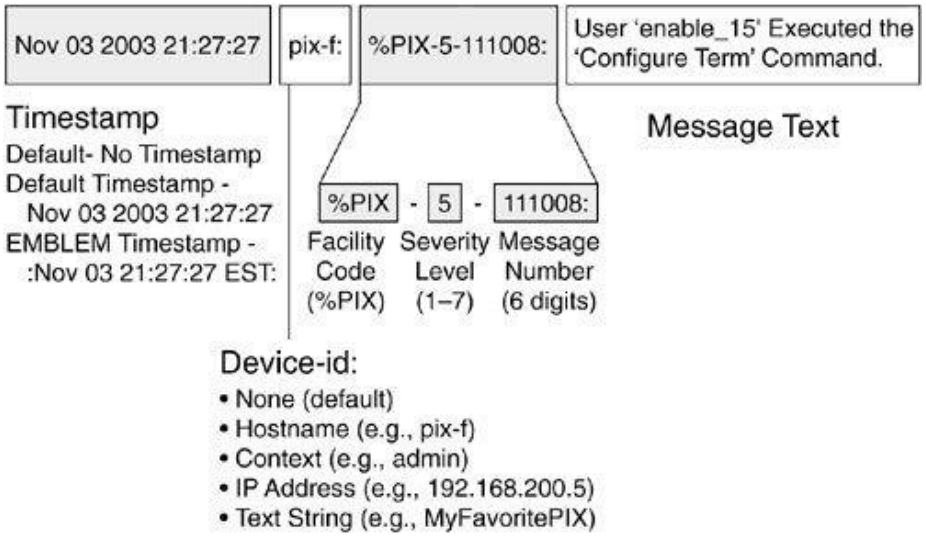


SIEM Architecture: Data Sources

- **Network Devices**
  - Router and switch
    - These could report to SIEM, e.g., every time a new configuration is set
  - Virtual Private Network (VPN)
    - Every new connection to a VPN, e.g., could generate a log to be sent to SIEM
- **Servers**
  - Operating System (OS)
    - OS can provide very valuable logs to SIEM reporting, e.g., on potential access to restricted resources (privileges escalation)
  - Web server
    - For every new configuration of the server, or whenever an invalid request is received, for instance, a number of logs can be sent to SIEM
- **Applications**
  - App native logs
    - Every application running on your system (e.g., a database, an authentication server, etc.) could potentially deliver logs to SIEM

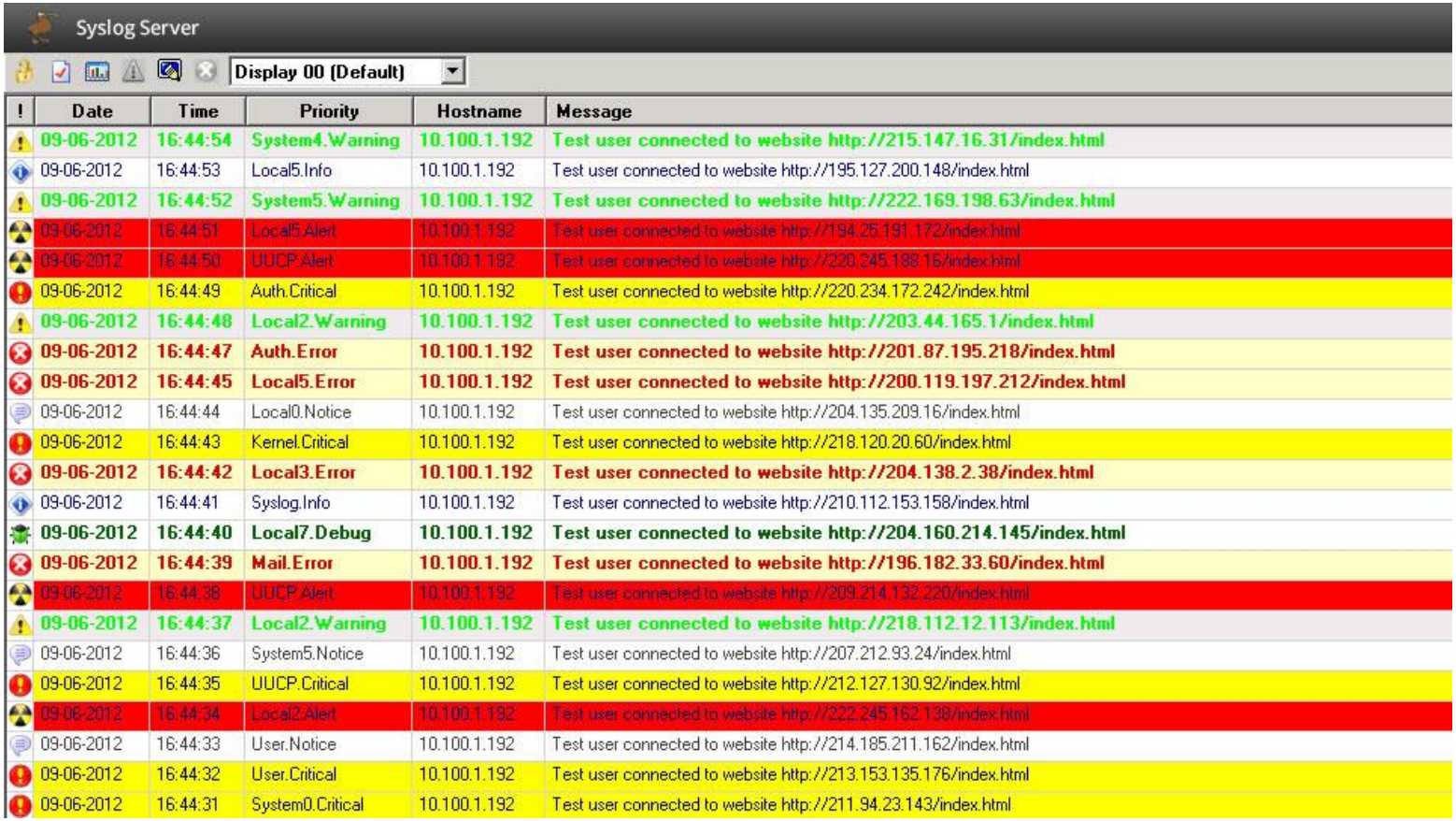
SIEM Architecture: Data Aggregation

- Syslog (RFC 5424)
  - Industry standard method for devices to record and report events
  - Most network devices are capable of producing syslog messages
  - While header is standard, message text is vendor-specific
  - Besides timestamp and device-id, a facility code is used to specify the type of program logging the message (kernel, user-level, etc.)
  - The severity level can take the values ‘emergency’, ‘alert’, ‘critical’, ‘error’, ‘warning’, ‘notice’, ‘informational’ and ‘debug’



SIEM Architecture: Data Aggregation

- Syslog (RFC 5424)



!	Date	Time	Priority	Hostname	Message
	09-06-2012	16:44:54	System4.Warning	10.100.1.192	Test user connected to website http://215.147.16.31/index.html
	09-06-2012	16:44:53	Local5.Info	10.100.1.192	Test user connected to website http://195.127.200.148/index.html
	09-06-2012	16:44:52	System5.Warning	10.100.1.192	Test user connected to website http://222.169.198.63/index.html
	09-06-2012	16:44:51	Local5.Alert	10.100.1.192	Test user connected to website http://194.25.191.172/index.html
	09-06-2012	16:44:50	UUCP.Alert	10.100.1.192	Test user connected to website http://220.245.188.16/index.html
	09-06-2012	16:44:49	Auth.Critical	10.100.1.192	Test user connected to website http://220.234.172.242/index.html
	09-06-2012	16:44:48	Local2.Warning	10.100.1.192	Test user connected to website http://203.44.165.1/index.html
	09-06-2012	16:44:47	Auth.Error	10.100.1.192	Test user connected to website http://201.87.195.218/index.html
	09-06-2012	16:44:45	Local5.Error	10.100.1.192	Test user connected to website http://200.119.197.212/index.html
	09-06-2012	16:44:44	Local0.Notice	10.100.1.192	Test user connected to website http://204.135.209.16/index.html
	09-06-2012	16:44:43	Kernel.Critical	10.100.1.192	Test user connected to website http://218.120.20.60/index.html
	09-06-2012	16:44:42	Local3.Error	10.100.1.192	Test user connected to website http://204.138.2.38/index.html
	09-06-2012	16:44:41	Syslog.Info	10.100.1.192	Test user connected to website http://210.112.153.158/index.html
	09-06-2012	16:44:40	Local7.Debug	10.100.1.192	Test user connected to website http://204.160.214.145/index.html
	09-06-2012	16:44:39	Mail.Error	10.100.1.192	Test user connected to website http://196.182.33.60/index.html
	09-06-2012	16:44:38	UUCP.Alert	10.100.1.192	Test user connected to website http://209.214.132.220/index.html
	09-06-2012	16:44:37	Local2.Warning	10.100.1.192	Test user connected to website http://218.112.12.113/index.html
	09-06-2012	16:44:36	System5.Notice	10.100.1.192	Test user connected to website http://207.212.93.24/index.html
	09-06-2012	16:44:35	UUCP.Critical	10.100.1.192	Test user connected to website http://212.127.130.92/index.html
	09-06-2012	16:44:34	Local2.Alert	10.100.1.192	Test user connected to website http://222.245.162.138/index.html
	09-06-2012	16:44:33	User.Notice	10.100.1.192	Test user connected to website http://214.185.211.162/index.html
	09-06-2012	16:44:32	User.Critical	10.100.1.192	Test user connected to website http://213.153.135.176/index.html
	09-06-2012	16:44:31	System0.Critical	10.100.1.192	Test user connected to website http://211.94.23.143/index.html

SIEM Architecture: Data Aggregation

- Alerts
  - Security devices (AV, FW, IDS, IPS) are usually capable of generating alerts when a harmful or suspicious situation happens
- Flow Data
  - Produced by network devices, it provides information on specific streams of data between endpoints
  - Source and destination IP address and port, amount of data transmitted and service (e.g., HTTP over port 80)
  - Useful to gather a high-level view of the traffic within your network
- Vulnerability Assessment (VA) Data
  - For very asset in the system, the list of CVEs (together with their CVSS) affecting it might be sent to SIEM

SIEM Architecture: Data Aggregation

- Push Log Collection
  - The source devices send logs to the SIEM autonomously
  - Pros
    - Easy to setup and configure the SIEM (e.g., syslog)
  - Cons
    - Syslog using UDP cannot guarantee the reception of logs
    - Malicious data source could send bogus or ill-intentioned logs to SIEM if proper access control mechanisms are neglected
- Pull Log Collection
  - The SIEM explicitly requests logs from source devices
  - Pros
    - Reception of logs is ensured
  - Cons
    - Logs might no longer come in real-time to the SIEM
    - SIEM has to explicitly traverse every data source looking for logs

SIEM Architecture: Data Aggregation

- Prebuilt Log Collection
  - Some SIEM solutions come along with predefined log collection methods for vendor-specific solutions (e.g., an Oracle database)
  - Pros
    - Easy to retrieve logs from these vendor-specific solutions
  - Cons
    - If the SIEM does not have a prebuilt log collection method for a critical vendor-specific solution in the system, we must resort to Push/Pull alternatives
- Custom Log Collection
  - Some special data sources might need a tailored log collection
  - Pros
    - Highest performance, coverage and accuracy of log collection
  - Cons
    - Tedious and time-consuming process to develop your own customized log collection
- Most SIEMs have a mixture of log collection strategies

SIEM Architecture: Normalization

- Due to the heterogeneity of data sources and the lack of a standard for event messages, a normalization is needed
  - E.g., a firewall blocking a connection could generate a syslog with the text “blocked”, while a different FW could use the word “dropped”
- Enrichment of messages with missing contextual information is also possible at this stage
- Creating and maintaining this normalization over a wide range of product vendors and versions is a significant effort for SIEM developers
- Normalization also enables a standard format of rule generation

SIEM Architecture: Correlation

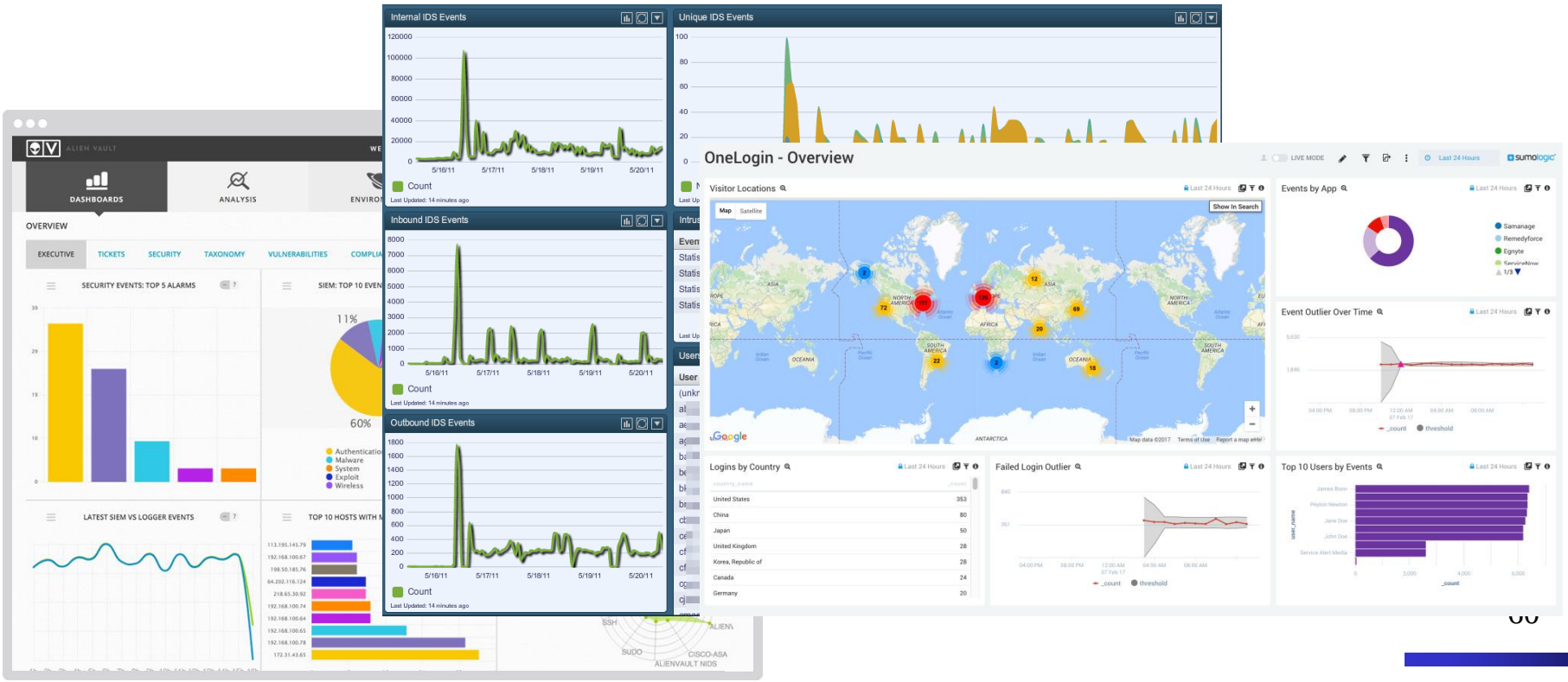
- Correlation is what really helps evolving from security events to security incidents
  - Looks for common attributes, and links events together into meaningful bundles
  - Provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information
  - Correlation is typically a function of the Security Event Management (SEM) portion of a full SIEM solution
  - Correlation rules are the “secret sauce” of commercial SIEMs
  - E.g.
  - `If [(failed logins >= 3) and then (Successful Login)] from the same source within 20 seconds → Possible Brute Force Attack`

SIEM Architecture: Alerting

- Correlated events are automatically analyzed and, when necessary, an alert is generated to warn either the sysadmin and/or the end user of a potential attack
- Alerting can be performed through several channels such as
  - Dashboard → With useful graphs and charts helping to interpret the ongoing situation
  - Email → Reporting on the potential attack and maybe including a link for further details
  - Pop-up message → As an alternative to email, more direct
  - Push notifications → More suitable for mobile devices

SIEM Architecture: Dashboards

- Either web- or application-based, dashboards are tools that can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern



SIEM Architecture: Compliance

- SIEMs a are a magnificent tool to ensure the compliance of the protected system(s) to existing security, governance and auditing regulations and processes
  - Enabling a more accurate real-time view of the environment (awareness rise)
  - Enabling incident response and system recovery/healing
- Some regulations examples are
  - ISO/IEC 27001, Information Security standard, 2013
  - EU Directive on Security of Network and Information Systems (NIS Directive), 2016
  - EU General Data Protection Regulation (GDPR), 2018

SIEM Architecture: Retention

- Long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements
- Long-term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring
- Encryption of long-term data guarantees its integrity
- Alternatives for data retention are
  - Database
    - Most popular option for many SIEMs due to its numerous advantages
  - Flat text file
    - Not so frequent as it does not scale well
  - Binary file
    - Vendor-specific for a particular SIEM solution

SIEM Architecture: Forensic Analysis

- SIEM allows forensic analysis, i.e, searching across logs on different nodes and time periods based on specific criteria
- Identify what went wrong regarding a cyber-intrusion and how to improve for the future
  - Prevention
    - Avoid the same intrusion happening again by applying appropriate mechanisms
  - Detection
    - Increase detection accuracy in case the intrusion happens again
  - Reaction
    - Enhance the enforced countermeasures for this specific intrusion
- SIEM mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs

SIEMs Comparison

SIEMs Commercial Solutions

- Enterprise-class SIEM system
- Ingests data from more than 350 sources
- Processes up to 75,000 security events per second
- Delivered via appliance, software or cloud

- Integration with the User Behavior Analytics (UBA) and Machine Learning toolkit
- Ingests petabytes of data a day
- Available as a software or cloud offering

SIEMs Commercial Solutions

- It boasts over 400 support modules for data ingestion
- Rate of millions of events per second and billions of events per day
- Risks prioritization into a manageable list
- Available on premises or in the cloud

- Lower-cost SIEM option thanks to its open source Open Threat Exchange (OTX)
- It handles up to 15,000 events per second
- Available as a virtual or hardware appliance or in the cloud
- Open Source version → **OSSIM**

SIEMs Commercial Solutions

- Unifies SIEM, log management, security analytics and network and endpoint monitoring and forensics
- It scales from SMEs up to large enterprises thanks to its decentralized architecture
- Can be deployed as an appliance, software or virtual instance

- It processes tens of thousands of events per second and can store billions of events and flows
- Particularly popular with public sector, higher education and healthcare
- Available as a physical or virtual appliance

UNIVERSIDAD DE MURCIA

SIEMs Commercial Solutions

- Aimed at managed security services providers (MSSPs) and enterprises with distributed IT environments
- Analyzes data from a range of applications and devices
- Offered as software or a virtual appliance

- Easy to use, lower-cost SIEM option
- Processes up to 250 million events per day
- Allows for automated incident response
- Available as a virtual appliance

SIEMs Commercial Solutions

- Aimed at mid-market and enterprise users
- Can retain data from millions of daily events for up to five years
- Incorporates analytics & threat intelligence
- Available as an appliance, software or managed service

- Most popular option with financial, government, energy and telecom organizations
- Processes 30,000 events per second, ingests up to 10Gbps and supports up to 100,000 endpoints per scalable system

Comparison Criteria

1. How much native support does the SIEM provide for the relevant log sources?
2. Can the SIEM supplement existing logging capabilities?
3. How effectively can the SIEM make use of threat intelligence?
4. What forensic capabilities can the SIEM provide?
5. What features does the SIEM provide that assist in data examination and analysis?
6. How timely, secure and effective are the SIEM's automated response capabilities?
7. For which security compliance initiatives does the SIEM provide built-in reporting support?

SIEMs Comparison

- Gartner 2017 Magic Quadrant for SIEM
- Ability to execute VS Completeness of vision
  - Niche players
  - Visionaries
  - Challengers
  - Leaders

SIEMs Comparison

Vendor/Product	Use Cases	Metrics	Intelligence	Delivery	Pricing
HPE ArcSight	Enterprises	350+ data sources, 75,000 events per second (EPS)	Integrates with machine learning, intelligence platforms	Appliance, software or cloud	Based on data ingested and events per second (EPS)
Splunk Enterprise Security	Highly-regulated industries	Most users ingest several petabytes daily	Integrates with Splunk UBA & machine learning toolkit	Software or cloud	Based on max daily data volume; starts at $1,800/GB/day
IBM Security QRadar	Enterprises and regulated industries	400+ sources, scales to millions of events per second	UBA, forensics, packet inspection, Watson integration	Cloud or hardware, software or virtual appliance	Cloud starts at $800/month; on-premises at $10,400
AlienVault Unified Security Management	Lower-cost option for on-premises or AWS	Up to 15,000 EPS	Global network sharing 1 million threats daily	Cloud or virtual or hardware appliance	Lower-cost open source-based product
LogRhythm	Scales from midrange to enterprise	Highly scalable decentralized architecture	Machine analytics for advanced threats	Appliance, software or virtual instance	Subscription pricing tied to volume consumption
McAfee Enterprise Security Manager	Support for public sector, education and healthcare	50,000+events per second, billions of events stored	Automated task and policy changes	Physical or virtual appliance	Based on EPS capacity, starting at $39,995
Micro Focus Sentinel Enterprise	MSSPs and distributed enterprises	Event taxonomy comprises more than 200 fields	Integrates with NetIQ technologies	Software or virtual appliance	Based on EPS and per device
Solar Winds Log & Event Manager	Security teams looking for easy, lower-cost solution	Up to 250 million events per day	Thresholds can be set for abnormal behavior	Virtual appliance	Starts at $4,495 for 30 nodes
Trustwave SIEM Enterprise	Mid-market and enterprise	Millions of daily events	Analytics and threat intelligence from SpiderLabs	Appliance, software or managed service	Subscription or fee-based consulting
RSA NetWitness	Financial, government, energy, telecoms	30,000 EPS, 10Gbps & 100,000 endpoints per scalable system	Streaming analytics, machine learning, automation	On-premises, virtual, cloud and hybrid options	Based on throughput per 50 GB of logs and 1TB of packets

Bibliography

[1] Howell, D., **“Building better data protection with SIEM”**, *Computer Fraud & Security*, no. 8, pp. 19-20, 2015

[2] Aguirre, I., & Alonso, S., "**Improving the automation of security information management: A collaborative approach**", *IEEE Security & Privacy*, vol. 10, no.1, pp 55-59, 2012

[3] Miller, D. R., Harris, S., Harper, A., VanDyke, S., & Blask, C., **“Security Information and Event Management (SIEM) Implementation”**, *(Network Pro Library)*, McGraw Hill, 2010

[4] Suarez-Tangil, G., Palomar, E., Ribagorda, A., & Sanz, I., **“Providing SIEM systems with self-adaptation”**, *Information Fusion*, no. 21, pp. 145-158, 2015

Bibliography

[5] Granadillo González, G., El-Barbori, M., & Debar, H., **"New types of alert correlation for security information and event management systems"**, *New Technologies, Mobility and Security (NTMS), 2016 8th IFIP International Conference on*. IEEE, 2016

[6] Rieke, R., Prieto, E., Diaz, R., Debar, H., & Hutchison, A., **"Challenges for advanced security monitoring–the MASSIF project"**, *TrustBus*. 2012.

[7] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., Nespoli, P., Gómez Mármol, F., "**Shielding IoT against cyber-attacks: An event-based approach using SIEM**", Wireless Communications and Mobile Computing, 2018