Module-2 Topics to be discussed:

Introduction to Tools and Methods used in Cybercrime:

Introduction to basic security hygiene & tools

SIEM (Security Information & Event Management) Tools

UEBA (User & Entity Behavior Analytics) Tools

EDR (Endpoint Detection & Response) Tools

SOAR (Security Orchestration & Response) Tools

Encryption Tools

IRT (Incident Response) Tools

PEN (Penetration testing) Tools

Introduction to basic security hygiene & tools

Cyber **hygiene** is an array of practices to minimize the risk of **security** crises.

Alternatively,

Security hygiene is **the day-to-day practice of maintaining the basic health and security of software and hardware assets**. Examples include making sure that only the right ports are open to perform tasks, ensuring proper software patch levels, and cybersecurity awareness training.

Or

Cyber hygiene refers to **fundamental cybersecurity best practices that an organization's security practitioners and users can undertake**. As you have personal hygiene practices to maintain your own health, cyber hygiene best practices help protect the health of your organization's network and assets.

General Security Attack tools

Various Tools and technologies used to launch attacks against the target

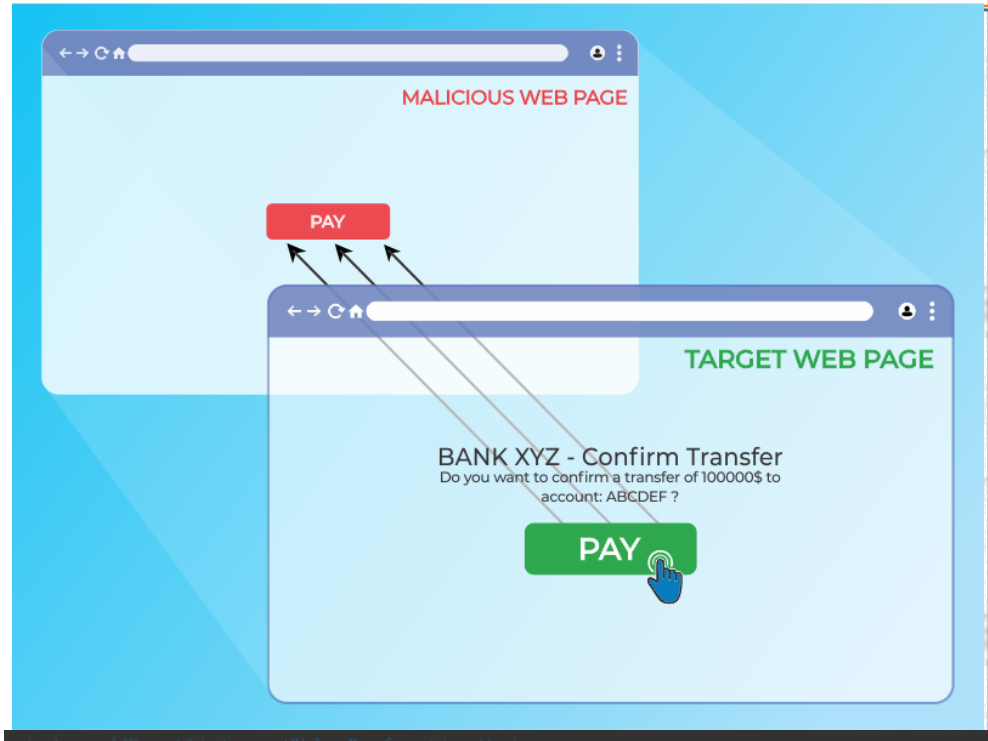
- Scareware
- Malvertising
- Clickjacking
- Ransomware

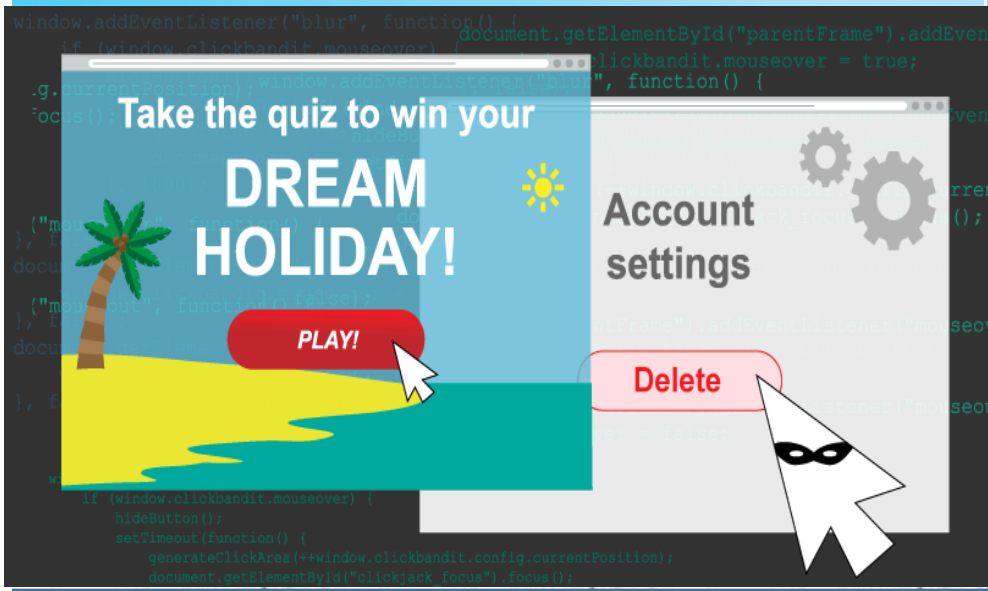
Malvertising:

- "malicious software (malware) advertising")
- **Malvertising** is the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.

Clickjacking:

- **Clickjacking** is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element.
- This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.





Ransomware:

- **Ransomware** is a form of malware that encrypts a victim's files.
- The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee to get the decryption key.

Basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. Initial uncovering

Two Steps involved: i. Reconnaissance ii. Attacker uncover information

2. Network Probe
3. Crossing the line toward E-crime
4. Capturing the network
5. Grab the data
6. Covering tracks

Proxy Server and Anonymizers

Proxy Server:

- It is computer on a network which acts as an intermediary for connections with other computers on that network
- 1st attacker connects to proxy server
- Proxy server can allow an attacker to hide ID

Purpose of Proxy Server:

- Keep the system behind the curtain
- Speed up access to resource
- Specialized proxy servers are used to filter unwanted content such as advertisement
- Proxy server can be used as IP address multiplexer to enable to connect number of computers on the internet.

Anonymizers:

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the internet untraceable.

It accesses the Internet user's behalf, protecting personal information by hiding the source computer's identifying information.

What is Password?

- String of characters for authentication and log on computer, web application, software, Files, Network, and Mobile Phones
- Password Comprises of : [A-Z a-z, 0-9, Symbols, space]

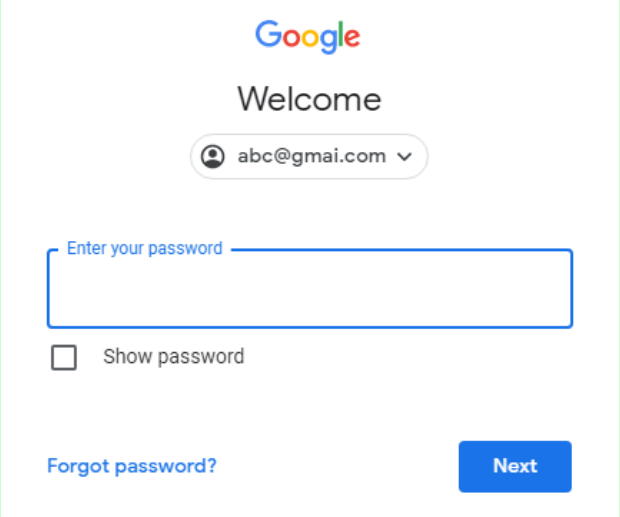
A-Z – A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

a-z – a b c d e f g h I j k l m n o p q r s t u v w x y z

0-9 – 0 1 2 3 4 5 6 7 8 9

Symbols - ` ~ ! @ # $ % ^ & * ( ) _ - + = \ | ‘ “ ; : / ? . , < >

Space -



Password Characteristics

- No short Length
- No birthday or phone number, real name, company name
- Don’t use complete words or Shakespeare quotes
  - Example
    - Hello123: weak
    - @(H311l0)@: Strong
    - Easy to remember, hard to guess

Password Security

- Don’t use your old passwords
- Don’t use working or private email for every website registration such as games, news, business …. Etc

Password Cracking

- Guessing or recovering a password
- Unauthorized access
- To recover a forgotten password
- A penetration testing step (e.g. Network and applications)
- Password cracking is illegal purpose to gain unauthorized access
- To retrieve password for authorize access purpose (misplacing, missing) due to various reason.

(e.g. what was my password?)

What to avoid while selecting your password

Using a dictionary word: Dictionary attacks are designed to test every word in the dictionary (and common permutations) in seconds.

Using personal information: A pet's name, relative's name, birthplace, favorite sport and so on are all dictionary words. Even if they weren't, tools exist to grab this information from social media and build a wordlist from it for an attack.

Using patterns: Passwords like 1111111, 12345678, qwerty and asdfgh are some of the most commonly used ones in existence. They're also included in every password cracker's wordlist.

Using character substitutions: Character substitutions like 4 for A and $ for S are well-known. Dictionary attacks test for these substitutions automatically.

What to avoid while selecting your password contd…

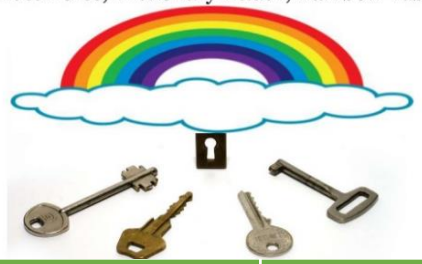
Using numbers and special characters only at the end: Most people put their required numbers and special characters at the end of the password. These patterns are built into password crackers.

Using common passwords: Every year, companies like Splashdata publish lists of the most commonly used passwords. They create these lists by cracking breached passwords, just like an attacker would. Never use the passwords on these lists or anything like them.

Using anything but a random password: Passwords should be long, random, and unique. Use a password manager to securely generate and store passwords for online accounts.

Password Cracking Types

- Brute Force, Dictionary Attack, Rainbow Table

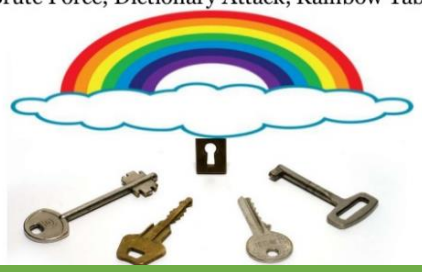


Password Cracking Types

- Brute Force, Dictionary Attack, Rainbow Table

Password Cracking Types

- Brute Force, Dictionary Attack, Rainbow Table



Type of Password Attack	Definition
Dictionary Attack	This method involves the use of a wordlist to compare against user passwords.
Brute Force Attack	This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@$$word using the brute force attack.
Rainbow table attack	This method uses pre-computed hashes. Let’s assume that we have a database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found, then we have the password.
Guess	As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.
Spidering	Most organizations use passwords that contain company information. This information can be found on company websites, social media such as facebook, twitter, etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

Password Cracking Tools:

John the Ripper, Cain & Abel, Rainbow Crack, Ophcrack, Brutus, crackStation, Password Cracker, AirCrack

Types of Password Attacks contd…

Type of Password Attack
Social Engineering
Offline Cracking
Phishing
Malware

Password Cracking Types: (Social Engineering)

- sometimes very lazy genius non-IT Geeks can guess or find out your password

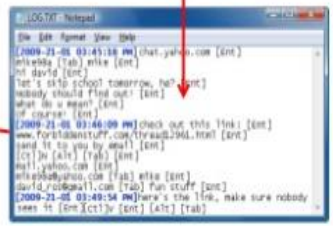

Password Cracking Types: (Phishing)


Password Cracking Types: (Offline Cracking)

- We have enough time to break the password
- Usually take place for big data
- Or very strong and complicated password
- After attack
- Forensics investigation

Application Password Cracking: (Malware)





Password Cracking Tools

- Brutus
  - Remote online cracking tool, Windows base, free, supports:(HTTP, POP3, FTP, SMB, ...etc), resume/pause option .no recent update but still on top ranking.
- RainbowCrack
  - Hash cracker tool, windows/linux based, faster than traditional brute force attack, compare both plain text and hash pairs. Commercial and free version
- Wfuzz
  - Web application brute forcing (GET and POST), checking (SQL, XSS, LDAP,etc) injection
- Cain and Able ***
  - Few features of password cracking ability: Syskey Decoder,VNC Password decoder , MS SQl MYSQL and Oracle password extractor Based64, Credential Manager Password Decoder, Dialup Password Decoder,PWL Cached Password Decoder, Rainbowcrack-online client, Hash Calculator,
- John the Ripper
  - Offline mode, Unix/linux based, auto hash password type detector, powerful, contain several built-in password cracker
- THC Hydra
  - Dictionary attack tool for many databases, over 30 protocols (e.g. FTP,HTTP,HTPPS,...etc)
- Medusa
- AirCrack-NG
  - WEP and WPA-PSK keys cracking, faster than other WEP cracker tools

- OphCrack
- LophtCrack

Password Cracking Depends on

- Attacker's strengths
- Attacker's computing resources
- Attacker's knowledge
- Attacker's mode of access [physical or online]
- Strength of the passwords
- How often you change your passwords?
- How close are the old and new passwords?
- How long is your password?
- Have you used every possible combination: alphabets, numbers and special characters?
- How common are your letters, words, numbers or combination?
- Have you used strings followed by numbers or vice versa, instead of mixing them randomly?

SIEM (Security Information & Event Management) Tools – Leveraging Logs, Feature of SIEM systems, Log Analysis

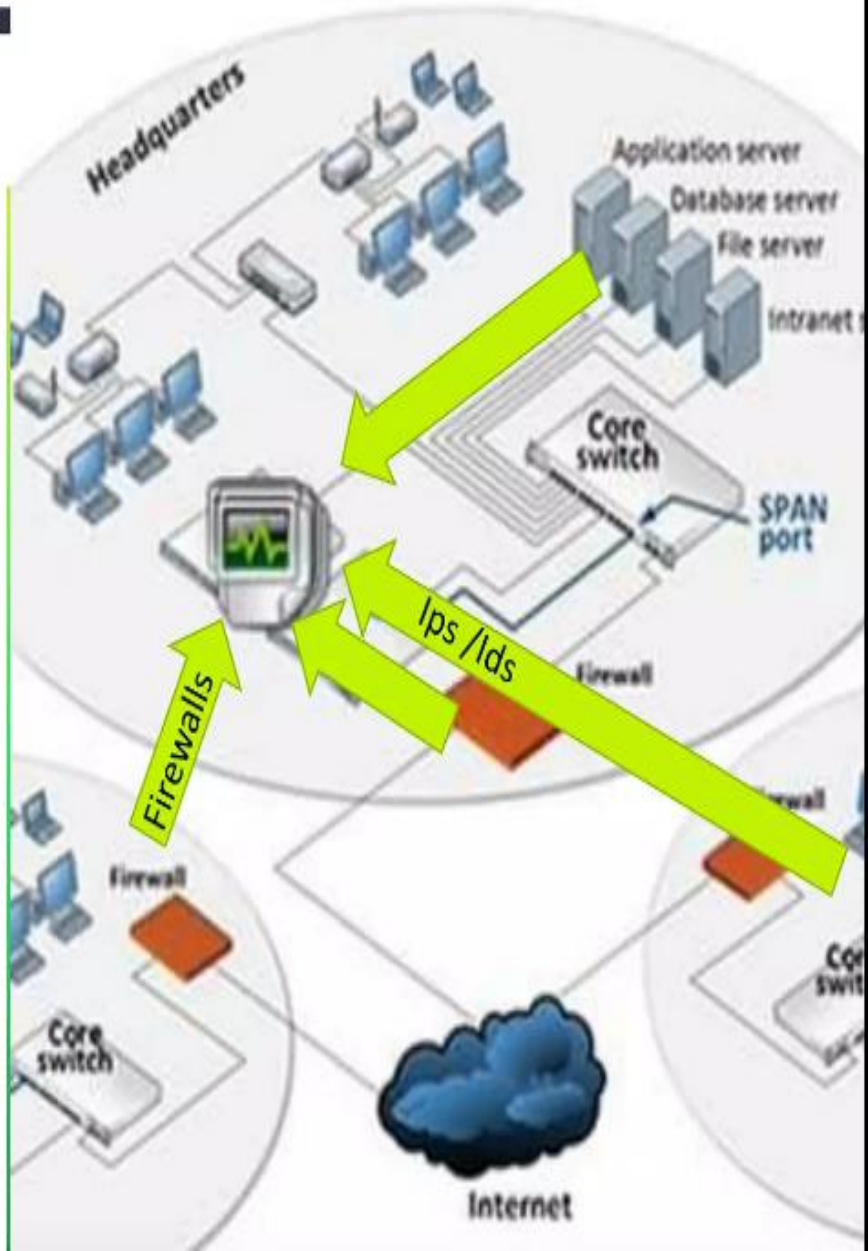
Security Information & Event Management,

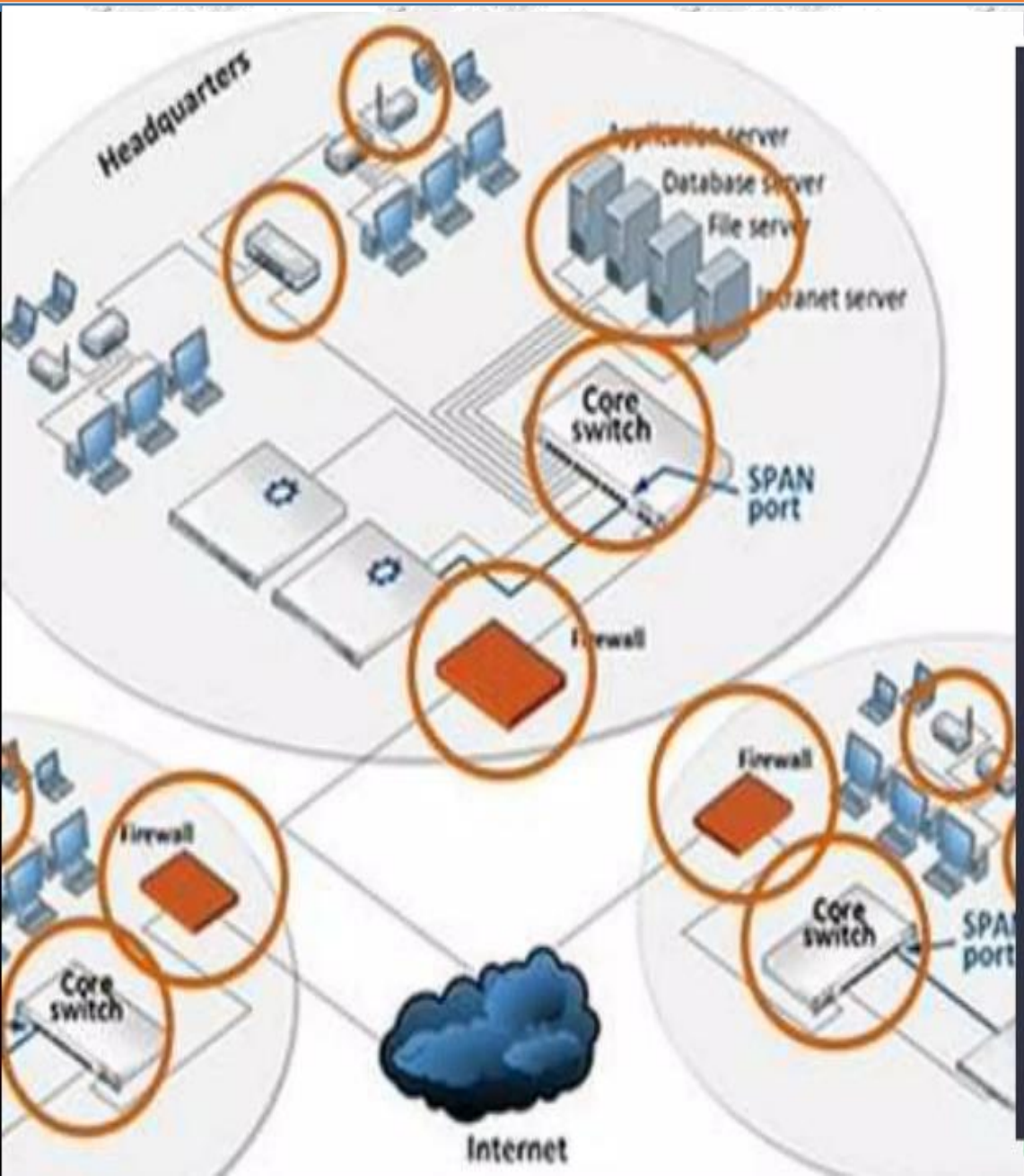
Combining security information management (SIM) and security event management (SEM), security information and event management (SIEM) offers **real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes**.

WHAT IS SIEM

LOG aggregation

- Centralized all security notifications from various security technology (Firewalls ,IDs ,IPs ,Antivirus console ,wireless active points and active directories).
- It all generate tons of notification every day.
- Siem allows you to centralize all logs in one place in set of report.





HOW IT WORKS

Event management

RULES

- Repeat Attack-Login Source — RULE
- Brute force attacks, Password guessing — GOAL
- Alert on 3 or more failed logins in 1 minute from a single host. — Trigger
- Active Directory, Syslog (Unix Hosts, Switches, Routers, VPN) — Event

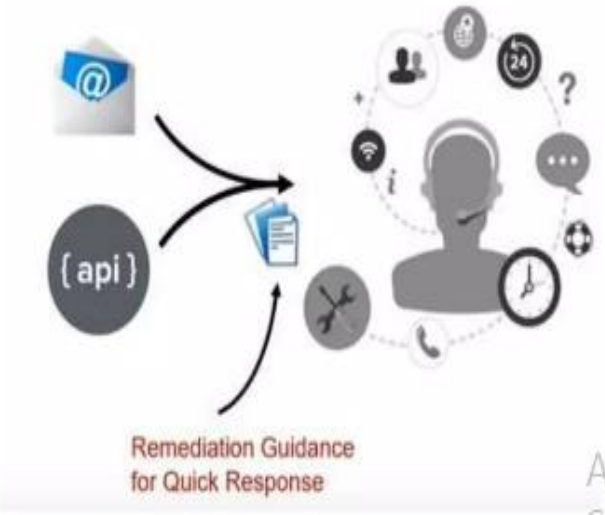
HOW IT WORKS

Incident

- Simply logged
- Written in report to be viewed later
- Immediate Attention

Notification

- Sent by email / api
- How they can solve it



SIEM PROCESS

STEP 1

Collect data from various sources
(network devices, servers, domain controllers and more)

STEP 2

Normalize and aggregate collected data

STEP 3

Analyze the data to discover and detect threats

STEP 4

Pinpoint security breaches and enable organizations to investigate alerts

SIEM CAPABLITIES

MAIN FEATURES

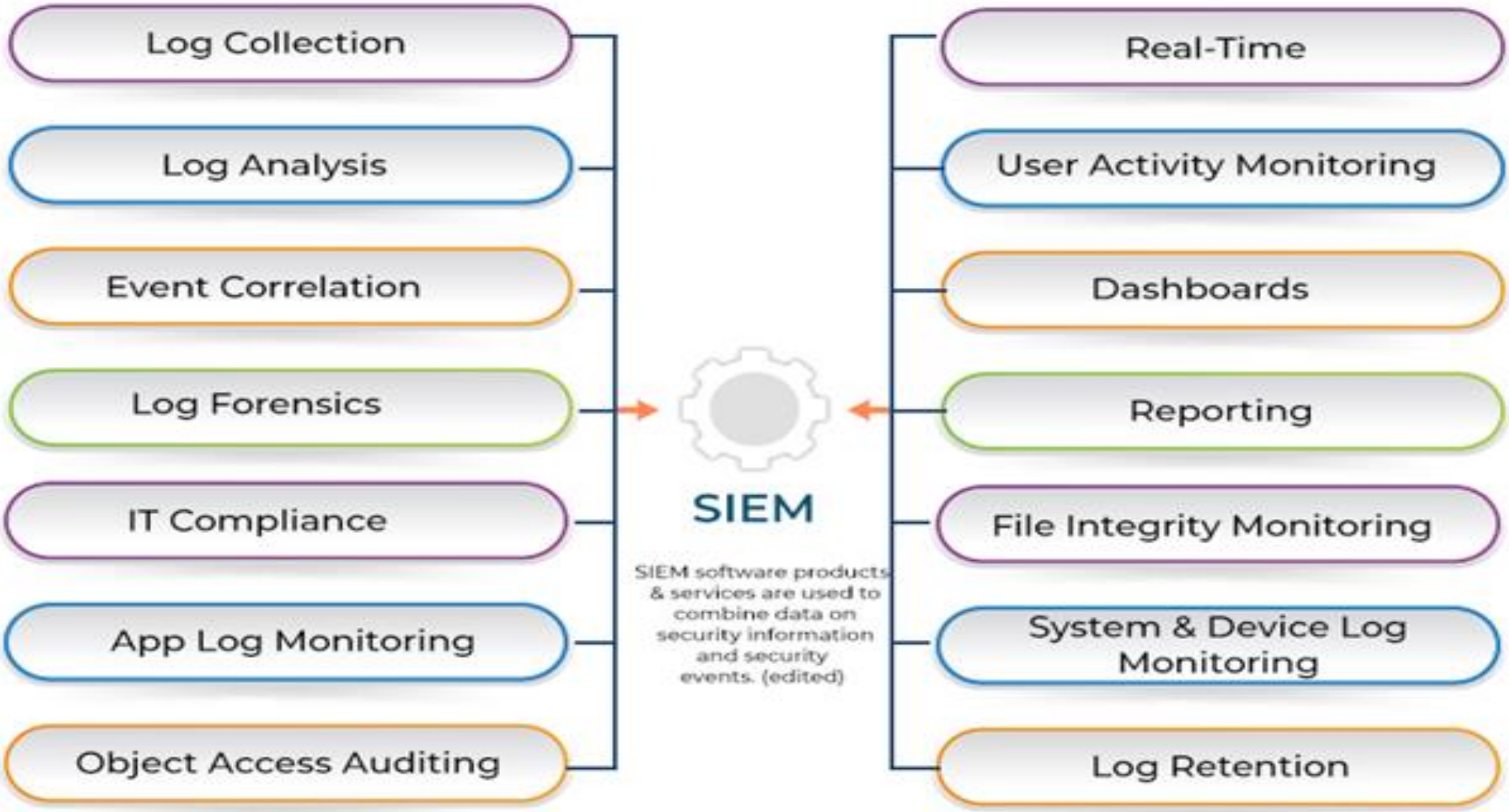
- Threat detection
- Investigation
- Time to respond

ADDITIONAL FEATURES

- Basic security monitoring
- Advanced threat detection
- Forensics & incident response
- Log collection
- Normalization
- Notifications and alerts
- Security incident detection
- Threat response workflow

What is a SIEM?

SECURITY INFORMATION AND EVENT MANAGEMENT



Security information and event management (SIEM) is defined as a security solution that helps improve security awareness and identify security threats and risks. It collects information from various security devices, monitors and analyzes this information, and presents the results in a manner that is relevant to the enterprise using it.

SIEM is a combination of security information management (SIM) and security event management (SEM). It alerts organizations about potential attacks, information security incidents, or even compliance issues. SIEM solutions offer real-time monitoring and analysis of events by strengthening threat detection and security incident management through pulling live data and historical security event data.

SIEM's core functioning includes a range of tracking, logging, collection, and management of security data for compliance or auditing purposes, including operational capabilities such as reporting, data aggregation, security monitoring, and user activity monitoring.

How does SIEM work?

Organizations can utilize SIEM software to monitor, audit, and re-engage with all of the logs that their systems generate, be it applications, devices, or home computers. **This will alert them about any security issues before they occur instead of relying on responsive action**.

SIEM software helps collect the data generated by various applications, network devices, and security systems such as host systems, networks, firewalls, and antivirus events, to name a few. It then brings all the information together into a single central place.

For example, when SIEM identifies a threat, it generates an alert and notifies and flags the attack to appropriate stakeholders. SIEM's custom dashboards also help reduce the time spent looking into false positives

The Characteristics of a Modern SIEM

- Fully managed
  - Infrastructure
  - Security content and correlation rules
  - Monitored 24x7
- Big data
- Unlimited scale
- Cloud ready
- Can collect data without access to underlying cloud host infrastructure
- DevOps

The Characteristics of a Modern SIEM

- Configuration Management
  - Ex: Chef, Ansible, AWS Cloud Formation Templates
- Support cloud provider data types
  - Ex: AWS cloud trail
- Easily extensible
- Not limited by domain, source, message, or event frequency or uniqueness
- Automatically incorporates 3rd party watch lists
- Dynamically generate watch lists based on real time data

Weighing Risks

Threat	x	Vulnerability	x	Impact
Severe		Critical		Sensitive, Restricted
				Critical
High		High		Internal
				High-Priority
Elevated		Medium		Public
				Supportive
Low		Low		None
				None

Intelligence is needed to weigh risks

Threats

- AntiVirus
- IDP
- FireEye
- Firewall
- SNORT
- Bro
- DNS
- Departmental devices

Vulnerabilities

- NeXpose
- Departmental Nessus

Impact

- ASSETs
- DLP
- SSNCap
- Manual reporting

Incident Actions

Notification

Alarm

Ignore

True Positive

Unknown

False Positive

Notification

2012-02-09 17:58:52 128.192.x.6 0.0.0.0
OfficeScan Virus: Failed to Clean or Quarantine Mal_Hifrm

2012-02-06 13:18:56 128.192.x.6 98.139.135.21
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 243) "

2012-02-01 14:48:36 128.192.x.6 0.0.0.0 Malicious Domain Lookup img717.imageshack.us malicious domain aggressive

2012-02-01 13:05:25 207.171.162.95 128.192.x.6 snort: "SPECIFIC-THREATS Microsoft IE malformed iframe buffer overflow attempt

Alarms

Ungrouped | Grouped

(1-50 of 337) Next 50 -> Last ->>

Apply label to

#	Alarm	Risk	Sensor	First event GMT-4:00	Last event GMT-4:00	Source	Destination
	Tuesday 01-May-2012 [Delete]						
1	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 13:45:04	2012-05-01 13:45:04	128.192.	198.24
2	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:50:27	2012-05-01 12:50:27	173.1	128.192.8
3	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:50:27	2012-05-01 12:50:27	173.1	128.192.8
4	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:30:08	2012-05-01 12:30:08	69.55	128.192
5	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:30:08	2012-05-01 12:30:08	69.55	128.192
6	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:30:08	2012-05-01 12:30:08	69.55	128.192
7	**SSNCAP: Full Packet Data**	1	ossim-sensor.infosec.uga.edu	2012-05-01 12:30:08	2012-05-01 12:30:08	69.55	128.192
8	**AV Scan, SSH service discovery detected from 1.252.62.39** [34 events]	1	ossim-sensor.infosec.uga.edu	2012-05-01 10:10:37	2012-05-01 10:10:37	1.252	128.19
9	**SSH Scanning Detected** [111 events]	1	128.192.252.146	2012-05-01 10:10:27	2012-05-01 10:10:27	1.252	128.192.
10	**AV Malware, trojan Nine Ball detected on 172.21.32.63** [1 events]	0	ossim-sensor.infosec.uga.edu	2012-05-01 10:07:56	2012-05-01 10:07:56	172.	210.2
11	**snort: "ET COMPROMISED Known Compromised or Hostile Host Traffic TCP (2)"**	1	ossim-sensor.infosec.uga.edu	2012-05-01 10:05:24	2012-05-01 10:05:24	1.9	128.192.1
12	**AV Malware, spyware Fun Web Products Agent detected on 172.20.136.127** [5 events]	2	ossim-sensor.infosec.uga.edu	2012-05-01 10:02:34	2012-05-01 10:02:35	172.20	173.19

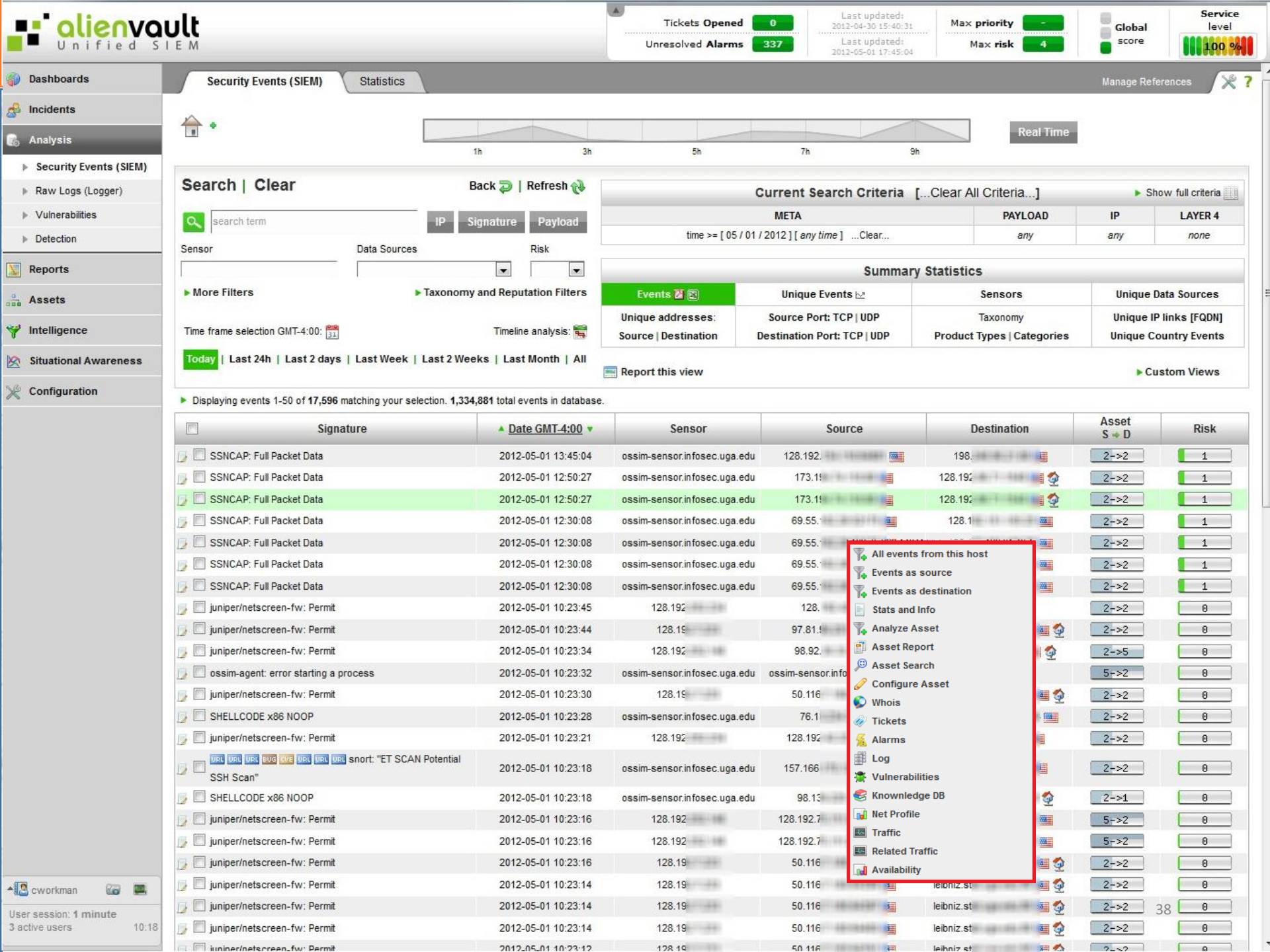
Resulting Actions

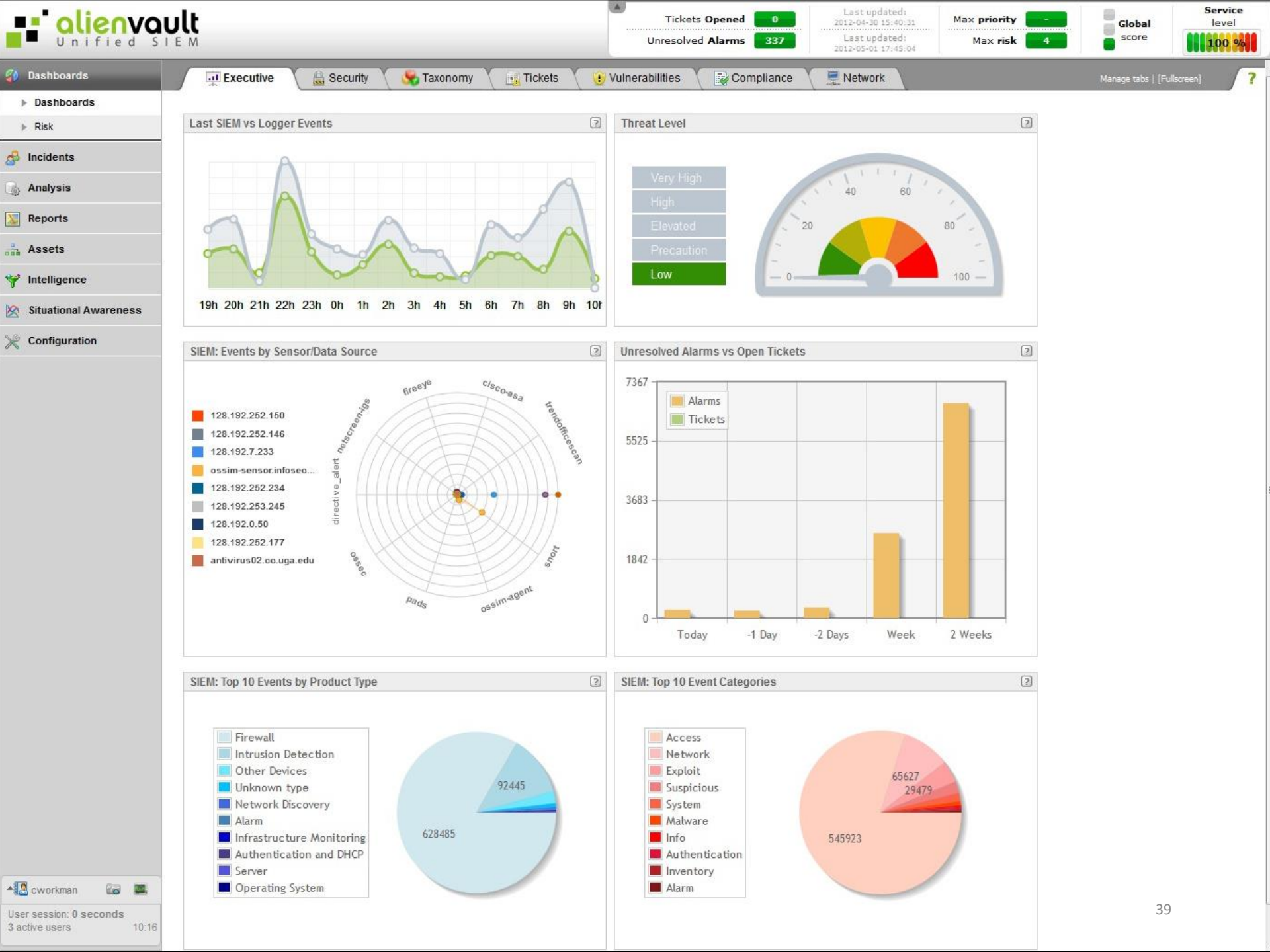
Notice of incident sent to department or student

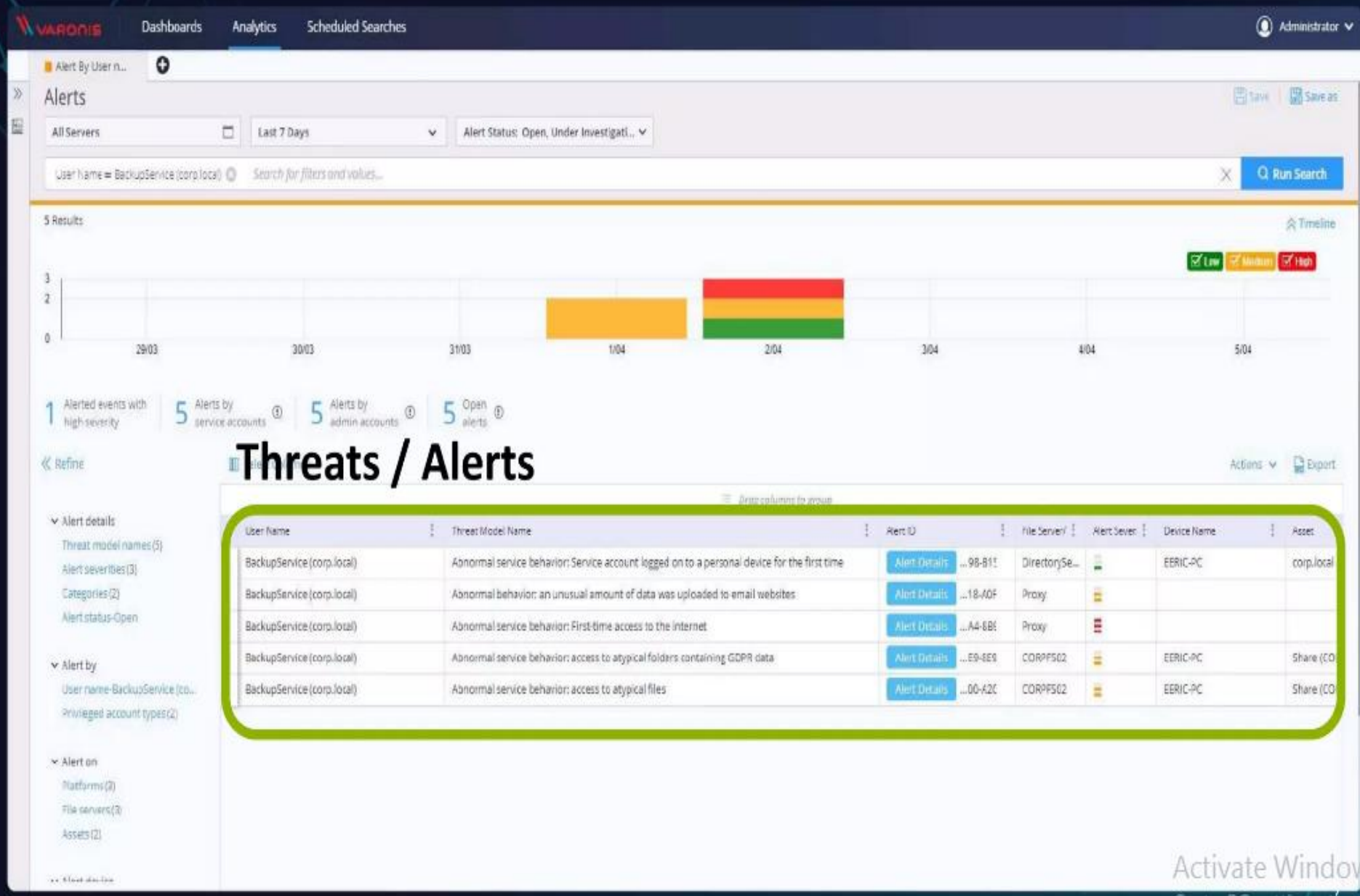
Repeat offenders blocked

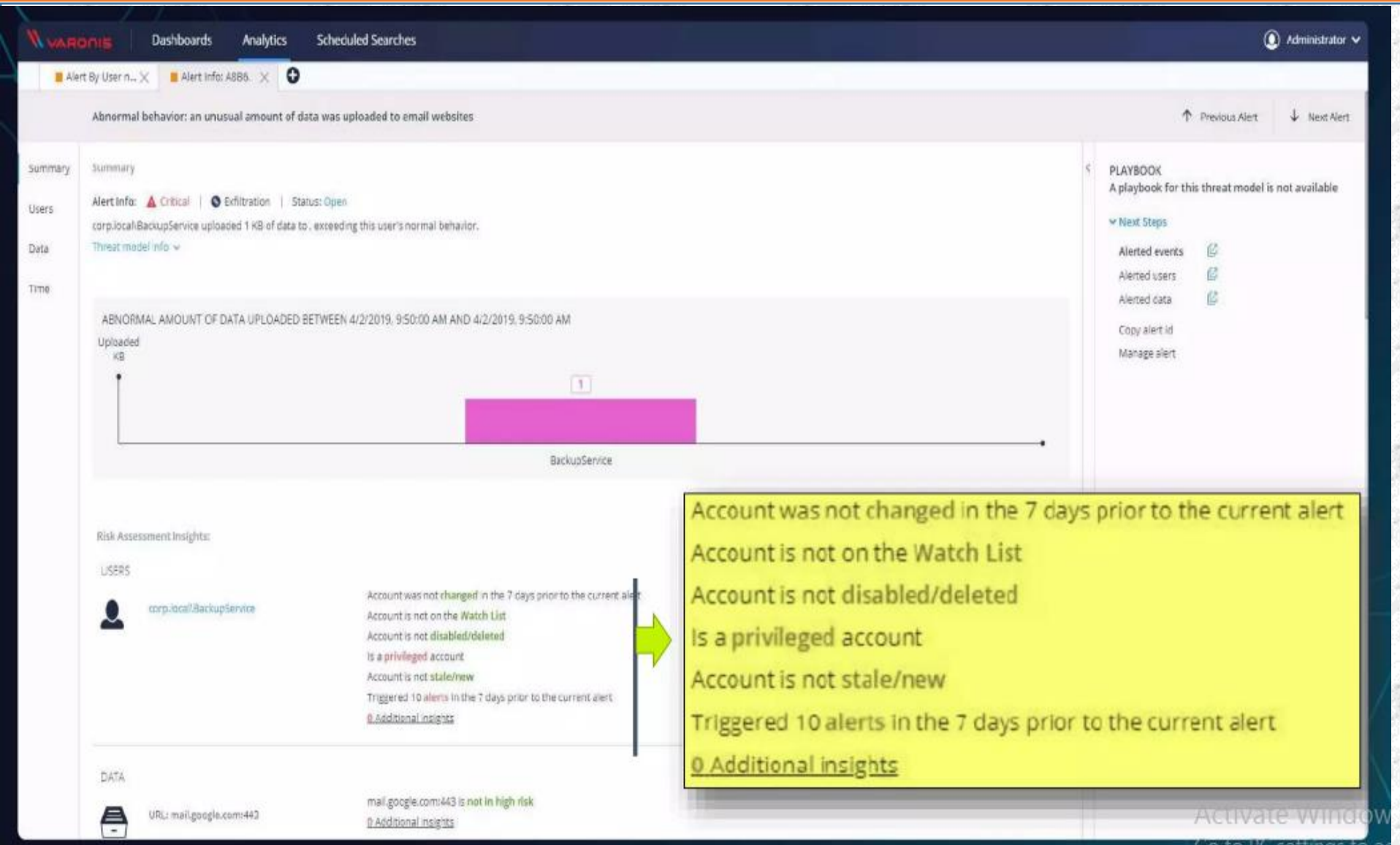
SOC Incident Response Team handles critical incidents

- Containment
- Remediation
- Resolution
- Closure


alienvault Unified SIEM
Tickets Opened 0
Unresolved Alarms 337
Last updated: 2012-04-30 15:40:31
Last updated: 2012-05-01 17:45:04
Max priority -
Max risk 4
Global score
Service level 100 %
Dashboards
Incidents
Analysis
Security Events (SIEM)
Raw Logs (Logger)
Vulnerabilities
Detection
Reports
Assets
Intelligence
Situational Awareness
Configuration
Security Events (SIEM)
Statistics
Manage References
1h 3h 5h 7h 9h
Real Time
Search | Clear
Back | Refresh
search term
IP
Signature
Payload
Sensor
Data Sources
Risk
More Filters
Taxonomy and Reputation Filters
Time frame selection GMT-4:00:
Timeline analysis:
Today | Last 24h | Last 2 days | Last Week | Last 2 Weeks | Last Month | All
Current Search Criteria [...Clear All Criteria...]
Show full criteria
META
PAYLOAD
IP
LAYER 4
time >= [05 / 01 / 2012] [any time] ...Clear...
any
any
none
Summary Statistics
Events
Unique Events
Sensors
Unique Data Sources
Unique addresses: Source | Destination
Source Port: TCP | UDP
Destination Port: TCP | UDP
Taxonomy
Product Types | Categories
Unique IP links [FQDN]
Unique Country Events
Report this view
Custom Views
Displaying events 1-50 of 17,596 matching your selection. 1,334,881 total events in database.
Signature
Date GMT-4:00
Sensor
Source
Destination
Asset S → D
Risk
SSNCAP: Full Packet Data 2012-05-01 13:45:04 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:50:27 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:50:27 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:30:08 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:30:08 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:30:08 ossim-sensor.infosec.uga.edu 2->2 1
SSNCAP: Full Packet Data 2012-05-01 12:30:08 ossim-sensor.infosec.uga.edu 2->2 1
juniper/netscreen-fw: Permit 2012-05-01 10:23:45 2->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:44 2->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:34 2->5 0
ossim-agent: error starting a process 2012-05-01 10:23:32 ossim-sensor.infosec.uga.edu 5->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:30 2->2 0
SHELLCODE x86 NOOP 2012-05-01 10:23:28 ossim-sensor.infosec.uga.edu 2->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:21 2->2 0
snort: "ET SCAN Potential SSH Scan" 2012-05-01 10:23:18 ossim-sensor.infosec.uga.edu 2->2 0
SHELLCODE x86 NOOP 2012-05-01 10:23:18 ossim-sensor.infosec.uga.edu 2->1 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:16 5->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:16 5->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:16 2->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:14 2->2 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:14 2->2 38 0
juniper/netscreen-fw: Permit 2012-05-01 10:23:14 2->2 0
All events from this host
Events as source
Events as destination
Stats and Info
Analyze Asset
Asset Report
Asset Search
Configure Asset
Whois
Tickets
Alarms
Log
Vulnerabilities
Knowledge DB
Net Profile
Traffic
Related Traffic
Availability
cworkman
User session: 1 minute
3 active users
10:18


alienvault
Unified SIEM
Tickets Opened 0
Unresolved Alarms 337
Last updated: 2012-04-30 15:40:31
Last updated: 2012-05-01 17:45:04
Max priority -
Max risk 4
Global score
Service level
100 %
Dashboards
Dashboards
Risk
Incidents
Analysis
Reports
Assets
Intelligence
Situational Awareness
Configuration
Executive
Security
Taxonomy
Tickets
Vulnerabilities
Compliance
Network
Manage tabs | [Fullscreen]
Last SIEM vs Logger Events
19h 20h 21h 22h 23h 0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h
Threat Level
Very High
High
Elevated
Precaution
Low
0
20
40
60
80
100
SIEM: Events by Sensor/Data Source
128.192.252.150
128.192.252.146
128.192.7.233
ossim-sensor.infosec...
128.192.252.234
128.192.253.245
128.192.0.50
128.192.252.177
antivirus02.cc.uga.edu
fireeye
cisco-asa
trendofficescan
snort
ossim-agent
pads
ossec
directive_alert
netscreen-idp
Unresolved Alarms vs Open Tickets
7367
5525
3683
1842
0
Alarms
Tickets
Today
-1 Day
-2 Days
Week
2 Weeks
SIEM: Top 10 Events by Product Type
Firewall
Intrusion Detection
Other Devices
Unknown type
Network Discovery
Alarm
Infrastructure Monitoring
Authentication and DHCP
Server
Operating System
92445
628485
SIEM: Top 10 Event Categories
Access
Network
Exploit
Suspicious
System
Malware
Info
Authentication
Inventory
Alarm
65627
29479
545923
cworkman
User session: 0 seconds
3 active users
10:16



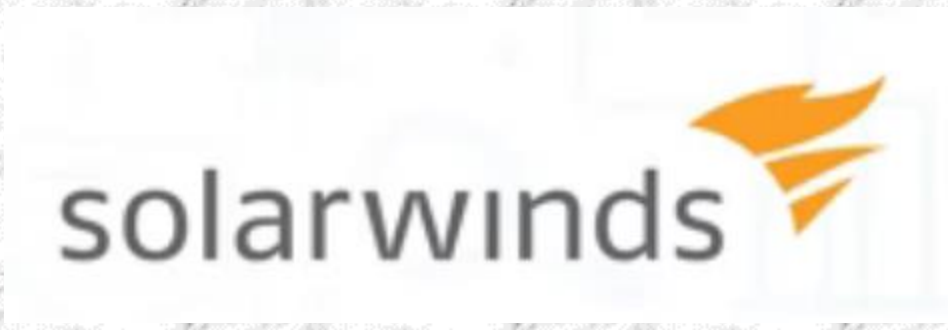

VARONIS
Dashboards
Analytics
Scheduled Searches
Administrator
Alert By User n...
Alert Info: A886
Abnormal behavior: an unusual amount of data was uploaded to email websites
Previous Alert
Next Alert
Summary
Users
Data
Time
Summary
Alert Info: Critical | Exfiltration | Status: Open
corp.local\BackupService uploaded 1 KB of data to . exceeding this user's normal behavior.
Threat model info
ABNORMAL AMOUNT OF DATA UPLOADED BETWEEN 4/2/2019, 9:50:00 AM AND 4/2/2019, 9:50:00 AM
Uploaded
KB
1
BackupService
PLAYBOOK
A playbook for this threat model is not available
Next Steps
Alerted events
Alerted users
Alerted data
Copy alert id
Manage alert
Risk Assessment Insights:
USERS
corp.local\BackupService
Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Is a privileged account
Account is not stale/new
Triggered 10 alerts in the 7 days prior to the current alert
0 Additional insights
DATA
URL: mail.google.com:443
mail.google.com:443 is not in high risk
0 Additional insights
Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Is a privileged account
Account is not stale/new
Triggered 10 alerts in the 7 days prior to the current alert
0 Additional insights

Use Cases with SIEM

- ✓ Inbound/outbound suspicious activities
- ✓ Event correlation for advanced threats
- ✓ DDOS attacks
- ✓ Unauthorised remote access
- ✓ Critical service monitoring
- ✓ Malware monitoring
- ✓ IP Reputations
- ✓ Risk & Compliance
- ✓ Security Threats analysis

SIEM Tools

1. Small and Medium Sized Businesses – Solar Winds



2. Event Driven Security – Enterprise size

3. Data Enrichment

4. IBM Qradar – Sophisticated Coorelation engine

5. exabeam– small businesses

Source: https://youtu.be/3JVJy35VdW4

UEBA (User & Entity Behavior Analytics) Tools

UEBA can be defined as a security solution that analyzes the behaviors of people that are connected to an organization's network and entities or end-points such as servers, applications, etc. to figure out the anomalies in the security.

UEBA uses behavioral analysis to monitor the activities of the users and entities.

It keeps a track of where do people usually log in from and what applications or file servers they use, what is their degree of access, etc.

UEBA then correlates this information to gauge if a certain activity performed by the users is different from their daily tasks and establishes a baseline of what is usual behavior.

If something unusual happens that doesn't comply with the baseline, UEBA detects it and sends alerts of the probable threat.

Advantages of UEBA

- Provides behavior based analytics for detecting insider and targeted cyber attacks.
- User centric monitoring across hosts, network and applications.
- Privileged account monitoring and misuse detection
- Provides huge reduction in security events warranting investigations.

Benefits of UEBA

- Detection of hijacked accounts
- Reduced attack surface
- Privilege Abuse and Misuse
- Improved Operational Efficiency
- Data Exfiltration Detection

BENEFITS OF USER ENTITY BEHAVIOR ANALYTICS (UEBA)

- **Detection of hijacked accounts** - Attackers who steal valid user credentials behave differently than real users. UEBA uses real-time detection to ascertain if something is out of norm and responds to the threat through various real-time responses such as Block, Modify, Re-authenticate or Multi-factor authentication. This ensures that the real threats are getting addressed before they try to harm the system.

- **Reduced Attack Surface** - UEBA sends insights to the users and the security teams through interactive analytics which allows them to know about the loopholes or weak points before an incident happens. These insights help reduce the attack surface which makes it difficult for the cyber attacker to breach the network.

- **Privilege Abuse and Misuse** - In any organization the privileged users have extensive access to the system, data and applications which is why they present a higher risk to the organization. UEBA's algorithms ensure that the access rights are used appropriately and give an overview of what kind of privileges individual users should have.

- **Improved Operational Efficiency** - It takes a lot of efforts to identify threats manually through alerts. UEBA can manually identify and validate threat without manual intervention through automation and security intelligence. This level of automation allows security to focus on real threats rather than alert chasing.
- **Data Exfiltration detection** - UEBA analytics help to detects potential data exfiltration before it happens, thus allowing businesses time to prepare a strategic plan to prevent data theft. It can even help identify Advanced Persistent Threats (APT).

UEBA has proved itself to be an indispensible asset in the world of cyber security. According to experts user and entity behavior analytics is a better model for attack detection and maintain that it is going to enable more accurate detection of cyber attackers threatening networks.

Data Sets for Analytics

Core Data

- Netflow
- HTTP traffic or Web proxy Logs
- DNS traffic or DNS Logs
- AD Logs

User-Hostname-IP Mapping

- DHCP
- VPN
- AD Logs
- Aruba Clearpass

System Data

- Windows system logs from critical servers
- Linux audit and system logs
- Other server/app logs: DB, git, web server

Data Enrichment

- GeoIP
- ASN
- Threat Intel

Case Study – HP Enterprise Worldwide network*

Scale of Core Data Sets

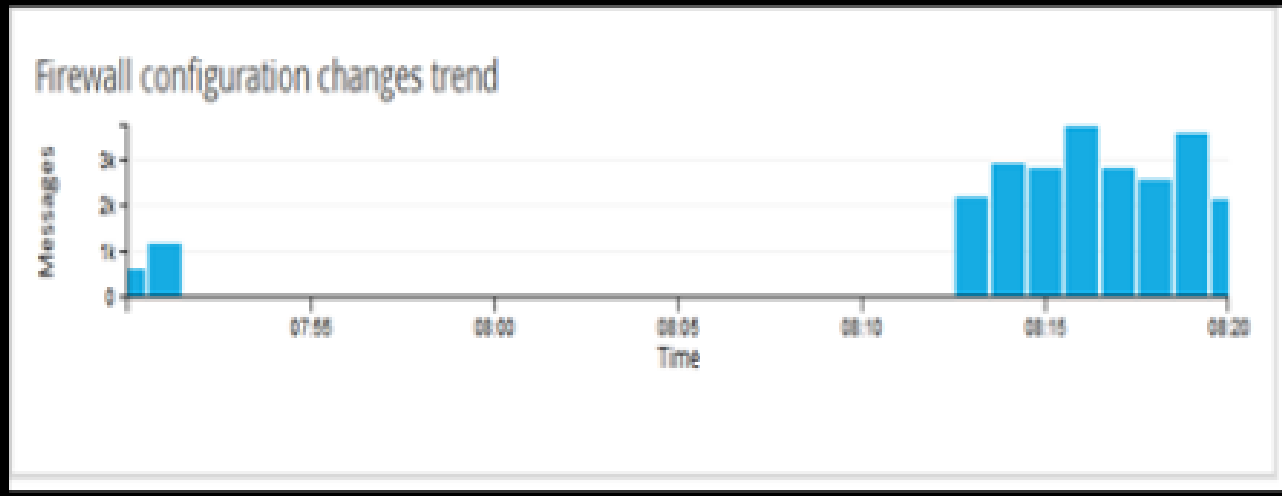
Volume and Size within HPE worldwide network

Data Type	# Events/day (after filtering)	TB/day	Avg Event Size
Netflow	**34 Billion** (3 collection points)	3.40 TB	100 B
DNS	**150 Million** (4 collection points)	0.15 TB	1 KB
HTTP	**65 Million** (central collection)	0.13 TB	2 KB
AD	**153 Million**		
TOTAL	~ 35 Billion/day	~ 3.7 TB/day	

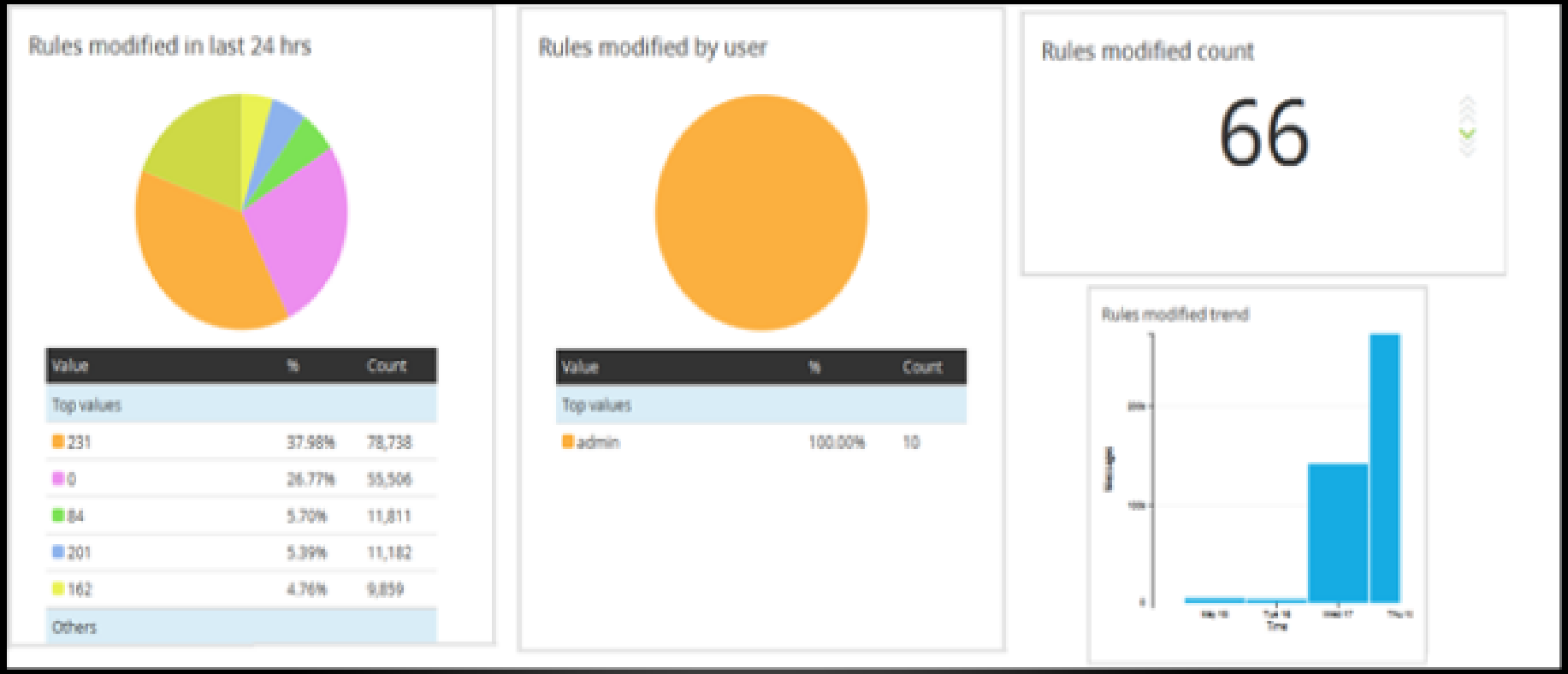
*2016

USE CASES

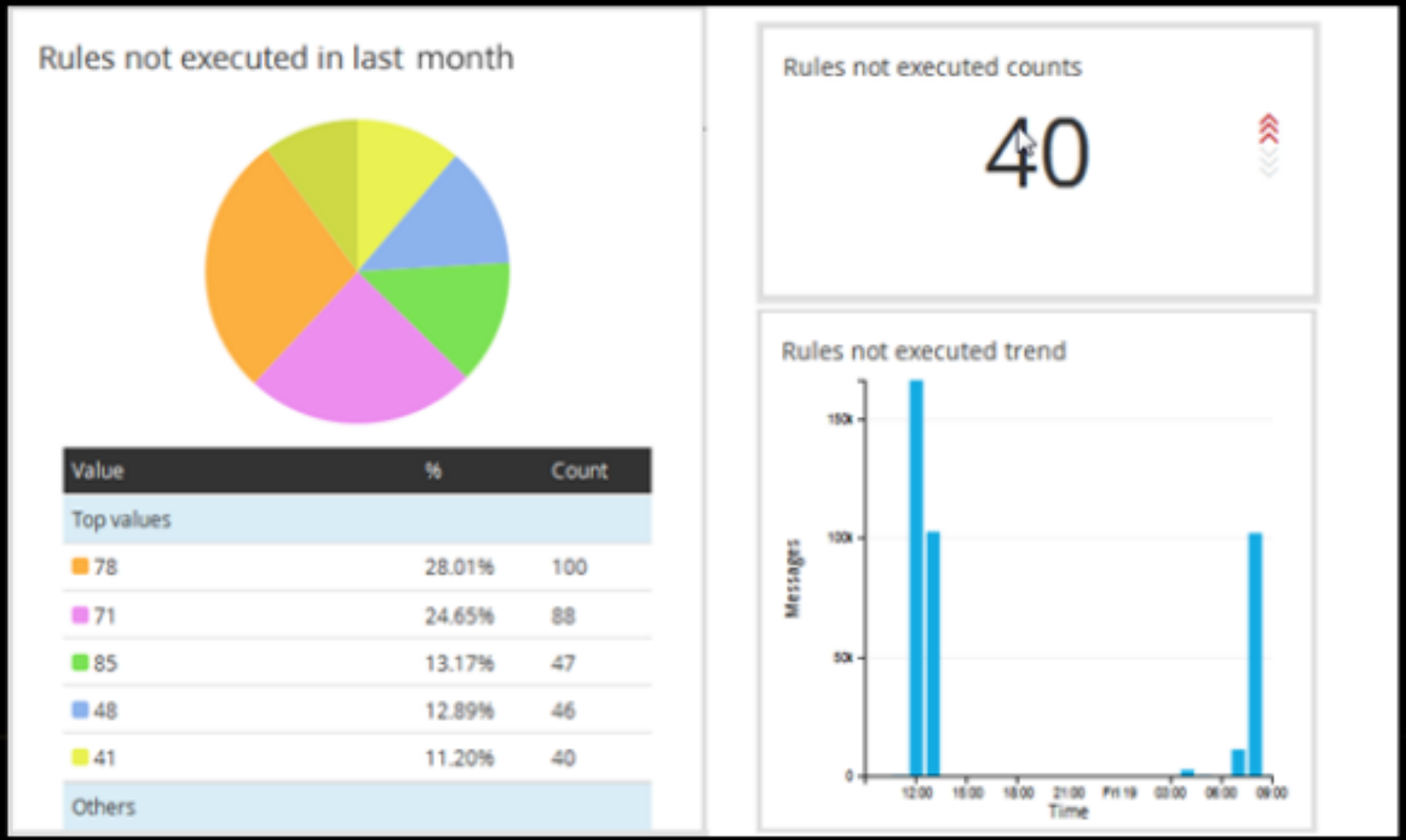
- **Firewall configuration analytics-** Keep an eye on the changes being made to the network security infrastructure. Administrators may make some intentional or unintentional error or carry out an improper change while acting on a firewall configuration change request giving room for breaches. This Firewall Change Management report precisely helps in detecting such events. It helps find out 'who' made 'what' changes, 'when' and 'why'. Not only that, it alerts you in real-time on your mobile phone when changes happen. The Firewall change management can generates alerts for the Firewall device configuration changes in real-time and it notifies via Email, HTTP alerts.



- **Rules created / modified in a particular time span-** This will help to analyze the rules crated / modified in a particular time frame. i.e. : last 24 hours. This will be useful to monitor administrator activity on day to day basis and would be very effective to find such occurrences. Tracking the number of rules modified within a particular time span can ensure no security mishap.

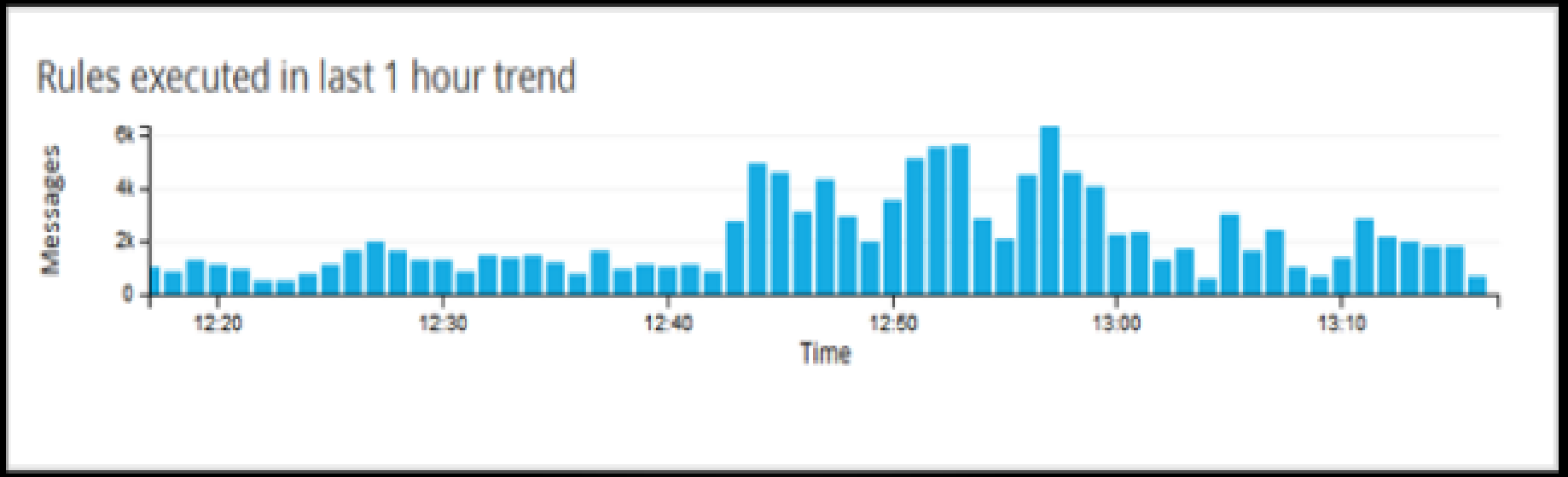


- **Rules not executed in a particular time span-** Administrator creates lot of rules on need basis and forgets to remove them if not required. After a certain period of time, we will be having a huge set of rules in firewall which may not be even executing for a long period time. This report would help to find such rules which can be removed from the system and can help the administrator to manage the system more efficiently.



VISIBILITY

- The system provides trend of events happening over a period of time which would help the system analyst to understand the behavior of such events and can predict the trends of such occurrence. This would prove very helpful in finding or investigating critical system issues.

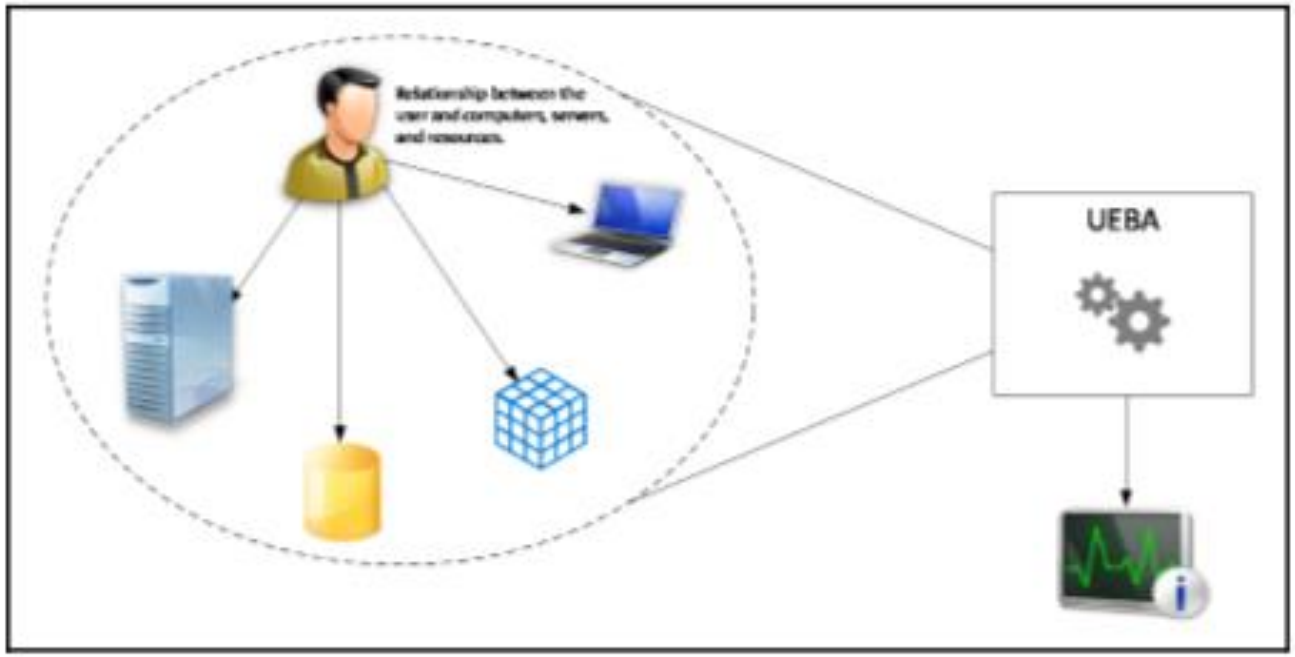


Behavior Analytics on-Premises

The core business still happens on-premises.
There is where the critical data is located, the majority of the users are working, and the key assets are located.
The attacker tends to silently infiltrate/intrude your on-premises network, move laterally, escalate privilege, and maintain connectivity with command and control until he/she is able to execute his/her mission.
For this reason, having behavior analytics on premises is imperative to **quickly break the attack kill chain.**

According to Gartner, it is primal to **understand how users behave**, and by tracking legitimate processes, organizations can enlist User and Entity Behavior Analytics (UEBA) **to spot security breaches**.

There are many advantages in using an UEBA to detect attacks, but one of the most important ones is ***the capability to detect attacks in the early stages*** and take corrective action to contain the attack.



- UEBA system on premises knows what servers your users usually access, what shares they usually visit, what operating system they usually use to access these resources, and the user's geo-location.

Having a UEBA system on-premises can help the Blue Team to be more proactive, and have more tangible data to accurately react.

The UEBA system is composed of multiple modules and another module is the advanced threat detection, which looks for known vulnerabilities and attack patterns.

Behavior Analytics in a hybrid cloud

In a hybrid cloud, most companies will opt to use an IaaS model and, although IaaS adoption is growing, the security aspect of it is still the main concern, according to an Oracle survey on IaaS Adoption.

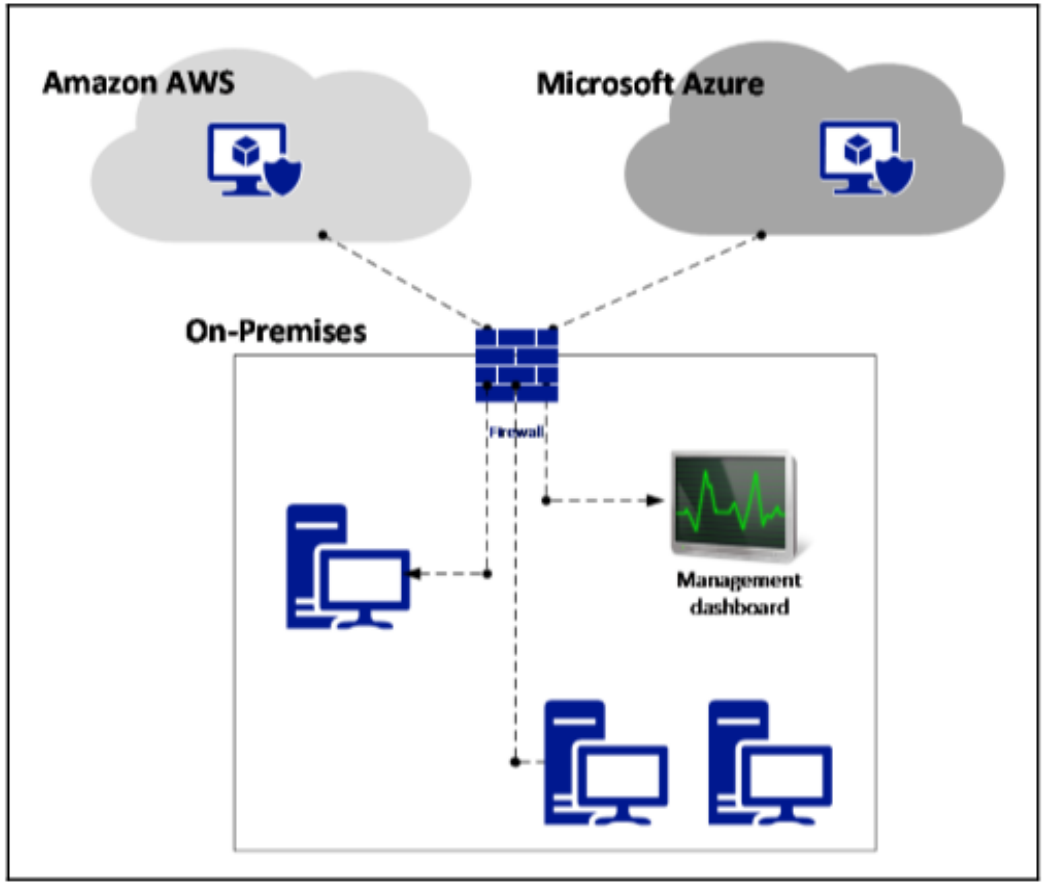
The intent is to leverage hybrid cloud capabilities to benefit the overall security posture. The first step is to establish a good partnership with your cloud provider and understand what security capabilities they have, and how these security capabilities can be used in a hybrid environment.

This is important, because some capabilities are only available in the cloud, and not on-premises.

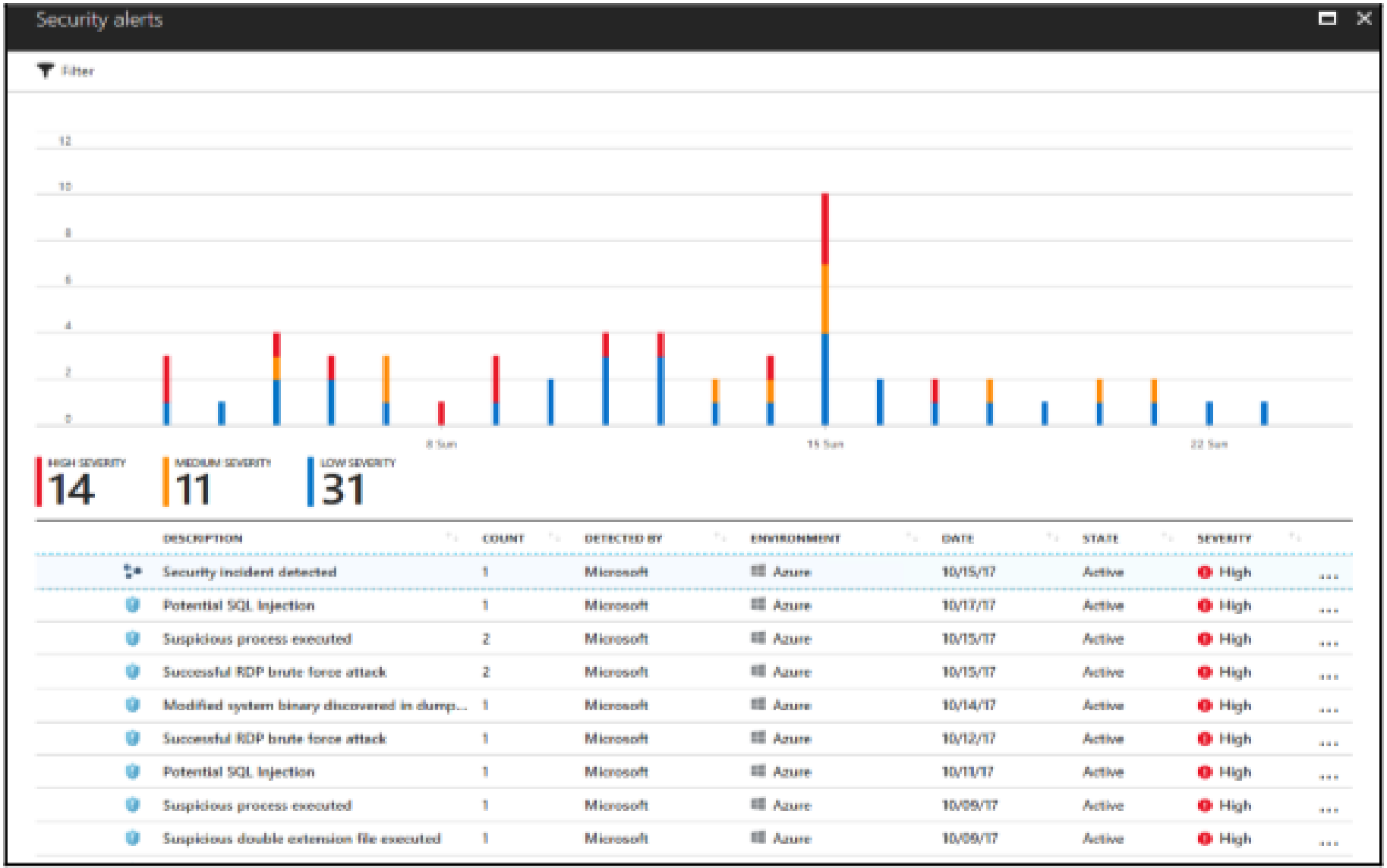
Azure Security Center – Illustration only

The reason we are using Azure Security Center to monitor hybrid environment is because the Security Center agent can be installed on a computer (Windows or Linux) on-premises, in a VM running in Azure, or in AWS.

When the Security Center is installed on these computers, it will collect Event Tracing for Windows (ETW) traces, operating system log events, running processes, machine name, IP addresses, and logged in users. These events are sent to Azure, and stored in your private workspace storage. Security Center will analyze this data using the following methods: Threat intelligence Behavioral analytics Anomaly detection



Once this data is evaluated, Security Center will trigger an alert based on priority and add in the dashboard, as shown in the following screenshot:



DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	Azure	10/15/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/17/17	Active	High
Suspicious process executed	2	Microsoft	Azure	10/15/17	Active	High
Successful RDP brute force attack	2	Microsoft	Azure	10/15/17	Active	High
Modified system binary discovered in dump...	1	Microsoft	Azure	10/14/17	Active	High
Successful RDP brute force attack	1	Microsoft	Azure	10/12/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/11/17	Active	High
Suspicious process executed	1	Microsoft	Azure	10/09/17	Active	High
Suspicious double extension file executed	1	Microsoft	Azure	10/09/17	Active	High

Behavior Analytics Device Placement

The location where you will install your UEBA will vary according to the company's needs and the vendor's requirements.

UEBA Tools

Log360 is a SIEM solution that helps combat threats on premises, in the cloud, or in a hybrid environment.

ManageEngine Log360

UEBA Trends

LogRhythm

Microsoft Sentinel

Splunk

eSecurity Planet

Fortinet

Cynet

Gurucul UEBA

Exabeam

Rapid7

Many More....

EDR (Endpoint Detection & Response) Tools

Endpoint detection and response tools are a central component of a modern endpoint security strategy because they are the most effective means of detecting intrusions. They monitor the target environment to identify attacks and collect telemetry data to support rapid triage and investigative processes.

What are EDR Tools?

EDR tools are technology platforms that can alert security teams of malicious activity, and enable fast investigation and containment of attacks on endpoints. An endpoint can be an employee workstation or laptop, a server, a cloud system, a mobile or IoT device.

Endpoint Detection and Response (EDR)

Endpoint Data Recording	Investigation of Data & Responding
• Network, event, process, files, commands, operation, etc.	**Sweep** (search) for indicators of Compromise to understand the impact of detections
• Many telemetry data points	Find the **root cause** of a detection and remediate/prevent/invastigate again
• Stored on endpoints or in server, or a hybrid approach	**Hunt** for indicators pf Attack based on behavior rules or threat intelligence. Automatic (**detection**) or manual

Endpoint Detection and Response (EDR) is a new security category defined by Gartner in 2013. It fills an important gap in protection of endpoints, helping security teams gain visibility into malicious activity on an endpoint, and remotely control endpoints to contain and mitigate attacks.

EDR solutions typically aggregate data on endpoints including process execution, endpoint communication, and user logins;

Analyse data to discover anomalies and malicious activity; and record data about malicious activity, enabling security teams to investigate and respond to incidents.

In addition, they enable automated and manual actions to contain threats on the endpoint, such as isolating it from the network or wiping and reimaging the device.

Unlocking the Black Box of Endpoint Protection:

On modern networks there is an explosion in the number of endpoints, including physical and virtual workstations, servers, and cloud machine instances. Each endpoint is potentially vulnerable to attack, but security teams have limited access to endpoints, limited visibility into malicious activity taking place on an endpoint, and limited ability to reach out to an endpoint to investigate and contain an attack.

EDR is a subset of cyber security that enables security teams to investigate and mitigate security threats on endpoints. EDR security solutions are a last line of defense against attackers who have already breached endpoints. They can help defend against severe threats like multi stage attacks, fileless malware, and malicious insiders.

EDR vs SIEM:

Gartner defines endpoint detection and response (EDR) as a solution for recording endpoint-system-level behaviors, detecting suspicious behavior in a system, and providing information in context about incidents. Security information and event management (SIEM) offers enterprises detection, analysis, and alerting for security events.

What is the Difference Between EDR and Antivirus?

Antivirus software can stop threats based on malware, but is not effective against other types of threats. It also cannot protect against malware that evades detection. EDR is able to detect and respond to threats that evade antivirus and other traditional defenses on the endpoint device.

Security Center can integrate with many other solutions, such as Barracuda, F5, Imperva, and Fortinet for web application firewall (WAF), among others for endpoint protection, vulnerability assessment, and next-generation firewall.

EDR Features:

- **Threat examination**—shows entire process tree, timeline, and all malicious activity across machines for each process
- **Third party alerts**—combines EDR data with alerts from firewall and SIEM tools
- **Attack full scope**—see all related attack elements, including root cause, affected machines and users, incoming and outgoing communications, attack timeline
- **Customization**—custom rules and behavioral whitelisting
- **Guided remediation**—execute commands from a complete remediation toolbox on the endpoint, enables access to remote shell
- **Enterprise-wide remediation**—responds to threats affecting many machines, by executing remediation actions on all affected machines in one step

EDR Tools*

Cybereason

FireEye

Symantec

Cynet Security Platform

CrowdStrike Falcon

FireEye

RSA NetWitness Endpoint

SOAR (**Security Orchestration, Automation and Response) Tools**

SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

SOAR (security orchestration, automation and response) is a stack of compatible software programs that enables an organization to collect data about security threats and respond to security events without human assistance. The goal of using a SOAR platform is to improve the efficiency of physical and digital security operations.

SOAR platforms have three main components:

- security orchestration,
- security automation and
- security response.

Security orchestration

- Security orchestration connects and integrates disparate internal and external tools via built-in or custom integrations and application programming interfaces (APIs).

- Connected systems may include vulnerability scanners, endpoint protection products, end-user behavior analytics, firewalls, intrusion detection and intrusion prevention systems (IDSes/IPSes), and security information and event management (SIEM) platforms, as well as external threat intelligence feeds.

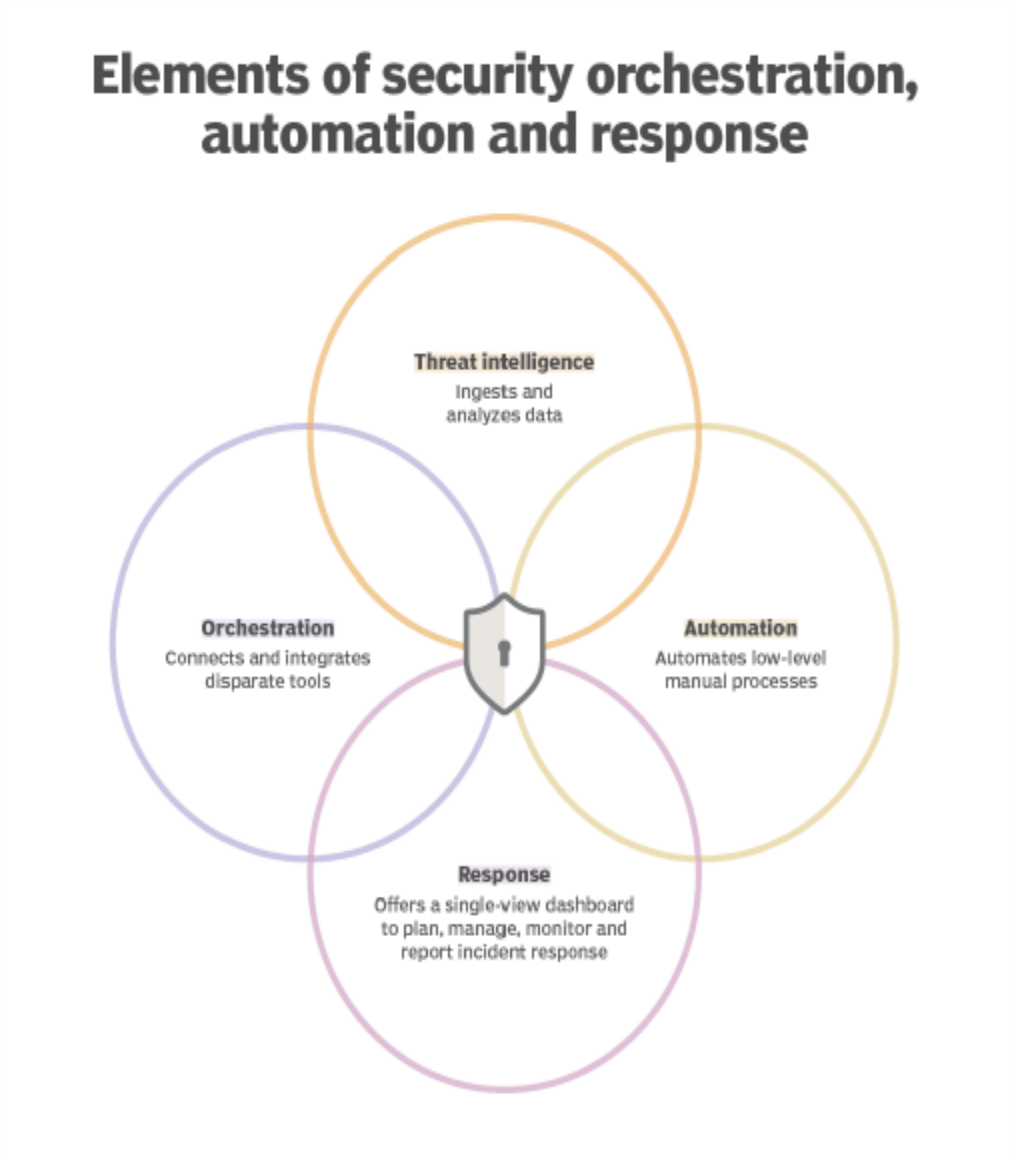
- With all the data gathered comes a better chance at detecting threats, along with more thorough context and improved collaboration. The tradeoff, however, is more alerts and more data to ingest and analyze. Where security orchestration consolidates data to initiate response functions,

Security automation

- Security automation, fed by the data and alerts collected from security orchestration, ingests and analyzes data and creates repeated, automated processes to replace manual processes.
- Tasks previously performed by analysts, such as vulnerability scanning, log analysis, ticket checking and auditing capabilities, can be standardized and automatically executed by SOAR platforms.
- Using artificial intelligence (AI) and machine learning to decipher and adapt insights from analysts, SOAR automation can make recommendations and automate future responses. Alternately, automation can elevate threats if human intervention is needed.

Security response

- Security response offers a single view for analysts into the planning, managing, monitoring and reporting of actions carried out once a threat is detected.
- It also includes post-incident response activities, such as case management, reporting and threat intelligence sharing.



Benefits of SOAR

SOAR platforms offer many benefits for enterprise security operations (SecOps) teams, including the following:

Faster incident detection and reaction times. The volume and velocity of security threats and events are constantly increasing. SOAR's improved data context, combined with automation, can bring lower mean time to detect (MTTD) and mean time to respond (MTTR). By detecting and responding to threats more quickly, their impact can be lessened.

Better threat context. By integrating more data from a wider array of tools and systems, SOAR platforms can offer more context, better analysis and up-to-date threat information.

Simplified management. SOAR platforms consolidate various security systems' dashboards into a single interface. This helps SecOps and other teams by centralizing information and data handling, simplifying management and saving time.

Scalability. Scaling time-consuming manual processes can be a drain on employees and even impossible to keep up with as security event volume grows. SOAR's orchestration, automation and workflows can meet scalability demands more easily.

Boosting analysts' productivity. Automating lower-level threats augments SecOps and security operations center (SOC) teams' responsibilities, enabling them to prioritize tasks more effectively and respond to threats that require human intervention more quickly.

Streamlining operations. Standardized procedures and playbooks that automate lower-level tasks enable SecOps teams to respond to more threats in the same time period. These automated workflows also ensure the same standardized remediation efforts are applied organization-wide across all systems.

Reporting and collaboration.

SOAR platforms' reporting and analysis consolidate information quickly, enabling better data management processes and better response efforts to update existing security policies and programs for more effective security.

A SOAR platform's centralized dashboard can also improve information sharing across disparate enterprise teams, enhancing communication and collaboration.

Lowered costs.

In many instances, augmenting security analysts with SOAR tools can lower costs, as opposed to manually performing all threat analysis, detection and response efforts.

SOAR challenges

- SOAR is not a silver bullet technology, nor is it a standalone system. SOAR platforms should be part of a defense-in-depth security strategy, especially as they require the input of other security systems to successfully detect threats.
- SOAR is not a replacement for other security tools, but rather is a complementary technology. SOAR platforms are also not a replacement for human analysts, but instead augment their skills and workflows for more effective incident detection and response.
- Some **other potential drawbacks of SOAR** include the following:
- failure to remediate a broader security strategy;
- conflated expectations;
- deployment and management complexity; and
- lack of or limited metrics.

Benefits and drawbacks of SOAR tools

Benefits

- Improves productivity
- Builds risk resilience
- Faster incident response
- Centralized management of multivendor tools
- Alleviates alert fatigue
- Streamlines processes and operations

Drawbacks

- Cannot fix security strategy or culture
- Overinflated expectations
- Limited success metrics
- Undervalues human analysts
- Diverts resources for staff to technology

Important SOAR capabilities

The term, coined by Gartner in 2015, initially stood for ***security operations, analytics and reporting***. It was later updated to its current form in 2017, with Gartner defining **SOAR's three main capabilities as the following:**

- threat and vulnerability management technologies that support the remediation of vulnerabilities, providing formalized workflow, reporting and collaboration capabilities;
- security incident response technologies that support how an organization plans, manages, tracks and coordinates the response to a security incident; and
- security operations automation technologies that support the automation and orchestration of workflows, processes, policy execution and reporting

- Gartner expanded the definition further, refining SOAR's technology convergence to the following:
- security incident response platforms, which include capabilities such as vulnerability management, case management, incident management, workflows, incident knowledge base, auditing and logging capabilities, reporting and more;
- security orchestration and automation, which include integrations, workflow automation, playbooks, playbook management, data gathering, log analysis and account lifecycle management; and
- threat intelligence platforms, which include threat intelligence aggregation, analysis and distribution, alert context enrichment and threat intelligence visualization.

- **SOAR vs. SIEM**
- While SOAR and SIEM platforms both aggregate data from multiple sources, the terms are not interchangeable. SIEM systems collect data, identify deviations, rank threats and generate alerts. SOAR systems also handle these tasks, but they have additional capabilities. First, SOAR platforms integrate with a wider range of internal and external applications, both security and nonsecurity. Second, whereas SIEM systems only alert security analysts of a potential event, SOAR platforms use automation, AI and machine learning to provide greater context and automated responses to those threats.
- Many companies use SOAR services to augment in-house SIEM software. In the future, SIEM vendors are expected to add SOAR capabilities to their services, which means the market for these two product lines will merge.
- Many SIEM vendors offer SOAR capabilities in their SIEM products. Other products, such as email security gateways, endpoint detection and response (EDR), network detection and response (NDR) and extended detection and response (XDR), are also adopting SOAR capabilities.

SOAR vendors *

Gartner's 2020 SOAR market guide provides a list of representative vendors and their products, including the following:

Anomali ThreatStream
Cyware Virtual Cyber Fusion Center
D3 Security D3 SOAR
DFLabs IncMan SOAR
EclecticIQ Platform
FireEye Helix
Fortinet FortiSOAR
Honeycomb SOCAutomation
IBM Security Resilient
LogicHub SOAR+
Micro Focus ArcSight SOAR
Palo Alto Networks Cortex XSOAR
Rapid7 InsightConnect
ServiceNow Security Operations
Siemplify SOAR Platform
Splunk Phantom
Swimlane SOAR
ThreatConnect SOAR Platform
ThreatQuotient ThreatQ
Tines

*2021

Encryption Tools

Strong encryption standards – the industry standard for encryption today is **Advanced Encryption Standard (AES) with a 256-bit key**.

AES 256-bit encryption is the strongest and most robust encryption standard that is commercially available today. While it is theoretically true that AES 256-bit encryption is harder to crack than AES 128-bit encryption, AES 128-bit encryption has never been cracked.

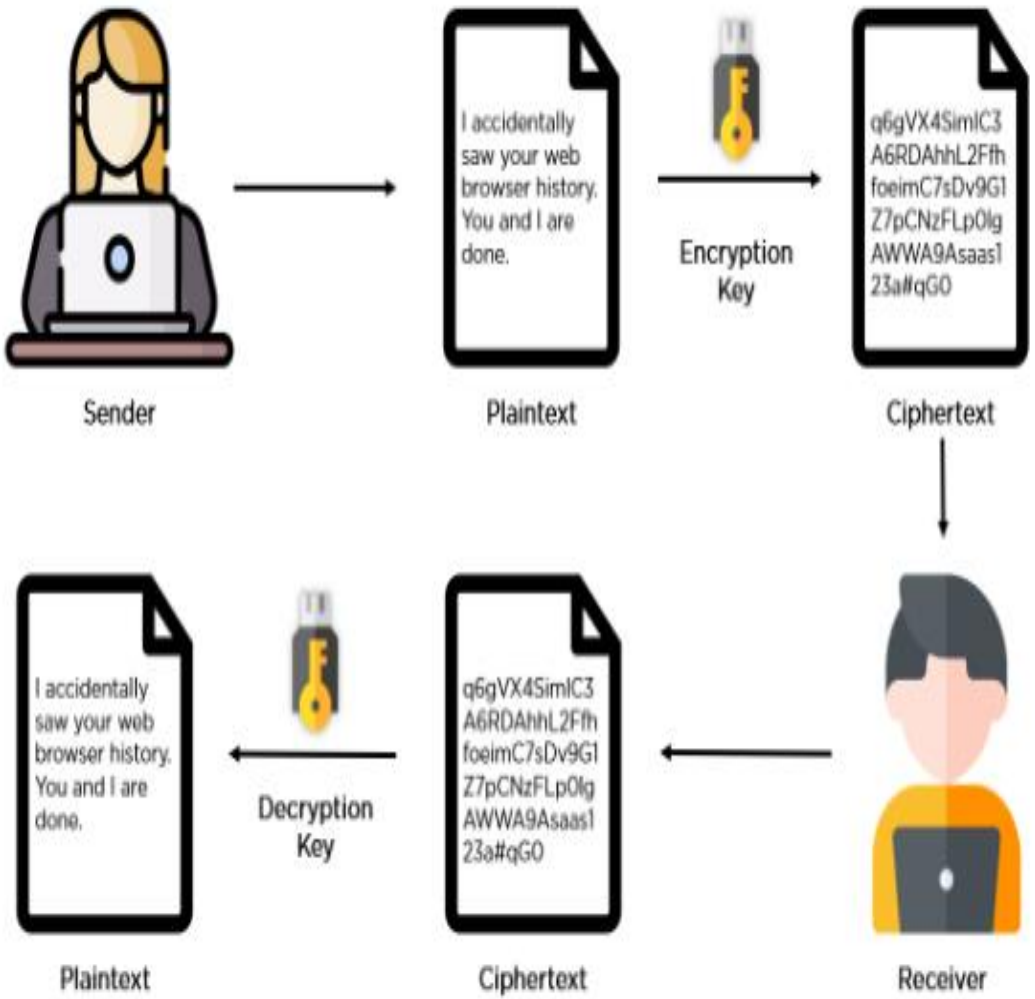
3 types of encryption devices:

3 Types of Encryption to Protect Your Data

- **Symmetric.** The symmetric encryption method uses a single key both to encrypt and decrypt the data. ...
- **Asymmetric.** The second major encryption method is asymmetric encryption, also sometimes known as public key encryption. ...
- **Hashing.** Hashing generates a unique signature of fixed length for a data set or message.

Best Encryption Algorithms*

- AES. The Advanced Encryption Standard (AES) is the trusted standard algorithm used by the United States government, as well as other organizations. ...
- Triple DES. ...
- RSA. ...
- Blowfish. ...
- Twofish. ...
- Rivest-Shamir-Adleman (RSA).



- Encryption Explained
- https://youtu.be/LA3fah6i-4A

Virtru makes military-grade encryption easy and affordable. We equip organizations of all sizes to take control of their data with flexible, end-to-end encryption for data flowing in and out of your business.

Using the Best Encryption Software

1. AxCrypt
2. CryptoExpert
3. CertainSafe
4. VeraCrypt -is an open-source encryption program that runs on multiple operating systems. It conceals encrypted data twice, hiding encrypted datasets within another dataset, using a single encryption key thanks to AES support. As it is an open-source tool, you can also change or upgrade the tool whenever you want. Source: Google*
5. Folder Lock
6. Boxcryptor
7. NordLocker
8. CryptoForge
9. Advanced Encryption Package

What is IRT (Incident Response) Tools

Incident Response and Malware Analysis will assist you gauge the influence of cyber breaches. An investigation is necessary, and a containment and recovery technique needs to be carried out by experts.

Any corporation that is uncovered to an incident, faces a dent to their brand popularity and additionally any felony liability.

Alternatively, Incident response is the process of identifying a cyberattack, blocking it, and recovering from the damage that it caused. Incident response tools include **support software and services that help identify a cyberattack and also those tools that automatically block attacks**. Source: Google*

IRT (Incident Response) Tools*

SolarWinds Security Event Manager A SIEM tool that includes analysis and action triggers that make it an incident response tool.

ManageEngine Log360 This SIEM generates notifications to service desk systems for incident response. Runs on Windows Server.

AT&T Cybersecurity USM Anywhere A full cloud-based SOAR service built around AlienVault OSSIM.

Splunk Phantom An attack investigation system and response automation tool. This system plugs in as an add-on to the standard Splunk tool or any other SIEM system.

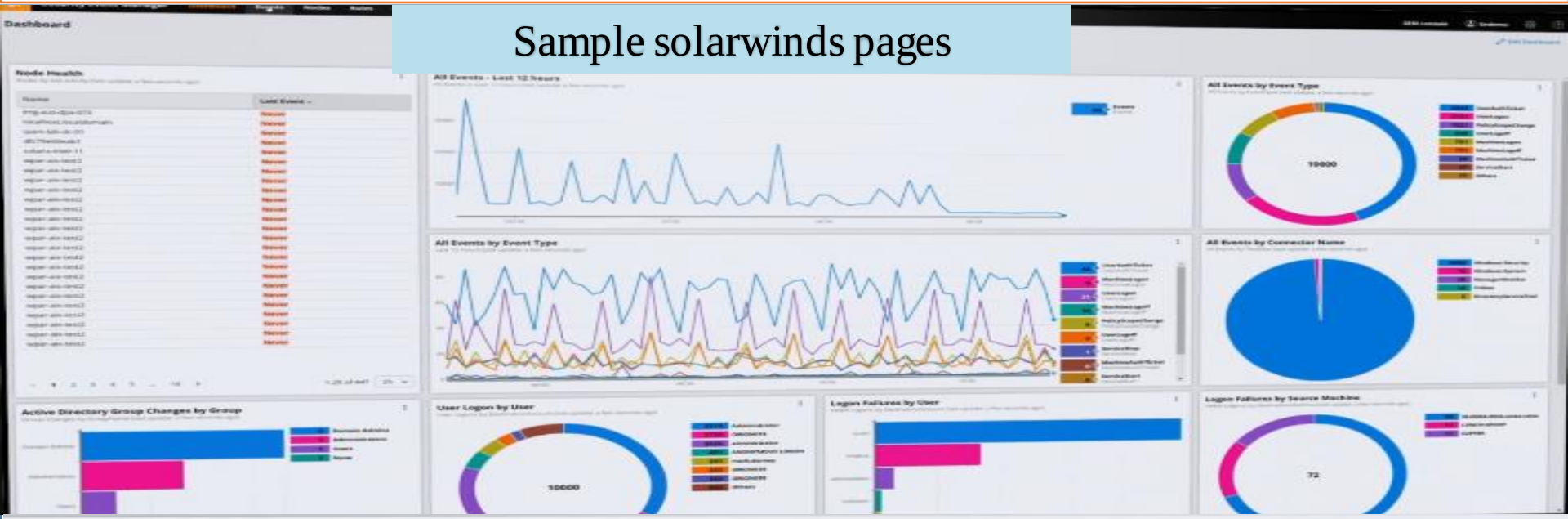
CrowdStrike Falcon Insight A hybrid solution that supports attack detection by coordinating event data gathered from every endpoint on a network.

Exabeam A SaaS security platform that includes a SIEM, analytics, and automated incident response.

LogRhythm SIEM A next-gen SIEM platform that includes user and entity behavior analytics, threat hunting, and a SOAR.

*Source: https://www.comparitech.com/net-admin/incident-response-tools/

Sample solarwinds pages



Live Filter

Show results from history

NAME	EVENT INFO
UserLogoff	PAM User Logoff "root" from service "pam_unix"
ConfigurationTrafficAudit	DHCP: Renew from 192.168.168.48 ()
ObjectAudit	Privileged Object Operation from "CORP\POST$" to "DS\3197451476"
MachineLogoff	Logoff "CORP\JESTER$"
WebTrafficAudit	Secure URL Access By scotty.corp.trigeo.com
WebTrafficAudit	BARE BYTE UNICODE ENCODING
WebTrafficAudit	URL Access By megatron.corp.trigeo.com
MachineLogoff	

NIST Incident Response Plan: Building Your Own IR Process Based on NIST Guidelines

7 Reasons You Need an Incident Response Plan

A strong incident response process can dramatically reduce the damage caused to an organization when disaster strikes. An incident response plan helps codify and distribute the incident response plan across the organization.

Here are the main reasons you must have a strong incident response plan in place:

1. **Prepares you for emergency**—security incidents happen without warning, so it's essential to prepare a process ahead of time
2. **Repeatable process**—without an incident response plan, teams cannot respond in a repeatable manner or prioritize their time
3. **Coordination**—in large organizations, it can be hard to keep everyone in the loop during a crisis. An incident response process can help achieve this
4. **Exposes gaps**—in mid-sized organizations with limited staff or limited technical maturity, an incident response plan exposes obvious gaps in the security process or tooling which can be addressed before a crisis occurs
5. **Preserves critical knowledge**—an incident response plan ensures critical knowledge and best practices for dealing with a crisis are not forgotten over time and lessons learned are incrementally added
6. **Practice makes perfect**—an incident response plan creates a clear, repeatable process that is followed in every incident, improving coordination and effectiveness of response over time
7. **Documentation and accountability**—an incident response plan with clear documentation reduces an organization's liability—it allows you to demonstrate to compliance auditors or authorities what was done to prevent the breach

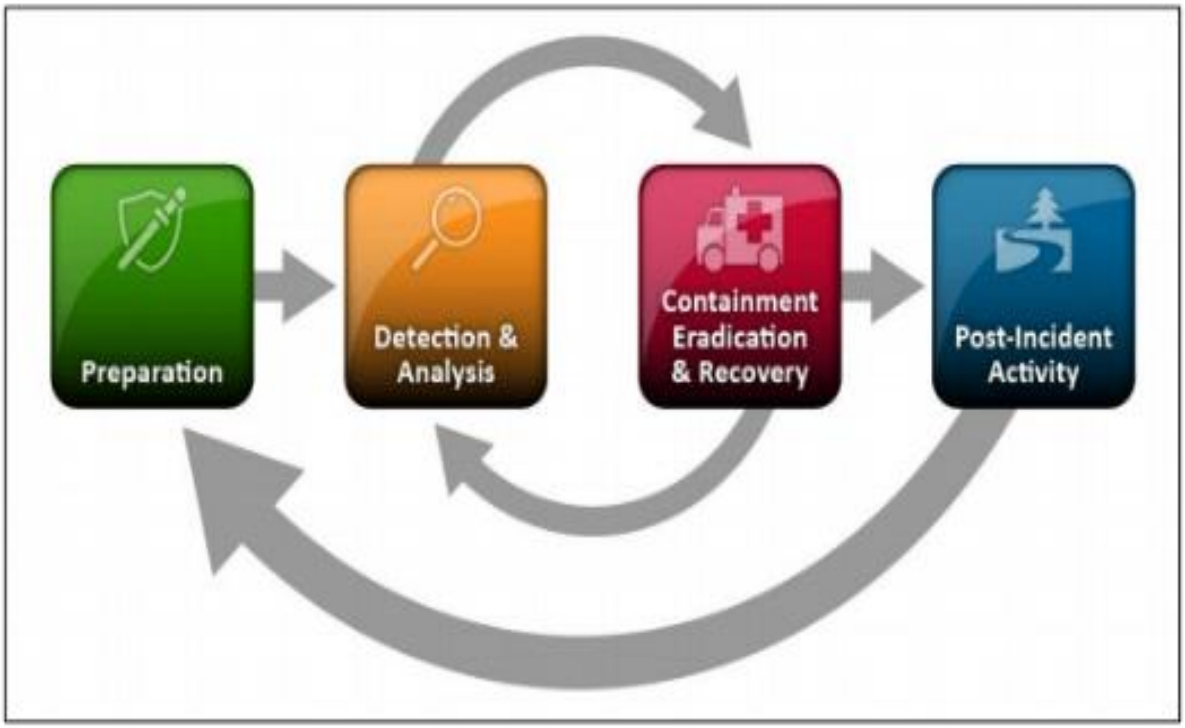
Key Roles in an Incident Response Team

The following are essential roles within the team:

- **Incident response managers**—have at least two members of staff responsible for approving the incident response plan and coordinating activity when an incident occurs.
- **Security analysts**—review alerts, identify possible incidents and perform an initial investigation to understand the scope of an attack.
- **Threat researchers**—responsible for providing contextual information around a threat, using information from the web, threat intelligence feeds, data from security tools, etc.
- **Other stakeholders**—these can include senior management or board members, HR, PR, and senior security staff such as the Chief Information Security Office (CISO)
- **Third parties**—such as lawyers, outsourced security services, or law enforcement agencies.

The NIST Incident Response Life Cycle

NIST defines a four-step process for incident response, illustrated in the diagram below. The NIST process emphasizes that incident response is not a linear activity that starts when an incident is detected and ends with eradication and recovery. Rather, incident response is a cyclical activity, where there is continuing learning and improvement to discover how to better defend the organization.



Source: NIST

4. Post-Incident Activity

A central part of the NIST incident response methodology is learning from previous incidents to improve the process.

You should ask, investigate and document the answers to the following questions:

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do differently next time if the same incident occurred?
- Could staff have shared information better with other organizations or other departments?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

Use your findings to improve the process, adjust your incident response policy, plan, and procedures, and feed the new data into the preparation stage of your incident response process.

What is PEN (Penetration testing) Tools

- Penetration Testing (Pen Testing) Tools provide means to conduct **authorized, ethical (white-hat)** hacking of applications in production.
  These simulated attacks by testers **help organizations locate vulnerabilities** that may be **exploited by hackers** and determine the **possible risk associated** with said vulnerabilities.
  The tools then **report the exploited vulnerabilities** to the organization for remediation.
  They are usually used either as part of a comprehensive security assessment, or part of the QA process in application or system development.

Penetration testing tools are closely related to the **Application Security Testing** space.

Various tools and managed services exist to provide continuous testing, besides application security platforms that include app testing as part of their functionality.

Penetration testing can extend beyond applications by testing networks, services, or social engineering vulnerabilities.

Most common testing types supported by these tools include:

- White box tests
- Blind tests
- Double-blind tests
- External tests
- Internal tests

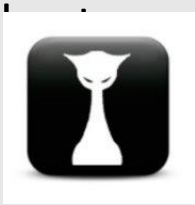
Penetration testing tools also provide testers the assurances and data to

PEN (Penetration testing) Tools*

Veracode	**is an application security platform that performs five types of analysis; static analysis, dynamic analysis, software composition analysis, interactive application security testing, and penetration testing. Veracode offers on-demand expertise and aims to help companies fix…**
Wireshark	Wireshark is an open source network troubleshooting tool.
PortSwigger Burp Suite	The Burp Suite, from UK-based alcohol-themed software company PortSwigger Web Security, is an application security and testing solution.
Metasploit	Metasploit is open source network security software described by Rapid7 as the world's most used penetration testing framework, designed to help security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness.
HackerOne	HackerOne is a hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited, from the company of the same name in San Francisco. The

Titania Nipper	Nipper discovers vulnerabilities in firewalls, switches and routers, automatically prioritizing risks to an organization. Its virtual modelling is designed to reduce false positives and identify exact fixes to help users stay secure and compliant. Audits: Firewalls | Switches | Routers…
Secureworks Security Consulting Services	Secureworks offers Security Consulting Services covering architecture guidance and analysis, continual assessments and testing, and compliance audits.
Kali Linux	Kali Linux is an open source, advanced penetration testing platform supported by Offensive Security headquartered in New York.
Pentest-Tools.com	allows users to discover and report vulnerabilities in websites and network infrastructures. They provide a set of integrated pentesting tools designed to enable users to perform easier, faster, and more effective pentest engagements. Quickly discover the attack…

*Source: https://www.trustradius.com/penetration-testing

Nikto 	Nikto is an open source fast (not stealthy) vulnerability testing tool that can be used in penetration testing or purple team exercises.
Mobile 	Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. MobSF support mobile app binaries (APK, IPA & APPX) along with…
Has 	Hashcat is a password recovery tool that can also be used in security testing (e.g. password cracking, exposing flaws).
	John the Ripper is a penetration testing tool used to find and crack weak passwords.

*Source: https://www.trustradius.com/penetration-testing

Hydra 	Hydra is a password cracking tool used for penetration testing.
Claranet 	Claranet headquarteredin London offers web, mobile, and infrastructure penetration testing services, approved by CREST, aiming to help clients find security issues before others do. Additionally, Claranet cybersecurity awareness training is offerd to protect users from the threats…
ZSecurity 	zSecurity, headquartered in Dublin is a provider of ethical hacking and cyber security training. They teach hacking and security to help customers become ethical hackers so they can test and secure systems from black-hat hackers. They state their goal is to educate people and increase…
SQLMap 	qlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a detection engine and features for the ultimate penetration tester and a range of switches lasting from…

*Source: https://www.trustradius.com/penetration-testing

- References:
  https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-siem/
  https://www.slideshare.net/osamaellahi/siem-security-information-and-event-management
  https://www.esecurityplanet.com/products/best-user-and-entity-behavior-analytics-ueba-tools/
  https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compared/
  https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
  https://www.techtarget.com/searchsecurity/definition/SOAR
  https://www.g2.com/categories/encryption/free
  https://www.simplilearn.com/data-encryption-methods-article
  https://www.greengeeks.com/blog/best-encryption-software/
  https://www.comparitech.com/net-admin/incident-response-tools/
  https://www.trustradius.com/penetration-testing