MALWARE ANLYSIS & PREVENTION STRATEGY

INDEX

Our Team

Introduction

Chapter 1

Chapter 2

Chapter 3

Reporting

OUR TEAM

Abd-Elrahman Sayed

Computer Science
Helwan

Ahmed Sayed

Computer Science
Helwan

Abd-Elrahman Mohamed

Computer Science
Octobar

Sohila Saeed

Communication Engineering
MUST

Reem Khalid

Computer Science
Cairo


LET'S START

1-INTRODUCTION

Stresses the importance of malware analysis to counter growing cyber threats. Malware refers to harmful software designed to damage or infiltrate systems. Analyzing it through techniques like static and dynamic analysis helps improve cybersecurity defenses and responses.

CHAPTER 1

Malwares Types & Classification	2	Malware's Concealment	2.3
Malware's Circulation	2.1	Malware's payload Capabilities	2.4
Malware's Infection	2.2	Malware's Real-life Examples	2.5

2-MALWARE'S ANALYSIS : TYPES & CLASSIFICATION

1

CIRCULATION :

spreads rapidly through networks

EX: Virus & Worms

2

INFECTION :

one-time execution or by remaining for repeated activation

EX: Trojan , Ransomware & Crypto-malware

3

CONCEALMENT :

involves malware techniques to evade detection, such as code obfuscation and using rootkits.

4

PAYLOAD CAPABILITIES

This could include stealing passwords and sensitive data, deleting essential programs, or altering system security settings

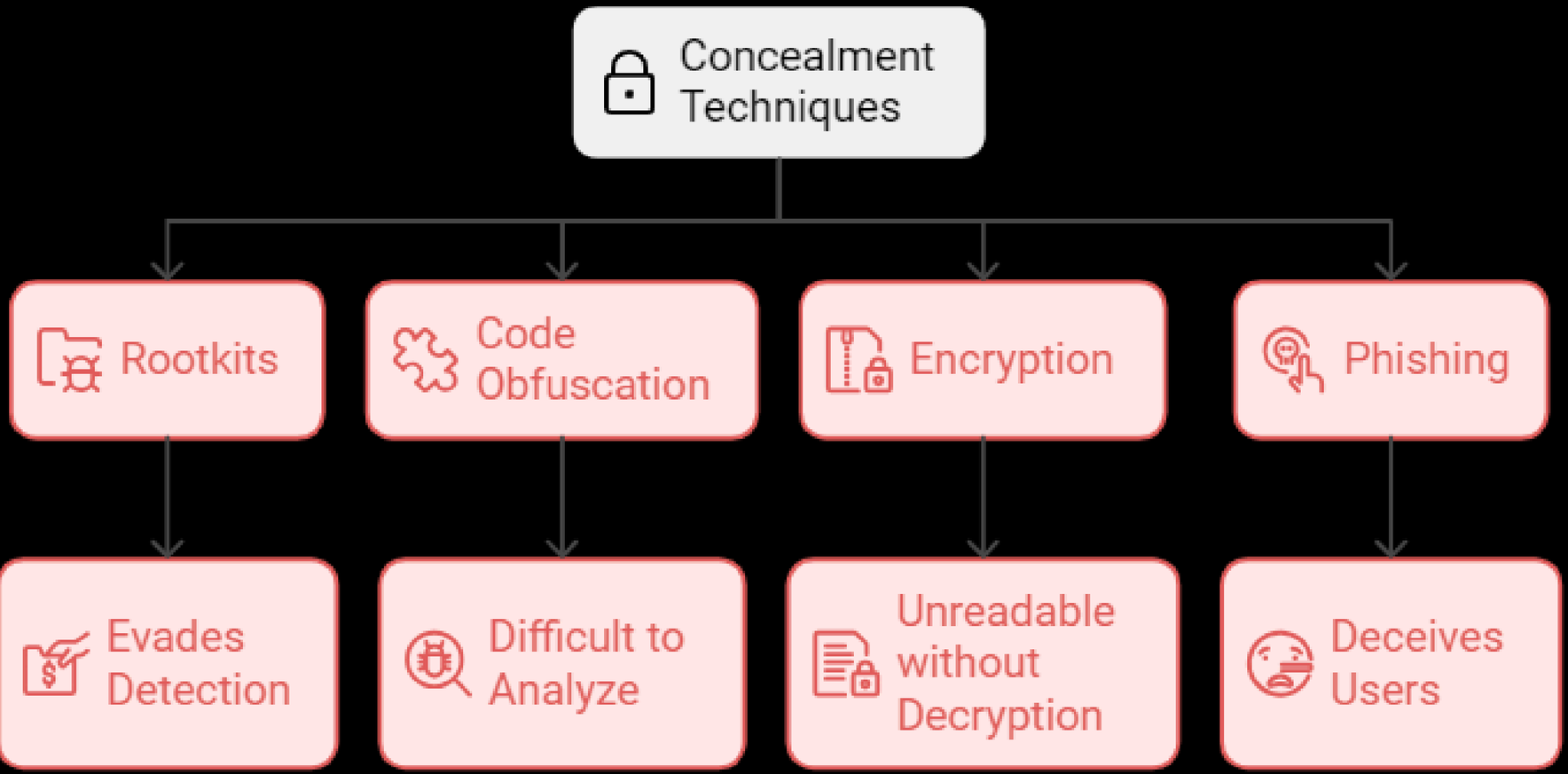
MALWARE'S CIRCULATION

ACTION	VIRUS	WORM
What does it do ?	Inserts malicious code into a program or data file.	Exploits a vulnerability in an application or operating system
How does it spread to other computers ?	User transfers infected files to other devices	Uses a network to travel from one computer to another
Does it infect a file ?	Yes	No
Does there need to be user action for it to spread ?	Yes	No

MALWARE'S INFECTION

FEATURE	TROJAN	RANSOMWARE	CRYPTO-MALWARE
Primary Trait	Deception (masquerades as legitimate apps)	Locks system access	Encrypts files, making them unusable
Malicious Activity	Steals data (passwords, credit cards)	Blocks device until ransom is paid	Encrypts files; demands ransom for decryption
Method of Infection	User unknowingly installs malicious software	Embeds into system, launches on boot	Encrypts files after receiving key from C&C
Severity	Medium: Can be detected and removed	High: Prevents system use until payment	Critical: Loss of data unless ransom is paid
Subtypes	Remote Access Trojan (RAT)	Blocker ransomware	Advances include file & network encryption
Impact on Networks	Can spread to other devices in network	Typically isolated to one device	Can infect multiple devices & network storage
Target Devices	Computers and networks	Computers and mobile devices	Computers, networks, cloud storage, mobile devices

MALWARE'S CONCEALMENT



MALWARE'S PAYLOAD CAPABILITIES

2.5 MALWARE'S REAL-LIFE EXAMPLES

Target Data Breach (2013) → Phishing Attack → Access Target's Network → Deploy Malware → Steal Credit Card Data

WannaCry Ransomware (2017) → Exploit Windows Vulnerability → Encrypt Files → Demand Bitcoin Ransom

Twitter Bitcoin Scam (2020) → Social Engineering → Access Internal Tools → Compromise High-Profile Accounts → Promote Bitcoin Scam

Video Explanation 1: (196) Target 2013 Data Breach Explained -YouTube
Video Explanation 2: WANNACRY: The World's Largest Ransomware Attack (Documentary) - YouTube
Video Explanation 3: The Teenager Who Hacked Twitter And Stole Millions In Bitcoin (youtube.com)

CHAPTER 2

What's SIEM ?

Pros & cons of SIEM

Open source SIEMs

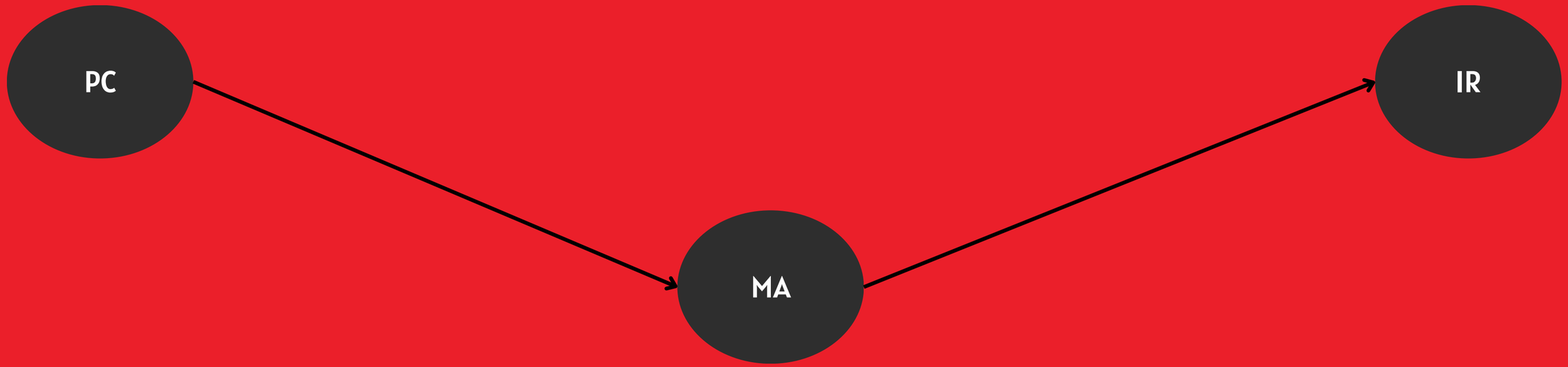
What's Wazuh ?

How to build Wazuh ?

Integrating Wazuh with Windows Defender Rules

CyberSecurity Frame Work

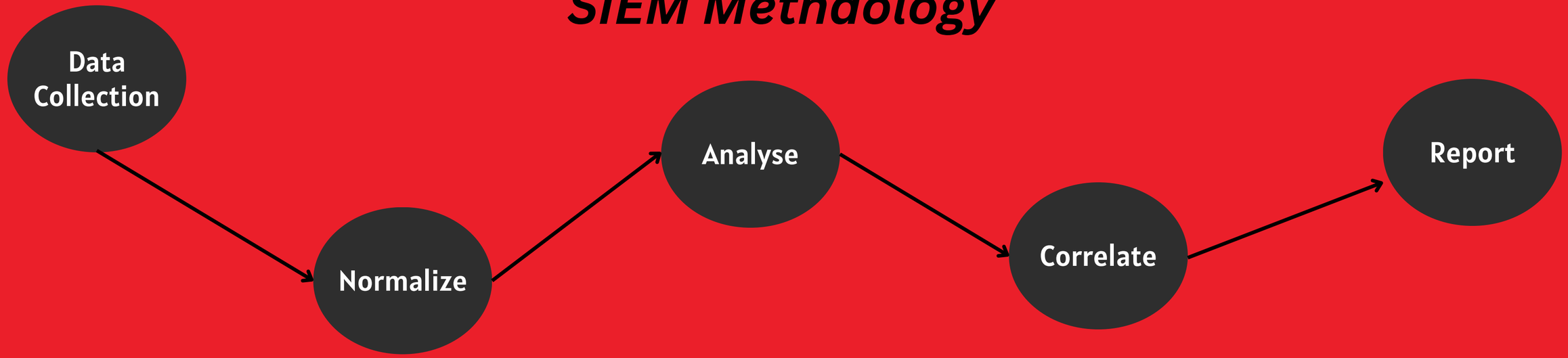
to reach the maximum effort of secure enterprise for any service provider must applying a three main aspects



What's SIEM ?

SIEM (Security Information and Event Management) combines Security Information Management (SIM) and Security Event Management (SEM) to offer real-time visibility by collecting, analyzing, and correlating security data from various sources.

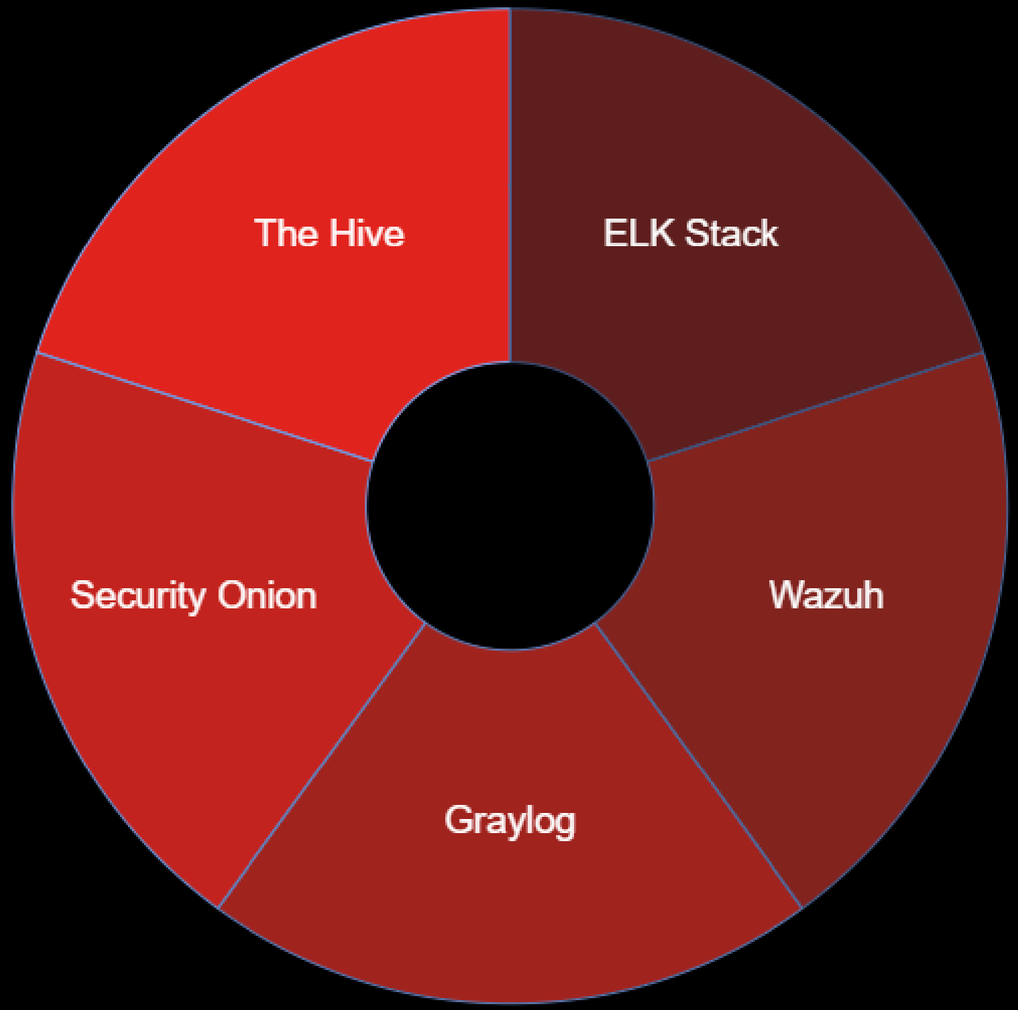
SIEM Methdology



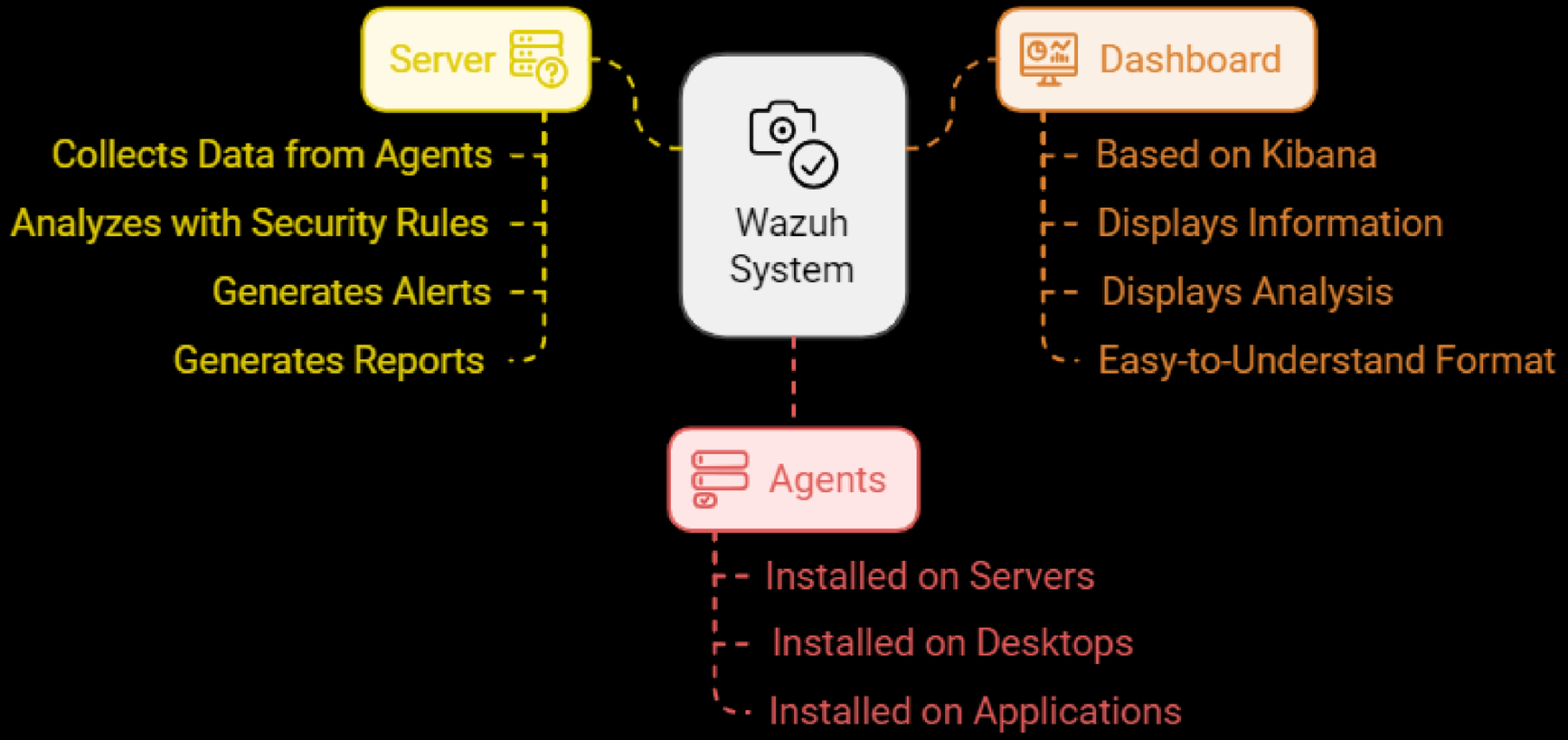
PROS & CONS OF SIEM

PORS	CONS
Centralized Management	High Cost
Faster Response	Complexity
Advanced Threat Detection	Resource Intensive
Regulatory Compliance	False Positives Alerts

OPEN SOURCE SIEMS



WHAT'S WAZUH?


Server
Collects Data from Agents
Analyzes with Security Rules
Generates Alerts
Generates Reports
Wazuh System
Dashboard
Based on Kibana
Displays Information
Displays Analysis
Easy-to-Understand Format
Agents
Installed on Servers
Installed on Desktops
Installed on Applications

HOW TO BUILD WAZUH ?

1-System Requirements: Linux OS (e.g., Ubuntu, CentOS); 2 CPUs, 4GB RAM, 20GB disk.

2-Install Wazuh Server: Add repository, install Wazuh, Elastic Stack (Elasticsearch, Kibana, Filebeat), configure manager & API.

3-Install Agents: Deploy Wazuh agents on endpoints (Windows, Linux, macOS) and configure log forwarding.

4-Set Up Kibana: Install the Wazuh Kibana plugin and access the dashboard for monitoring.

5-Configure Alerts: Customize alert rules and integrate threat intelligence.

6-Ongoing Monitoring: Continuously monitor events via Kibana and keep the system updated.

INTEGRATING WAZUH WITH WINDOWS DEFENDER RULES

01 **Wazuh:**
Open-source security platform for threat detection, incident response, and compliance.

02 **Windows Defender:**
Built-in antivirus software on Windows, generating logs and alerts.

03 **Goal:**
Configure rules in Wazuh to monitor Windows Defender alerts.

04 **Prerequisites:**

- Wazuh agent installed on Windows.
- Wazuh manager installed and running.
- Ensure Windows Defender logs are enabled in Windows Event Viewer.

WINDOWS DEFENDER ALERTS → WAZUH AGENT → WAZUH MANAGER

STEPS TO CONFIGURE RULES

01 Enable Defender Logs:

- Open Event Viewer → Applications and Services → Microsoft → Windows → Windows Defender.

02 Deploy the Wazuh Agent on Windows:

- Download Wazuh agent from the official site.
- Configure it to connect to Wazuh Manager.

03 Edit Wazuh Rules:

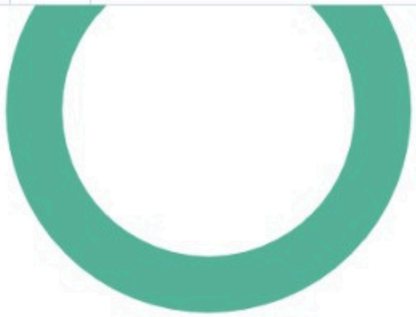
- Go to the Wazuh Manager's rules folder:
- /var/ossec/etc/rules/ (on Linux Wazuh Manager).
- Add or modify the Defender rule (windows_defender_rules.xml).

04 Restart Wazuh Manager:

Use "sudo systemctl restart wazuh-manager" to apply changes.

05 Monitor Alerts:

Check alerts in Wazuh Dashboard.



38 hits

Oct 16, 2024 @ 03:54:05.732 - Oct 17, 2024 @ 03:54:05.732

Export Formated | **699 columns hidden** | Density | **1 fields sorted** | Full screen

timestamp	agent.id	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Oct 17, 2024 @ 00:38:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62128
Oct 17, 2024 @ 00:20:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62124
Oct 17, 2024 @ 00:20:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	12	62123
Oct 17, 2024 @ 00:04:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62124
Oct 17, 2024 @ 00:04:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	12	62123
Oct 16, 2024 @ 23:52:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62128
Oct 16, 2024 @ 22:31:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62124
Oct 16, 2024 @ 22:31:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	12	62123
Oct 16, 2024 @ 22:30:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62128
Oct 16, 2024 @ 21:37:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	3	62124
Oct 16, 2024 @ 21:37:...	003	DESKTOP-1GFUGR7			Windows Defender: An...	12	62123

wazuh-alerts-*

Search | Filter by type 0

Selected fields

_source

Available fields

_index
agent.id
agent.ip
agent.name
data.command
data.integration
data.origin.module
data.origin.name
data.parameters.alert.agent.id
data.parameters.alert.agent.ip
data.parameters.alert.agent.name
data.parameters.alert.data.integration
data.parameters.alert.data.virustotal.found
data.parameters.alert.data.virustotal.malicious
data.parameters.alert.data.virustotal.permalink

windows_defender | DQL | Last 24 hours | Show dates | Refresh

manager.name: wazuh-server × | rule.level: 12 to 14 × | + Add filter

16 hits

Oct 16, 2024 @ 05:01:00.289 - Oct 17, 2024 @ 05:01:00.289 per Auto

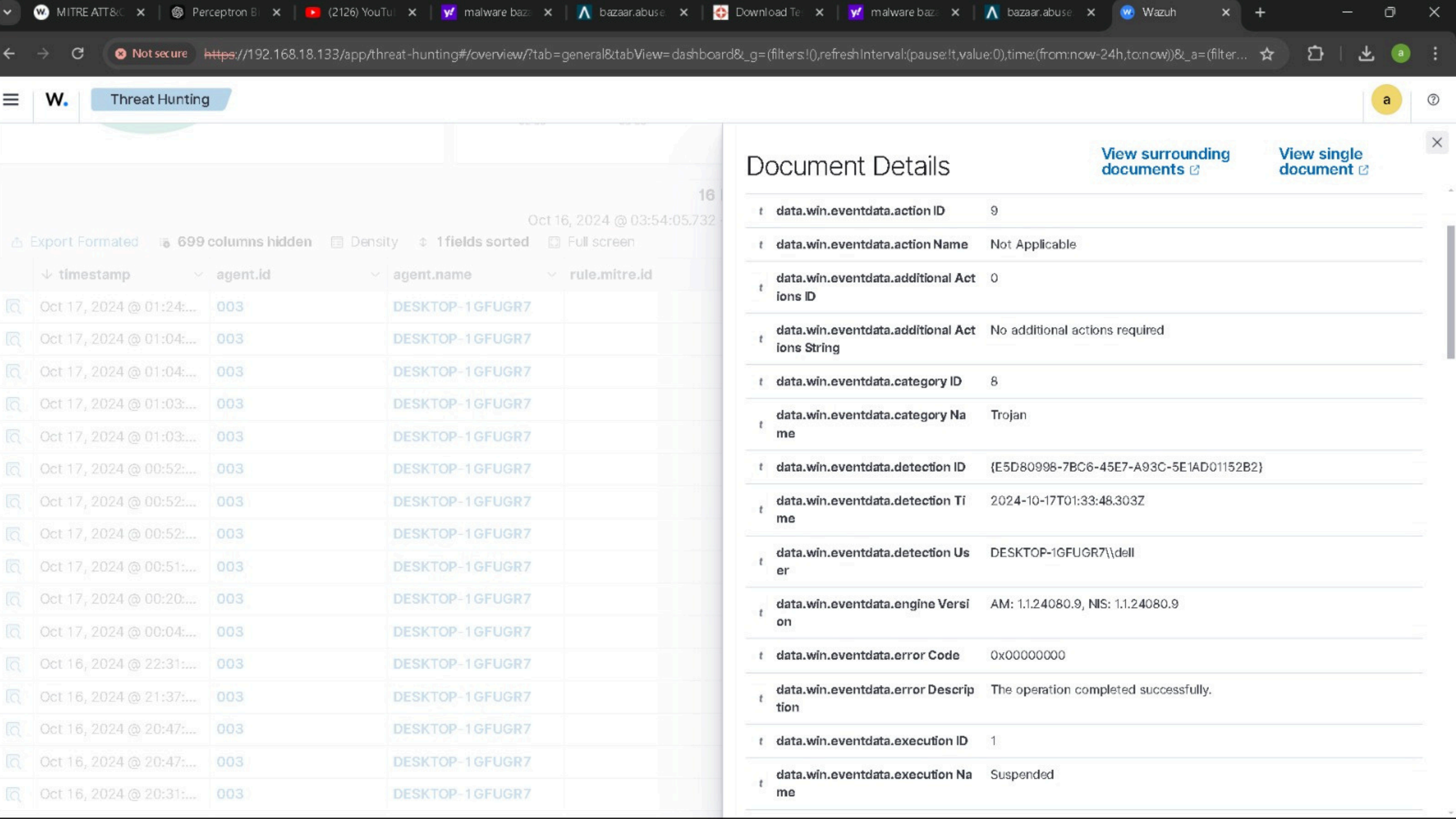
Time	_source
Oct 17, 2024 @ 02:24:55.970	input.type: log agent.ip: 192.168.18.1 agent.name: DESKTOP-1GFUGR7 agent.id: 003 manager.name: wazuh-server data.win.eventdata.error Description: The operation completed successfully. data.win.eventdata.source ID: 3 data.win.eventdata.origin ID: 1 data.win.eventdata.threat ID: 2147814524 data.win.eventdata.action Name: Not Applicable data.win.eventdata.additional Actions String: No additional actions required data.win.eventdata.severity

Expanded document

View surrounding documents | View single document

Table | JSON

t _index	wazuh-alerts-4.x-2024.10.16
t agent.id	003
t agent.ip	192.168.18.1


MITRE ATT&C
Perceptron B
(2126) YouTu
malware baz
bazaar.abuse
Download Te
malware baz
bazaar.abuse
Wazuh
Not secure
https://192.168.18.133/app/threat-hunting#/overview/?tab=general&tabView=dashboard&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filter...
Threat Hunting
a
16
Oct 16, 2024 @ 03:54:05.732
Export Formated
699 columns hidden
Density
1 fields sorted
Full screen
timestamp
agent.id
agent.name
rule.mitre.id
Oct 17, 2024 @ 01:24:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 01:04:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 01:04:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 01:03:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 01:03:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:52:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:52:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:52:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:51:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:20:...
003
DESKTOP-1GFUGR7
Oct 17, 2024 @ 00:04:...
003
DESKTOP-1GFUGR7
Oct 16, 2024 @ 22:31:...
003
DESKTOP-1GFUGR7
Oct 16, 2024 @ 21:37:...
003
DESKTOP-1GFUGR7
Oct 16, 2024 @ 20:47:...
003
DESKTOP-1GFUGR7
Oct 16, 2024 @ 20:47:...
003
DESKTOP-1GFUGR7
Oct 16, 2024 @ 20:31:...
003
DESKTOP-1GFUGR7
Document Details
View surrounding documents
View single document
t data.win.eventdata.action ID 9
t data.win.eventdata.action Name Not Applicable
t data.win.eventdata.additional Actions ID 0
t data.win.eventdata.additional Actions String No additional actions required
t data.win.eventdata.category ID 8
t data.win.eventdata.category Name Trojan
t data.win.eventdata.detection ID {E5D80998-7BC6-45E7-A93C-5E1AD01152B2}
t data.win.eventdata.detection Time 2024-10-17T01:33:48.303Z
t data.win.eventdata.detection User DESKTOP-1GFUGR7\\dell
t data.win.eventdata.engine Version AM: 1.1.24080.9, NIS: 1.1.24080.9
t data.win.eventdata.error Code 0x00000000
t data.win.eventdata.error Description The operation completed successfully.
t data.win.eventdata.execution ID 1
t data.win.eventdata.execution Name Suspended

LET'S TAKE A BREAK

CHAPTER 3

Malware Prevention Strategy

User Awareness Training

MALWARE PREVENTION STRATEGY

A multi-layered strategy protects against malware across various attack vectors.

01

Update Software:

Regularly patch operating systems and applications to fix vulnerabilities.

02

Antivirus & Antimalware:

Use security tools to detect and block malicious programs.

03

Firewalls & IDS:

Monitor network traffic to prevent unauthorized access.

04

Employee Training:

Educate staff on spotting phishing and unsafe practices.

05

Network Segmentation:

Isolate critical systems to limit malware spread.

06

Limit User Access:

Apply the least privilege principle to reduce entry points.

07

Regular Backups:

Ensure frequent backups for quick recovery.

08

Email & Web Filtering:

Block malicious emails and restrict access to harmful websites.

09

Threat Intelligence:

Stay informed about emerging malware threats.

USER AWARENESS TRAINING

1- Think before click

01 <u>Look for Red Flags:</u> Suspicious email addresses, urgent language, unexpected attachments.

02 <u>Verify Links:</u> Hover over links before clicking to check for fake URLs.

03 <u>Report It:</u> If unsure, report phishing attempts to your IT team immediately

3.2-USER AWARENESS TRAINING

2-Build a Strong Password

01 Use at least 12 characters with a mix of letters, numbers, and symbols.

02 Avoid common words and personal info.

03 Enable MFA (Multi-Factor Authentication) for extra security.

3.2-USER AWARENESS TRAINING

3-Stay Safe While Surfing the Web

01 <u>Check for HTTPS</u>: Always use secure websites.

02 <u>Avoid Suspicious Links</u>: Don't click on unknown or pop-up links.

03 <u>Update Your Browser:</u> Keep your browser up-to-date for protection.

3.2-USER AWARENESS TRAINING

4-Keep Your Devices Secure

01 Update Software Regularly : Always install the latest security patches.

02 Use Antivirus Software : Regular scans keep malware away.

03 Lock Your Device : Always lock your screen when stepping away.

3.2-USER AWARENESS TRAINING

5-Handle Data with Care!

01 Encrypt Sensitive Data both in transit and at rest.

02 <u>Share Securely:</u> Use secure methods (VPN, encrypted email) for sharing sensitive info.

03 <u>Access Control:</u> Only authorized personnel should have access to sensitive data.

REPORTING

Malware Incident Response

Incident Response Framework

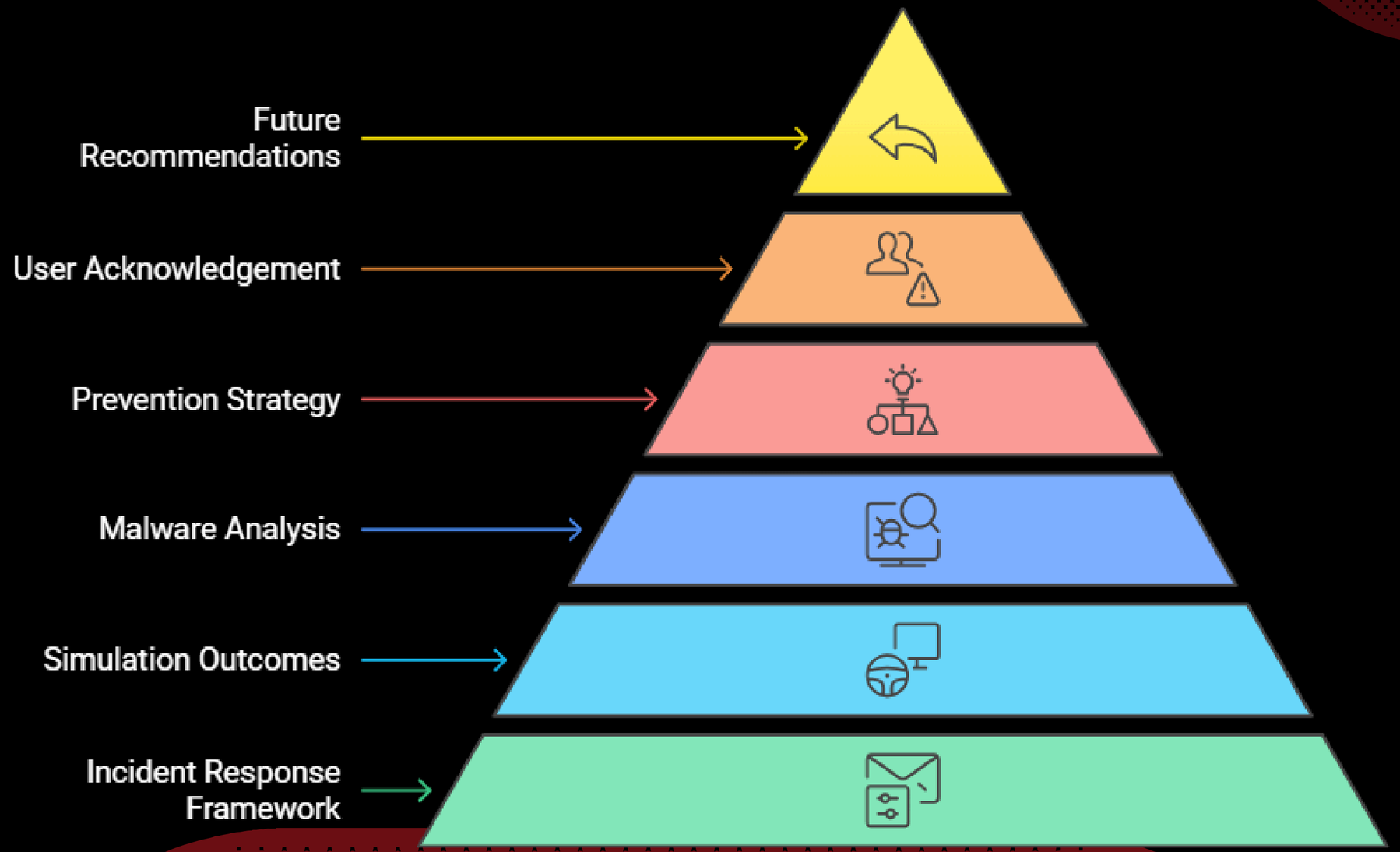
Simulation

Malware Analysis

User Acknowledgement

Future Recommendations

MALWARE INCIDENT RESPONSE



INCIDENT RESPONSE FRAMEWORK

01

Preparation : prepared incident response teams and playbooks for malware incidents.

02

Identification : behavioral analysis to identify known malware and detect suspicious activities like unusual file executions and network connections.

03

Containment: Isolating the affected device to prevent further infection.

04

Eradication: Removing the malware and cleaning the infected system.

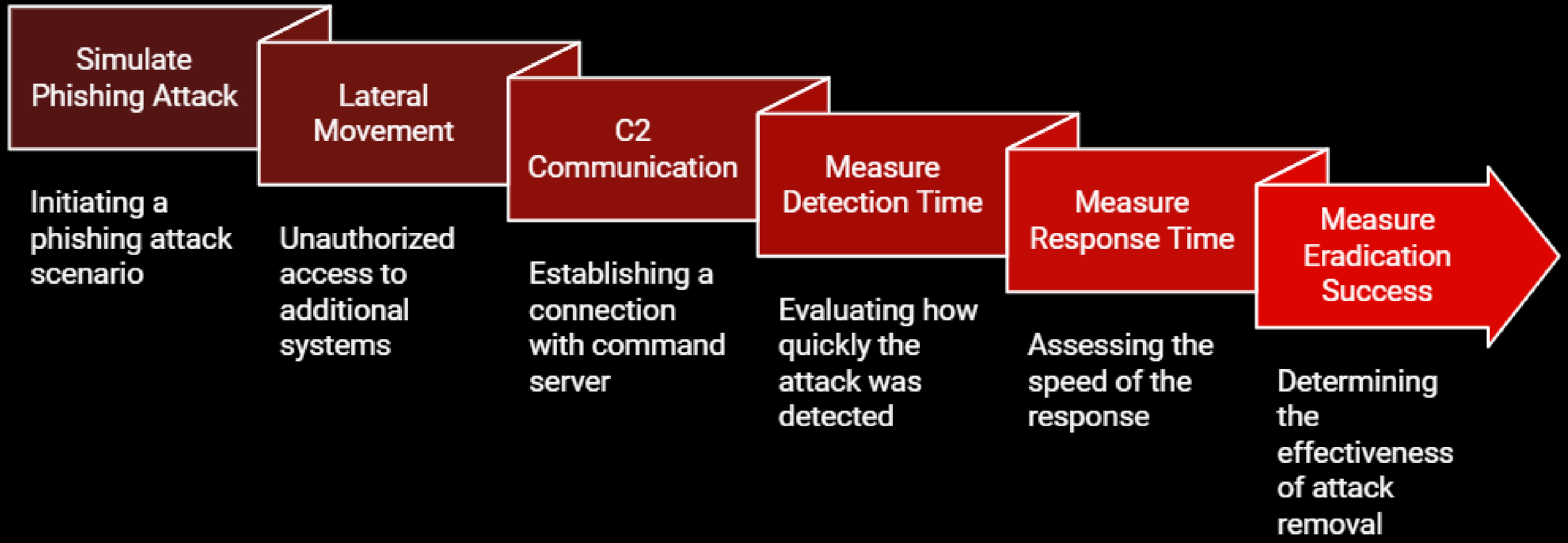
05

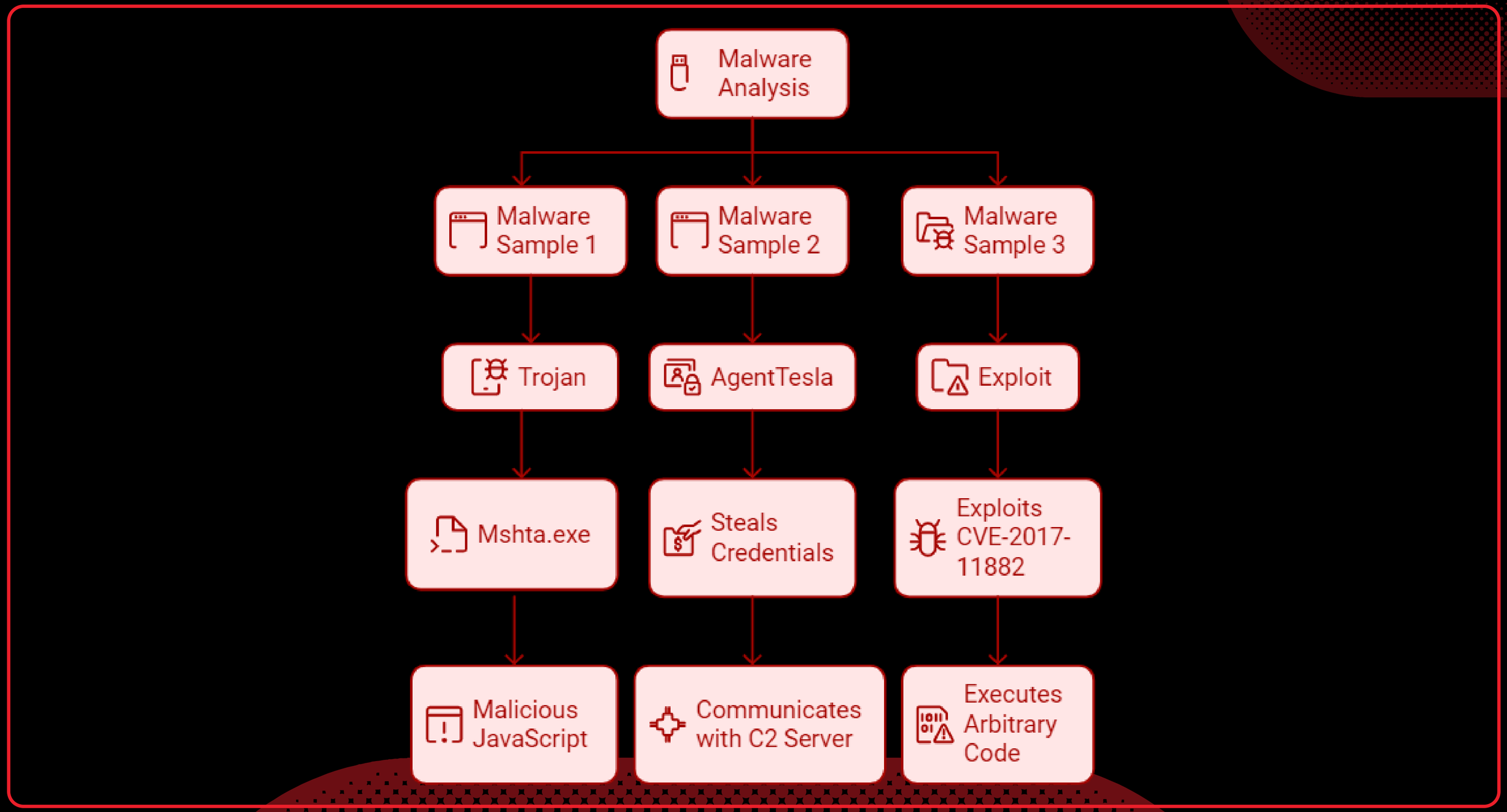
Recovery: Restoring the system from a clean backup, followed by validation.

06

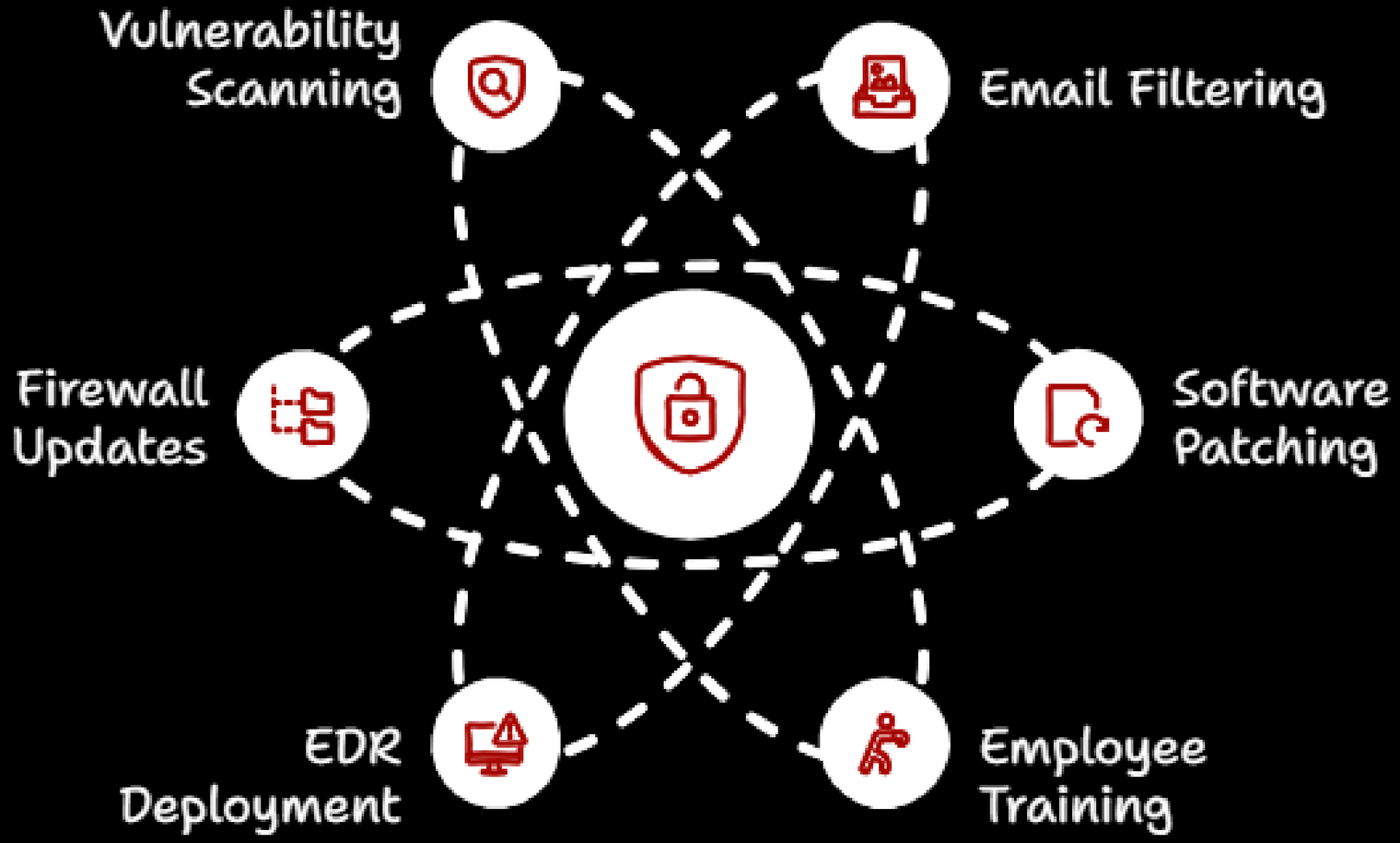
Lessons Learned: Identifying gaps in the response process and refining playbooks.

SIMULATION


Simulate Phishing Attack
Initiating a phishing attack scenario
Lateral Movement
Unauthorized access to additional systems
C2 Communication
Establishing a connection with command server
Measure Detection Time
Evaluating how quickly the attack was detected
Measure Response Time
Assessing the speed of the response
Measure Eradication Success
Determining the effectiveness of attack removal


Malware Analysis
Malware Sample 1
Malware Sample 2
Malware Sample 3
Trojan
AgentTesla
Exploit
Mshta.exe
Steals Credentials
Exploits CVE-2017-11882
Malicious JavaScript
Communicates with C2 Server
Executes Arbitrary Code

PREVENTION STRATEGY



USER ACKNOWLEDGEMENT

Outline Next Steps

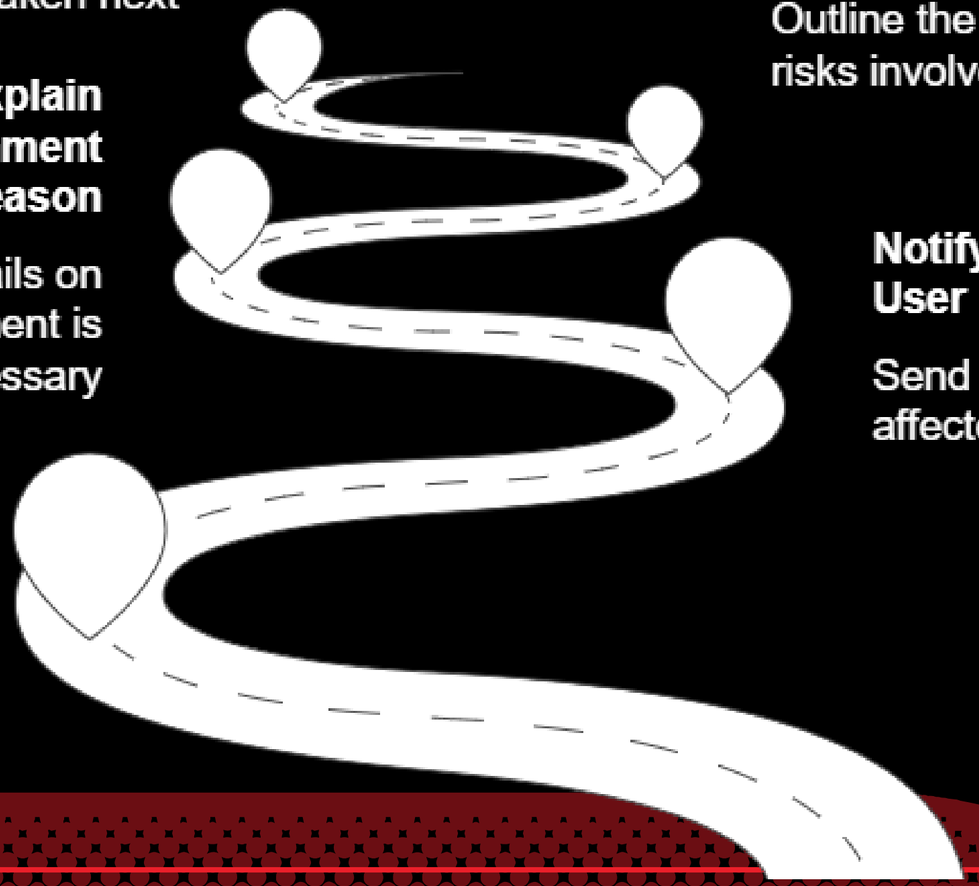
Detail the actions to be taken next

Explain Containment Reason

Provide details on why containment is necessary

Identify Security Incident

Detect and confirm the security breach



Describe Potential Threat

Outline the potential risks involved

Notify Affected User

Send an email to the affected user

FUTURE RECOMMENDATIONS

How to improve cybersecurity posture?

Strengthen User Awareness Training

Reduce human error by educating users on phishing threats.

Enhanced Detection Capabilities

Invest in advanced tools for better threat detection.

Routine Simulation Drills

Test and improve incident response through regular simulations.


WARNING