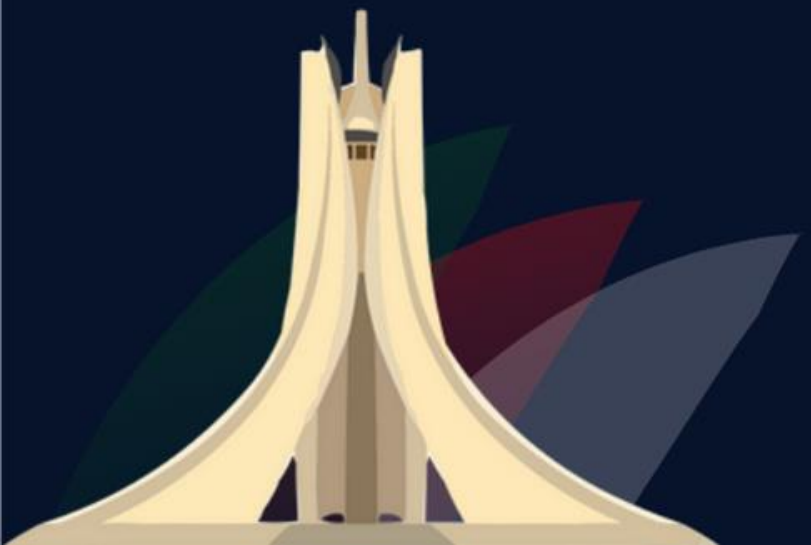
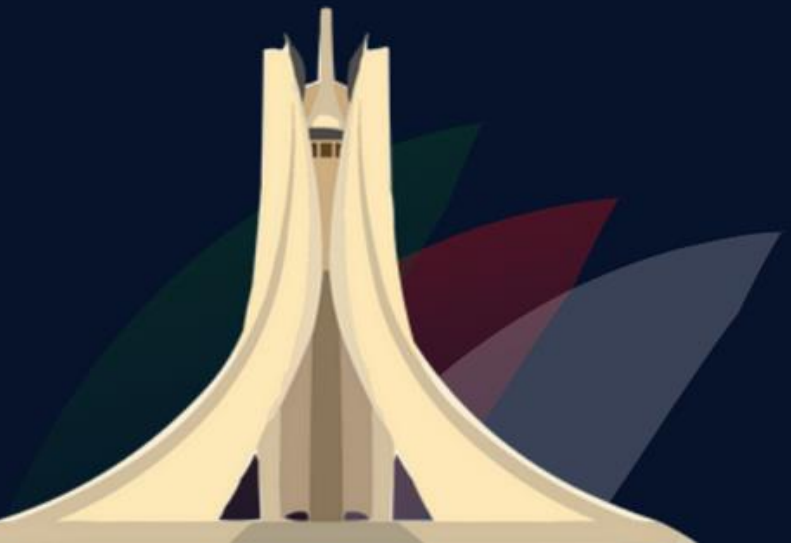
OWASP ALGIERS



OWASP ALGIERS



WORKSHOP

Incident Detection within Financial Institutions: SIEM for Cyber Defense

OWASP ALGIERS

SPEAKER

Wissam BOUATTOU

OWASP Algiers Chapter Board Member

- Cybersecurity Auditor at a public bank.
- SIEM Solution Technical Project Manager
- PRA solution Administrator.
- Vulnerability Assessment | SOC Analyst | Audit Compliance missions.

AGENDA

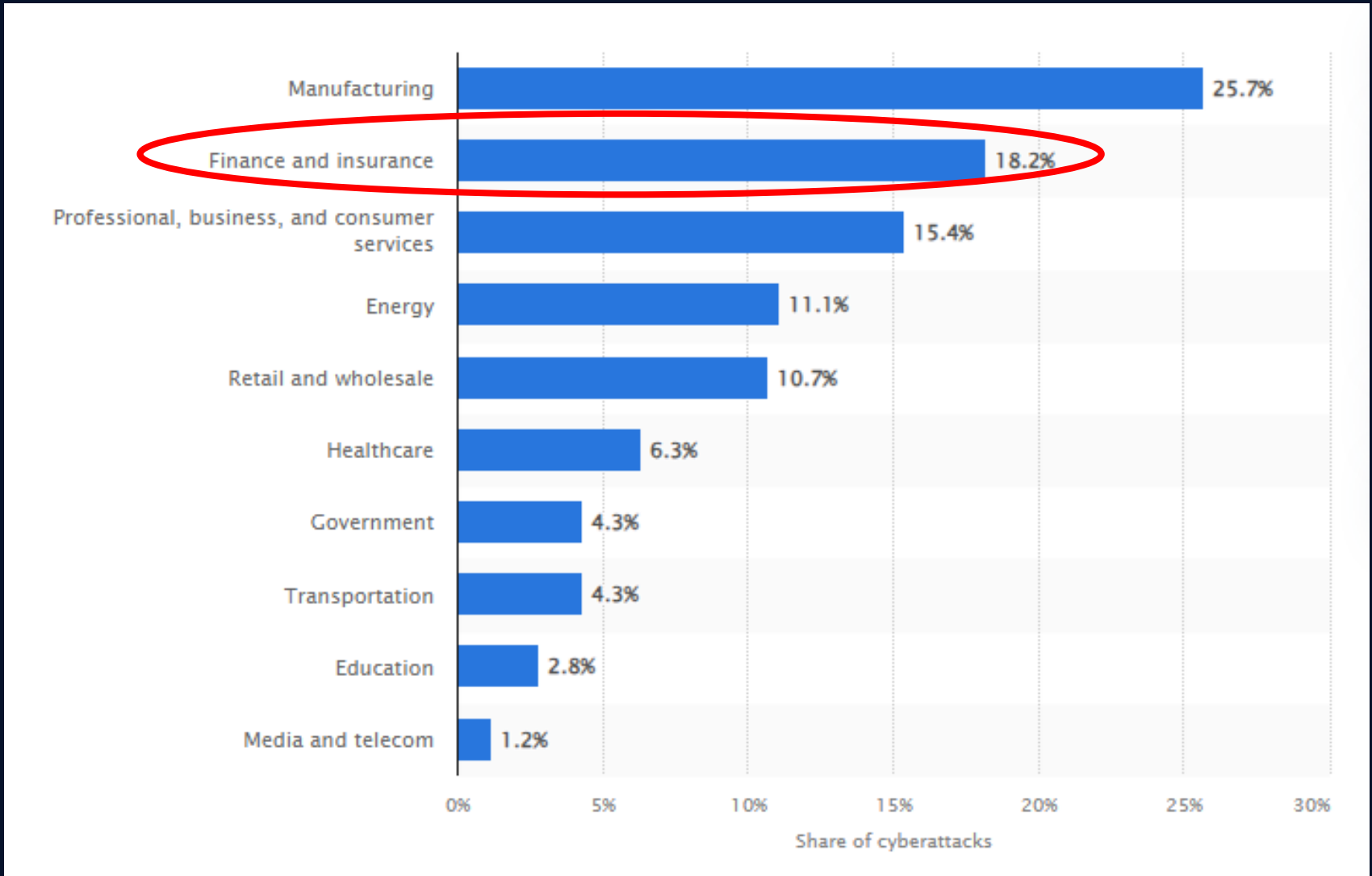
1. Introduction
2. Common Cyber Attacks
3. Incident Management Process
4. Introduction to SIEM
5. Interactive Demo
6. Conclusion

1. Introduction:
The Persistent Threat Landscape

Cyber Threats

- The term "threat landscape" refers to the current and evolving panorama of potential risks, vulnerabilities, and malicious actors that pose threats to an organization's cybersecurity posture

Distribution of cyberattacks across worldwide industries in 2023

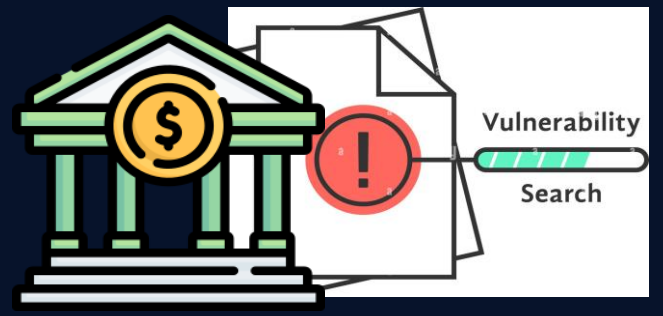


Cyber Threats

- The threat landscape confronting financial institutions is characterized by its relentless evolution.

Cybercriminals

Advanced Techniques & Tools



Vulnerabilities in financial systems

=

Exploit weakness for a specific gain

Central Bank of Lesotho – Cybersecurity Incident

CENTRAL BANK OF LESOTHO
BANKA E KHOLO EA LESOTHO

OWASP ALGIERS

Central Bank of Lesotho – Cybersecurity Incident

Impact

Transactions paralyzing

Inter and international payments off

Financial losts

Remediation

Following Incident Management Process

Suspending systems

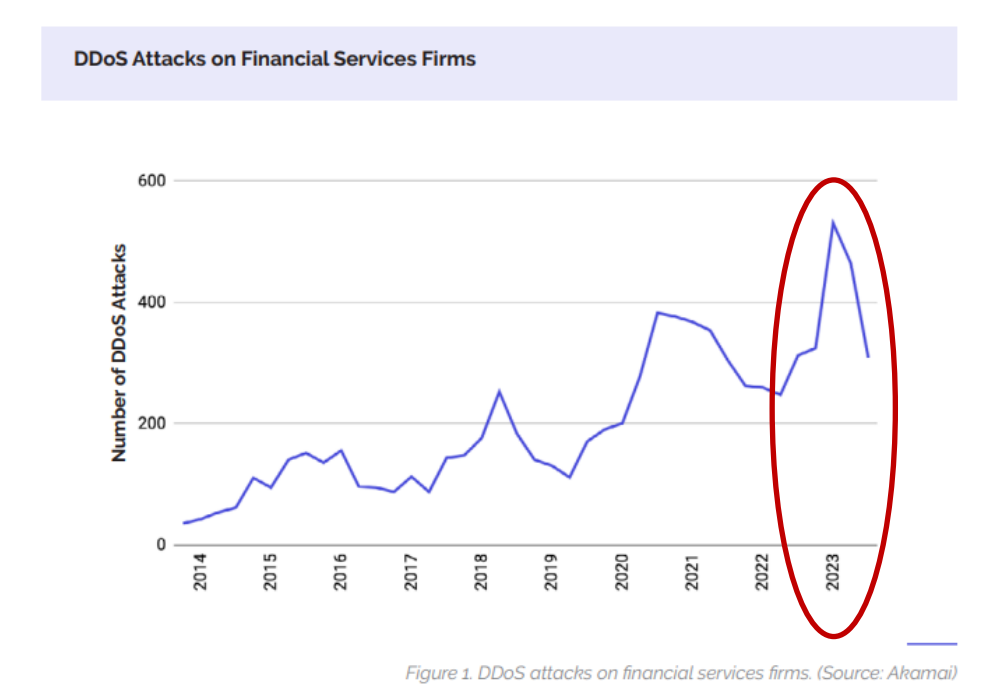
Business Continuity Process

OWASP ALGIERS

2. Common Cyber Attacks

DDoS Attacks

- Financial Services: The Top Target for DDoS

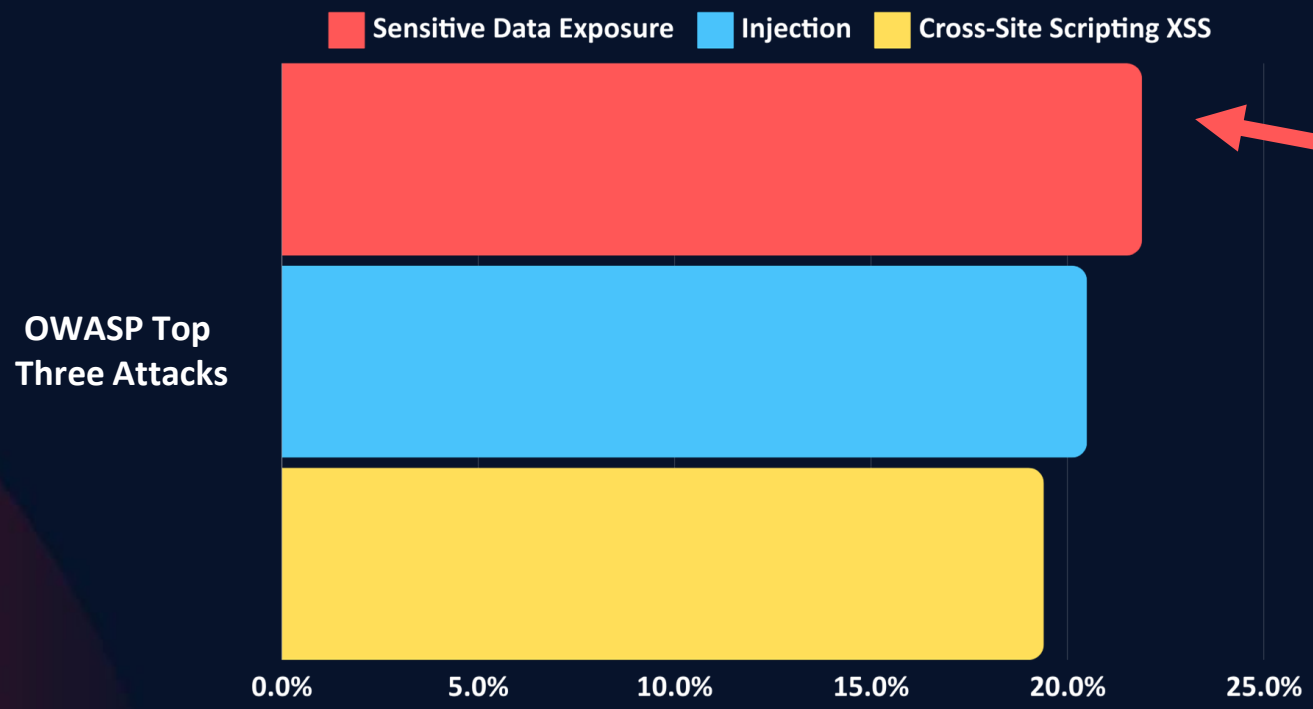


Report : « DDoS: Here to Stay » -FS-ISAC 2024

Distributed Denial of Service (DDoS):

- Floods a network, server, or service.
- Disruption and unavailability of service.
- Interrupting services such as online banking and payment systems.

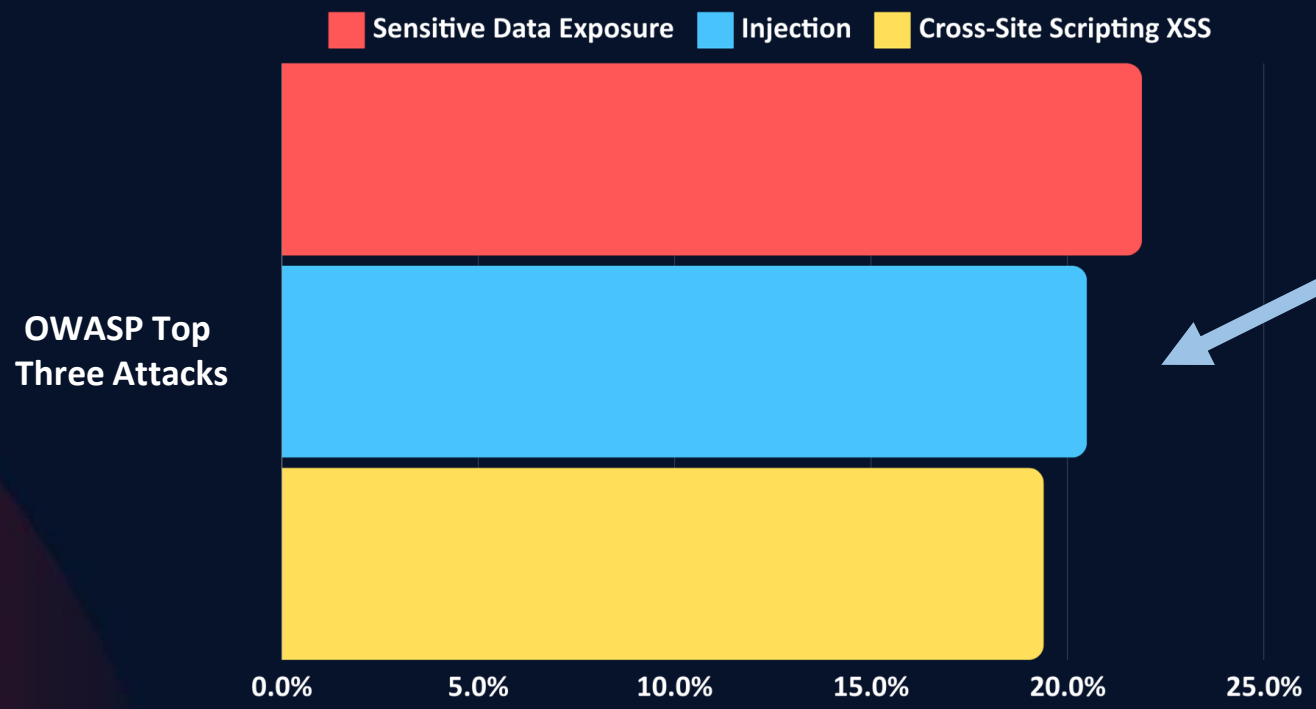
OWASP top three attacks- Financial Services



Data leakage : (21,9%)

- Steal or modify protected high-value sensitive financial data.
- Commit credit card fraud, identity theft, or other crimes…

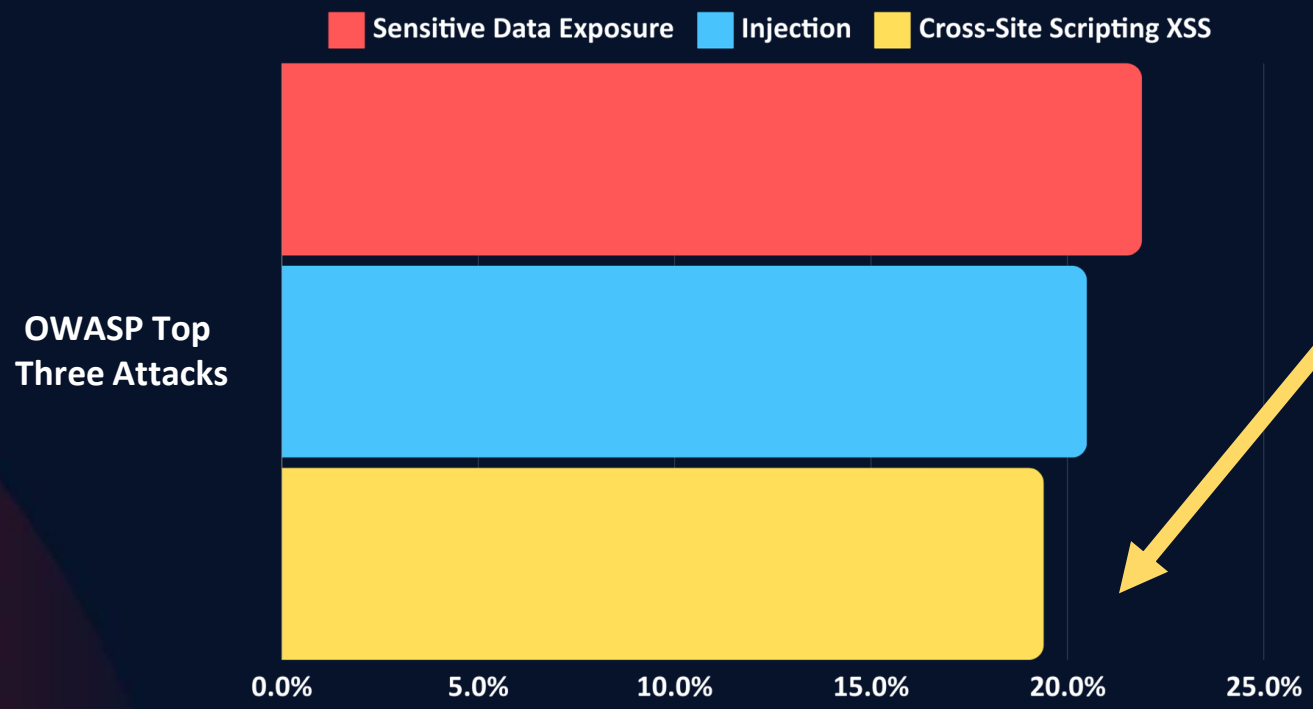
OWASP top three attacks- Financial Services



Injection: (20,5%)

- Running malicious code on servers to exfiltrate sensitive data.
- Commit credit card fraud, identity theft…

OWASP top three attacks- Financial Services



Cross-Site Scripting XSS: (19.4%)

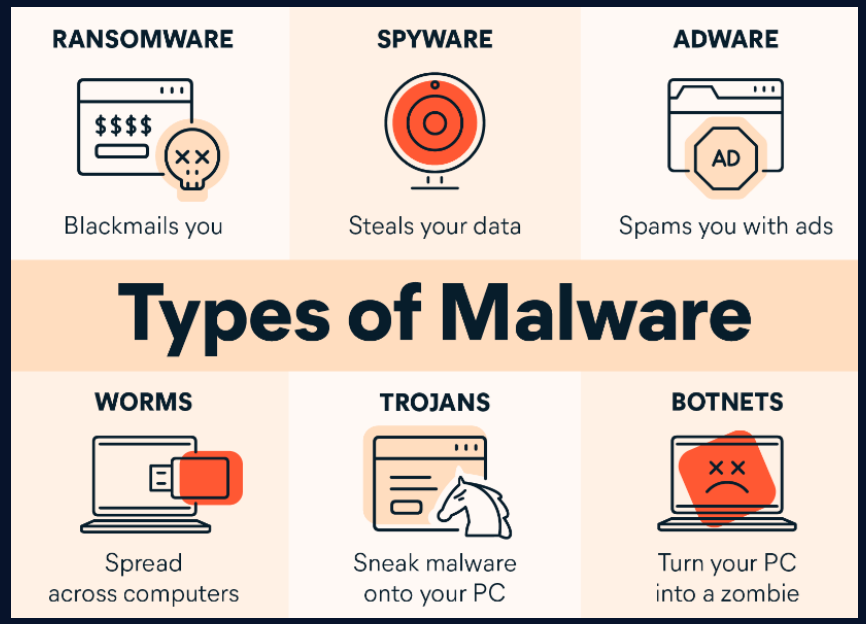
- Cybercriminals Injecting client-side scripts into web pages.
- Steal information like session cookies, enabling account takeover on financial services sites.

OWASP ALGIERS

Malware Attacks

Malware (malicious software) infiltrates systems, compromising data integrity, confidentiality, and availability.

- ***Impact:*** It can lead to unauthorized access, data theft, and system disruption.
- ***Prevalence:*** Around **40%** of financial and insurance organizations worldwide experienced malware attacks between October 2021 and September 2022.



Phishing

Attackers send fraudulent emails, texts, or messages impersonating banks, credit card companies, or investment firms, it contains links or attachments, leading victims to fake websites.

- ***Impact:***

Data breaches: Stolen login credentials grant unauthorized access to accounts.

Financial Fraud: Attackers manipulate victims into transferring funds or revealing sensitive data.

Reputation Damage: Breaches erode customer trust and harm an institution's image.

Have you ever wondered how these institutions effectively detect and prevent such cyber attacks?

OWASP ALGIERS

3. Incident Management Process

IMP Definition

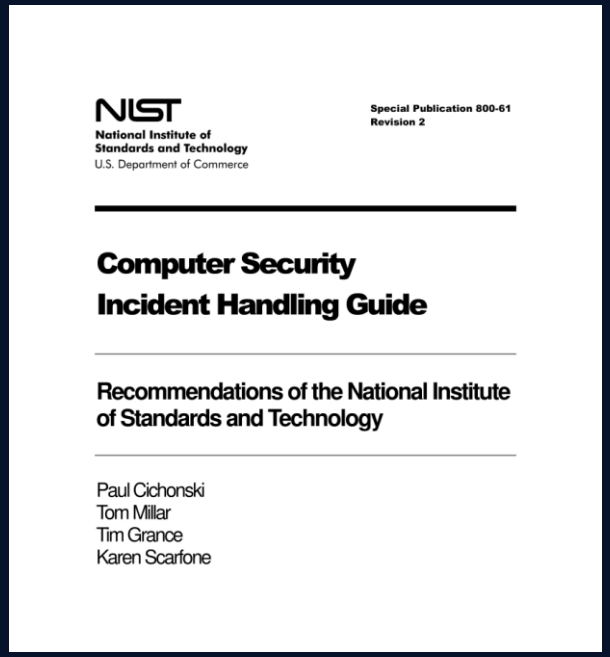
- To effectively navigate these challenges, it is imperative to implement a robust Incident Management Process (IMP).
- It is a structured approach used by organizations.
- It encompasses a series of coordinated steps aimed at minimizing the impact of incidents on the organization's operations, data, and reputation.

IMP in international Standards

National Institute of Standards and Technology

NIST Special Publication 800-61

"Computer Security Incident Handling Guide"


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

International Organization for Standardization

ISO/IEC 27035

"Information Security Incident Management"


INTERNATIONAL STANDARD

ISO/IEC 27035-1

Second edition
2023-02

Information technology — Information security incident management —

Part 1:
Principles and process

Technologies de l'information — Gestion des incidents de sécurité de l'information —
Partie 1: Principes et processus

ISO IEC

Reference number
ISO/IEC 27035-1:2023(E)

© ISO/IEC 2023

OWASP ALGIERS

Incident Management Process

1- Preparation:

sets up policies, procedures | identifying critical assets| incident response teams | incident response plans and playbooks |training personnel.

Incident Management Process

1- Preparation:

sets up policies, procedures | identifying critical assets| incident response teams | incident response plans and playbooks |training personnel.

2- Detection and Analysis:

monitoring networks and systems | implementing security tools to spot anomalous behavior | analyzing incidents according to their scope and impact| prioritizing incidents.

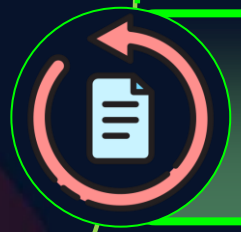
Incident Management Process

1- Preparation:

sets up policies, procedures | identifying critical assets| incident response teams | incident response plans and playbooks |training personnel.

2- Detection and Analysis:

monitoring networks and systems | implementing security tools to spot anomalous behavior | analyzing incidents according to their scope and impact| prioritizing incidents.



3- Containment, Eradication, and Recovery:

controlling incident | eliminate root cause | restoring normal operations | isolating affected systems | removing malware| patching vulnerabilities | securing accounts |data restoration| system reconfiguration.

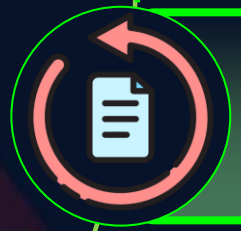
Incident Management Process

1- Preparation:

sets up policies, procedures | identifying critical assets| incident response teams | incident response plans and playbooks |training personnel.

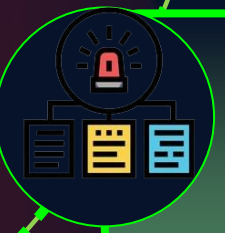
2- Detection and Analysis:

monitoring networks and systems | implementing security tools to spot anomalous behavior | analyzing incidents according to their scope and impact| prioritizing incidents.



3- Containment, Eradication, and Recovery:

controlling incident | eliminate root cause | restoring normal operations | isolating affected systems | removing malware| patching vulnerabilities | securing accounts |data restoration| system reconfiguration.



4- Post-Incident Activity:

learning from the incident | improving future response efforts | updating IRP - DRP - BCP | conducting post-mortem reviews to identify root causes and systemic issues | sharing insights with stakeholders to strengthen cybersecurity awareness and resilience.

OWASP ALGIERS

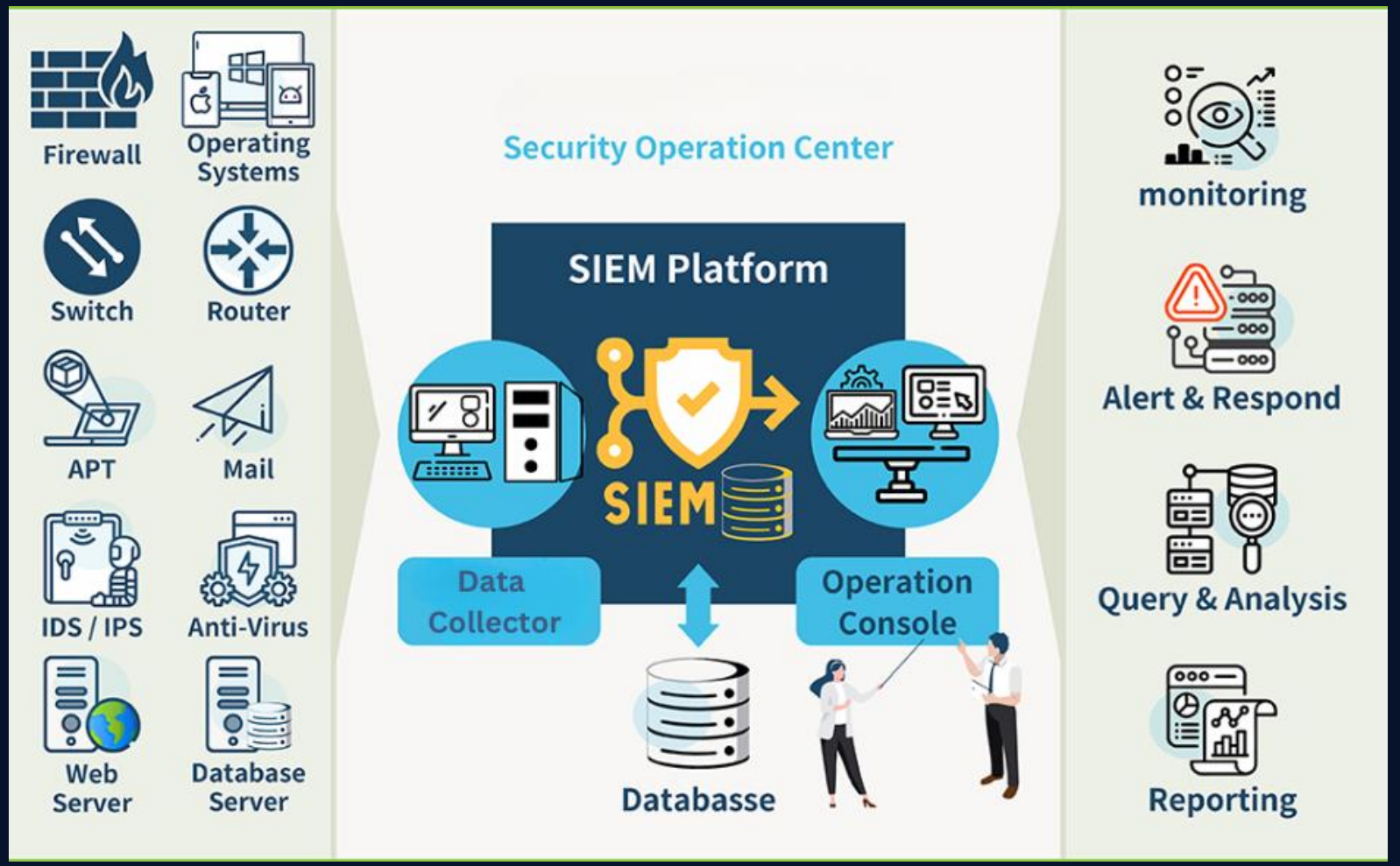
4. Introduction to SIEM

SIEM Definition

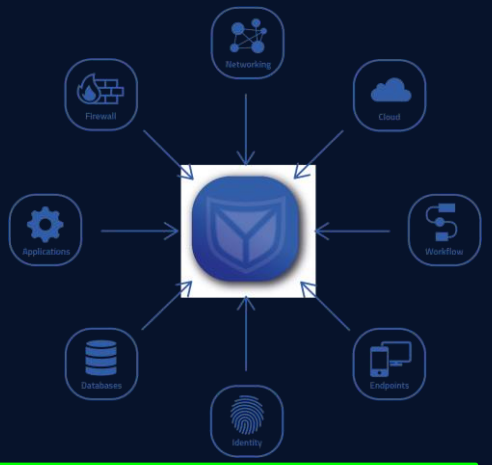
Security Information Management (SIM)

Security Event Management (SEM)

SIEM Definition



SIEM Features



Log Management

Real-time Monitoring

Threat Detection

SIEM Features

Fraud Detection and Prevention

Incident Detection

Compliance Reporting

SIEM Solutions

Commercial

IBM QRadar

FortiSIEM

LogRhythm

splunk>

Open Source

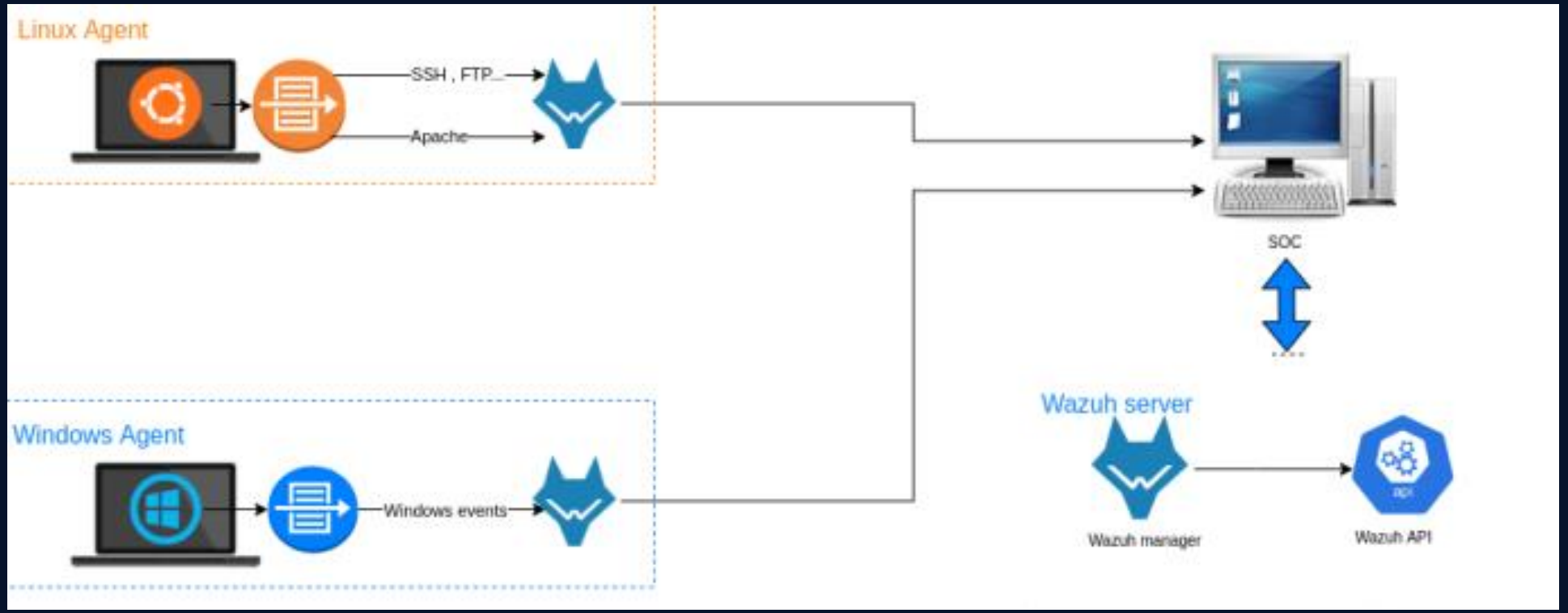
elastic

WAZUH

ALIEN VAULT OSSIM

5. Interactive Demo: SIEM for Incident Detection

Demo Lab



Lab Environment Architecture

6. Conclusion: Strengthening Cyber Resilience with SIEM

Role of SIEM in Bolstering Cyber Resilience

- Real-time monitoring for early threat detection.
- Centralization and correlation of security event data.
- Prioritization of incidents based on severity and impact.
- Compliance reporting to meet regulatory requirements.

Documentation

- **NIST Computer Security Incident Handling Guide:**

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

- **MITRE ATT&CK Website:**

https://attack.mitre.org/

- **MITRE DEFEND:**

https://d3fend.mitre.org/

Free Tranings

TryHackMe

https://tryhackme.com/module/security-information-event-management

https://tryhackme.com/module/security-operations-and-monitoring

Security Blue Team

https://www.securityblue.team/

LetsDefend – Blue Team Training

https://www.letsdefend.io/

Splunk

https://www.splunk.com/en_us/training/free-courses/overview.html

Elastic

https://www.elastic.co/fr/training/free#fundamentals

Thanks for your attention

OWASP ALGIERS

Contact us

ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/

owasp-algiers

OWASP.Algiers