

# 0790326

# Intrusion

# Detection and Prevention

# Systems

2023/2024 – Semester 2

Week 4

17<sup>th</sup> to 19<sup>th</sup> March 2024



جامعة فيلادلفيا  
Philadelphia University

**Dr. Basil Elmasri**

[balmasri@philadelphia.edu.jo](mailto:balmasri@philadelphia.edu.jo)

# SIM and SEM

- Security Information Management (SIM) is a process of gathering, monitoring and investigating log data to find and report suspicious activities on the system.
- This process is *automated* by security information management systems or tools.
- Security Event Management (SEM) is the process of managing the security events happening across the network of an organisation. This process is automated by SEM systems (tools).
- Both are very similar; the main difference is SEM is more an event monitoring while the SIM is more general information monitoring.
- SIM can be a longer term or broader process; more diverse data sets may be analysed in more methodical ways.
- SEM is looking at the specific types of user events that may constitute red flags or tell administrators specific things about network activity.

# SIEM (I)

- Security Information and Event Management (SIEM).
- Combining Security Information Management (SIM) and Security Event Management (SEM) to improve security awareness of an IT environment.
- Enhancing threat detection, compliance, and security incident management through the gathering and analysis of real-time and historical security event data and sources.
  - Supports the incident response capabilities of a SOC.
- SIEM offers enterprise visibility, the entire network of devices and apps.
- Combining data from event, including host systems, networks, firewalls and antivirus security devices.
- Gain attacker insights with threat rules derived from insight into attacker Tactics, Techniques and Procedures (TTP) and known Indicators of Compromise (IoC).

# SIEM (II)

- When an incident or event is identified, analysed and categorised, SIEM works to deliver reports and notifications to the appropriate stakeholders within the organisation.
- Also analysing User and Entity Behaviour Analytics (UEBA) which analyses behaviours and activities to monitor for abnormal behaviours which could indicate a threat.
  - It can also detect behaviour anomalies, and compromised accounts.
- Benefits of SIEM:
  1. Threat Hunting and Detection.
  2. Reduced Response Time Using Enhance Situational Awareness.
  3. Integration & Real-time Visibility.
  4. Security Staffing and Resources.
  5. Compliance Benefits.

# SIEM (III)

- **SIEM Best Practices**
- Setting the scope.
- Fine-tuning correlation rules.
- Identifying compliance requirements.
- Monitoring access to critical resources.
- Defending network boundaries.
- Testing the SIEM.
- Implementing response plan.

# SIEM Best Practices (I)

- Setting the scope:
  - Determining the scope of the SIEM implementation.
  - Building policy-based rules defining activities and logs a SIEM software should monitor.
  - Use that policy and compare its rules to external compliance requirements to determine what type of dashboard and reporting the organisation requires.
- Fine-tuning correlation rules:
  - Setting pre-configured correlation rules.
  - Fine-tuning the software according to the organisation's needs by enabling everything by default, observe the behaviour.
  - Identify tuning opportunities to increase detection efficacy and reduce false positives.

# SIEM Best Practices (II)

- Identify compliance requirements:
  - An organisation should analyse a software's ability to support specific compliance.
- Monitor access to critical resources:
  - Monitor critical resources including privileged and administrative addresses, unusual user behaviour on systems, and remote login attempts, and system failure.
- Defend Network Boundaries:
  - SIEM should monitor vulnerable areas on a network, e.g. firewalls, routers, ports, and wireless access points.
- Testing the SIEM:
  - Reconfiguration can be produced when testing the SIEM implementation and assessing how it reacts.
- Implement response plan:
  - A proper incident response plan to deal with security incidents a timely manner. As well as planning how it will alert staff following a SIEM alert.

# SOC Functions

1. Take Stock of Available Resources.
2. Preparation and Preventative Maintenance.
3. Continuous Proactive Monitoring.
4. Alert Ranking and Management.
5. Threat Response.
6. Recovery and Remediation.
7. Log Management.
8. Root Cause Investigation.
9. Security Refinement and Improvement.
10. Compliance Management.