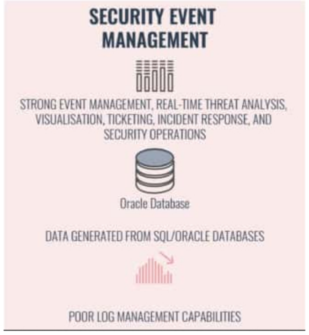
Security Event Management (SEM)

Blue Team Level 1 Certification (Standard) > SI1) Introduction to SIEM > Security Event Manage... IN PROGRESS

Security Event Management, also known as **SEM** is a security software specialized in the identification, collection, monitoring, evaluation, notification and correlation in real-time of events and alerts of a computer system (network devices, security systems (IDS, IPS, Firewall), specialized software (Antivirus), etc.), whose purpose is to identify "suspicious" behavior within the system, to provide an effective and timely response from the security team to any incident that occurs within the network.


SECURITY EVENT MANAGEMENT
STRONG EVENT MANAGEMENT, REAL-TIME THREAT ANALYSIS, VISUALISATION, TICKETING, INCIDENT RESPONSE, AND SECURITY OPERATIONS
Oracle Database
DATA GENERATED FROM SQL/ORACLE DATABASES
POOR LOG MANAGEMENT CAPABILITIES

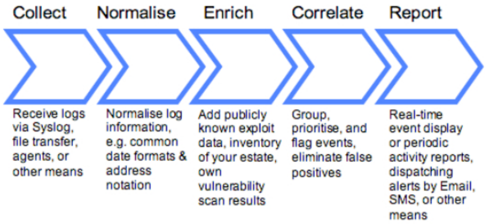
[Figure 1] Security Event Management (provided by Comparitech.com)

WHAT DOES SEM DO?

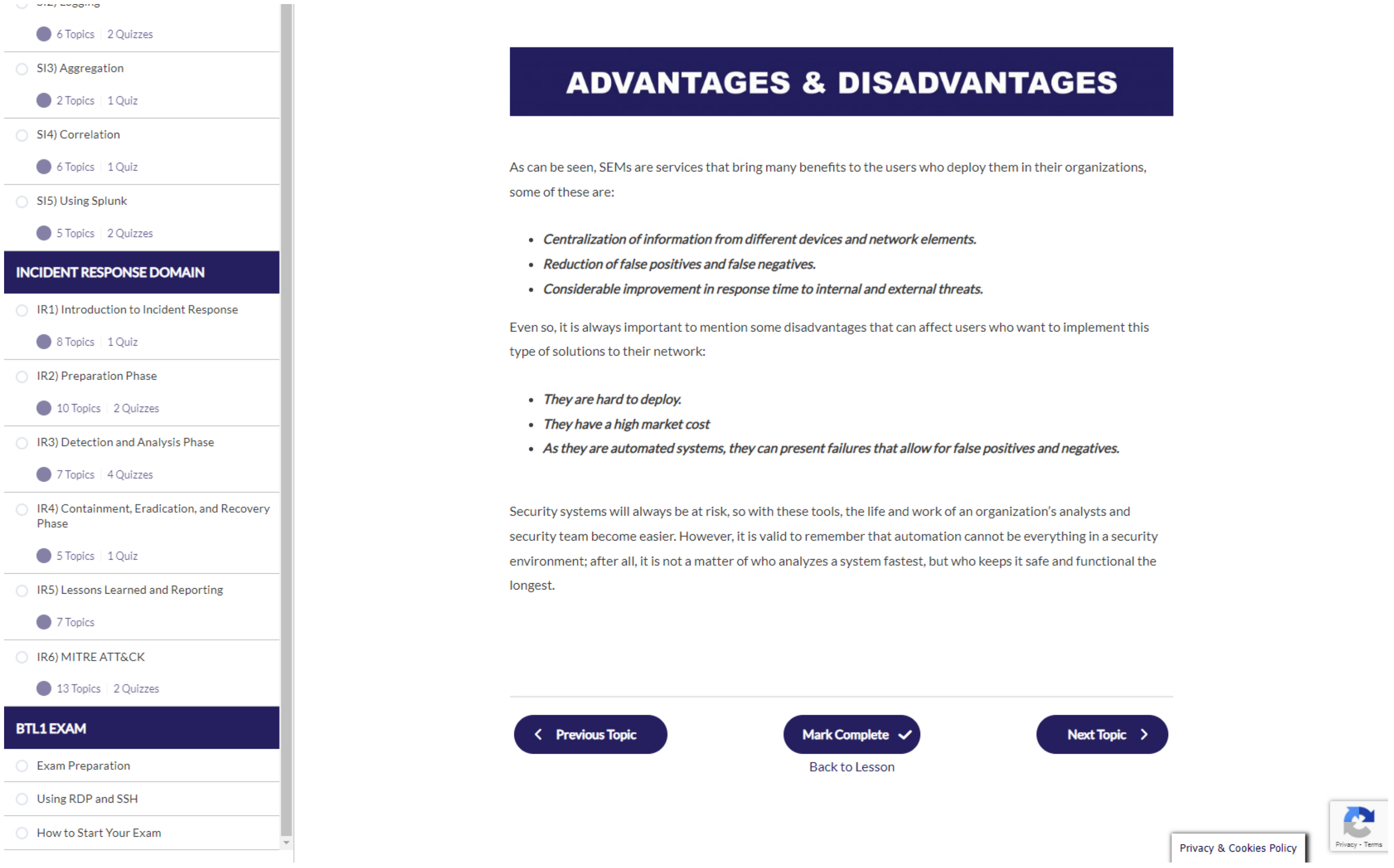
SEMs are mainly in charge of monitoring and analyzing in real-time the existing events in an IT system in search of any kind of anomalous behavior that could mean an infection, incident or threat existing in the system. Some of the actions carried out by SEM software are as follows:

- ***Real-time events monitoring.***
- ***Obtaining security events in devices and applications within the system.***
- ***Correlation of events to provide a clear picture of the information system.***
- ***Analyze logs according to their level of importance.***
- ***Real-time incident response.***

These systems meticulously analyze each record collected, using various security algorithms, statistical calculations, and even vulnerability databases (which contain common weaknesses and its corresponding exploits) to determine whether the system presents any threat, vulnerability or risk at the time of the evaluation (such as anomalous logins, unusual web requests, outdated software, etc.). And then report this information to the organization's security body through reports, graphics, and even alerts via SMS (in case of obtaining a severe vulnerability).


Collect
Normalise
Enrich
Correlate
Report
Receive logs via Syslog, file transfer, agents, or other means
Normalise log information, e.g. common date formats & address notation
Add publicly known exploit data, inventory of your estate, own vulnerability scan results
Group, prioritise, and flag events, eliminate false positives
Real-time event display or periodic activity reports, dispatching alerts by Email, SMS, or other means

[Figure 2] The SEM process (provided by 360is) http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf



SI2) Logging

6 Topics | 2 Quizzes

○ SI3) Aggregation

2 Topics | 1 Quiz

○ SI4) Correlation

6 Topics | 1 Quiz

○ SI5) Using Splunk

5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response

8 Topics | 1 Quiz

○ IR2) Preparation Phase

10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

7 Topics

○ IR6) MITRE ATT&CK

13 Topics | 2 Quizzes

BTL1 EXAM

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam

ADVANTAGES & DISADVANTAGES

As can be seen, SEMs are services that bring many benefits to the users who deploy them in their organizations, some of these are:

- ***Centralization of information from different devices and network elements.***
- ***Reduction of false positives and false negatives.***
- ***Considerable improvement in response time to internal and external threats.***

Even so, it is always important to mention some disadvantages that can affect users who want to implement this type of solutions to their network:

- ***They are hard to deploy.***
- ***They have a high market cost***
- ***As they are automated systems, they can present failures that allow for false positives and negatives.***

Security systems will always be at risk, so with these tools, the life and work of an organization's analysts and security team become easier. However, it is valid to remember that automation cannot be everything in a security environment; after all, it is not a matter of who analyzes a system fastest, but who keeps it safe and functional the longest.

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >