Blue Team Level 1 Certification (Standard)

PA7) Report Writing
7 Topics | 1 Quiz
PA8) Phishing Response Challenge
3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 1 Quiz
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz

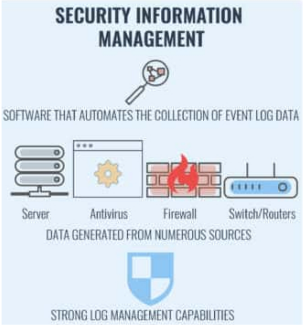
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
Section Introduction, SIEM
Security Information Management (SIM)
Security Event Management (SEM)
What is a SIEM?
SIEM Platforms
Further Reading Material, SIEM
SIEM Glossary
Activity) End of Section Review, SIEM
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk

Security Information Management (SIM)

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

Security Information Management, also known as **SIM** is specialized security software that helps with the collection, monitoring, and analysis of data and event logs generated from all security devices in a network (IDS, IPS, Antivirus Software, Firewalls). Facilitating the task of the investigators and the security team of an organization by centralizing all this information in a single service.


SECURITY INFORMATION MANAGEMENT
SOFTWARE THAT AUTOMATES THE COLLECTION OF EVENT LOG DATA
Server
Antivirus
Firewall
Switch/Routers
DATA GENERATED FROM NUMEROUS SOURCES
STRONG LOG MANAGEMENT CAPABILITIES

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

WHAT DOES SIM DO?

SIMs are mainly concerned with the collection and translation of information relating to the operation of a network. These elements collect data and logs from devices within an organization, and may even collect information from some devices or sources outside the organization (such as public threat identification services and correlation networks), looking for patterns that will allow the system to understand the activity, operation and behavior of these devices, and then make reports, graphs and charts that will be presented to the user. Some of the actions performed by a SIM are:

- *Monitoring of events in real-time.*
- *Sending and generating alerts and reports.*
- *Automatic response to incidents.*
- *Correlation of data from multiple sources to improve the quality of the information presented.*
- *Translation of event-logs from different resources through XML files.*

However, and despite the enormous help that this type of service provides, it is necessary to clarify that these are not applications that can operate correctly without the help of security personnel and members of the organization. Therefore, it is always recommended to have a good security policy that complements the operation of this type of product.

ADVANTAGES & DISADVANTAGES

SIMs are services that bring many benefits to the users who implement them in their organizations, some of which are:

○ 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

- *Easy to deploy.*
- *They can store and analyze large volumes of data.*
- *They allow a fast and efficient analysis of all events in a system.*
- *They correlate logs and events to provide the most accurate overview of the system.*
- *They allow for easy threat management (assessment, containment, and analysis)*

However, it is always important to mention some disadvantages that may affect users who want to apply this type of solution to their network:

- *They can be very expensive tools.*
- *It is not completely certain that they can be properly adapted to the working environment.*
- *Some providers do not provide full technical support for this type of service.*

IT system security will always be a real battleground, and investigators and security professionals can not always be aware of every situation, so these tools can be the difference between a well-timed response and a data breach. A SIM will not be able to protect you from all threats, but they can help you identify the vast majority.

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›