Blue Team Level 1 Certification (Standard) ‹

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

○ 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

○ Section Introduction, Incident Response

○ What is Incident Response?

○ Why is Incident Response Needed?

○ Security Events vs Security Incidents

○ Incident Response Lifecycle (NIST SP 800 61r2)

○ CSIRT and CERT Explained

○ Further Reading Material, Incident Response

○ Incident Response Glossary

Activity) End of Section Review, Incident Response

○ IR2) Preparation Phase

● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

Section Introduction, Incident Response

Blue Team Level 1 Certification (Standard) > IR1) Introduction to Incident Response > Section In... IN PROGRESS

This section is intended to provide an introduction to incident response. Therefore (and with the purpose of presenting good practices in this field) we will make use of the NIST SP 800-61r2 incident response standard.

You will learn what incident response is, will understand why the implementation of this kind of programs is crucial in the defense of systems and response to cyber-attacks. And you will have the opportunity to examine a variety of methodologies (such as the *Lockheed Martin Cyber Kill Chain*, and *MITRE's ATT&CK* Framework) that will allow you to understand not only the life cycle of computer attacks but also the importance of communication between organizations and security teams in the fight against cyber attacks.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand exactly what incident response is, and why it's a crucial part of cybersecurity operations.
- Understand the difference between security events and security incidents, and be able to provide examples.
- Understand the NIST SP 800 61r2 Incident Response lifecycle and cyber-attack frameworks such as the ***"Lockheed Martin Cyber Kill Chain"*** and the ***"MITRE ATT&CK"*** framework.

‹ Previous Lesson

Mark Complete ✓

Next Topic ›

Back to Lesson