Blue Team Level 1 Certification (Standard)
Management Principles
4 Topics | 1 Quiz
Section Introduction, Management Principles
Risk
Policies and Procedures
Compliance & Frameworks
Activity) End of Section Review, Management Principles
PHISHING ANALYSIS DOMAIN
PA1) Introduction to Emails and Phishing
7 Topics | 1 Quiz
PA2) Types of Phishing Emails
10 Topics | 2 Quizzes
PA3) Tactics and Techniques Used
12 Topics | 2 Quizzes
PA4) Investigating a Phishing Email
8 Topics | 2 Quizzes
PA5) Analysing URLs, Attachments, and Artifacts
8 Topics | 1 Quiz
PA6) Taking Defensive Actions
12 Topics | 1 Quiz
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 | 2 Quizzes
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

Risk

Simply put, a risk is the possibility of a negative impact on practically anything i.e., business, financial, security, there are many areas where risk may reside. A vulnerability is a weakness that can be exploited by a threat. Vulnerabilities can be managed whereas a threat cannot. Management of risk is done by applying controls to bring the risk to an acceptable level. Risk can be at different levels in an organization, from a single piece of equipment to a whole department or division.

The likelihood that a threat will exploit a vulnerability depends on the existence of the threat, the vulnerability, and how effective the controls in place are.

RISK ASSESSMENTS

Risk assessments are conducted to identify and determine the impacts of risk, the likelihood and the consequences should a risk materialize. These can help organizations make informed decisions based on the outcome of the assessment. Some risk assessments are required by law and so risk assessments are carried out to comply with these laws and regulations.

For example, there is a risk of a corporate laptop being lost by an employee, the likelihood is the probability it will occur and the consequence/impact is equipment & data loss. A risk assessment highlights this and enables mitigation to be put in place to prevent the consequence from ever materializing.

CONDUCTING AN ASSESSMENT

There are various ways risk assessments are carried out, but the basic steps are below:

- Identifying potential hazards
- Identifying who might be harmed by those hazards
- Evaluating risk (severity and likelihood) and establishing suitable precautions
- Implementing controls and recording your findings
- Reviewing your assessment and re-assessing if necessary.

Risk assessments should be dynamic to be effective, they should be periodically reviewed and updated. In the world of cybersecurity, things are always changing at a fast pace and so should a risk assessment change with the risks.

MANAGING RISK

Risk can be managed in four different ways depending on the organisation's risk appetite or objectives.

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
SI2) Logging
6 Topics 2 Quizzes
SI3) Aggregation
2 Topics 1 Quiz
SI4) Correlation

Previous Topic
Back to Lesson
Next Topic

Privacy & Cookies Policy
Privacy - Terms