

Blue Team Level 1 Certification
(Standard)

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 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

○ SI2) Logging

6 Topics 2 Quizzes

○ SI3) Aggregation

2 Topics 1 Quiz

○ SI4) Correlation

6 Topics 1 Quiz

Incident Response Metrics

Blue Team Level 1 Certification (Standard) > IR5) Lessons Learned and Reporting > Incident Res...

IN PROGRESS

Incident Response Domain METRICS AND REPORTING



Metrics are numerical values used for quantitative assessment, allowing us to assess, compare, and track performance. Regarding incident response, it can highlight areas where the team has responded efficiently or ineffectively. These metrics can also help to identify trends in incidents that the organization is facing so they can be addressed, using metrics to support a business case to receive more budget or personnel.

There are many different options for using metrics to summarise the response to an incident and compare it to previous and future incidents. In this lesson, we will cover several common metrics that can be used for reporting purposes, allowing security teams to highlight their strengths and weaknesses, and use them to support business decisions such as increased headcount or budget.

Please note that different organizations will use different metrics, this is aimed to give you a general idea of what metrics can be recorded.

IMPACT METRICS

- **Service Level Agreement (SLA)** – SLAs are an agreement between an organization and its customer that determines expectations for things such as uptime, responsiveness, and responsibilities of both parties. This is often calculated using percentages with two of the most common ones being 99% and 99.9%.
- **Service Level Objective (SLO)** – SLOs are an agreement that exist within the SLA that determines that specific metric being measured, such as the uptime of a critical virtual machine. Measuring these objectives can hold both the organization and potentially client liable in the case that the objective is not met.
- **Escalation Rate** – This metric will measure how often alerts in your SIEM are being assigned to the correct security team member. This can help prevent a brand-new analyst receiving an alert for a sophisticated ransomware attack and dismissing it or taking it on themselves, rather than escalating the alert, to a more senior level analyst who has handled this ransomware before and knows the signs of a breach.

TIME-BASED METRICS

- **Mean Time to Detect (MTTD)** – Also known as the mean time to acknowledge (MTTA), this is the average amount of time it takes for the security team to notice that a security incident has occurred. Measuring this metric is important because it can help increase the effectiveness of alerts sent to a SIEM or another logging platform.
- **Mean Time to Response (MTTR)** – Also known as the mean time to repair, resolve or recovery, this is the time from when something is detected, and when the security team can take action to address it. This is often one of the most important metrics to track because it can show how efficient the team was when responding to the incident and can help identify key areas where the response time could improve.
- **Incidents Over Time** – This metric looks at the average number of incidents over a period of time to determine whether there is an increase or decrease of incidents. This metric helps determine whether changes need to be made to allow for more security to prevent incidents or to determine if the lower incident count is correlating to another event.
- **Remediation Time** – How long did it take the incident responders and appropriate stakeholders to remediate the situation (recovering all affected systems and returning to production status)?

SIS) 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

Section Introduction, Lessons Learned and Reporting

What Went Well?

What Can be Improved?

Importance of Documentation

Incident Response Metrics

Reporting Format

Reporting Considerations

IR6) MITRE ATT&CK

13 Topics

2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam

INCIDENT TYPE METRICS

- **Cumulative Number of Incidents Per Types** – by categorizing incidents based on their type and comparing the total number of each incident category, this can provide security teams with an overview of where improvements need to be made. For example, if an organization had a high number of incidents caused by attackers exploiting vulnerabilities in internet-facing systems, then the organization would see they need to perform the vulnerability management process to patch these systems and apply mitigating controls such as web application firewalls and proxies.
- **Alerts Created per Incident** – This metric will help analyze how many alerts were created for the specific incident. For example, in an incident did the EDR send out an alert that a malicious file has been downloaded, but did your O365 environment not generate an alert as well? This metric can help see where in the Cyber Kill Chain process, you can improve your defenses, and, in this example, help prevent the malware from being downloaded in the first place.
- **Cost per Incident (CPI)** – This metric analyzes the perceived cost of the incident at the affected company and could be analyzed in a few different ways. One way would be analyzed by the duration of the incident and multiplying it by the cost of the security team and/or team member that worked on and resolved the case. Another way is calculated by analyzing the impact that the incident had on the business, such as a loss of sales made, productivity lost or destruction of equipment or computers. This metric can be most useful when a business impact analysis (BIA) has already been conducted with the client to establish the base costs of their organization.

<

Previous Topic

Mark Complete


✓

Back to Lesson

Next Topic

>

Privacy & Cookies Policy

Privacy & Terms