Blue Team Level 1 Certification (Standard)
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
Section Introduction, Tactical Intelligence
Threat Exposure Checks Explained
Watchlists/IOC Monitoring
Public Exposure Checks Explained
Threat Intelligence Platforms
Malware Information Sharing Platform (MISP)
Activity) Deploying MISP
Activity) End of Section Review, Tactical Intelligence
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

Watchlists/IOC Monitoring

IOC monitoring is an important part of security operations, and can help alert security analysts to malicious activity by monitoring for the presence of any precursors or indicators of compromise across the environment. Watchlists are typically created in either the SIEM or EDR platform (or both).

This allows Threat Exposure Checks (TECs) to be conducted continuously without a need for a human threat intelligence analyst to perform the searches themselves, freeing them up to work on more important tasks.

Let's go through an example to demonstrate how this capability could be utilised within a Security Operations Center:

Example – Malicious IP Watchlist

A Threat Intelligence Analyst is given a list of IP addresses that have been acting malicious (used for command-and-control, scanning IPs, used to host malware, etc). The Analyst decides to create a watchlist within their SIEM platform to generate an alert whenever a malicious IP address is observed as either the Source or Destination IP.

This alert fires when an employee clicks a malicious link in a phishing email, taking them to a webserver hosted on one of the monitored IPs that is used to distribute malware. A Security Analyst opens the alert and can determine what has happened and can take action to protect the user.