Blue Team Level 1 Certification (Standard)

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

Section Introduction, Strategic Intelligence

Intelligence Sharing and Partnerships

IOC/TTP Gathering and Distribution

OSINT vs Paid-for Sources

Traffic Light Protocol (TLP)

Activity) End of Section Review, Strategic Intelligence

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

SI5) Using Splunk

5 Topics | 2 Quizzes

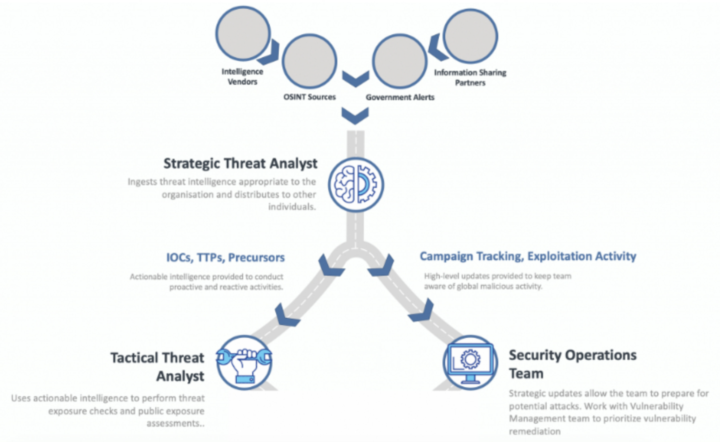
IOC/TTP Gathering and Distribution

Blue Team Level 1 Certification (Standard) > TI5) Strategic Threat Intelligence > IOC/TTP Gathe... IN PROGRESS

While the task of collecting and distributing indicators of compromise and TTPs can be complete by anyone, it makes sense for a strategic threat intelligence analyst to perform this duty, as they will regularly be in contact with information sharing partners and receive government-issued alerts from organizations such as NCCIC, US-Cert, NCSC, and more.

This task includes gathering IOCs regarding threat actors that are likely to target the organization, as trying to digest IOCs from every single cyberattack out there will generate a lot of noise and overwhelm defenders with alerts and false positives. If a threat actor is targeting banks and banking systems, the threat intelligence team at an aerospace company isn't going to be running the same equipment, and therefore is unlikely to encounter that specific threat agent.

IOCs that are gathered from threat intelligence vendors, government alerts, information sharing partners, and public sources are then passed down to tactical threat intelligence analysts, or the wider security team based on the information. We've created a diagram to help visualize this process.


Intelligence Vendors
OSINT Sources
Government Alerts
Information Sharing Partners
Strategic Threat Analyst
Ingests threat intelligence appropriate to the organisation and distributes to other individuals.
IOCs, TTPs, Precursors
Actionable intelligence provided to conduct proactive and reactive activities.
Campaign Tracking, Exploitation Activity
High-level updates provided to keep team aware of global malicious activity.
Tactical Threat Analyst
Uses actionable intelligence to perform threat exposure checks and public exposure assessments..
Security Operations Team
Strategic updates allow the team to prepare for potential attacks. Work with Vulnerability Management team to prioritize vulnerability remediation

EXAMPLE WALKTHROUGH

The strategic threat intelligence analyst at Organisation A receives an email from an analyst at Organisation B, who is in their industry-specific information sharing partnership (ISAC). Organisation B's analyst informs the strategic analyst that they have just been hit by an APT who specifically targets the industry they operate in, and during incident response, they collected IOCs including IP addresses that were used to scan and exploit systems at Org B. The strategic analyst then passes these IOCs to a tactical threat analyst who performs threat exposure checks within the SIEM platform to see if the same IPs have scanned Org A recently based on perimeter firewall logs.

The strategic analyst also provides the wider security operations team with a situational awareness email, informing everyone that a similar organization has been hit by an APT, and that they may target Org A in the near future.

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response

● 8 Topics | 1 Quiz

○ IR2) Preparation Phase

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson

Privacy & Cookies Policy

Privacy - Terms