Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- Welcome to Blue Team Level 1!
  - 4 Topics
- Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

- Introduction to Security Fundamentals
  - 1 Topic
- Soft Skills
  - 7 Topics
- Security Controls
  - 5 Topics | 1 Quiz
  - Section Introduction, Security Controls
  - Physical Security
  - Network Security
  - Endpoint Security
  - Email Security
  - Activity) End of Section Review, Security Controls
- Networking 101
  - 6 Topics | 1 Quiz
- Management Principles
  - 4 Topics | 1 Quiz

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

Endpoint Security

This lesson will introduce you to some basic endpoint defenses, and what they do to protect systems from attack. These security controls will be expanded on in future domains of this course; this lesson is purely designed to provide a foundation that will be continuously built on.

HOST INTRUSION DETECTION

Host intrusion detection systems, also known as HIDS, is software installed on an endpoint that allows for the detection of suspicious or malicious activity using rules which are checked against activity to see if it matches any known malicious patterns. This security control will generate alerts (hence the name host intrusion "detection" system) so that human analysts can investigate further from a HIDS solution interface. Alternatively, alerts can also be pushed to a SIEM platform (covered below under the Security Monitoring heading) to inform analysts to investigate.

HOST INTRUSION PREVENTION

Host intrusion prevention systems, also known as HIPS, is software installed on an endpoint that works similarly to HIDS but is able to take autonomous actions to defend systems once malicious activity has been detected instead of just alerting human analysts (hence the name host intrusion "prevention" system). Rules are written to search for specific patterns of activity, but with HIPS these rules contain actions, so the software knows what to do when unusual activity is detected. This can include terminating connections to websites or IP addresses, deleting malicious files, or generating an alert.

ANTI-VIRUS SOLUTIONS

Anti-virus software, commonly abbreviated to "AV" should be deployed on all endpoints, such as desktops, laptops, and servers. This is a fundamental security control that works to detect and remove known malware that is present on the system. There are two types of anti-virus solutions:

- **Signature-based:**

The AV solution will use signatures which are specific patterns of activity to identify previously documented malware, either removing the file, generating an alert, or quarantining the malware. Unfortunately, if the AV vendor doesn't have the signature of a certain type of malware, it will not be detected by this type of anti-virus and can potentially execute successfully.

- **Behavior-based:**

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
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
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH

This type of unconventional AV works to identify suspicious behavior by creating a baseline of "normal" activity and working to identify any deviations or anomalies that don't fit the baseline, as these could indicate suspicious or malicious activity.

EVENT MONITORING

Endpoints can be configured to send logs to a centralized location, a SIEM platform, where this data is aggregated, normalized, and is matched against a number of rules designed to detect and flag suspicious or unusual activity so it can be investigated by security analysts. If an endpoint is sending logs, whether it's a desktop, laptop, or server, and it starts acting unusually the SIEM should pick this up and generate an alert to signal a human investigation. We can use Syslog to achieve this level of logging and monitoring by combining it with a SIEM platform. We'll cover this in a lot more detail during the SIEM domain.

ENDPOINT DETECTION & RESPONSE

EDR agents are pieces of software that sit silently on endpoints and provide logging, monitoring, and reactive capabilities. Similar to HIDS and HIPS, EDR agents will report activity back to a platform similar to a SIEM, where analysts can log in and investigate alerts generated by the EDR solution. These solutions will typically allow analysts to conduct investigations straight from the platform and see exactly what processes are running on monitored systems, and conduct in-depth investigations to analyze the suspicious activity. EDR platforms can also be utilized to monitor for insider threat by closely watching exactly what certain users are doing, combining this with other forensic-grade tools can retrieve specific information from a system such as sites visited, messages sent, and programs run.

VULNERABILITY SCANNING

Routine vulnerability scans should be conducted against endpoints to detect misconfigurations, security flaws, and vulnerabilities that could be exploited by an attacker to gain access to a system, execute malicious code, or cause a denial-of-service. These scans can be conducted either internally or externally.

- **External scans –** typically conducted by scanners in the cloud can provide an organization with an "attackers view" by seeing what systems and weaknesses are discovered on internet-facing systems with security controls and firewalls working.
- **Internal scan –** give a more comprehensive view of the security posture of internal systems, but does not necessarily reflect what an attacker would see, unless they gained access inside the network and started vulnerability scanning from within.

Scans can either be non-credentialed or credentialed, meaning that the scanner is able to log in to systems with high privileges and collect a lot more information about configurations, program versions, and more. However, a non-credentialed scan can give a better view of what an attacker would see, and can help to prioritize what vulnerabilities have a higher likelihood of being exploited, so they can be remediated first.

Once a vulnerability scan is complete, the results should be analyzed and sent to appropriate system owners so they can be addressed.

COMPLIANCE SCANNING

Some compliance frameworks require endpoints to meet a minimum standard of security, and vulnerability scanners will often have profiles or pre-set setting configurations to look specifically for details that the compliance framework covers, allowing defenders to see if any systems do not meet the requirements. We will cover compliance in more detail in the next section of the Security Fundamentals domain.

How to Start Your Exam

Previous Topic

Back to Lesson

Next Topic

Privacy & Cookies Policy

Privacy - Terms