

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

✓ 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

○ 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

Prevention: Host Defenses

Blue Team Level 1 Certification (Standard) > IR2) Preparation Phase > Prevention: Host Defenses

IN PROGRESS

Incident Response Domain PREVENTION: HOST DEFENSES



We have already looked at some basic host defenses in the Security Fundamentals domain. This lesson is going to cover host defenses in greater detail, to help you understand common security controls to defend systems themselves. We will be covering HIDS and HIPS, anti-virus, endpoint detection, and response (EDR) agents, local firewalls, vulnerability scanning, and group policies for Windows domains.

HOST INTRUSION DETECTION

Host intrusion detection systems, also known as HIDS, are 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. Typically this security control will generate alerts (detection) so that human analysts can investigate further.

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. 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:**

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

<input type="radio"/> DF3) Digital Evidence Collection
8 Topics 1 Quiz
<input type="radio"/> DF4) Windows Investigations
3 Topics 3 Quizzes
<input type="radio"/> DF5) Linux Investigations
4 Topics 2 Quizzes
<input type="radio"/> DF6) Volatility
3 Topics 1 Quiz
<input type="radio"/> DF7) Autopsy
4 Topics 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
<input type="radio"/> SI1) Introduction to SIEM
7 Topics 1 Quiz
<input type="radio"/> SI2) Logging
6 Topics 2 Quizzes
<input type="radio"/> SI3) Aggregation
2 Topics 1 Quiz
<input type="radio"/> SI4) Correlation
6 Topics 1 Quiz
<input type="radio"/> SI5) Using Splunk
5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN
<input type="radio"/> IR1) Introduction to Incident Response
8 Topics 1 Quiz
<input checked="" type="radio"/> IR2) Preparation Phase
10 Topics 2 Quizzes
<input type="radio"/> Section Introduction, Preparation
<input type="radio"/> Preparation: Incident Response Plan
<input type="radio"/> Preparation: Incident Response Teams
<input type="radio"/> Preparation: Asset Inventory and Risk Assessments
<input type="radio"/> Prevention: DMZ
<input checked="" type="radio"/> Prevention: Host Defenses
<input type="radio"/> Prevention: Network Defenses
<input checked="" type="radio"/> Legacy Activity) Setting up a Firewall
<input type="radio"/> Prevention: Email Defenses
<input type="radio"/> Prevention: Physical Defenses
<input type="radio"/> Prevention: Human Defenses
<input checked="" type="radio"/> Activity) End of Section Review, Preparation
<input type="radio"/> IR3) Detection and Analysis Phase
7 Topics 4 Quizzes
<input type="radio"/> IR4) Containment, Eradication, and Recovery Phase
5 Topics 1 Quiz
<input type="radio"/> IR5) Lessons Learned and Reporting
7 Topics
<input type="radio"/> IR6) MITRE ATT&CK
13 Topics 2 Quizzes
BTL1 EXAM
<input type="radio"/> Exam Preparation
<input type="radio"/> Using RDP and SSH
<input type="radio"/> How to Start Your Exam

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 threats by closely watching exactly what certain users are doing. This can be combined with other forensic-grade tools to retrieve specific information from a system such as sites visited, messages sent, and programs run.

LOCAL FIREWALLS

Operating in the same way as hardware firewalls, local firewalls or web application firewalls can provide even tighter security using rules that apply to the system the firewall is running on. The software will allow administrators to decide what ports should be open, and allow or deny connections coming in or going out of the system.

GROUP POLICIES

If you care about data security, you need to understand group policies. We will discuss what group policies and GPOs are and how system administrators use them to protect, secure and lockdown computers and user accounts. A Group Policy Object is a collection of settings systems administrators create with the Microsoft Management Console (MMC) Group Policy Editor. The GPO can be associated with one or more of the Active Directory containers, such as sites, domains, or organizational units(OUs).

Active Directory applies GPOs in the following predictable and logical order.

1. **Local policies**
2. **Site policies**
3. **Domain policies**
4. **OU policies**

So what can GPOs actually do? One example is using Group Policy Objects to completely disable Local Administrator rights globally in your network and instead, grant administrative permissions to a single individual or group based on their job. Ideally, you are implementing a least-privileged model where even the system administrators are limited to administering only the servers they are assigned.

Strengths of GPOs

There are several advantages to implementing GPOs outside of security.

- **Ease of management:** Setting up new users on the network used to be a long and tedious process. Pre-existing GPOs apply a standardized environment to each new user and computer that joins your domain which saves many hours of configurations.
- **One-stop administration:** Sysadmins can deploy patches, software, and other updates via GPO.
- **Password policy enforcement:** Passwords can be easily brute-forced if they aren't changed regularly, contain simple words, or are short. GPOs establish length, reuse rules, and other requirements for passwords to keep your network safe.
- **Folder redirections:** Do you want users to keep important company files on a centralized and monitored storage system? Use a folder redirection GPO to redirect their user folder to your NAS.

Weaknesses of GPOs

By now it sounds like GPOs are the bee's knees. There are a few pitfalls to using GPOs you want to consider before you dive in headfirst.

GPOs update randomly every 90 to 120 minutes or so, or when the computer gets rebooted. You can specify an update rate from 0 to 64,800 minutes (or 45 days), but if you select 0 minutes, the computer tries to update GPOs every 7 seconds. That's going to murder a network with traffic. If you must implement an emergency GPO update, you have to keep this in mind and use another method to get users to reboot.

Also, the GPO editor isn't the best and most intuitive thing in the world. You can learn to use PowerShell instead to make all the updates, which could be easier for a command line person.


[Previous Topic](#)

Mark Complete ✓

Back to Lesson

[Next Topic](#)

Privacy & Cookies Policy

Privacy & Terms