Blue Team Level 1 Certification (Standard)
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
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

Email Security

Phishing is the number one attack vector for compromising organizations, leading to data breaches. Even today it seems that email security is always an afterthought when it really should be a top priority. This lesson will introduce you to some basic email defenses, and what they do to protect the organization from attacks. These security controls will be expanded on in future domains of this course, this lesson is designed to provide a foundation which will be constantly built on. It is important to note that malicious emails are targeting the human instead of any IT systems, and employees need to be trained to spot and respond to malicious emails that bypass any technical defenses that are put in place.

SPAM FILTER

A spam filter is a piece of software that scans incoming emails to see if they have telltale signs of spam or malicious emails and prevents them from being delivered to employee mailboxes so that they don't fill up with junk or dangerous messages. This is a basic but core security control when considering emails, and whilst some emails will get through, this provides a frontline defense reducing the work for security analysts and other security technologies.

DATA LOSS PREVENTION

Data loss prevention (DLP) or data leak prevention is a security control that works to prevent an unauthorized sensitive business or personal information from leaving the organization. This data can be categorized as files, banking information, account credentials, or PII; for the purpose of this module, we are focusing on the application of DLP technologies to email communication (we'll cover the other applications of DLP later in the course). Depending on the DLP solution in use, it can monitor outgoing emails at different levels, such as:

- email body content
- email headers
- email attachments of various types

If the DLP solution deems important information is about to be sent out of the organization, these emails will not make it past the email gateway and will not be sent. Emails can be scanned for specific keywords or use regex queries to flag messages containing certain content. If a disgruntled employee wants to send business-critical information to a rival organization before they are fired, they could attempt to send documents outside the organization by email – DLP would detect this, alert the security team, and prevent the email from being sent.

EMAIL SCANNING

Typically phishing emails will contain either a malicious URL or a malicious attachment (or both), and specially designed scanners will read the email header and body, and work to identify malicious indicators either using patterns or signatures, or blacklists that include lists of known malicious email senders, file hashes, and domain

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

patterns or signatures, or blacklists that include lists of known malicious email senders, file hashes, and domain names. When a suspicious email has been detected it can be quarantined so it's not delivered to an employee mailbox, and an alert generated to inform the security team to investigate.

SECURITY AWARENESS TRAINING

Security awareness training should be a mandatory program that new employees must complete, as well as be completed routinely by all employees, with time frames often dictated under different compliance frameworks (which we cover in a lesson under the Management Principles section within this domain). While this will focus on all different areas of security, phishing should play a large role in this. Employees need to be told clearly how to spot suspicious or malicious indicators, and what steps the organization wants them to take, such as messaging or ringing the security team to alert them, or forwarding emails to a specific mailbox. Emails will get through technical controls, so it is crucial that employees who receive them know what to do, and don't click on any links or run any attachments. Security awareness training can also be paired with simulated phishing campaigns conducted by the security team, to highlight metrics such as the number of employees that have reported the email to security and employees that have clicked on the (harmless) malicious link.

Previous Topic
Back to Lesson
Next Lesson

Privacy & Cookies Policy
Privacy - Terms