**Introduction to Cyber Security**

This course introduces the fundamentals of cybersecurity, including the concepts needed to recognize and potentially mitigate attacks against home networks and mission-critical infrastructure.

After you complete this training, you should be able to:

* Describe the current cybersecurity landscape
* Identify cybersecurity threats
* Evaluate different malware types and cyberattack techniques
* Describe the relationship between vulnerabilities and exploits
* Identify how spamming and phishing attacks are performed
* Describe Wi-Fi vulnerabilities, attacks, and advanced persistent threats
* Explain perimeter-based Zero Trust security models
* Identify capabilities of the Palo Alto Networks prevention-first architecture

***Lesson Topics:***

This course comprises five lessons and takes about two hours to complete.

* Lesson 1: Cyber Security Landscape
* Lesson 2: Cyberattack Types
* Lesson 3: Cyberattack Techniques
* Lesson 4: APTs and Wi-Fi Vulnerabilities
* Lesson 5: Security Models

***Lesson 1: Cyber Security Landscape:***

The modern cybersecurity landscape is a rapidly evolving hostile environment with advanced threats and increasingly sophisticated threat actors. This lesson describes the current cybersecurity landscape, explains SaaS application challenges, describes various security and data protection regulations and standards, identify cybersecurity threats and attacker profiles, and explains the steps in the cyberattack lifecycle.

***Modern Computing Trends:***

The nature of enterprise computing has changed dramatically over the past decade.

**Introduction to Web 2.0 and Web 2.0 Applications**

Core business applications are now commonly installed alongside Web 2.0 apps on a variety of endpoints. Networks that were originally designed to share files and printers are now used to collect massive volumes of data, exchange real-time information, transact online business, and enable global collaboration. Many Web 2.0 apps are available as software-as-a-service (SaaS), web-based, or mobile apps that can be easily installed by end users or that can be run without installing any local programs or services on the endpoint

**Web 3.0**

The vision of Web 3.0 is to return the power of the internet to individual users, in much the same way that the original Web 1.0 was envisioned. To some extent, Web 2.0 has become shaped and characterized, if not controlled, by governments and large corporations dictating the content that is made available to individuals and raising many concerns about individual security, privacy, and liberty. AI and Machine Learning

**New Application Threat Vectors**

Exploiting vulnerabilities in core business applications has long been a predominant attack vector, but threat actors are constantly developing new tactics, techniques, and procedures (TTPs).

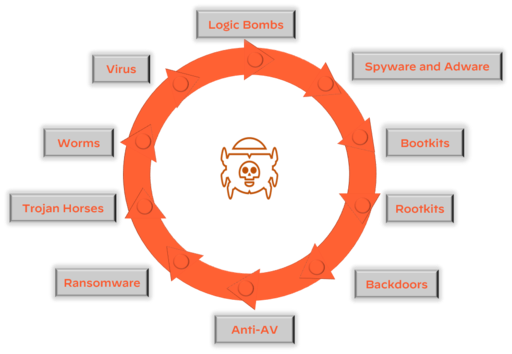
**Protect Networks and Cloud Environments**

To effectively protect their networks and cloud environments, enterprise security teams must manage the risks associated with a relatively limited, known set of core applications, as well as the risks associated with an ever-increasing number of known and unknown cloud-based applications. The cloud-based application consumption model has revolutionized the way organizations do business, and applications such as Microsoft Office 365 and Salesforce are being consumed and updated entirely in the cloud.

***Lesson 2: Cyberattack Types:***

Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack strategy. This lesson describes the different malware types and properties, the relationship between vulnerabilities and exploits, and how modern malware plays a central role in a coordinated attack against a target. This lesson also explains the timeline of eliminating a vulnerability.

***Malware Types:***



**Logic Bombs**

A logic bomb is malware that is triggered by a specified condition, such as a given date or a particular user account being disabled.

**Spyware and adware**

Spyware and adware are types of malwares that collect information, such as internet surfing behavior, login credentials, and financial account information, on an infected endpoint. Spyware often changes browser and other software settings and slows computer and internet speeds on an infected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as pop-up banners.

**Rootkits**

A rootkit is malware that provides privileged (root-level) access to a computer. Rootkits are installed in the BIOS of a machine, which means operating system-level security tools cannot detect them.

**Backdoors**

A backdoor is malware that allows an attacker to bypass authentication to gain access to a compromised system.

**Trojan Horses**

A Trojan horse is malware that is disguised as a harmless program but actually gives an attacker full control and elevated privileges of an endpoint when installed. Unlike other types of malware, Trojan horses are typically not self-replicating.

**Worms**

A worm is malware that typically targets a computer network by replicating itself to spread rapidly. Unlike viruses, worms do not need to infect other programs and do not need to be executed by a user or process.

**Virus**

A virus is malware that is self-replicating but must first infect a host program and be executed by a user or process.

**Ransomware Types:**

Ransomware is malware that locks a computer or device (locker ransomware) or encrypts data (crypto ransomware) on an infected endpoint with an encryption key that only the attacker knows, thereby making the data unusable until the victim pays a ransom (usually in cryptocurrency such as Bitcoin).

***Lesson 3: Cyberattack Techniques***

Attackers use a variety of techniques and attack types to achieve their objectives. Spamming and phishing are commonly employed techniques to deliver malware and exploits to an endpoint via an email executable or a web link to a malicious website. Once an endpoint is compromised, an attacker typically installs back doors, remote access Trojans (RATs), and other malware to ensure persistence. This lesson describes spamming and phishing techniques, how bots and botnets function, and the different types of botnets.

**Business Email Compromise (BEC)**

Business email compromise (BEC) is one of the most prevalent types of cyberattacks that organizations face today. The FBI Internet Crime Complaint Center (IC3) estimates that "in aggregate" BEC attacks cost organizations three times more than any other cybercrime and BEC incidents represented nearly a third of the incidents investigated by Palo Alto Networks Unit 42 Incident Response Team in 2021. According to the Verizon 2021 Data Breach Investigations Report (DBIR), BEC is the second most common form of social engineering today.

**Phishing Attacks**

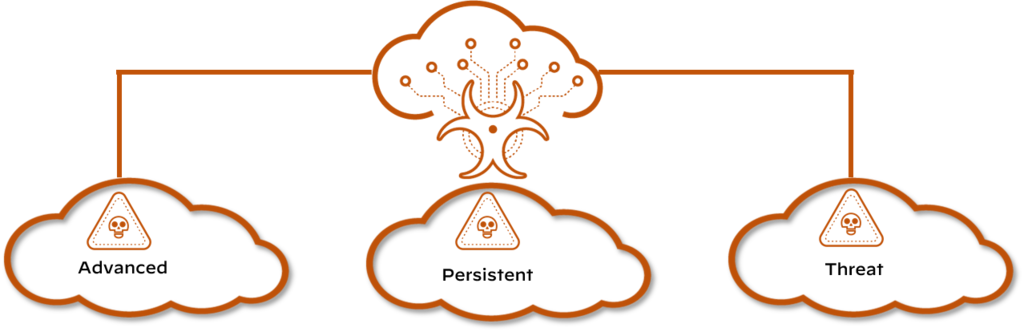
We often think of spamming and phishing as the same thing, but they are actually separate processes, and they each require their own mitigations and defenses. Phishing attacks, in contrast to spam, are becoming more sophisticated and difficult to identify and many more types of attacks

***Lesson 4: Advanced Persistent Threats and Wi-Fi Vulnerabilities***

With the explosive growth in fixed and mobile devices over the past decade, wireless (Wi-Fi) networks are growing exponentially—and so is the attack surface for advanced persistent threats (ATP). This lesson describes Wi-Fi vulnerabilities and attacks and APTs.

**Advanced Persistent Threats**

Advanced persistent threats, or APTs, are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. APTs are generally coordinated events that are associated with cybercriminal groups.



**Lazarus**

Attacks against nation-states and corporations are common, and the group of cybercriminals that may have done the most damage is Lazarus. The Lazarus group is known as an APT. The Lazarus group has been known to operate under different names, including Bluenoroff and Hidden Cobra. They were initially known for launching numerous attacks against government and financial institutions in South Korea and Asia. In more recent years, the Lazarus group has been targeting banks, casinos, financial investment software developers, and crypto-currency businesses. The malware attributed to this group recently has been found in 18 countries around the world.

***Lesson 5:Security***

**Models**

The goal of a security model is to provide measurable threat prevention through trusted and untrusted entities. This can be a complicated process, as every security model will have its own customizations and many variables need to be identified. This lesson describes the core concepts of a security model and why the model is important, the functions of a perimeter-based security model, the Zero Trust security model design principles, and how the principle of least privilege applies to the Zero Trust security model.

**Perimeter-Based Security Model**

Perimeter-based network security models date back to the early mainframe era (circa late 1950s), when large mainframe computers were located in physically secure “machine rooms.” These rooms could be accessed by a limited number of remote job entry (RJE) terminals directly connected to the mainframe in physically secure areas.

**Relies on Physical Security**

Today’s data centers are the modern equivalent of machine rooms, but perimeter-based physical security is no longer sufficient. Click the arrows for more information about several obvious but important reasons for the security issues associated with perimeter-based security.

