**Security for Non-Developers**



|  |  |  |  |
| --- | --- | --- | --- |
| **Duration** | 2 Days | **Modality** | Virtual / ILT |
| **Platform** | Windows, Linux, MacOS | **Level** | Introduction |

**Overview**

Cybersecurity is a critical consideration for product and software development. Ransomware and other critical cyberattacks have circled the globe the past couple of years. The Colonial Pipeline ransomware incident is an example of the disruptiveness of these attacks and the worldwide impact. Being able to defend against cyberattacks is critical for every technology company and financial institution.

Everyone, the entire team, is responsible for security! Securing a product, system, or device is not simply the responsibility of engineers and software developers. Product Managers, Quality Assurance, Pen Testers, Product Owners, and anyone that contributes to product development is responsible for security. This course provides the security knowledge and best practices for everyone to participate in security, regardless of their role.

Learn to manage vulnerabilities, create security diagrams, define an attack surface, manage threat intelligence, and more.

As importantly, understand the adversarial perspective. The ability to think like a cyber adversary is essential to creating secure solution. In class, this is reinforced with the introduction of the Cyber Kill Chain and Mitre ATT$CK.

This class is a combination of lecture and hands-on exercises.

**Audience**

The audience for this class is anyone that contributes to product development.

**Solutions**

Emerge from the Security for Non-Developers class with an understanding of cybersecurity terminology and concepts. You will also be able to productively participate in the security development lifecycle of product development.

**What you learn:**

**Security terminology**

* CIA Triad
* Threat terminology
* Data security: P!, P2, and P3
* Attack surface
* Authentication and related terms
* Threat maps

**Vulnerabilities**

* STRIDE
* CVSS
* Attack Tree
* Threat Profile
* NIST NVD

**General Security**

* Security Development Lifecycle
* Accessing risk
* Common attacks
* Testing
* Rootkits and Bootkits

**Cryptography**

* Hashing
* Asymmetric encryption
* Symmetric encryption
* Algorithms
* Network security
* Digital signatures
* Randomness

**Domains**

* API / Desktop
* Web application security
* Cloud security

**Hardware security**

* UEFI firmware
* Secure Boot
* Implants
* Kernel attacks
* Hardware implants

**Kill Chains**

* Threat Intelligence
* Cyber Kill Chain
* Mitre ATT$CK
* Gap Analysis