Cyber Security Essentials Bootcamp Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Cybersecurity Essentials Bootcamp is a 4-day instructor-led course packed full of hands-on labs and practical exercises, which teach the effective steps to prevent, detect and respond to a cyber incident. With actionable techniques acquired within the course that can directly apply, making a genuine difference in the workplace. Each module is packed with extensive hands-on exercises that covers leading edge skills, applied knowledge of best practice preventative tooling, in addition to the existing threat landscape of emerging technologies such as: Internet of Things, Cloud, Smart Cities, Connected and Autonomous Vehicles and Cryptocurrency and blockchain.

Prerequisites

- Basic knowledge of networking is desirable but not essential, particularly awareness of protocols and internet services.
- Basic knowledge of Windows and Linux operating systems is desirable but not essential.
- QACISMP and or QAFCCS are ideal prerequisite courses for those completely new to applied technical security concepts, tools and services.

Target Audience

This course is designed for IT and Security Professionals and Managers who want to understand the essentials of cybersecurity and current threat landscape. Perfect for those wishing to build and or pivot to a defensive security posture, for those charged with maintaining and defending against cyber attacks. This course will be of benefit to junior and mid level cyber roles, who are interested in Security Operations, Forensic Analysis, GRC Officers, Security Auditors and Secure Developers, all with a passion to be as effective as possible in their security discipline.

What You Will Learn

- Understand the threats faced by modern networks, systems and application platforms
- Understand the techniques used to detect, prevent and respond to these threats
- Build enablement solutions for detection and situational awareness
- Respond, contain and start hunting out known and unknown threats
- Use leading ‘open source’ security tools to serve active and passive defence techniques
- Discover and analyse ‘high risk’ weakness within systems
- Create an actionable and auditable policies
- Understand cryptography and its applications in a digital world
- Begin to analyse, attribute and predict the threats and create an active defence posture

Outline

Critical Security Control

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Introduction to Cybersecurity
- Social Engineering and Malware
- Defence in Depth and Security Controls
- Security Tools
- Incident Management

Module Labs:

- Lab 1: Intelligence Gathering
- Lab 2: Using a Forensic Tool to Investigate a Data Leak
- Lab 3: Mapping the Attack Surface

Modern Network Architecture

- Network Security Tools
- Wireless Security
- Physical Security Controls
- Secure Protocols and Services
- Secure System and Network Design
- Secure Cloud Services and Virtualisation

Module Labs:

- Lab 4: Introduction to Network Analysis with Wireshark
- Lab 5: Windows Security
- Lab 6: Securing a Web Server
- Lab 7: Auditing Compliance in Linux Using Lynis
- Lab 8: Security within the Internet of Things
- Lab 9: Investigating Security in the Cloud

Principles of Risk

- Business Continuity
- Risk Management
- Vulnerability Scanning and Penetration Test
- Corporate Security Policies
- Forensic Collection and Preservation

Module labs:

- Lab 10: Using MITRE ATT&CK for Threat Hunting
- Lab 11: Digital Forensics Tools
- Lab 12: Scanning a Web Server for Vulnerabilities

Operation System & Application Security

- Application Exploits
- Web Server Exploits
- Web Browser Exploits
- Secure Application Design
- Secure Coding
- Auditing Applications

Module labs:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Lab 13: Performing SQL Injection on a Vulnerable Web Server
- Lab 14: Exploiting a Vulnerable Web Server

Applied Cryptography

- Cryptography Application
- Identity and Access Management
- Cryptocurrency and Blockchain

Module Labs:

- Lab 15: Setting Password Security Baselines on Windows
- Lab 16: Auditing Security Baselines on Windows
- Lab 17: Investigating Cryptocurrency Using OSINT (Part 1)
- Lab 18: Investigating cryptocurrency Using OSINT (Part 2)