CTR – 910 Incident Response

About this course

In this course you will learn how to use open-source tools for incident response purposes. This course utilizes firsthand explanations and screencast demonstrations of how to use these tools in a step-by-step manner so you can start incident response work immediately on your own.

Audience profile

The course is intended for business stakeholders and workload administrators who plan and implement security strategies. It is also suitable for those who ensure that the solutions comply with the policies and regulations of the organization. These professionals respond to threats, conduct investigations, and enforce data governance policies. Individuals in this capacity should have good skills and experience in identity protection, information protection, threat protection, security management, and data governance

At course completion

By the end of the course, participants will have gained a comprehensive understanding of incident response, including how to manage the aftermath of a security breach or attack. They will be equipped with the knowledge to follow a step-by-step process when an incident occurs and will be able to use SIEM solutions and predictive capabilities using threat intelligence

Course Details

Introductory Lesson

Incident Response - Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

Cyber Attacks - Here we will cover Cyber Attacks on Wi-Fi networks and over the web so you can understand how to respond to them.

Virtualization and Cloud Security - So virtualization can mean many things at different layers of the stack. At the network layer you have VLAN's, MPLS networks and even SDN (Software Defined Network) technologies such as Open flow.   At the storage layer you have VSAN's.   At the Hardware and OS layer you have hypervisors for machine virtualization and containers for runtime virtualization and isolation. Databases have even gotten in on the act using container technology.

Malware - In this section we will define Malware categories and characteristics and talk through protective countermeasures to keep networks, systems and data safe from compromise. '

Static Malware Analysis – Examine malware without executing it. This technique involves analyzing the code and structure of the malware to understand its functionality and identify any malicious activity.

Operational Security - Once we have a Risk Management program in place we need to implement operational security to manage the day-to-day aspects of security.   In this lesson you will learn about Operational Security Controls, what they consist of and how they help us to incrementally manage risk daily Basis.

Disaster Recovery - While at first glance DR might not seem like a natural fit with cybersecurity after further analysis, we realize that disasters are threats that can inflict much more damage than any hacker. Here we will talk about DR planning, strategies and best practices.

Platform Hardening and Baselining - Minimizing the attack surface area of operating systems, databases and applications is a key tenet of operational security. In this lesson you will learn about techniques for OS/DB and App hardening.

Advanced Perimeter Security - While many argue that with the advent of mobile technologies and the cloud the perimeter is dissolving, it will remain a key component in securing network resources for years to come. Here we'll cover Load balancers, forward and reverse proxies, API Security Gateways, Firewall rules and Unified Threat Management technologies.

IDS - Intrusion Detection technology is offered in multiple flavors. They are either network based or host based and can be detective or preventive in nature.

Advanced IDS - Previously we've talked about IDS basic concepts. Now it's time to cover advanced IDS architectures, standards and further explore the inner workings of statistical and Rule based IDS.

Snort and Bro – In this lesson you will learn how to use Snort and Bro NIDS/HIDS by example.

Honeypots and Honeynets - Luring attackers away from critical data and studying their behavior can help us to protect the data that matters most. Let's found out how we can use honeypots to tie up attackers and find out what they are up to.

Kippo SSH Honeypot - medium-interaction SSH honeypot designed to log brute-force attacks and the entire shell interaction

Firewalls - In this lesson we will cover the evolution of firewalls and their capabilities.

Apache Security Logging – Apache is still the most popular web server by install base on the web. Let's learn how to log malicious activities using Apache logging.

SIM - Management of logs is a key component of operational security. These days the velocity, variety and volume of data collected via logs has catapulted log management into the realm of Big Data. You will learn how to effectively manage these logs and derive useful security information from them.

Forensic Duplication - process of creating an exact copy of data from a digital device for the purpose of investigation.
You'll Learn how to acquire a forensic duplicate using Linux based tool

Prerequisites

deep background in security operations and familiarity with basic security concepts would be beneficial