Edward Jones Threat Detection Course Recommendations

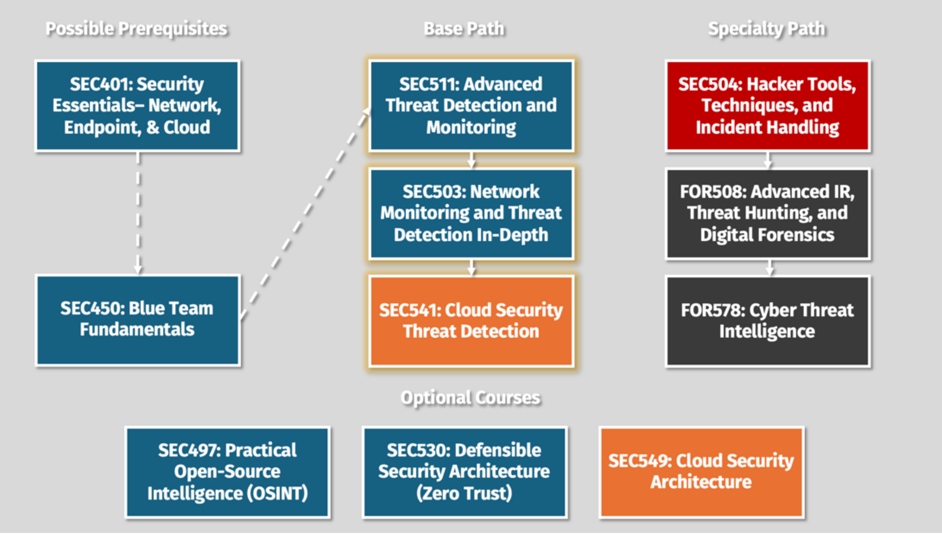
Summary

This document intends to provide a logical progression pathway for individuals at any level to learn more about, excel at, and upskill their knowledge, capabilities, and skills in the areas of Threat Detection. Whether the individual is new to the Threat Detection, looking to specialize, or aiming to become an expert, this roadmap offers tailored course recommendations to guide one's educational journey through a progression of different SANS courses.

Paths Overview

1. Possible Prerequisites: To outline potential recommended prerequisites. Such prerequisites are not required but serve as possible steppingstones.
2. **Base Path:** For Beginners or those looking to upskill their general threat detection capabilities. Designed for a broad audience, this path provides foundational knowledge and essential skills.
3. **Specialty Path:** For Focused Learning. This path is designed for individuals aiming to specialize in specific areas of threat detection, offering more targeted course selections.

Course Recommendation Roadmap


Possible Prerequisites
SEC401: Security Essentials– Network, Endpoint, & Cloud
SEC450: Blue Team Fundamentals
Base Path
SEC511: Advanced Threat Detection and Monitoring
SEC503: Network Monitoring and Threat Detection In-Depth
SEC541: Cloud Security Threat Detection
Specialty Path
SEC504: Hacker Tools, Techniques, and Incident Handling
FOR508: Advanced IR, Threat Hunting, and Digital Forensics
FOR578: Cyber Threat Intelligence
Optional Courses
SEC497: Practical Open-Source Intelligence (OSINT)
SEC530: Defensible Security Architecture (Zero Trust)
SEC549: Cloud Security Architecture

Possible Prerequisites

1. **SEC401: Security Essentials – Network, Endpoint, & Cloud**
   - SEC401 will provide the essential information security skills and techniques you need to protect and secure your critical information and technology assets, whether on-premises or in the cloud. SEC401 will also show you how to directly apply the concept learned into a winning defensive strategy, all in the terms of the modern adversary.
2. **SEC450: Blue Team Fundamentals: Security Operations and Analysis**
   - Provides essential context regarding Security Operations Centers (SOC), modern defense operation, monitoring, and analysis. (Great as a prerequisite.)

Base Path: For Threat Detection Upskilling

1. **SEC511: Cybersecurity Engineering: Advanced Threat Detection and Monitoring**
   - SEC511 teaches the principles of continuous monitoring, emphasizing the importance of a proactive approach to security operations. Additionally, this course builds on the foundational skills by focusing on continuous monitoring strategies that are crucial for identifying threats in real-time across both on-premises and cloud environments.
2. **SEC503: Network Monitoring and Threat Detection In-Depth**
   - SEC503 is designed to help you master the core concepts of intrusion detection, providing a comprehensive understanding of network traffic analysis and monitoring. That said, this course lays the groundwork for threat detection, covering essential skills such as analyzing network traffic, detecting intrusions, and understanding the tools used in monitoring environments.
3. **SEC541: Cloud Security Threat Detection**
   - SEC541 focuses on the critical skills needed to detect and respond to threats in cloud environments. It covers various cloud platforms and the specific challenges of cloud-based threat detection. Furthermore, this course provides a thorough understanding of cloud security architecture, monitoring techniques, and threat detection, making it essential for anyone moving into cloud security.

Specialty Path: For Focused Learning

1. **SEC504: Hacker Tools, Techniques, and Incident Handling**
   - SEC504 helps you develop the skills to conduct incident response investigations. You will learn how to apply a dynamic incident response process to evolving cyber threats, and how to develop threat intelligence to mount effective defense strategies for cloud and on-premises platforms. As a course that covers a combination of offense and defense, SEC504 is great to understand both sides of the equation.
2. **FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics**
   - FOR508 teaches advanced skills to hunt, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hacktivists. To add, this course assists in upgrading detection capabilities through better understanding of novel attack techniques and helps to focus on critical attack paths and knowledge of available forensic artifacts.
3. **FOR578: Cyber Threat Intelligence**
   - FOR578 trains individuals in the tactical, operational, and strategic level of cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate incident response more effective, and organizations more aware of the evolving threat landscape. Given that, this course is excellent for organizations that need or already have a Threat Intelligence program in place.

Optional Courses:

- **SEC497: Practical Open-Source Intelligence (OSINT)**
  - Learn how to gather and analyze information from publicly available sources.
- **FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response**
  - FOR572 covers the tools, technology, and processes required to integrate network evidence sources into your investigations to provide better findings, and to get the job done faster.
- **SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise**
  - SEC530 provides comprehensive training on how to build and maintain security architectures that are resilient against cyber threats. It emphasizes engineering principles that ensure robust threat detection and response capabilities within various environments. On top of that, this course is ideal for those specializing in designing and implementing secure infrastructures that can effectively support advanced threat detection and incident response.
- **SEC549: Cloud Security Architecture**
  - SEC549 teaches security professionals how to design an enterprise-ready, scalable cloud organization. With nearly 20 hands-on labs, students will

learn to design cloud solutions for their organization at any stage of the cloud journey, whether planning for the first workload, managing complex legacy environments, or operating in an advanced cloud-native ecosystem.