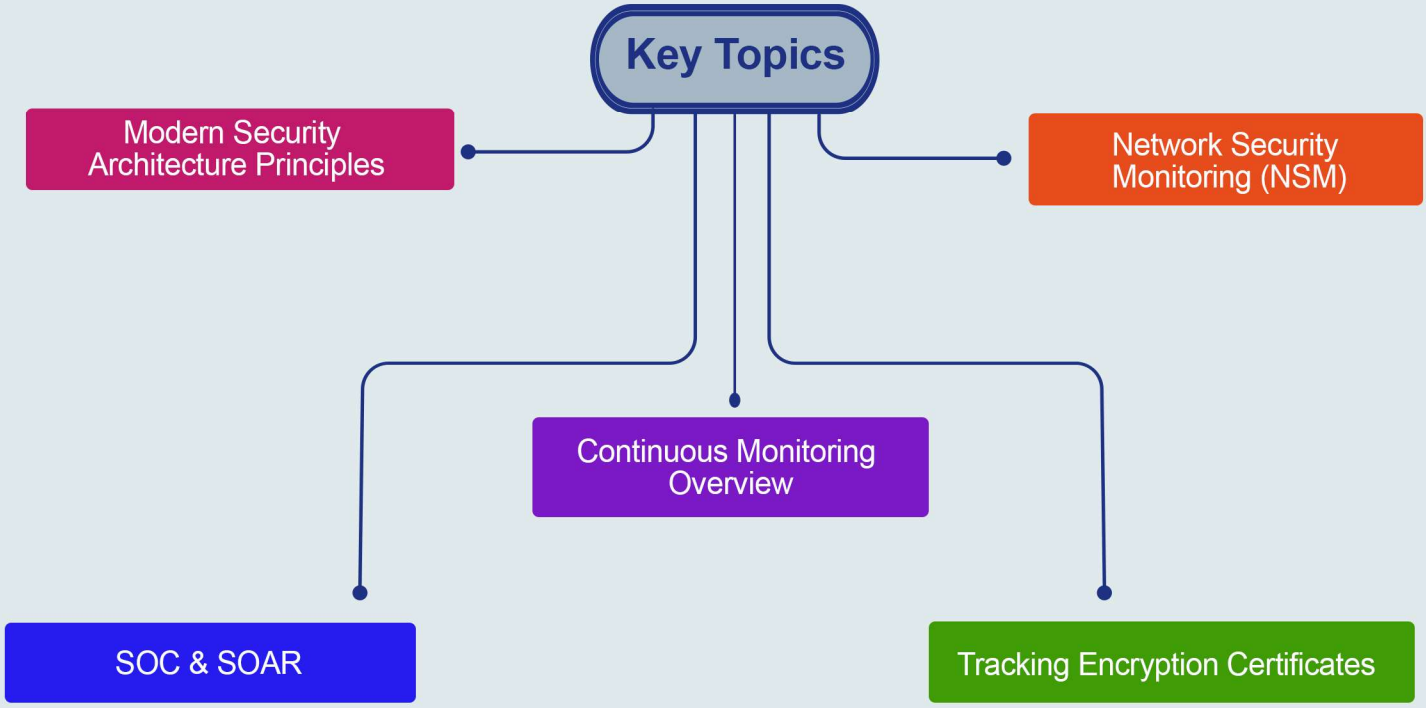
## About the Course

The most important element of a modern security architecture is the emphasis on detection. We must figure out how to look at the data and continuously monitor the enterprise for evidence of compromise or changes that increase the likelihood of compromise. We must first understand the approach and goals of monitoring and define a methodology for analysis. Speaking of best practices, we will emphasize the continuous monitoring of the Critical Security Controls. This course is about to continuous monitoring and developing a model for employing robust Cybersecurity Monitoring.

## Learning Objectives

1. Monitoring Security Posture
2. Understanding Network Security Monitoring
3. Familiarity with Security Operation Center
4. Familiarity with SOAR
5. Tracking Encryption Certificates
6. Familiarity with Modern Security Architecture Principles

## Key Topics




## Pre Requisites

- Incident Management Course
- Log Management Course
- Threat Hunting Course

## What You Will Receive

- Course Presentation File
- Complementary Files
- Cybersecurity Monitoring eBook

## Who Should Attend

- Network Administrators
- Security Engineers
- CTOs
- System Administrators

# Syllabus

## Modern Security Architecture

- Detection-oriented
- Post-Exploitation-focused
- Decentralized Information Systems/Data
- Risk-informed
- Layer 7 Aware
- Security Operations Centers
- Network Security Monitoring
- Continuous Security Monitoring
- Modern Attack Techniques
- Adversarial Dominance
- Threat Intelligence

## Network Security Monitoring (NSM)

- Evolution of NSM
- The NSM Toolbox
- NIDS Design
- Analysis Methodology
- Understanding Data Sources
- Practical NSM Issues
- Cornerstone NSM

## Security Operations Center (SOC)

- Concepts
- Architecture
- Design
- Implementation
- Management

# Syllabus

## Security Orchestration, Automation & Response

- What is SOAR?
- Critical Components
- SOAR Use Cases
- Selecting a SOAR Solution

## Tracking Encryption Certificates

- How to track encryption certificates

# Hands-on Training

- Lab 1 – Log Correlation
- Lab 2 – Asset Discovery
- Lab 3 – Dashboard Definition
- Lab 4 - Reporting
- Lab 5 – SOC Configuration