Performing CyberOps Using Cisco Security Technologies

Durée: 5 Jours **Réf de cours: CBRCOR** **Version: 1.0**

Résumé:

The Performing CyberOps Using Cisco Security Technologies (CBRCOR) course guides you through cybersecurity operations fundamentals, methods, and automation. The knowledge you gain in this course will prepare you for the role of Information Security Analyst on a Security Operations Center (SOC) team.
You will learn foundational concepts and their application in real-world scenarios, and how to leverage playbooks in formulating an Incident Response (IR). The course teaches you how to use automation for security using cloud platforms and a SecDevOps methodology. You will learn the techniques for detecting cyberattacks, analyzing threats, and making appropriate recommendations to improve cybersecurity.

This course also earns you 40 Continuing Education (CE) credits towards recertification and prepares you for the 350-201 CBRCOR core exam.
Mise à jour : 09.01.2023

Public visé:

Cybersecurity analysts, engineers, investigators and incident responders.

Objectifs pédagogiques:

- **After completing this course, you should be able to:**
- Describe the types of service coverage within a SOC and operational responsibilities associated with each.
- Compare security operations considerations of cloud platforms.
- Describe the general methodologies of SOC platforms development, management, and automation.
- Explain asset segmentation, segregation, network segmentation, micro-segmentation, and approaches to each, as part of asset controls and protections.
- Describe Zero Trust and associated approaches, as part of asset controls and protections.
- Perform incident investigations using Security Information and Event Management (SIEM) and/or security orchestration and automation (SOAR) in the SOC.
- Use different types of core security technology platforms for security monitoring, investigation, and response.
- Describe the DevOps and SecDevOps processes.
- Explain the common data formats, for example, JavaScript Object Notation (JSON), HTML, XML, Comma-Separated Values (CSV).
- Describe API authentication mechanisms.
- Analyze the approach and strategies of threat detection, during monitoring, investigation, and response.
- Determine known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Interpret the sequence of events during an attack based on analysis of traffic patterns.
- Describe the different security tools and their limitations for network analysis (for example, packet capture tools, traffic analysis tools, network log analysis tools).
- Analyze anomalous user and entity behavior (UEBA).
- Perform proactive threat hunting following best practices.

Pré-requis:

Attendees should meet the following pre-requisites:

- Familiarity with UNIX/Linux shells (bash, csh) and shell commands
- Familiarity with the Splunk search and navigation functions
- Basic understanding of scripting using one or more of Python,

Test et certification

Recommended as preparation for the following exam:

- **350-201 CBRCOR** - Performing CyberOps Using Cisco Security Technologies Exam

JavaScript, PHP or similar.
- CBROPS - Understanding Cisco Cybersecurity Operations Fundamentals
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

This course has not yet been released but will be the concentration course for the Cisco Certified CyberOps Professional Certification

- **CBRFIR** - Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

Contenu:

Understanding Risk Management and SOC Operations

Understanding Analytical Processes and Playbooks

Investigating Packet Captures, Logs, and Traffic Analysis

Investigating Endpoint and Appliance Logs

Understanding Cloud Service Model Security Responsibilities

Understanding Enterprise Environment Assets

Implementing Threat Tuning

Threat Research and Threat Intelligence Practices

Understanding APIs

Understanding SOC Development and Deployment Models

Performing Security Analytics and Reports in a SOC

Malware Forensics Basics

Threat Hunting Basics

Performing Incident Investigation and Response

Labs

- Explore Cisco SecureX Orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Malicious File to Cisco Threat Grid for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Evaluate Assets in a Typical Enterprise Environment
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs from Cisco Talos Blog Using Cisco SecureX
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Query Cisco Umbrella Using Postman API Client
- Fix a Python API Script
- Create Bash Basic Scripts
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur