Cybersecurity Academy Advanced Courses

Security Operations Architecture

Course Description:

This course provides the student with an overview of Security Orchestration and Response (SOAR) with Threat Intelligence collection including the roles they play in configuring the Security Operations Center (SOC) for automated protection of enterprise networks and critical infrastructure. Students will learn about continuous improvement processes designed to collect threat intelligence with contextual data, and to apply automated prevention workflow playbooks that quickly identify and respond to fast-evolving and dangerous cyber threats. Students will also learn how to leverage automation to reduce strain on analysts and configure the SOC to effectively hunt for, identify, and mitigate threats that circumvent traditional defense mechanisms.

NIST/NICE Alignment and Work Roles:

- Protection and Defense - Threat Analysis (PD-WRL-006)
- Protection and Defense – Insider Threat Analysis (PD-WRL-005)
- Protection and Defense – Defensive Cybersecurity (PD-WRL-001)
- Potential Job Roles: Threat Analyst; Security Analyst; Cyber Defense Associate; Incident and Intrusion Analyst

Course Objectives:

- Examine how security orchestration, automation, and response (SOAR) methods use automation to improve end-to-end business operations cybersecurity posture.
- Identify and review Security Orchestration and Response Use Cases.
- Explain the benefits of Security Operations Architecture and Implementation.
- Explore Phishing Playbooks that execute repeatable tasks to identify false positives.
- Investigate Endpoint Malware Infection and Failed User Login Playbooks.
- Examine SSL Certificate, Vulnerability, and Endpoint Diagnostics Playbooks.
- Investigate how Cortex XSOAR automates security response actions.
- Review how Cortex XSOAR automates responses to ransomware attacks.
- Identify how to streamline the aggregation and sharing of threat intelligence.
- Examine the top ransomware variant threats across the cybersecurity landscape.
- Describe how threat intelligence and adversarial playbooks are utilized to deploy automated controls and mitigation for each stage of the Cyber Attack Life Cycle
- Explore how to resolve unknown exposures with Cortex XPANSE Automation.
- Investigate how Cortex XPANSE can actively discover, learn about, and respond to unknown risks in all connected systems and exposed services.
- Identify and Review Attack Surface Management Use Cases.
- Review how Cortex XSIAM automates security response actions.
- Discover how Cortex XSIAM unites SOC capabilities that include XDR, SOAR, SIEM, ASM and others into a single SecOps platform.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Security Orchestration and Response (SOAR) • Advanced Endpoint Protection – Cortex XDR • Threat Intelligence Playbooks – Cortex XSOAR • Attack Surface Management – Cortex XPANSE • Secure the Future - Cortex XSIAM	Successful completion of the Security Operations Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits – 45 contact hours **Format:** Instructor-Led or Self-Paced	• Analyzing Firewall Logs • Using Dynamic Block Lists • Cortex XSIAM Phishing Console • Cortex XSIAM Network Analysis Console