Palo Alto Networks Cybersecurity Academy Security Operations Fundamentals

Course Description:

This course provides the student with an understanding of Security operations (SecOps) and the role it plays in protecting our digital way of life, for businesses and customers. Students will learn continuous improvement processes to collect high-fidelity intelligence, contextual data, and automated prevention workflows that quickly identify and respond to fast-evolving threats. They will also learn how to leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate and mitigate threats.

Course Objectives:

Upon completion of this course students will be able to perform the following:

- Identify the key elements of security operations (SecOps) and describe SecOps processes.
- Configure and test log forwarding for traffic analysis investigation and response.
- Describe SecOps infrastructure including security information and event management (SIEM), analysis tools, and security operations center (SOC) engineering.
- Define security orchestration, automation, and response (SOAR) for SecOps.
- Configure the Next Generation Firewall to stop Reconnaissance Attacks.
- Recognize the major components of the Cortex XDR deployment architecture and explain how it protects endpoints from malware and exploits.
- Configure the Next Generation Firewall with Vulnerability Profiles to secure Endpoints.
- Outline how AutoFocus delivers contextual threat intelligence to SOC teams to enable actionable insight into real-world attacks.
- Identify how to streamline the aggregation, enforcement, and sharing of threat intelligence.
- Configure Mindmeld for threat intelligence gathering and response.
- Review how Cortex XSOAR automates security response actions.
- Explain how SOC teams can leverage Cortex Data Lake to collect, integrate, and normalize enterprise security data with advanced artificial intelligence (AI) and machine learning.
- Configure the Next Generation Firewall to use Dynamic Block Lists.