Overview

AutoFocus: Prioritize, Research, and Mitigate Threats is a self-paced course with about 5 hours of narrated modules, demonstrations, and knowledge check questions. It describes and demonstrates how to configure, and use AutoFocus to quickly prioritize, research, and respond to malware threats.

Module 1: AutoFocus Introduction
- AutoFocus advantages and architecture
- Fundamental AutoFocus concepts
- AutoFocus web-based portal introduction

Module 2: Viewing Threat Visibility on the Dashboard
- View different threat contexts
- View threats in date ranges
- View threats by network paths
- View threats by application
- View threats by industry relevance
- View threats by geographic source

Module 3: Prioritizing Malware Threats
- Prioritize by abundance
- Prioritize by severity
- Prioritize using alerts and notifications

Module 4: Researching Threats Using AutoFocus
- Distinguish between commodity and advanced persistent threats
- Find endpoint indicators of compromise

Module 5: AutoFocus and Threat Mitigation
- Create custom tags and alerts
- View downloaded firewall malware protections
- Export IP addresses, domain names, and URL block lists
- Use AutoFocus information to protect and remediate endpoint systems

Module 6: MineMeld and AutoFocus
- Salient features of MineMeld
- MineMeld integration with AutoFocus

Module 7: Use Case Scenarios
- Create MineMeld nodes and connect them in a graph
- Customize a prototype
- Integrate MineMeld with AutoFocus

Module 8: AutoFocus Enhancements
- Enhancements made to tags, artifacts, process trees, etc.
- Threat Summary report

Module 9: Dashboard Enhancements
- Latest enhancements made to AutoFocus Dashboard
- Customize Dashboard
- Configure and use the new AutoFocus widgets

Module 10: Miscellaneous Enhancements
- Enhancements made to AutoFocus reporting
- Simplified searches
- Tag groups
- Secure AutoFocus alerts
- Use case scenario to demonstrate the enhancements

Course Objectives
Successful completion of this e-Learning course will help students to log in and efficiently use the AutoFocus web-based portal to monitor malware threats and protect their data center systems. Students will be shown how to view, prioritize, search for, and analyze malware threats. They will see how to export IP addresses, domain names, and URL block lists to Palo Alto Networks® next-generation firewalls, SIEMs, and endpoint protection software systems, where the lists can be used to block malware threats. They will be shown the salient features of MineMeld and how it integrates with AutoFocus. They will see use case scenarios that demonstrate the power and functionality of AutoFocus. Students also will be shown the latest AutoFocus enhancements.

Scope
- **Course level:** Introductory
- **Course duration:** About 5 hours of narrated coursework, demonstrations, and knowledge checks
- **Course format:** Narrated coursework with knowledge check questions

Target Audience
Security operations center workers, threat analysts, incident responders

Prerequisites
None. Knowledge of TCP/IP networking and Palo Alto Networks® firewalls will be helpful.

This e-Learning course is available at the Learning Center.

Palo Alto Networks Education
Training from a Palo Alto Networks® Authorized Training Center delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Palo Alto Networks® Security Operating Platform knowledge necessary to prevent successful cyberattacks and safely enable applications.