Trellix Application and Change Control

Education Services Instructor-Led Training

Earn up to 32 CPEs after completing this course

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system security.

Recommended Pre-Work

- Working knowledge of Microsoft Windows and Network Administration
- Prior experience using Trellix ePolicy Orchestrator (ePO)

Related Courses

- Trellix ePolicy Orchestrator Administration
- Trellix ePO-On-prem Essentials

Learn More

To order, or for further information, please email SecurityEducation@trellix.com.

The Trellix Application and Change Control Administration course from Education Services provides in- depth training on the tools you need to efficiently install, configure, operate, and troubleshoot issues relating to TACC to safeguard intellectual property and ensure compliance. The course details how this solution uses Trellix ePolicy Orchestrator (Trellix ePO) for centralized management. It also explains how to use Application Control for dynamic allowlisting to ensure that only trusted applications run on devices servers, and desktops and how to use Change Control to monitor and prevent changes to the file system, registry, and user accounts.

Learning Objectives

Welcome
Provide an overview of course design, logistics and helpful resources.

Trellix ePolicy Orchestrator Overview
Describe ePO solution basics, ePO solution components and features and how ePO fits into security connected model.

Trellix Application and Change Control Overview
Describe Application Control and Change Control components, features, and functionality.

Planning a Managed Deployment and Install TACC Extension
Describe the prerequisites and key parts of a deployment plan and identify solution considerations, pilot plan phases, how to add the Trellix Application and Change Control extension to the ePO server and verify installation.

Trellix Application and Change Control Server Tasks and Permission Sets
Identify default permissions sets included with ePO, Application Control, Change Control and understand the product-specific server tasks created after deployment.

Solidcore Client
Describe how to enable and disable Solidcore Client tasks, describe enduser notifications, events, and approvals, and customize end-user notifications.

Application Control Rule Groups and Rules
Explain rule groups, rule group ownership, and rule groups permissions, configure and manage rule groups, and describe Application Control, Change Control, and Integrity Monitoring rule group tabs.

Change Control and Integrity Monitoring Rule Groups and Rules
Describe Change Control and Integrity Monitoring Rules and rules tabs, Trusted Local Groups and Wildcard pattern.

Application Control Policies
Describe Application Control policies and their relationship to rule groups, define the role of a policy, and configure policies.

Application Control Trust Model
Understand the basics of allowlisting and dynamic Trust Model.

Modify Protected Files
Understand how to use Update Mode, Observe Mode and Inventory Mode and describe how to make rule modifications..

Application Control Inventory
Navigate the Inventory menus, describe how to fetch, manage, and compare an Inventory.

Change Control
Discuss how to use write protection and read protection in policies, define updaters, update mode and authorized users, and configure Change Control.

Integrity Monitoring
Configure Integrity Monitoring policies, reduce "noise" using an Advanced Exclusion Filter, and understand how to use content change tracking.

Events and Alerts
Describe how Solidcore events are handled in ePO, understand when to use one-click exclusion, and configure Solidcore alerts in ePO.

Dashboards and Reporting
View and use Solidcore Dashboards and queries, and view Solidcore reports.

Troubleshooting
Identify Client versus ePO handling, locate log file and key resources, use troubleshooting tools, and discuss troubleshooting feature implementation issues.

Administration using the Command Line Interface
Use the command line interface to administer systems not connected to ePO.

Recommended Practices
Identify best practices for deploying and using TACC.

Case Studies
Create your own Application Control and Change Control policies without guidance and create a notification for violations of these policies.

Agenda at a Glance

Day 1:

- Welcome
- Ex. Trellix ePolicy Orchestrator overview
- Trellix Application Control and Change Control Overview
- Planning a Managed Deployment and Install TACC extension
- TACC Server Tasks and Permission Sets
- Solidcore Client

Day 2:

- Application Control Rule Groups and Rules
- Change Control and Integrity Monitoring Rule Groups and Rules
- Application Control Policies
- Application Control Trust Model
- Modify Protected Files

Days 3:

- Application Control Inventory
- Change Control
- Integrity Monitoring
- Events and alerts
- Dashboards and Reporting

Days 4:

- Troubleshooting
- Administration using the Command Line Interface
- Recommended Practices
- Case Studies

Trellix

Visit Trellix.com to learn more.

052023-05