BeyondTrust PowerBroker for Windows Foundations Training

Course Description

The PowerBroker for Windows Foundations Training is designed for the IT security professional tasked with administering, monitoring and reporting on PowerBroker for Windows.
Students learn how to install the products components, create path, publisher & shell rules for privilege delegation, customize user messages, setup secondary authorization and challenge/response mechanisms. They will create risk & compliance rules, and file integrity rules. They will learn how to use BeyondInsight to review event data, create new rules from captured events, and setup and view captured sessions.

Prerequisites

There are no prerequisites for this course, but the student should have hands on experience of general networking environments and operating systems.

Who Should Attend

This course is for network managers, system administrators, security administrators, systems professionals, and consultants who are charged with the configuration, and day-to-day management of PowerBroker for Windows in a variety of network environments, and who are responsible for administration of this product in the enterprise environment.

Delivery Method

This course is available in the following delivery methods:

- Web-based training (WBT) – Self-paced
- Instructor-led training (ILT) – 2 days
- Virtual Instructor-led training (VILT) – 15 hours over 3 days.

Course Outline

Introduction
- Product Overview
- The classroom lab environment

Installation
- Install & Configure PowerBroker Policy Editor, PowerBroker for Windows Client
- Configure for PBW events and captured sessions are sent to BeyondInsight
- Lab Exercise: Install PowerBroker for Windows

Creating Rules
- Create and test path-based PBW rules
- Create and test a publisher-based PBW rule
- Create and test the Shell rule
- Import sample rules
- Lab Exercise: Path, Publisher and Shell Rules

Communicating with the User
- Create custom justification message, re-authorization message, challenge/response message, blocked application message
- Create Collections
- Lab Exercise: User Messages, Passcode Generator, Collections

Risk and Compliance, and File Integrity Rules
- Create Risk and Compliance rules
- Create File Integrity rules
- Lab Exercise: Risk and Compliance, File Integrity and Rule Order

BeyondInsight and PowerBroker for Windows
- Filter and explore captured PBW event data
- Create PBW rules from captured client events
- Enable session recording
- View recorded sessions
- Lab Exercise: Session recording

Agent architecture

- Architecture and protections
- How the agent works

GPO deployment and item level targeting

- GPO primer
- GPO deployment Windows tools - timing
- Location of policy details
- Item Level Targeting
- How to modify rules from the template library
- Deploy with GPO
- Lab Exercise: Deploy agent and certificate with GPO

Security tokens

- How security tokens work
- Using Process Explorer to examine tokens
- Modify a custom security token
- Troubleshooting with Process Explorer
- Lab Exercise: Create a custom token

Central policy

- Central policy - when to apply
- Central policy - how to configure
- Central policy - remote clients
- Switching client from GPO to central policy
- Export rules from GPO to Central Policy
- Smart rules for central policy to automate
- Lab Exercise: Configure client for central policy

Actionable reports

- Actionable reports
- Fix vulnerabilities and review reports - Risk & Compliance events
- Reporting in BI
- Reporting in A&R
- Lab Exercise: Advanced reporting for PowerBroker for Windows

Product integration

- Password cycling with Password Safe
- Run process as user with Password Safe credentials
- Lab Exercise: Configure Password Safe integration