IBM Systems Lab Services

Security and Compliance with PowerSC

Overview

The Security and Compliance with PowerSC service is a proof of concept (PoC) service. In this PoC, a single PowerSC Graphical User Interface(GUI) Server is installed and configured on a PoC virtual machine(VM). Additionally, a few endpoint VMs are installed and configured with the PowerSC GUI Agent daemon. The PowerSC GUI Server and Agent deployments allow PowerSC to provide centralized security management from the GUI Server on a web browser. The remainder of the service focuses on providing knowledge transfer and configuration assistance with the following components of PowerSC:

Security and Compliance Automation

Learn how to change the default settings of your AIX, Linux, or IBM i VMs running on Power using the pscxpert tool. Pscxpert provides different types of security hardening profiles in order to fulfill the specific type of security or regulatory requirements of your organization.

Allowlisting

Learn how allowlisting can be implemented on AIX with trustchk and RHEL with fapolicyd. Allowlisting is a malware prevention technique in which you require executable files to be authorized before execution. An executable file not properly authorized would either be prohibited from execution, or an error message would be generated, depending on configuration.

Intrusion Detection Service

Learn how to configure the Port Scan Attack Detector (psad) tool on RHEL, which makes use of iptables log messages to detect, alert, and (optionally) block port scans and other suspect traffic.

File Integrity Monitoring

Learn how to configure the component, Real Time Compliance (RTC), on AIX to provide security file monitoring for the 300 most important AIX operating system files. For file integrity monitoring on Linux, the auditd subsystem is configured to interface with the PowerSC GUI Server.

Endpoint Detection and Response

Learn how to configure the PowerSC functionality that is designed to continually monitor and respond to mitigate cyberthreats. PowerSC provides host-based granular detection and prevention capabilities.

Automation with REST API

Learn how the PowerSC GUI Server's REST API can be used to automate security tasks. The REST API allows execution of PowerSC tasks without needing an administrator to log in to the PowerSC GUI Server's web interface.

Reporting

Learn how to configure the various PowerSC reporting options. PowerSC provides reports for the compliance and file integrity monitoring components. The timeline report is an interactive page that reports on a single endpoint. The Event Analysis report allows searching of security events by using various criteria for filtering events that occur on an endpoint.

Miscellaneous

Learn about more topics for well-rounded PowerSC knowledge transfer. Such topics as troubleshooting, configuring limited access, LDAP integration, logging, backup, and other topics are discussed.

Common Use Cases

- An organization that would like a guided deep introduction to PowerSC
- An organization that would like to learn how to install and configure PowerSC
- An organization that would like to implement an EDR solution for their Power virtual machines
- An organization that would like to reduce the effort and complexity of securing their VMs running on Power
- An organization that would like to automate security configuration
- An organization that would like to evaluate PowerSC before they purchase PowerSC licensing
- An organization that would like a centrally managed security solution for deploying cybersecurity safeguards

Engagement Process

- Consultant arranges prep call to discuss requirements, scheduling, and agenda
- Consultant works with client to install and configure PowerSC in client environment
- Consultant provides advice on best practice implementation
- Consultant works with client to verify PowerSC functions most important to the client
- Consultant provides presentations to facilitate knowledge transfer concerning the numerous security and compliance capabilities of PowerSC

Deliverables

1. Presentation Slides – an electronic copy of presentation slides
2. Configuration documents – an electronic copy of configuration documents
3. Compliance scripting – scripting designed to automate the creation of compatible compliance profiles

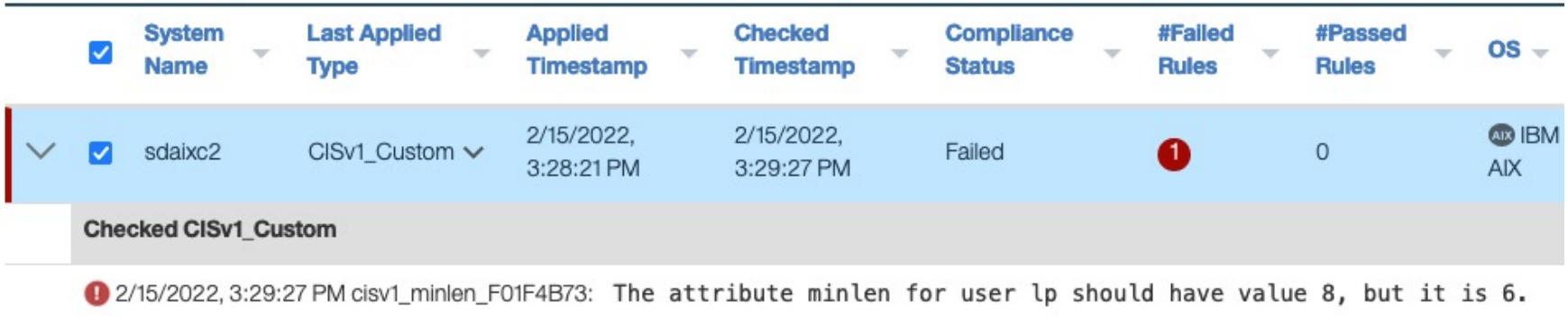

Fig. 1 – The image above is taken from compliance section of the PowerSC GUI Server. In this example, a user, "lp", has the minlen attribute set to 6 instead the PowerSC requirement of 8.