Server Compliance Check Implementation

# Overview

This document outlines the steps taken to implement compliance checks across Windows and Linux servers using automation tools. The objective is to ensure all servers meet the defined security and operational standards.

# Compliance Requirements

* Operating System: Ensure no servers are running End-of-Life (EOL) operating systems. Check for proper activation of Windows/Linux OS.
* Antivirus Installation: Verify that SentinelOne antivirus is installed and active on all servers.
* Logging: Confirm that logging is enabled across all servers to facilitate Security Operations Center (SOC) monitoring.
* Security Patches: Ensure all security patches are installed on the servers.
* NTP Configuration: Validate the Network Time Protocol (NTP) configuration and its synchronization with current NTP servers.
* Service Status: Check that essential services related to Antivirus (SentinelAgent.exe) and Log Collector (WinCollect, msrpc for Windows; Syslog for Linux) are running.

# Implementation Strategy

## Windows Servers

1. \*\*Script Development\*\*: A Python script was created to run PowerShell commands remotely. It performs checks on operating systems, SentinelOne status, logging, security patches, NTP configuration, and essential services.  
2. \*\*Challenges\*\*:  
- \*\*Centralized Server\*\*: Currently, no centralized server is available to test all Windows servers. Domain-specific centralized servers need to be set up.  
- \*\*Reachability\*\*: Staging revealed limited reachability to all servers, impacting script execution.  
3. \*\*Next Steps\*\*:  
- Work with the SysEng team to establish domain-specific centralized servers.  
- Explore alternative solutions for better server reachability and testing pipelines.

## Linux Servers

1. \*\*Script Development\*\*: Using a combination of Ansible for server checks and Python for reporting, compliance is verified for all Linux servers from a single centralized server.  
2. \*\*Current Status\*\*: The Ansible scripts are yet to be tested in the target environment. Further testing is required to validate the setup across all servers.  
3. \*\*Challenges\*\*: While the Linux setup is relatively stable, ongoing testing is needed to ensure the scripts cover all compliance parameters accurately.

# Manual Report Validation

To ensure the accuracy of automated reports, a manual report or one from an external source is needed. This will serve as a benchmark to validate the results generated by the scripts.

# Testing and Validation

Initial testing on Windows has shown issues with reachability. More robust testing environments are required to fully validate the scripts.  
Linux scripts have not been fully tested in the environment yet. Complete testing is necessary to confirm the scripts' functionality and reliability.

# Next Steps

## Windows

- Set up domain-specific centralized servers.  
- Continue testing and refine scripts based on results.  
- Finalize the solution after discussions with the SysEng team.

## Linux

- Complete testing for all servers in the environment.  
- Automate report validation and exception handling.

# Automated Report Generation

A separate script is planned to automate the verification of generated reports. This will ensure that all identified gaps and non-compliances are properly highlighted and addressed.

# Report Validation Process

Validate the automated reports against a manually created report or external source to ensure the accuracy and completeness of the compliance checks.

# Flowchart

The flowchart below illustrates the process of compliance checks for servers, from loading the server list to manual report validation and highlighting gaps.

