



NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

A PRIMER FOR MAPPING AND AUTOMATING TECHNICAL CONTROLS FOR
OPERATING SYSTEMS

CAVIRIN SYSTEMS, INC.

5201 GREAT AMERICA PKWY, SUITE #419, SANTA CLARA, CA 95054

+1-408-200-3544 | SALES@CAVIRIN.COM | PRESS@CAVIRIN.COM | INFO@CAVIRIN.COM

CONTENTS

- Introduction.....4
 - Introduction to the framework4
 - Introduction to the Cavidin Platform8
- Mapping the framework with Red Hat® Enterprise Linux 7.....10
- Cavidin’s Implementation of the framework.....16
 - Step 1 - Prioritize and Scope16
 - Step 2 - Orient17
 - Step 3 - Create a Current Profile18
 - Step 4 - Conduct a Risk Assessment20
 - Step 5 - Create a Target Profile21
 - Step 6 - Determine, Analyze, and Prioritize Gaps22
 - Step 7 - Implement Action Plan23
- Conclusion.....26

CAVIRIN'S MAPPING TABLES

- Table 1: ID.RA-1 - Asset Vulnerabilities are Identified.....10
- Table 2: PR.AC-1 - Identities and Credentials.....11
- Table 3: PR.AC-3 - Remote Access is Managed.....11
- Table 4: PR.AC-4 - Access Permissions and Authorizations are Managed.....12
- Table 5: PR.AC-5 - Network Integrity is Protected.....12
- Table 6: PR.AC-6 - Identities are Proofed and Bound to Credentials.....12
- Table 7: PR.DS-4 - Adequate Capacity to Ensure Availability is Maintained..13
- Table 8: PR.DS-5 - Protections Against Data Leaks are Implemented.....13
- Table 9: PR.IP-1 - Baseline Configuration.....14
- Table 10: PR.PT-1 - Audit/Log Records are Determined.....15
- Table 11: DE.CM-7 - Monitoring is Performed.....15
- Table 12: DE.CM-8 - Vulnerability Scans are Performed.....15

FRAMEWORK ASSESSMENT ON CAVIRIN PLATFORM

- Figure 1: Discover Resources17
- Figure 2: Create asset groups18
- Figure 3: NIST CSF Policy Pack filtered for RHEL 719
- Figure 4: NIST CSF Policy Details20
- Figure 5: Resource Risk Assessment Score Summary20
- Figure 6: Risk Assessment Details21
- Figure 7: Dashboard depicting cyber security assessment trends22
- Figure 8: Prioritize control gaps22
- Figure 9: Implement Action Plan via various integrations23
- Figure 10: Example Integration with Pager Duty24
- Figure 11: Example Integration with JIRA25

INTRODUCTION

This paper provides technical insights on mapping and automating various controls suggested by the [NIST Framework for Improving Critical Infrastructure Cybersecurity](#) at an operating system level. This paper helps organizations better prepare to automate technical controls as detailed by the framework. It also describes the next generation Cvirin platform that enables automation of such cybersecurity controls for cloud as well on-premise infrastructure covering various cloud resources, operating systems, containers, applications and network devices. This paper uses [Red Hat® Enterprise Linux 7](#) as an example for the target of evaluation against the framework.

INTRODUCTION TO THE FRAMEWORK

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructures. The Framework provides organization and structure to today’s multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The overall framework is divided into five Framework Core Functions.

- **Identify (ID)** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect (PR)** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect (DE)** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS)** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover (RC)** - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

These core functions are further categorized as follows:

| Functions | Category |
|-----------|------------------------------|
| Identify | Asset Management |
| | Business Environment |
| | Governance |
| | Risk Assessment |
| | Risk Management Strategy |
| | Supply Chain Risk Management |

| | |
|---------|---|
| Protect | Access Control |
| | Awareness and Training |
| | Data Security |
| | Information Protection Processes and Procedures |
| | Maintenance |
| | Protective Technology |
| Detect | Anomalies and Events |
| | Security Continuous Monitoring |
| | Detection Processes |
| Respond | Response Planning |
| | Communications |
| | Analysis |
| | Mitigation |
| | Improvements |
| Recover | Recovery Planning |
| | Improvements |
| | Communications |

Each of the above categories is further divided into various sub-category controls advised to meet the control function. For example, the *Asset Management* category for *Identify* function suggests the following descriptive controls.

| Functions | Category |
|---|------------------|
| Identify | Asset Management |
| Sub-category | |
| ID.AM-1: Physical devices and systems within the organization are inventoried | |
| ID.AM-2: Software platforms and applications within the organization are inventoried | |
| ID.AM-3: Organizational communication and data flows are mapped | |
| ID.AM-4: External information systems are catalogued | |
| ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value | |
| ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | |

These controls are open and flexible and permit organization to customize them as per their target infrastructure. The exercise of mapping these controls to target of evaluation is time consuming and requires institutional knowledge of information security best practices and infrastructure administration skills. Multiplying this with the heterogeneity of the typical infrastructure, such as multiple flavors of operating systems, applications, containers, network

devices and cloud elements, requires hard work and coordination. This is exactly where organizations require automation that aligns with the framework and helps in heavy lifting the controls.

INTRODUCTION TO THE CAVIRIN PLATFORM

The Cavidin Platform identifies blind spots in the organization's infrastructure. It collects diverse set security data points from various infrastructural elements and assesses them against various risk-based or compliance-based standards.

The Top 3 concerns it helps alleviate are:

ORGANIZATIONS LACK VISIBILITY INTO THEIR HYBRID ENVIRONMENT AND THE INCREASED VELOCITY OF CHANGE HAS MADE SECURITY MANAGEMENT EXTREMELY CHALLENGING.

ENSURING THAT ALL SYSTEMS - INCLUDING ON-PREMISES VIRTUAL MACHINES, CLOUD INSTANCES AND CONTAINER IMAGES - ARE ALL PROPERLY PATCHED AND SECURED. THIS IS A SOURCE OF ONGOING CONCERN.

ORGANIZATIONS HAVE FULLY EMBRACED THE CLOUD BUT ENSURING COMPLIANCE WITH PCI, HIPAA, AND A RAFT OF OTHER SECURITY BEST PRACTICES CONSUMES SIGNIFICANT TIME.

Locking down security misconfiguration is important as established by various other security and research organizations. It is

- 5th on [OWASP Top 10](#)
- 3rd on [CIS CSC Top 20](#) and

- [Gartner reports that only 0.1 % are zero-day attacks](#) and remaining come from known vulnerabilities.

The NIST Framework for Improving Critical Infrastructure Cybersecurity provides guidelines against which such security misconfigurations could be locked down. Cavirin's automated technical controls address specific categories and sub-categories within the framework, covering over 4300 individual tests spread across Windows and Linux operating systems. It directly addresses the cybersecurity control functions outlined below depending upon the target of evaluation (Windows or Linux OS).

ID.RA-1 - ASSET VULNERABILITIES ARE IDENTIFIED

PR.AC-1 - IDENTITIES AND CREDENTIALS ARE ISSUED, MANAGED, VERIFIED, REVOKED, AND AUDITED

PR.AC-3 - REMOTE ACCESS IS MANAGED

PR.AC-4 - ACCESS PERMISSIONS AND AUTHORIZATIONS ARE MANAGED

PR.AC-5 - NETWORK INTEGRITY IS PROTECTED

PR.AC-6 - IDENTITIES ARE PROOFED AND BOUND TO CREDENTIALS

PR.DS-4 - ADEQUATE CAPACITY TO ENSURE AVAILABILITY IS MAINTAINED

PR.DS-5 - PROTECTIONS AGAINST DATA LEAKS ARE IMPLEMENTED

PR.IP-1 - BASELINE CONFIGURATION

PR.PT-1 - AUDIT/LOG RECORDS ARE DETERMINED

DE.CM-7 - MONITORING IS PERFORMED

DE.CM-8 - VULNERABILITY SCANS ARE PERFORMED

MAPPING THE FRAMEWORK WITH RED HAT® ENTERPRISE LINUX 7

Below is a sample mapping of the NIST Framework for Improving Critical Infrastructure Cybersecurity against Red Hat® Enterprise Linux 7 target capabilities.

| NIST CSF Control | Red Hat® Enterprise Linux 7 |
|---|--|
| ID.RA-1 - ASSET VULNERABILITIES ARE IDENTIFIED | <i>Ensure separate partition exists for /tmp</i> |
| | <i>Ensure nodev option set on /tmp partition</i> |
| | <i>Ensure nosuid option set on /tmp partition</i> |
| | <i>Ensure noexec option set on /tmp partition</i> |
| | <i>Ensure separate partition exists for /var</i> |
| | <i>Ensure separate partition exists for /var/tmp</i> |
| | <i>Ensure nodev option set on /var/tmp partition</i> |
| | <i>Ensure nosuid option set on /var/tmp partition</i> |
| | <i>Ensure noexec option set on /var/tmp partition</i> |
| | <i>Ensure separate partition exists for /var/log</i> |
| | <i>Ensure separate partition exists for /var/log/audit</i> |
| | <i>Ensure separate partition exists for /home</i> |
| | <i>Ensure nodev option set on /home partition</i> |
| | <i>Ensure nodev option set on /dev/shm partition</i> |
| | <i>Ensure nosuid option set on /dev/shm partition</i> |
| | <i>Ensure noexec option set on /dev/shm partition</i> |
| | <i>Ensure nodev option set on removable media partitions</i> |
| | <i>Ensure nosuid option set on removable media partitions</i> |
| | <i>Ensure noexec option set on removable media partitions</i> |
| | <i>Disable Automounting</i> |
| | <i>Ensure bootloader password is set</i> |
| | <i>Ensure core dumps are restricted</i> |
| | <i>Ensure XD/NX support is enabled</i> |
| | <i>Ensure address space layout randomization (ASLR) is enabled</i> |
| | <i>Ensure prelink is disabled</i> |
| | <i>Ensure SELinux is not disabled in bootloader configuration</i> |
| | <i>Ensure the SELinux state is enforcing</i> |
| | <i>Ensure SELinux policy is configured</i> |
| | <i>Ensure no unconfined daemons exist</i> |
| | <i>Ensure cron daemon is enabled</i> |
| | <i>Ensure SSH LoginGraceTime is set to one minute or less</i> |
| | <i>Ensure password hashing algorithm is SHA-512</i> |
| | <i>Ensure default user umask is 027 or more restrictive</i> |
| <i>Audit SUID executables</i> | |
| <i>Audit SGID executables</i> | |
| <i>Ensure no Legacy "+" entries exist in /etc/passwd</i> | |
| <i>Ensure no Legacy "+" entries exist in /etc/shadow</i> | |
| <i>Ensure no Legacy "+" entries exist in /etc/group</i> | |
| <i>Ensure root PATH Integrity</i> | |
| <i>Ensure all users' home directories exist</i> | |
| <i>Ensure no users have .forward files</i> | |
| <i>Ensure no users have .netrc files</i> | |
| <i>Ensure no users have .rhosts files</i> | |
| <i>Ensure all groups in /etc/passwd exist in /etc/group</i> | |

Table 1: ID.RA-1 - Asset Vulnerabilities are Identified

| | |
|---|--|
| PR.AC-1 - IDENTITIES AND CREDENTIALS ARE ISSUED, MANAGED, VERIFIED, REVOKED, AND AUDITED | <i>Ensure Logging is configured</i> |
| | <i>Ensure logging is configured</i> |
| | <i>Ensure SSH MaxAuthTries is set to 4 or Less</i> |
| | <i>Ensure SSH Idle Timeout Interval is configured</i> |
| | <i>Ensure lockout for failed password attempts is configured</i> |

Table 2: PR.AC-1 - Identities and Credentials

| | |
|---|---|
| PR.AC-3 - REMOTE ACCESS IS MANAGED | <i>Ensure IP forwarding is disabled</i> |
| | <i>Ensure packet redirect sending is disabled</i> |
| | <i>Ensure source routed packets are not accepted</i> |
| | <i>Ensure ICMP redirects are not accepted</i> |
| | <i>Ensure secure ICMP redirects are not accepted</i> |
| | <i>Ensure suspicious packets are logged</i> |
| | <i>Ensure broadcast ICMP requests are ignored</i> |
| | <i>Ensure bogus ICMP responses are ignored</i> |
| | <i>Ensure Reverse Path Filtering is enabled</i> |
| | <i>Ensure TCP SYN Cookies is enabled</i> |
| | <i>Ensure IPv6 router advertisements are not accepted</i> |
| | <i>Ensure IPv6 redirects are not accepted</i> |
| | <i>Ensure IPv6 is disabled</i> |
| | <i>Ensure TCP Wrappers is installed</i> |
| | <i>Ensure /etc/hosts.allow is configured</i> |
| | <i>Ensure /etc/hosts.deny is configured</i> |
| | <i>Ensure loopback traffic is configured</i> |
| <i>Ensure outbound and established connections are configured</i> | |
| <i>Ensure firewall rules exist for all open ports</i> | |
| <i>Ensure wireless interfaces are disabled</i> | |

Table 3: PR.AC-3 - Remote Access is Managed

| | |
|---|---|
| PR.AC-4 - ACCESS PERMISSIONS AND AUTHORIZATIONS ARE MANAGED | <i>Ensure sticky bit is set on all world-writable directories</i> |
| | <i>Ensure permissions on bootloader config are configured</i> |
| | <i>Ensure permissions on /etc/motd are configured</i> |
| | <i>Ensure permissions on /etc/issue are configured</i> |
| | <i>Ensure permissions on /etc/issue.net are configured</i> |
| | <i>Ensure permissions on /etc/hosts.allow are configured</i> |
| | <i>Ensure permissions on /etc/hosts.deny are 644</i> |
| | <i>Ensure permissions on /etc/crontab are configured</i> |
| | <i>Ensure permissions on /etc/cron.hourly are configured</i> |
| | <i>Ensure permissions on /etc/cron.daily are configured</i> |
| | <i>Ensure permissions on /etc/cron.weekly are configured</i> |
| | <i>Ensure permissions on /etc/cron.monthly are configured</i> |
| | <i>Ensure permissions on /etc/cron.d are configured</i> |
| | <i>Ensure at/cron is restricted to authorized users</i> |
| | <i>Ensure permissions on /etc/ssh/ssh_config are configured</i> |
| | <i>Ensure SSH access is limited</i> |
| | <i>Ensure root login is restricted to system console</i> |
| | <i>Ensure access to the su command is restricted</i> |
| | <i>Ensure permissions on /etc/passwd are configured</i> |
| | <i>Ensure permissions on /etc/shadow are configured</i> |
| | <i>Ensure permissions on /etc/group are configured</i> |
| | <i>Ensure permissions on /etc/gshadow are configured</i> |
| | <i>Ensure permissions on /etc/passwd- are configured</i> |
| | <i>Ensure permissions on /etc/shadow- are configured</i> |
| | <i>Ensure permissions on /etc/group- are configured</i> |
| | <i>Ensure permissions on /etc/gshadow- are configured</i> |
| | <i>Ensure no world writable files exist</i> |
| | <i>Ensure no unowned files or directories exist</i> |
| | <i>Ensure no ungrouped files or directories exist</i> |
| | <i>Ensure users' home directories permissions are 750 or more restrictive</i> |
| <i>Ensure users own their home directories</i> | |
| <i>Ensure users' dot files are not group or world writable</i> | |
| <i>Ensure users' .netrc Files are not group or world accessible</i> | |

Table 4: PR.AC-4 - Access Permissions and Authorizations are Managed

| | |
|---|--|
| PR.AC-5 - NETWORK INTEGRITY IS PROTECTED | <i>Ensure iptables is installed</i> |
| | <i>Ensure default deny firewall policy</i> |

Table 5: PR.AC-5 - Network Integrity is Protected

| | |
|--|--|
| PR.AC-6 - IDENTITIES ARE PROOFED AND BOUND TO CREDENTIALS | <i>Ensure authentication required for single user mode</i> |
| | <i>Ensure SSH PermitEmptyPasswords is disabled</i> |
| | <i>Ensure password creation requirements are configured</i> |
| | <i>Ensure password reuse is limited</i> |
| | <i>Ensure password expiration is 90 days or less</i> |
| | <i>Ensure minimum days between password changes is 7 or more</i> |
| | <i>Ensure password expiration warning days is 7 or more</i> |
| | <i>Ensure inactive password lock is 30 days or less</i> |
| | <i>Ensure system accounts are non-Login</i> |
| | <i>Ensure default group for the root account is GID 0</i> |
| | <i>Ensure password fields are not empty</i> |
| | <i>Ensure root is the only UID 0 account</i> |
| | <i>Ensure no duplicate UIDs exist</i> |
| | <i>Ensure no duplicate GIDs exist</i> |
| | <i>Ensure no duplicate user names exist</i> |
| <i>Ensure no duplicate group names exist</i> | |

Table 6: PR.AC-6 - Identities are Proofed and Bound to Credentials

| | |
|---|--|
| PR.DS-4 - ADEQUATE CAPACITY TO ENSURE AVAILABILITY IS MAINTAINED | <i>Ensure audit log storage size is configured</i> |
|---|--|

Table 7: PR.DS-4 - Adequate Capacity to Ensure Availability is Maintained

| | |
|---|---|
| PR.DS-5 - PROTECTIONS AGAINST DATA LEAKS ARE IMPLEMENTED | <i>Ensure audit logs are not automatically deleted</i> |
| | <i>Ensure the audit configuration is immutable</i> |
| | <i>Ensure rsyslog default file permissions configured</i> |
| | <i>Ensure rsyslog is configured to send logs to a remote log host</i> |
| | <i>Ensure remote rsyslog messages are only accepted on designated log hosts.</i> |
| | <i>Ensure syslog-ng default file permissions configured</i> |
| | <i>Ensure syslog-ng is configured to send logs to a remote log host</i> |
| | <i>Ensure remote syslog-ng messages are only accepted on designated log hosts</i> |
| | <i>Ensure permissions on all logfiles are configured</i> |
| | <i>Ensure logrotate is configured</i> |
| | <i>Ensure only approved ciphers are used</i> |
| | <i>Ensure only approved MAC algorithms are used</i> |
| | <i>Audit system file permissions</i> |

Table 8: PR.DS-5 - Protections Against Data Leaks are Implemented

PR.IP-1 - BASELINE CONFIGURATION

| |
|---|
| <i>Ensure mounting of cramfs filesystems is disabled</i> |
| <i>Ensure mounting of freevxfs filesystems is disabled</i> |
| <i>Ensure mounting of jffs2 filesystems is disabled</i> |
| <i>Ensure mounting of hfs filesystems is disabled</i> |
| <i>Ensure mounting of hfsplus filesystems is disabled</i> |
| <i>Ensure mounting of squashfs filesystems is disabled</i> |
| <i>Ensure mounting of udf filesystems is disabled</i> |
| <i>Ensure mounting of FAT filesystems is disabled</i> |
| <i>Ensure SETroubleshoot is not installed</i> |
| <i>Ensure the MCS Translation Service (mcstrans) is not installed</i> |
| <i>Ensure SELinux is installed</i> |
| <i>Ensure message of the day is configured properly</i> |
| <i>Ensure local login warning banner is configured properly</i> |
| <i>Ensure remote login warning banner is configured properly</i> |
| <i>Ensure GDM login banner is configured</i> |
| <i>Ensure chargen services are not enabled</i> |
| <i>Ensure daytime services are not enabled</i> |
| <i>Ensure discard services are not enabled</i> |
| <i>Ensure echo services are not enabled</i> |
| <i>Ensure time services are not enabled</i> |
| <i>Ensure tftp server is not enabled</i> |
| <i>Ensure xinetd is not enabled</i> |
| <i>Ensure X Window System is not installed</i> |
| <i>Ensure Avahi Server is not enabled</i> |
| <i>Ensure CUPS is not enabled</i> |
| <i>Ensure DHCP Server is not enabled</i> |
| <i>Ensure LDAP server is not enabled</i> |
| <i>Ensure NFS and RPC are not enabled</i> |
| <i>Ensure DNS Server is not enabled</i> |
| <i>Ensure FTP Server is not enabled</i> |
| <i>Ensure HTTP server is not enabled</i> |
| <i>Ensure IMAP and POP3 server is not enabled</i> |
| <i>Ensure Samba is not enabled</i> |
| <i>Ensure HTTP Proxy Server is not enabled</i> |
| <i>Ensure SNMP Server is not enabled</i> |
| <i>Ensure mail transfer agent is configured for local-only mode</i> |
| <i>Ensure NIS Server is not enabled</i> |
| <i>Ensure rsh server is not enabled</i> |
| <i>Ensure talk server is not enabled</i> |
| <i>Ensure telnet server is not enabled</i> |
| <i>Ensure tftp server is not enabled</i> |
| <i>Ensure rsync service is not enabled</i> |
| <i>Ensure NIS Client is not installed</i> |
| <i>Ensure rsh client is not installed</i> |
| <i>Ensure talk client is not installed</i> |
| <i>Ensure telnet client is not installed</i> |
| <i>Ensure LDAP client is not installed</i> |
| <i>Ensure DCCP is disabled</i> |
| <i>Ensure SCTP is disabled</i> |
| <i>Ensure RDS is disabled</i> |
| <i>Ensure TIPC is disabled</i> |
| <i>Ensure SSH Protocol is set to 2</i> |
| <i>Ensure SSH LogLevel is set to INFO</i> |
| <i>Ensure SSH X11 forwarding is disabled</i> |
| <i>Ensure SSH IgnoreRhosts is enabled</i> |
| <i>Ensure SSH HostbasedAuthentication is disabled</i> |
| <i>Ensure SSH root login is disabled</i> |
| <i>Ensure SSH PermitUserEnvironment is disabled</i> |
| <i>Ensure SSH warning banner is configured</i> |

Table 9: PR.IP-1 - Baseline Configuration

| | |
|--|---|
| PR.PT-1 - AUDIT/LOG RECORDS ARE DETERMINED | <i>Ensure time synchronization is in use</i> |
| | <i>Ensure ntp is configured</i> |
| | <i>Ensure chrony is configured</i> |
| | <i>Ensure system is disabled when audit logs are full</i> |
| | <i>Ensure events that modify date and time information are collected</i> |
| | <i>Ensure events that modify user/group information are collected</i> |
| | <i>Ensure events that modify the system's network environment are collected</i> |
| | <i>Ensure events that modify the system's Mandatory Access Controls are collected</i> |
| | <i>Ensure login and logout events are collected</i> |
| | <i>Ensure session initiation information is collected</i> |
| | <i>Ensure discretionary access control permission modification events are collected</i> |
| | <i>Ensure unsuccessful unauthorized file access attempts are collected</i> |
| | <i>Ensure use of privileged commands is collected</i> |
| | <i>Ensure successful file system mounts are collected</i> |
| | <i>Ensure file deletion events by users are collected</i> |
| | <i>Ensure changes to system administration scope (sudoers) is collected</i> |
| <i>Ensure system administrator actions (sudolog) are collected</i> | |
| <i>Ensure kernel module loading and unloading is collected</i> | |

Table 10: PR.PT-1 - Audit/Log Records are Determined

| | |
|---|--|
| DE.CM-7 - MONITORING IS PERFORMED | <i>Ensure AIDE is installed</i> |
| | <i>Ensure filesystem integrity is regularly checked</i> |
| | <i>Ensure auditd service is enabled</i> |
| | <i>Ensure auditing for processes that start prior to auditd is enabled</i> |
| | <i>Ensure rsyslog Service is enabled</i> |
| | <i>Ensure syslog-ng service is enabled</i> |
| <i>Ensure rsyslog or syslog-ng is installed</i> | |

Table 11: DE.CM-7 - Monitoring is Performed

| | |
|--|--|
| DE.CM-8 - VULNERABILITY SCANS ARE PERFORMED | <i>Ensure package manager repositories are configured</i> |
| | <i>Ensure gpgcheck is globally activated</i> |
| | <i>Ensure GPG keys are configured</i> |
| | <i>Ensure Red Hat Network or Subscription Manager connection is configured</i> |
| | <i>Disable the rhnsd Daemon</i> |
| <i>Ensure updates, patches, and additional security software are installed</i> | |

Table 12: DE.CM-8 - Vulnerability Scans are Performed

In general, such mapping exercises are tedious and require some deeper understanding of the framework and target of evaluation.

CAVIRIN'S IMPLEMENTATION OF THE FRAMEWORK

The Cybersecurity Framework defines 7 steps for establishing a cybersecurity program:



The Cavidin platform automates the above defined steps. The steps are detailed as follows:

STEP 1 - PRIORITIZE AND SCOPE

This helps organization to identify and scope their cybersecurity elements. It provides a unified mechanism to prioritize and scope the on-premise infrastructure components as well as cloud resources. The first step is discovering these resources on Cavidin's platform. For example, the snapshot below details on-premise discovery on Linux.

Discover Resources & Assess for Risk, Security and Compliance

DISCOVER RESOURCES
SELECT POLICY PACKS
SCHEDULE TESTS

Cloud
 On-Prem
 Docker Image

CIDR

 Validate CIDR

Starting IP

Ending IP

Asset group name

Asset group description

RESOURCE CREDENTIALS ⓘ

Select Credentials (1 selected)

rhel-7

Figure 1: Discover Resources

STEP 2 - ORIENT

The orientation phase includes identifying departments and units and what infrastructure elements each is using. The Cavin platform creates asset groups to reflect the organization's units and segregate infrastructure elements based on departments. For example, one can discover a range of machines and segregate them into departments or organizational units as below.

Discover Resources & Assess for Risk, Security and Compliance


 DISCOVER
RESOURCES


 SELECT POLICY
PACKS


 SCHEDULE
TESTS

Cloud
 On-Prem
 Docker Image

CIDR

Validate CIDR

Starting IP

Ending IP

Asset group name

Asset group description

Figure 2: Create asset groups

STEP 3 - CREATE A CURRENT PROFILE

At this stage, the platform scans the organization’s assets groups against the Cybersecurity Framework. Cavirin’s platform provides, out of the box, automated technical controls, mapped to the various framework requirements. Such controls are automatically customized and tuned to match the target of evaluation. For example, if the target is a Windows machine, a particular set of safeguards are evaluated against a specific NIST cybersecurity control requirement. If the target is a Linux OS, the safeguards are automatically chosen to match the target capabilities.



NIST Cybersecurity Framework Policy Pack

Version 1.0.0, 08/14/2017

4358 policies



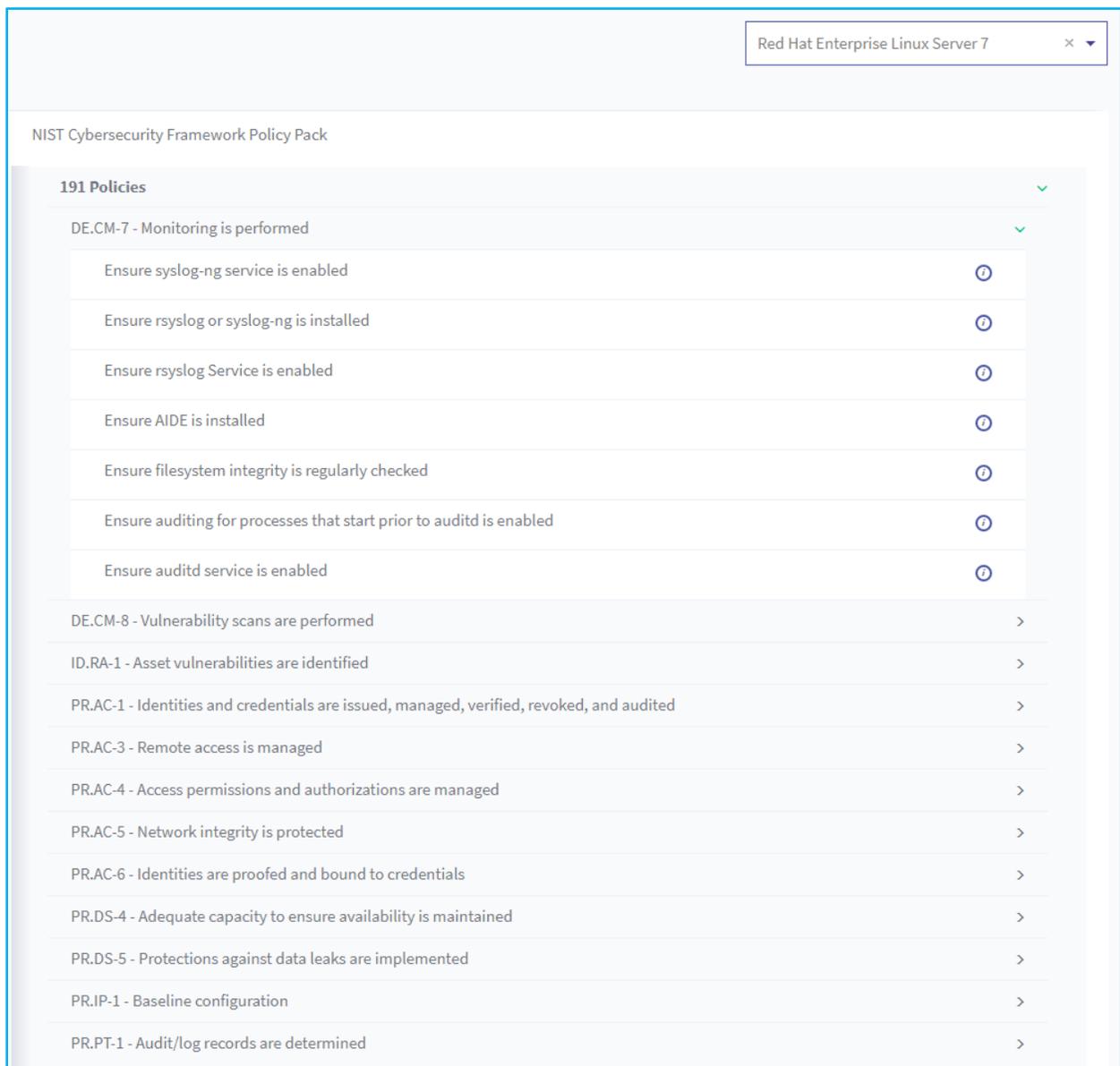


Figure 3: NIST CSF Policy Pack filtered for RHEL 7 (191 out of 4358 policies selected)

Detailed descriptions and other relevant information for each policy under the control functions is available at a click.

Ensure filesystem integrity is regularly checked

Weight: 1
Severity: MEDIUM

Description:
Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Rationale:
Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Audit:
'Run the following commands to determine if there is a cron job scheduled to run the aide check. # crontab -u root -l | grep aide # grep -r aide /etc/cron.* /etc/crontab Ensure a cron job in compliance with site policy is returned.'

Remediation:
Run the following command:# crontab -u root -eAdd the following line to the crontab:0 5 * * * /usr/sbin/aide --check

Figure 4: NIST CSF Policy Details

STEP 4 - CONDUCT A RISK ASSESSMENT

Once the assessment against the cybersecurity framework is complete, the platform presents a risk assessment report. The report provides control areas, risk assessment scoring and also the details to mitigate and manage the risks.

Resource Compliance Report

Report Details

Policy Pack: NIST Cybersecurity Framework Policy Pack
 Assessment started: 09/08/2017 @ 13:08
 Assessment completed: 09/08/2017 @ 13:15
 Analyst: administrator

Resource Summary

Host/Instance ID: ip-172-31-22-189.ap-south-1.compute.internal
 IP address: 13.126.140.27
 OS: RHEL 7

Archive Export Share

60

STATE WARNING

ISSUES COUNT PER CONTROL FAMILY

| Control Family | Low Severity | Medium Severity | High Severity | Fail | Pass |
|----------------------------------|--------------|-----------------|---------------|------|------|
| PR.AC-5 - Network integrity i .. | 0 | 1 | 0 | 1 | 1 |
| PR.AC-3 - Remote access is ma .. | 0 | 9 | 0 | 9 | 8 |
| DE.CM-7 - Monitoring is perfo .. | 0 | 1 | 0 | 1 | 4 |
| PR.DS-5 - Protections against .. | 0 | 5 | 0 | 5 | 1 |
| PR.AC-1 - Identities and cred .. | 0 | 3 | 0 | 3 | 0 |
| PR.IP-1 - Baseline configurat .. | 0 | 16 | 1 | 16 | 37 |

Legend: Low Severity (Blue), Medium Severity (Yellow), High Severity (Red)

Figure 5: Resource Risk Assessment Score Summary

| 191 Policies | | | | State | Severity Level | All Control Families |
|---|----------|-------|--|-------|----------------|----------------------|
| Policy Name | SEVERITY | STATE | CONTROL FAMILY | | | |
| <input type="radio"/> Ensure mounting of freevxfs filesystems is disabled | Low | Fail | PR.IP-1 - Baseline configuration | | | |
| <input type="radio"/> Ensure nodev option set on /tmp partition | Medium | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure nosuid option set on /tmp partition | Medium | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure nosuid option set on /var/tmp partition | Medium | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure noexec option set on /var/tmp partition | Medium | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure nosuid option set on /dev/shm partition | Medium | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure noexec option set on /dev/shm partition | Medium | Fail | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure gpgcheck is globally activated | Medium | Pass | DE.CM-8 - Vulnerability scans are performed | | | |
| <input type="radio"/> Ensure SELinux policy is configured | Low | Pass | ID.RA-1 - Asset vulnerabilities are identified | | | |
| <input type="radio"/> Ensure SELinux is installed | Low | Pass | PR.IP-1 - Baseline configuration | | | |

Figure 6: Risk Assessment Details

STEP 5 - CREATE A TARGET PROFILE

The organization then evaluates the risk assessment report and determines what the target posture should look like. One can also tune in the assessment to match unique organization specific risks.

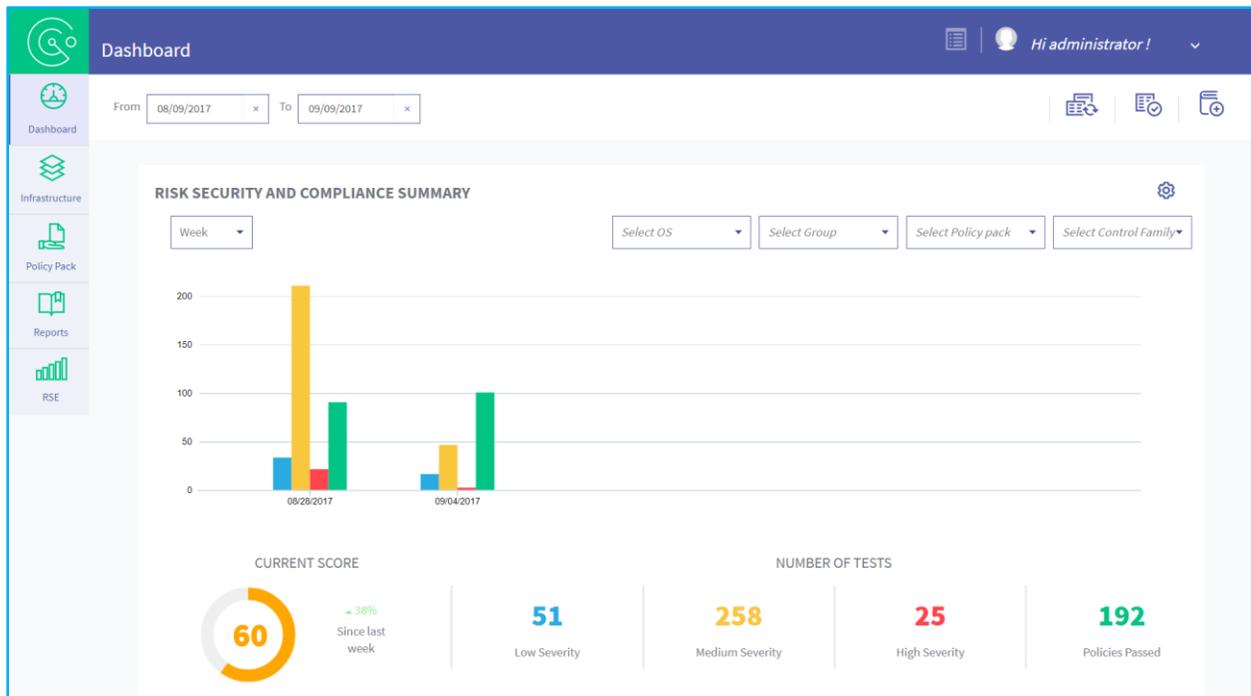


Figure 7: Dashboard depicting cyber security assessment trends

STEP 6 - DETERMINE, ANALYZE, AND PRIORITIZE GAPS

Once the organization has identified the target, the Cavin platform helps one identify the controls gaps and provide analytics on top of various control requirements.

| 3 Policies | | | | | Fail | High | All Control Families |
|---|----------|-------|--------|---|------|------|----------------------|
| Policy Name | SEVERITY | STATE | WEIGHT | CONTROL FAMILY | | | |
| Ensure SSH Protocol is set to 2 | High | Fail | 1 | PR.IP-1 - Baseline configuration | | | |
| Ensure password fields are not empty | High | Fail | 1 | PR.AC-6 - Identities are proofed and bound to credentials | | | |
| Ensure SSH PermitEmptyPasswords is disabled | High | Fail | 1 | PR.AC-6 - Identities are proofed and bound to credentials | | | |

Figure 8: Prioritize control gaps

STEP 7 - IMPLEMENT ACTION PLAN

The platform then supports the organization in creating an action plan. The action plans may be mitigating the risks by remediating the control gaps or may be integrating the finding with a ticketing or incident management systems.

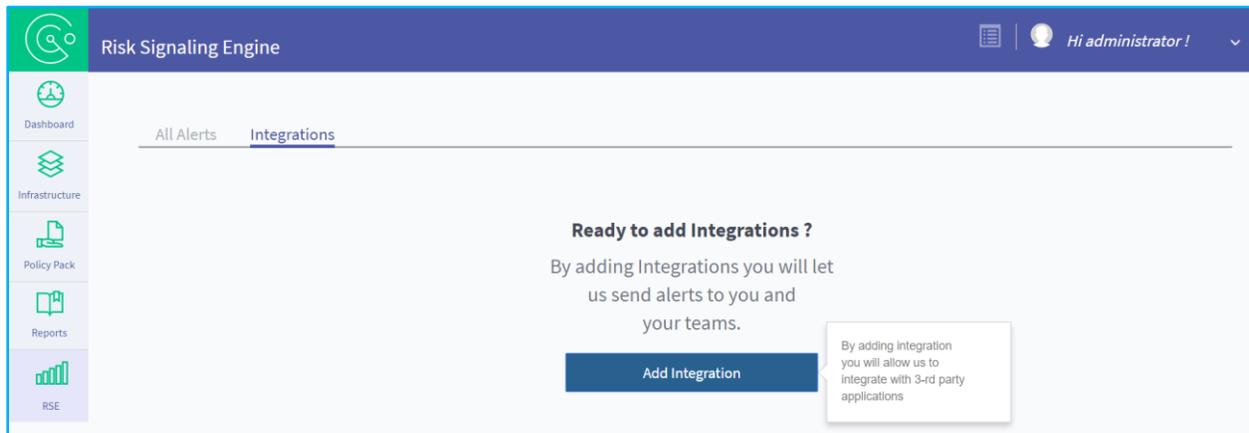


Figure 9: Implement Action Plan via various integrations

ADD INTEGRATION X

Cavirin can send alert(s) and notification(s) to a wide variety of monitoring and conflict resolution tools. Select the option below that best describes your case, and we will guide you through the integration steps.

Integration type

PagerDuty ▼

PAGERDUTY INTEGRATION

PagerDuty is Event Intelligence, Response Orchestration, Incident resolution platform, helping IT Operations and DevSecOps teams deliver alerting, on-call scheduling, compliance policies escalations, incident tracking and resolution, performance, and uptime of your infrastructure

Directions:

1. Go to [PagerDuty](#) and log in to your account
2. From the Configuration menu, select Services. ⓘ
3. On your Services page, click +Add New Service ⓘ
4. In General settings enter a Service Name ⓘ
5. Select Cavirin from the Integration Type menu ⓘ
6. Under Incident Settings, specify the Escalation Policy, Notification Urgency, and Incident Behavior for your new service
7. Click Add Service ⓘ
8. Copy Integration Key ⓘ
9. Enter the service Integration Key below

API Key:

Add Integration Key

Figure 10: Example Integration with Pager Duty

ADD INTEGRATION X

Cavirin can send alert(s) and notification(s) to a wide variety of monitoring and conflict resolution tools. Select the option below that best describes your case, and we will guide you through the integration steps.

Integration type

JIRA

JIRA is a proprietary issue tracking product, developed by Atlassian. It provides bug tracking, issue tracking, and project management functions.

JIRA Url

Provide Jira url

Username

UserName

Password

Password

JIRA Project Key

Add project key

Figure 11: Example Integration with JIRA

In essence, the Cavirin platform does the heavy lifting when it comes to the NIST Framework for Cybersecurity. It automates various technical controls to provide one with consistent view across the organization’s infrastructure. Apart from the NIST Cybersecurity Framework, Cavirin platform also provides various other out-of-the-box risk assessment standards such as PCI, HIPAA, CJIS, and ISO. It also covers other NIST standards such as

NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-171 - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST Special Publication 800-190 - Application Container Security Guide

This way CAVIRIN provides one of the most comprehensive platforms for helping you manage your Cybersecurity.

CONCLUSION

This paper demonstrates automating the NIST Framework for Improving Critical Infrastructure Cybersecurity at the operating system level. Various control functions can be mapped to the target capabilities and be automated across cloud and on-premises infrastructure.