Remediant : NIST 800-171/3.1/3.5.3 and 800-53 V5 (March 2020) referenced Access Controls Assessment and Alignment

Prepared by
Stan Quintana, Executive Vice President, TAG Cyber
squintana@tag-cyber.com

Version 1.0
May 28, 2020

Executive Summary

This report summarizes a mapping effort between the security provided by Remediant's SecureONE solution and the NIST 800-171/3.1/3.5.3 and 800-53 V5 (March 2020) referenced Access Controls framework. The mapping demonstrates that of the 23 800-171/3.1/3.5.3 requirements the platform validates 13 requirements (56.5%), provides complementary support for 4 requirements (17.4%), and is not applicable to 6 requirements (26.1%) in the NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls framework. Combining the Validate and Support criteria Remediant addresses 73.9% of the NIST 800-171/3.1/3.5.3 requirements. Based on this assessment, if Remediant's SecureONE is implemented correctly according to recommendations as outlined by Remediant one can expect a consumer to achieve significant level of access control in their PAM program.

Introduction

Decisions about passwords have traditionally been left in the hands of end-users who often make colossal errors in judgment in their selection, use, and sharing. When this involves passwords for critically essential resources in an enterprise, we often refer to the credential-based authentication information as a privilege. As one might expect, mishandling or poor decision-making with privileges can lead to more serious consequences. To deal with both problems, password management and privilege management tools have emerged that simplify the corresponding tasks. (Commercial vendors typically market tools for one or the other tasks, but often not both.) Whether for consumers or enterprise users, and whether for passwords or privileges, the general idea is that an automated tool simplifies the interface to the user, and then securely manages back-end authentication usage and handling. Both privilege and password management tools are getting easier to use, more commonly accepted, and better integrated into the usage patterns of consumer and enterprise users. Secure constructs such as password and privilege vaults, for example, are becoming more frequently cited in enterprise security policy requirements, and even showing up in security compliance frameworks. One challenge to the use of secure vaults involves the complexity and challenge of ensuring proper coverage across all privileged passwords for all relevant applications. Specifically, the vault can only protect the credentials that are in the vault – so any credentials that are missed continue to go unprotected. To that end, vendors have begun to build solutions that focus on the process of privilege management without need for a vault. Generally, two-factor authentication is an important element of this and all password and privilege management schemes. Password-less experiences are becoming much more discussed as a requirement for enterprise, as is the decision to avoid a centralized store of authentication information. It stands to reason that decentralizing the administration of passwords, for example, dramatically reduces the potential that a malicious actor can find one central place where a treasure trove of authentication information can be stolen at once.

2020 Trends for Password/Privilege Management

First generation privilege and password management involved early tools in the late 90's that were not as well-understood by customers as they are today. Second generation tools from 2007 to today saw considerable usage and security improvements; and third generation tools will become even more effective, as machine learning and advanced analytics find their way into the algorithms and utilities. The trend for both password and privilege management can be summed up pretty-well by the transition from simple, stand-alone administrative tools to more advanced, analytic controls, especially in the context of enterprise use. The capabilities are becoming more embedded into identity and access management (IAM) infrastructure, and even emerging Internet of Things (IoT) authentication and authorization.

Both capabilities will also benefit from increased use of cloud and virtualized as-a-service computing, if only because these emerging services increase the demand for non-homogeneous authentication and authorization for consumers and enterprise users. One might thus expect to see password and privilege management support integrate with cloud security solutions such as cloud access security brokers (CASBs). The future for privilege and password management continues to be positive, with privilege management tools in the enterprise likely seeing exponential growth due to increased demands from a compliance perspective. Password management is likely to see continued linear growth, as the typical consumer will remain somewhat uncertain about the best way to manage passwords, often just utilizing federated authentication between social media sites. It is worth mentioning here that some debate exists within the security community about whether a true password-less experience is a reasonable and attainable goal. This debate is somewhat orthogonal to the password and privilege management functions, as these capabilities will travel with whatever contextual or adaptive credential validation is in use by enterprise and consumers in the coming years. Biometrics, obviously, provide an important complement to passwords and privileges, in the context of adaptive multi-factor authentication. It is expected that both passwords, privileges, and other artifacts related to strong authentication will compete based on the ease of integration with adaptive validation, as well as on which can effectively minimize required proof actions by users.

CYBER security experts agree without exception that hackers target privileged access in their offensive campaigns. This stands to reason, simply because elevated access allows an attacker to target the most important applications, the

most critical business processes, the most valuable resources and permits the attacker to cover their tracks. Security privileges thus become an important aspect of any modern enterprise security protection strategy and require special attention from CISO-led teams. Remediant has pioneered Just In-Time security for privileged access, designed in a manner that avoids need for special agents or vaults. The Remediant SecureONE platform supports control and visibility into the distribution, usage, and protection of enterprise privileges.

Product Overview

Remediant's SecureONE is a privileged access management solution. Agent-less, vault-less, and never shared, SecureOne enables a new level of control and insight over the distribution, usage, and protection of privileged access across enterprise environments. Based on a Zero-trust model, SecureONE ensures privileged access is allocated and continuously inventoried by granting privileged access on a Just-In-Time, Just-Enough basis using two-factor authentication.

Remediant SecureONE Provides:

- Rapid deployment, inventory and protection with no agents or complicated infrastructure to support
- Administers privileged access Just-In-Time and Just-Enough. Individual users are given access to individual systems for a limited time with automatic removal.
- Continuous detection (scan) and prevention (protect) of unauthorized privileged access
- Continuous visibility to every administrator account on every system
- Removal of standing access enterprise-wide with a single action
- Privileged access without relying on shared accounts, or temporary accounts that complicate accountability and tracing
- Coverage of 100% of systems across Windows, macOS, Linux, desktops, servers, cloud, on-prem and hybrid

NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls – Mapping Summary

Remediant's SecureONE solution addresses many of the NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls standards. The following is a summary of the NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls category and Remediant relationship to this category, where the results are that the platform directly validates 13 of 23 requirements (56.5%), provides complementary support for 4 requirements (17.4%), and is not applicable to 6 requirements (26.1%) in the NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls framework. (See below with supporting details)

NIST 800-171/3.1/3.5.3 and 800-53 referenced Access Controls Mapping to Remediant Platform					
CUI Security Requirements	NIST 800-53 Relevant Security Controls	Remediant mapping description	Validate	Support	N/A
3.1.1 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC-2 - Account Mgmt AC-3 – Access Enforcement AC-17 Remote Access	Access is limited by Remediant SecureONE through the enforcement of enterprise wide Zero Standing Privilege. Specifically, this is done in three steps: (1) Continuous Inventory of access to critical systems: Critical access across an enterprise is surfaced and inventoried on an ongoing basis. Across Windows, Mac and Linux physical and virtual machines and without installing an agent, this solution can detect any changes in privileged access (2) Access revocation & right sizing: Accounts with critical access are removed from administrator groups and Sudoers across the enterprise (3) Just-in-time Administration: when privileged access is requested, it is only granted to the specified resource for the specified amount of time using the user's own account	1		
3.1.2 – Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2 - Account Mgmt AC-3 – Access Enforcement AC-17 Remote Access	Directly addressed for administrator level access. SecureONE limits information system access to authorized users to a just-in-time basis. Specifically, the access is limited to the resources authorized for a particular user and time limited to only what is necessary as well. Access is removed automatically at the conclusion of the authorized access period.	1		

3.1.3 - Control the flow of CUI in accordance with approved authorizations.	AC-4 – Information Flow Enforcement	Controlled through removing users from administrator groups and sudoers that have standing access to CUI. In addition, privileged access is provisioned just in time (JIT) to authorized users for the approved amount of time and only to a specific machine	1		
3.1.4 - Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5 – Separation of Duties	Controlled by removing standing access and shared accounts. Enhances typical role-based approaches to segregation of duty by removing unauthorized privileged access continuously.	1		
3.1.5 - Employ the principle of least privilege, including for specific security functions and privileged accounts	AC-6 – Least Privilege AC-6(1) – Least Privilege – Authorize Access to Security Functions AC-6(5) -Least Privilege - Privileged Accounts)	Controlled through enforcing Zero Standing Privilege by default. ZSP mode removes users from local administrator groups and sudoers and provisions elevated privileges just-in-time to only the specific systems where access is required.	1		
3.1.6 - Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2) – Least Privilege – Non-Privilege Access for Nonsecurity functions	Controlled through enforcing Zero Standing Privilege - Since no standing privilege is present on an endpoint in SecureONE's model, code execution requiring admin or privilege escalation is prevented. This applies to any action requiring administrative privileges to run – regardless of it is running Powershell, Command-Line Interface, is a scheduled task, is a script, executed manually by a user (or attacker). SecureONE provides an audit trail of each user's requests for privileged access and can show where and when a specific account had administrative access to a resource.	1		
3.1.7 - Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	AC-6(9) – Least Privilege – Auditing Use of Privileged Functions AC-6(10) – Least Privilege – Prohibit Non-Privileged Users from Executing Privileged Functions	Controlled through enforcing Zero Standing Privilege - Since no standing privilege is present on an endpoint in SecureONE's model, code execution requiring admin or privilege escalation is prevented. This applies to any action requiring administrative privileges to run – regardless of it is running Powershell, Command-Line Interface, is a scheduled task, is a script, executed manually by a user (or attacker).	1		
3.1.8 – Limit unsuccessful logon attempts	AC-7 – Unsuccessful	Remediant SecureONE limits unsuccessful logon attempts to a single try; however, works in conjunction with access control software as	1		

	Longson Attempts	third factor authentication. Reports and logs unsuccessful logon attempts to privileged accounts			
3.1.9 – Provide privacy and security notices consistent with applicable CUI rules.	AC-8 – System Use Notifications	Indirect - The messages SecureONE sends to logging solutions (SIEMs) can easily be leveraged to report on relevant notices pertaining to privileged access.		1	
3.1.10 – Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	AC-11 System/Device Lock, – Pattern-hiding Displays	Does not support			1
3.1.11 Terminate (automatically) a user session after a defined condition	AC-12 - Session Termination	For Linux - Sessions are terminated once the approved time limit has reached or if requested through the SecureONE console earlier For Windows - Account is removed from the relevant admin group to ensure user is not authorized to perform privileged functions once the defined condition or time limit is met.	1		
3.1.12 Monitor and control remote access sessions.	AC-17(1) - Remote Access Automated Monitoring /Control	Supports by logging successful and failed authentication and authorization attempts		1	
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2) - Remote Access Protection of Confidentiality / Integrity Using Encryption	N/A SecureONE does not provide session management.			1
3.1.14 Route remote access via managed access control points.	AC-17(3) - Remote Access Managed Access Control Points	N/A SecureONE does not provide a remote access capability			1
3.1.15 Authorize remote execution of privileged commands and remote access to security relevant information.	AC-17(4) - Remote Access Privileged Commands /Access	Managed through limiting local admin group access (for Windows) and sudoer access for Linux to just-in-time	1		
3.1.16 Authorize wireless access prior to allowing such connections.	AC-18 - Wireless Access	Indirectly - account is authorized via Just-in-Time access		1	

3.1.17 Protect wireless access using authentication and encryption.	AC-18(1) - Wireless Access Authentication and Encryption	Indirectly - account is authorized via Just-in-Time access		1	
3.1.18 Control connection of mobile devices.	AC-19 - Access Control for Mobile Devices	N/A - Currently supports desktop and server Windows, Linux and MacOS versions			1
3.1.19 Encrypt CUI on mobile devices.	AC-19(5) - Access Control for Mobile Devices Full Device / Cont.	N/A - Currently supports desktop and server Windows, Linux and MacOS versions			1
3.1.20 Verify and control/limit connections to and use of external information systems.	AC-20 - Use of External Information Systems AC-20(1) - Use of External Information Systems Limits on Authorized Use	Through the enforcement of Zero Standing Privilege to administrator level access that enable users to execute commands that connect to and use external information systems	1		
3.1.21 Limit use of organizational portable storage devices on external information systems.	AC-20(2) - Use of External Information Systems Portable Storage Devices	Does Not Support			1
3.1.22 Control information posted or processed on publicly accessible information systems.	AC-22 - Publicly Accessible Content	Through the enforcement of Zero Standing Privilege to administrator level access that enable users to execute commands that connect to and use external information systems	1		
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1) - Identification and Authentication (Organizational Users) Network Access to Privileged Accounts IA-2(2) - Identification and Authentication (Organizational Users) Network Access to Non-	Remediant SecureONE's Dynamic Access Control controls access to information systems based on a number of different criteria, those being: • Role Based Access Control (RBAC) • Attribute-Based Access Control (ABAC) – aligned to organization structure • Organization-based access control(OrBAC) • Segregation of Duties • Two-Factor Authentication • Privileged Account Management • Privileged Access Management • MFA-Protected privileged access to all systems	1		

	Privileged Accounts IA-2(3) - Identification and Authentication (Organizational Users) Local Access to Privileged Accounts				
Total			13	4	6