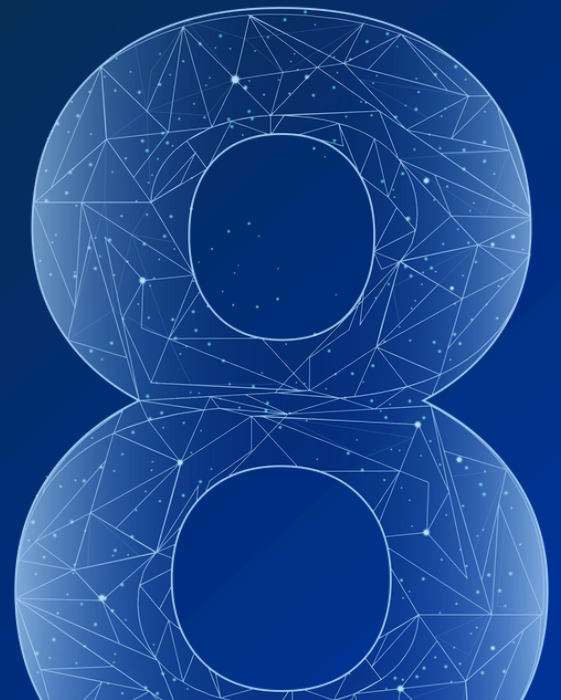




Meet ACSC's 8 Essential Strategies with PAM

Whitepaper



01 0 1 00 011

Index

| | |
|---|----|
| 1. The 8 Strategies Recommended by ACSC to Mitigate Risk..... | 03 |
| 2. Essential 8 - Levels of Maturity..... | 03 |
| 3. Requirements as per Maturity Levels..... | 04 |
| 5. Securden's Unified PAM Solution..... | 04 |
| 6. Security Controls Satisfied by Securden Unified PAM..... | 09 |

Introduction

The Essential Eight was designed by the ACSC (Australian Cyber Security Centre) to mitigate cybersecurity incidents and help protect organizations IT networks from various threats. The most effective strategies that were prioritized for risk mitigation are the Essential Eight.

It was first published in June 2017 and has been updated since then. Essential Eight was prepared based on Australian Signals Directorate ASD's learnings from producing cyber threat intelligence and conducting pen tests.

The 8 Strategies Recommended by ACSC to Mitigate Risk Are:



- 1 Patch Applications
- 2 Patch Operating Systems
- 3 Utilize Multi-Factor Authentication
- 4 Restrict Administrative privileges
- 5 Control Applications
- 6 Restrict Microsoft Office Macros
- 7 Implement User Application Hardening
- 8 Take Regular Backups.

Essential 8 - Levels of Maturity



ACSC has defined four levels of maturity (Level Zero through Three) to assist organizations with their implementation of Essential Eight. Each level of maturity shows how aligned an organization is with the intent of the mitigation strategy.

Maturity levels are based on mitigating increasing levels of tactics, techniques and tools used by attackers against targets. ACSC recommends that organizations consider what level of tradecraft and targeting they are prone to, rather than which malicious actors they are aiming to mitigate.

Requirements as per Maturity Levels


Requirements for Maturity Level One through to Maturity Level Three build upon one another like layers. So, if you have satisfied a level 2 maturity level – you will only need to satisfy some additional controls to obtain a level 3 maturity.


We will discuss the essential eight requirements under each category and specify which controls help satisfy which maturity level.

Securden's Unified PAM Solution




Securden Unified PAM is a solution designed to restrict privileged access, manage local administrative rights and control applications on Windows, Linux, Unix and Mac devices. It helps prevent malware execution and assists organizations to satisfy up to **Maturity Level 3** for specific requirement categories.

| Specific Security Control | Maturity Levels |  How Securden Unified PAM helps |
|--|---|---|
| ASCS Essential Eight Category 1. Multi-factor authentication (MFA) | | |
| 1. | Multi-factor authentication is used to authenticate users to their organization's / third-party services that process, store or communicate internal / external sensitive data. | <p>1, 2, 3</p> <p>Securden acts as the centralized repository of all accounts used to access online services.</p> <p>Sensitive organizational data is also stored in the encrypted repository.</p> <p>For any user in the organization to access these online services / data - they need to go through Securden Unified PAM.</p> <p>Multifactor Authentication can be enforced to access this repository - so users can access these resources securely after authentication through one or more factors.</p> |
| 2. | Multi-factor authentication is used to authenticate privileged and unprivileged users of systems and data repositories. | <p>1, 2, 3</p> <p>Privileged and unprivileged users who connect to remote systems and servers through SSH / RDP / SQL Securden Unified PAM can only do so after authenticating through multiple factors.</p> |
| 3. | Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are. | <p>1, 2, 3</p> <p>Securden Unified PAM integrates with several 2FA providers such as Duo, YubiKey, Google Auth, Microsoft Auth, Mail OTP etc.</p> <p>One of the factors can be a password / OTP that the users know.</p> <p>It can be a Yubikey or a physical authentication device that the user has.</p> <p>Or the user can authenticate through their own biometrics (what they are).</p> |
| 4. | Successful and unsuccessful multi-factor authentication events are centrally logged. | <p>2, 3</p> <p>Securden Unified PAM logs and audits all events including when users have a failed attempt at authenticating through MFA to access sensitive resources.</p> |
| 5. | Event logs are protected from unauthorized modification and deletion. | <p>2, 3</p> <p>All audit logs generated are tamper resistant and cannot be deleted or modified.</p> |

| Specific Security Control | | Maturity Levels |  How Securden Unified PAM helps |
|---|---|-----------------|---|
| 6. | Event logs from servers and workstations are analyzed in a timely manner to detect cyber security events. | 3 | All Windows security events occurring on endpoints are detected and logged in real time. These events can be notified to the administration when they occur. |
| 7. | Cyber security events are analyzed in a timely manner to identify cyber security incidents | 3 | All events that occur in Securden Unified PAM are logged and these event logs can be sent to an SIEM tool to analyze. |
| ASCS Essential Eight Category 2. Restrict Administrative Privileges | | | |
| 1. | Requests for privileged access to systems, applications and data repositories are validated when first requested. | 1, 2, 3 | Requests raised by users access to systems, applications and sensitive data can be validated by one or more approvers and automatically approved based on factors such as the user having a valid ticket corresponding to his/her access request. |
| 2. | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | 1, 2, 3 | Privileged access to remote systems, applications, and sensitive data can be granted to users for a specific time-period, after which they will not be able to access these resources unless a request is raised and validated. |
| 3. | Privileged access to systems and applications is disabled after 45 days of inactivity. | 1 | Securden Unified PAM detects inactive users and provides a report of all the systems they have access to. This report can help disable their access provisions in a timely manner. |
| 4. | Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access. | 1 | Securden Unified PAM acts as the centralized repository that stores all privileged accounts. All users onboarded in Securden Unified PAM can be assigned privileged account with granularity in the level of privileged access based on their duties and job responsibilities. |
| 5. | Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties | 1 | Securden Unified PAM helps enforce the Principle of Least Privilege (PoLP). Users are limited only to the systems and data that they require. |

| Specific Security Control | Maturity Levels |  How Securden Unified PAM helps | |
|---|--|---|--|
| ASCS Essential Eight Category 2. Restrict Administrative Privileges | | | |
| 6. | Secure Admin Workstations are used in the performance of administrative activities. | 1 | Agents deployed on workstations ensure that the local administrative privileges are removed, and all admin activity is performed in a time-restricted fully monitored manner. |
| 7. | Unprivileged accounts cannot log on to privileged operating environments. | 1 | Only the privileged accounts mapped to assets will be able to launch connections to them. |
| 8. | Just-in-time administration is used for administering systems and applications. | 1 | All access to system and applications can be administered in a Just-in-time fashion. After the duration ends, all access is revoked. |
| 9. | Administrative activities are conducted through jump servers. | 1 | Privileged sessions to remote resources are carried out through jump servers. |
| 10. | Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | 1 | Securden Unified PAM ensures that all passwords – local admin account passwords, domain passwords, Windows service accounts and dependencies are all long, unique, complex, and strong as per the password policy defined. |
| 11. | Privileged access events are centrally logged. | 1 | All events relating to privileged access are logged centrally and can be exported as reports. |
| 12. | Privileged account and group management events are centrally logged. | 1 | All events relating to privileged accounts and account groups are logged centrally. |
| 13. | Event logs are protected from unauthorized modification and deletion. | 1 | Event logs generated are tamper proof - and cannot be modified or deleted. |

| Specific Security Control | Maturity Levels |  How Securden Unified PAM helps | |
|--|--|---|---|
| ASCS Essential Eight Category 3. Application Control | | | |
| 1. | Application control is implemented on workstations. | 1 | Through centralized control policies, Securden Unified PAM lets administrators define which applications are allowed and blocked for users. |
| 2. | Application control is implemented on internet-facing servers. | 1 | Through the lightweight agent, applications can be controlled on internet facing and non-internet facing servers. |
| 3. | Application control is applied to user profiles and temporary folders. | 1 | Application control can be specifically applied to profiles of users who log in to systems. |
| 4. | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organization-approved set. | 1 | Through application control policies, execution of various scripts, installers, apps and applets etc. can be restricted. |
| 5. | Microsoft's recommended application blocklist is implemented. | 1 | Applications recommended by Microsoft to be blocked can be restricted through a blocklist policy. |
| 6. | Application control rulesets are validated on an annual or more frequent basis. | 1 | Application control rulesets / policies can be reviewed and validated by the administrator through reports. |
| 7. | Allowed and blocked application control events are centrally logged. | 1 | All application allowed and blocked events are logged centrally and can be downloaded as reports when needed. |
| 8. | Event logs are protected from unauthorized modification and deletion. | 1 | Event logs are tamper proof and protected from unauthorized modification and deletion. |

| Specific Security Control | Maturity Levels |  How Securden Unified PAM helps |
|---|--|---|
| ASCS Essential Eight Category 4. User Application Hardening | | |
| 1. | Internet Explorer 11 is disabled or removed. | 1, 2, 3 |
| | | Internet Explorer 11 can be blocked from usage. No user will be able to run or install this software. |
| 2. | PowerShell module logging, script block logging and transcription events are centrally logged. Command line process creation events are centrally logged. | 2, 3 |
| | | All processes that require admin rights such as PowerShell and Command Line are centrally logged. |
| 3. | Windows PowerShell 2.0 is disabled or removed. | 3 |
| | | Windows PowerShell 2.0 can be blocked from usage. No user will be able to run or install this software. |

Security Controls Satisfied by Securden Unified PAM



Securden Unified PAM addresses multiple requirement categories under Essential 8, specifically:

- Application Control
- User Application Hardening
- Admin Privileges Restriction and
- Multifactor Authentication

While other PAM solutions require multiple solutions and separate modules to satisfy these requirements – Securden Unified PAM is a single solution to cover security aspects across Privileged Account & Session Management, Remote Access Management, Password Management and Privilege Elevation and Delegation Management.