|  |
| --- |
|  |
| **3.5** | **Identification and authentication** |
| 3.5.1 | Identify information system users, processes acting on behalf of users or devices   * + Verify – Splunk Forwarder is sending Application Logs   + Support – Reports and Dashboards that can audit individual users by process and devices |
| 3.5.2 | Authenticate (or verify) the identities of those users, processes or devices as a prerequisite to allowing access to organizational information systems   * + Verify – Physical Access will require badge authentication. AD will require proper credentials and if 2FA is available then a RSA key.   + Execution – Alert when someone attempts to access key area   + Support – Reports and Dashboards of access changes and violations |
| 3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts   * + Verify – Check both indexed auth logs to ensure the user went through both authentications   + Support – Reports and Dashboards of failed auth |
| 3.5.4 | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts   * + Verify – the software is logging failed auth   + Execution – Alert brute force attacks   + Support – Reports and Dashboards of overall usage |
| 3.5.5 | Prevent reuse of identifiers after a defined period of inactivity   * + Verify – AD Logs that a group policy is set and search index when a user last set password and compare when they change it again   + Execution – Alert when it does such action   + Support – Report timeline of actions |
| 3.5.6 | Disable identifiers after a defined period of inactivity   * + Verify – AD Log showed account was locked   + Execution – Alert when key accounts are locked   + Support – overview of when it occurs time wise |
| 3.5.7 | Enforce a minimum password complexity and change of characters when new passwords are created   * + Verify – AD shows GPO was updated and search users who had to change passwords   + Execution – Alert when GPO was enforced   + Support – Overview of when it occurs the most |
| 3.5.8 | Prohibit password reuse for a specified number of generations   * + Verify – Search for GPO that shows it was changed to the following control   + Support – Review users who have had to do it in N period of time |
| 3.5.9 | Allow temporary password use for system logons with an immediate change to a permanent password   * + Verify – Monitor AD Log for UAC event on that user made by admin   + Execution – Alert on key accounts being told to do this   + Support – Report of when said event is done |
| 3.5.10 | Store and transmit only encrypted representation of passwords   * + Verify – Ensure that the encryptions setting was turned on   + Execution – Alert when it’s turned off |
| 3.5.11 | Obscure feedback of authentication information   * + Verify – Ensure that the service doing this action logged that it’s turned on   + Execution – Alert when it’s shut off. |
| **3.7** | **Maintenance** |
| 3.7.1 | Perform maintenance on organizational information systems   * + Verify – The changes made to the system were completed   + Execution – When critical settings are changed unintendedly   + Support – Report on changed files overtime |
| 3.7.2 | Provide effective controls on the tools, techniques, mechanisms and personnel used to conduct information system maintenance   * + Verify –   + Execution -   + Support - |
| 3.7.3 | Ensure equipment removed for off-site maintenance is sanitized of any CUI   * + Verify – Check win logs for “DELETE” of said files   + Execution – When a CUI file is accessed |
| 3.7.4 | Check media containing diagnostic and test programs for malicious code before the media are used in the information system   * + Verify – AV logs show whether it contained it or not   + Execution – Alert when event confirms malicious code |
| 3.7.5 | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete   * + Verify – Security logs check to ensure said connection was terminated   + Execution – Alert when not terminated   + Support – Overall time of when it fails |
| 3.7.6 | Supervise the maintenance activities of maintenance personnel without required access authorization   * + Verify – N/A   + Execution – N/A   + Support – N/A |
| **3.8** | **Media Protection** |
| 3.8.1 | Protect (i.e physically control and securely store) information system media containing CUI, both paper and digital   * + Verify – Badge ID verification and ensure they’re authenticated to go in   + Execution – Alert when someone fails to get in |
| 3.8.2 | Limit access to CUI on information system media to authorized users   * + Verify – Check flagged media devices and ensure proper permissions are set   + Execution – Alert when out of group user accesses it   + Support – Overview of usage access |
| 3.8.3 | Sanitize or destroy information system media containing CUI before disposal or release for reuse   * + Verify – Windows event log displayed DELETE for the object |
| 3.8.4 | Mark media with necessary CUI markings and distribution limitations   * + Verify – Check log for proper permissions being set to the following groups   + Execution – Alert if non-vetted group accesses it. |
| 3.8.5 | Control Access to media containing CUI and Maintain accountability for media during transport outside of controlled areas   * + Verify – Monitor which machines open the host file and have it written into.   + Execution – Nonvetted host attempts to access said file   + Support – Dashboard view of where it has been accessed |
| 3.8.6 | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards   * + Verify – Mechanism logs show that the behavior of said system is following correct policy.   + Execution – Alert Sysadmin if app is not behaving correctly. |
| 3.8.7 | Control the use of removable media on information system components   * + Verify – Vetted Drives only have access to certain media devices   + Execution – Alert when unauth tries to access   + Support – Overview of files accessed accept/denied |
| 3.8.8 | Prohibit the use of portable storage devices when such devices have no identifiable owner   * + Verify – Monitor removable storage events and alert when non-ATO is connected |
| 3.8.9 | Protect the confidentiality of backup CUI at storage locations   * + Verify – Monitor AD Logs and confirm that said CUI is only for permitted users   + Execution – Alert when attempted failed access |
| **3.1o** | **Physical Security** |
| 3.10.1 | Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals   * + Verify – Check badge logs on room access permission.   + Execution – Alert when secure areas are accessed with non-vetted user. |
| 3.10.2 | Protect and monitor the physical facility and support infrastructure for those information systems   * + Verify – Use Splunk UF to monitor all UF supported devices. |
| 3.10.3 | Escort visitors and monitor visitor activity   * + Verify – Monitor badge data and ensure guest badge has set permission |
| 3.10.4 | Maintain audit logs of physical access   * + Verify – HID Badge data is being forwarded. |
| 3.10.5 | Control and manage physical access devices   * + Verify – Said employee has proper credentials to access said device   + Execution – Someone attempts to access a non-approved device.   + Support - |
| 3.10.6 | Enforce safeguarding measures for CUI at alternate work sites (telework sites)   * + Verify – Ensure said applications are working as intended and protecting CUI.   + Execution – Alert when app logs aren’t forwarding. |
| **3.11** | **Risk Assessment** |
| 3.11.1 | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation) organizational assets and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.   * + Verify – Have flagged files monitered and determine score based off of users trying to access. Audit users individually   + Execution -   + Support - |
| 3.11.2 | Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified   * + Verify – Search through Symantec logs   + Execution – Alert when risk is found |
| 3.11.3 | Remediate vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified   * + Verify – Verify vulnerabilities are addressed   + Execution – Alert when not fixed in set amount of time |
| **3.12** | **Security Assessment** |
| 3.12.1 | Periodically assess the security controls in the organizational information system to determine if the controls are effective in their application   * + Verify – Risk Management Score and audit your workstations to find unacceptable behavior and insufficient app usage. |
| 3.12.2 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems   * + Verify – Verify said plans of action were executed on the technical side. |
| 3.12.3 | Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls   * + Verify – Ensure Splunk UF is logging both system and app logs. |