SCDIS-210 Information Security Technology Coverage Measurement Standards

for all South Carolina state agencies
version 1.1 draft 3
issued: 10-Jul-2015
effective: 01-Jul-2017

Purpose

These standards establish a simplified and consistent measurement for coverage of each of the security technologies listed below.

Scope

These standards are to be used for all South Carolina state agencies, including institutions, departments, divisions, boards, commissions, and authorities.

Coverage Levels per Technology

The coverage levels (0 to 4) are defined based on reduction of risk, considering factors such as estimated likelihood of compromise and potential impact of compromise. Low level coverage addresses only the largest risks, with Medium and High coverage addressing additional risk of compromise, or facilitating detection or remediation. See Appendix A for the guidelines used to select the specific criteria per technology.

* Within the scope of security controls available through a given technology, coverage levels marked with an asterisk satisfy the same scope of objectives specified in the Inspector General's directive in regard to compliance with the Governor's Executive Orders 2012-10 and 2012-12, which apply to cabinet agencies.

Future application of Coverage Levels

In future, specific information security compliance requirements within the state's Information Security Policy framework will refer to these standard measurements for these technologies.

Monitoring

Assess by the following criteria, as applied to a **given network scope**:

Level 0: Nonexistent/Ineffective

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Detects many forms of attack. But prone to over-alerting (false positive), as there is often insufficient information to determine when attacks fail.

- Collection of network edge firewall logs.
- Intrusion Detection System (IDS) positioned to observe events at all network edge devices, and associate these events with individual hosts (e.g. by private IP address), covering all hosts used for business purposes.
- IDS regularly updated to detect new threats.
- All of the above sources automatically correlated and alerted (such as via SIEM) and watched during business hours.

* Level 2: Medium

Detects additional forms of attack, and some additional indicators of compromise, including some cases of compromised credentials. Significant over-alerting still occurs.

- All criteria for Level 1.
- Collection of network flows for all network edge devices, including at least 1 kilobyte of payload per flow.
- Collection of logs from services providing remote access to non-public network resources (e.g. VPN).
- Collection of logs from central authentication services (e.g. AD, LDAP, RADIUS).
- Collection of logs from all public-facing services (e.g. web, FTP, RDP, SSH).
- Collection of DHCP lease logs for all hosts on networks intended for business purposes.
- Collection of DNS resolution logs for all hosts on networks intended for business purposes.
- All of the above sources automatically correlated and alerted (such as via SIEM) and watched during business hours.
- All log sources are retained for a minimum of 30 days, or longer as required for compliance with applicable statutes, regulations, or contracts.

Level 3: High

Detects additional indicators of compromise. False alerts are reduced.

- All criteria for Level 2.
- Collection of antivirus logs for all hosts used for business purposes.
- Collection of proxy connection logs for any business-use hosts that use a proxy.
- Collection of DHCP lease logs for all hosts on all networks.
- Collection of DNS resolution logs for all hosts on all networks.
- All of the above sources automatically correlated and alerted (such as via SIEM) and watched during business hours. Correlated events are matched against a reputable real-time threat intelligence signature source.

Level 4: Advanced

Additional log sources added tend to cover fewer hosts, but can detect signs of compromise deeper in the network.

Advanced monitoring coverage would include all criteria for Level 3, and correlating with one or more of the following:

- Collection of Host-based Intrusion Detection/Prevention System (HIDS/HIPS) server logs.
- Collection of security logs from sensitive data servers, all servers, or all hosts.
- Network flows including increased payload capture.
- Monitoring traffic at distribution or access layers.
- All sources automatically correlated and alerted (such as via SIEM) and watched 24/7.

Internet Border Protection

Assess by the following criteria, as applied to a **given Internet border scope**:

Level 0: Nonexistent/Ineffective

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Protects hosts within the network that are not well hardened against attack.

- Traditional firewall protection, including connection association ("stateful inspection").
- Default deny for inbound traffic, covering all hosts used for business purposes (permit by exception).

* Level 2: Medium

Provides protection against some forms of disguised attack. Provides protection against many forms of post-compromise data loss, or deeper compromise. Provides some protection against compromise of user devices.

- All criteria for Level 1.
- Default deny for all outbound traffic. Common protocols may be globally allowed, such as HTTP, FTP, SSH, etc.
- Deep packet inspection, including protection from fragmenting attacks and windowing attacks.
- Inline antivirus.

Level 3: High

Provides additional protection against compromise of user devices.

- All criteria for Level 2.
- Reputation filtering for inbound and outbound traffic, blocking known malicious hosts.
- Reputation filter updates rules daily or more often.

Level 4: Advanced

Provides additional protection against compromise of servers and user devices. But management may become more difficult. User liberties are reduced.

Advanced border protection coverage would include all criteria for Level 3, and one or more of the following:

- Blacklisting sites by content category (e.g. social networking, cloud storage, adult, etc.)
- Whitelisting sites by content category (e.g. only government).

Whole-Disk Encryption

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

*** Level 0: Nonexistent/Ineffective**

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Protects against the compromise of sensitive data normally resulting from theft or accidental loss of laptops.

- All laptops used by users who have access to Confidential or Restricted data have whole-disk encryption installed, protecting at least all partitions containing business data.
- All encryption keys are centrally managed.

Level 2: Medium

Protects against the compromise of sensitive data normally resulting from theft of desktops.

- All criteria for Level 1.
- All desktops used by users who have access to Confidential or Restricted data, are protected by whole-disk encryption as per Level 1 controls.

Level 3: High

Protects against the compromise of data of any classification normally resulting from loss or theft of user computers.

- All criteria for Level 2.
- All laptops are protected by whole-disk encryption as per Level 1 controls.
- All desktops are protected by whole-disk encryption as per Level 1 controls.

Level 4: Advanced

Protects against the compromise of data normally resulting from theft or accidental loss of portable storage devices or media.

Advanced whole-disk encryption coverage would include all criteria for Level 3, and one or more of the following:

- All user devices are configured to require encryption for all removable media written.
- All user devices are configured to require encryption for all removable storage devices written.

Multi-Factor Authentication

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

*** Level 0: Nonexistent/Ineffective**

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Provides significant protection against a remote attacker using compromised credentials to bypass the border firewall and gain access to the local network.

- Remote access to private network resources (e.g. VPN) requires at least 2 factors to authenticate.

Level 2: Medium

Provides significant protection against an attacker with external access using compromised credentials of privileged users or sensitive data users.

- All criteria for Level 1.
- Internet-accessible services, including cloud services, require at least 2 factors to authenticate users who have access to Confidential or Restricted data.
- All privileged users (e.g. administrators of systems, DBs, domains, or applications) require at least 2 factors to authenticate.

Level 3: High

Provides significant protection against an attacker with internal access using compromised user credentials to access sensitive data systems.

- All criteria for Level 2.
- All internal-use-only systems require at least 2 factors to authenticate users who have access to Confidential or Restricted data.

Level 4: Advanced

Wider deployment of multi-factor protection likely provides only marginal reduction in risk, while likely requiring additional user support.

Advanced multi-factor authentication coverage would include all criteria for Level 3, and one or more of the following:

- All internal-use-only systems require at least 2 factors to authenticate.
- Only hardware tokens are permitted to be used as 2nd factor.
- 3 or more factors are used to authenticate.

Vulnerability Assessment

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

*** Level 0: Nonexistent/Ineffective**

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Provides remediation of security vulnerabilities in Internet-accessible computers.

- All Internet-accessible services are scanned externally at least as often as monthly for known vulnerabilities.
- A process is in place to address all vulnerabilities appropriately according to risk.
- Vulnerability reports sent to DIS SIEM for central correlation.

Level 2: Medium

Also provides remediation of security vulnerabilities in vital network devices, and in a representative sample of user devices.

- All criteria for Level 1.
- All edge network devices are scanned using credentialed access at least as often as monthly for known vulnerabilities.
- At least 1 endpoint (user and server) from each distinct policy group (e.g. each Windows group policy OU or container, or baseline configuration) is scanned using credentialed access at least as often as monthly for known vulnerabilities.
- A process is in place to address all user endpoint vulnerabilities appropriately according to risk, across all policy group members.

Level 3: High

Also provides remediation of security vulnerabilities in all servers.

- All criteria for Level 2.
- All servers are scanned using credentialed access at least as often as monthly for known vulnerabilities.
- All access layer network devices are scanned using credentialed access at least as often as monthly for known vulnerabilities.

Level 4: Advanced

Wider deployment of vulnerability assessment likely provides only marginal reduction in risk, while likely requiring significant additional license cost and support resources.

Advanced vulnerability assessment coverage would include all criteria for Level 3, and one or more of the following:

- All user endpoints are scanned using credentialed access at least as often as monthly for known vulnerabilities.
- All distribution layer network devices are scanned using credentialed access at least as often as monthly for known vulnerabilities.

Third Party Patch Management (TPPM)

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

Level 0: Nonexistent/Ineffective

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

Provides managed remediation of application security vulnerabilities in high-risk user endpoints.

- All privileged user endpoints have TPPM installed.
- All commonly used applications directly interfacing with Internet services are patched appropriately according to risk.

Level 2: Medium

Also provides remediation of application security vulnerabilities for user endpoints with sensitive data. Expands the scope of patched applications.

- All criteria for Level 1.
- All sensitive data user endpoints have TPPM installed.
- All commonly used applications associated with commonly downloaded file types are patched appropriately according to risk.

*** Level 3: High**

Provides remediation of application security vulnerabilities in all user endpoints, and in all servers.

- All criteria for Level 2.
- All user endpoints have TPPM installed.
- All servers have TPPM installed.

Level 4: Advanced

Wider deployment of TPPM likely provides only marginal reduction in risk, while likely requiring significant additional support resources.

Advanced TPPM coverage would include all criteria for Level 3, and one or more of the following:

- All commonly used applications are patched appropriately according to risk.
- All applications supported by the TPPM product are patched appropriately according to risk.

Privileged User Management (PUM)

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

Level 0: Nonexistent/Ineffective

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

Level 1: Low

For systems containing sensitive data, as well as systems used to operate vital services, reduces risk of sensitive data compromise related to malicious insider system administrators, or compromised system administrator credentials. Also reduces risk of loss of administrative access due to unplanned loss of key personnel.

- Administrative access is managed by PUM for all authentication and policy servers (e.g. domain controls).
- Administrative access is managed by PUM for all shared database servers.
- Administrative access is managed by PUM for all email servers.
- Administrative users have administrative accounts separate from their standard user accounts.
- Administrative processes exercise the principle of Least Privilege.
- PUM is configured to log user actions.

* Level 2: Medium

As Level 1, and may also improve capability to investigate root cause of failures due to administrator error. Plus, basic PUM protection is extended to all servers.

- All criteria for Level 1.
- All servers indicated in Level 1 have administrative user sessions recorded by PUM.
- Administrative access is managed by PUM for all servers.
- Each local administrative user account on each server has a unique password.

Level 3: High

As Level 2, and may also improve capability to investigate root cause of failures due to administrator error, for all servers.

- All criteria for Level 2.
- Administrative access is recorded by PUM for all servers.

Level 4: Advanced

Wider deployment of PUM likely provides only marginal reduction in risk, while likely requiring significant additional support resources. May introduce higher risk of administrator lock-out. Advanced PUM coverage would include all criteria for Level 3, and one or more of the following:

- PUM is configured to prevent users from knowing credentials.
- Key network devices are protected by PUM.
- PUM is used to manage end user access to Restricted data.
- PUM is used for all internal users.
- PUM is used to protect sensitive/privileged applications.

Data Discovery (DD) / Data Loss Prevention (DLP)

Assess by the following criteria, as applied to a given agency, department, division, location, or other business unit scope:

<u>* Level 0: Nonexistent/Ineffective</u>

Provides no effective protection.

- Any level of coverage not qualifying as Level 1 or above.

<u>Level 1: Low</u>

Provides reduction of risk of sensitive data compromise, through reduction of occurrence of sensitive data. Also provides for improved incident response time.

- Sensitive data discovery is periodically performed on all file servers.
- A process is in place to address all findings appropriately according to risk.
- Results (positive/negative only) are reported to DIS for correlation in SIEM.

<u>Level 2: Medium</u>

Increases scope of protection to include more data locations.

- All criteria for Level 1.
- Sensitive data discovery is periodically performed on all user-data servers (e.g. file, web, email, ftp).
- Sensitive data discovery is periodically performed on all user devices used by persons who have access to sensitive data.

<u>Level 3: High</u>

Reduces risk further by performing sensitive data discovery in real time.

- All criteria for Level 2.
- Sensitive data discovery is performed on all user devices.
- Sensitive data discovery is configured to occur in real time.

<u>Level 4: Advanced</u>

A higher level of deployment provides additional reduction in risk, but also introduces a risk of denying legitimate access, and likely additional support costs.

Advanced vulnerability assessment coverage would include all criteria for Level 3, and one or more of the following:

- DLP is configured to prevent use or transmission of data against policy.
- DLP is configured to automatically encrypt sensitive data files when emailed.
- DLP is configured to automatically encrypt sensitive data files when copied to removable media.

Appendix A – Guidance on Coverage Level Criteria

To standardize reporting of security technology deployments at agencies, the following coverage levels are proposed for reporting and metrics. **Vulnerability to external threats** is the primary factor used to select coverage level criteria. These risks are estimated, based on information security incidents investigated by DIS:

Level 0: Nonexistent/Ineffective

Level 0 (zero) indicates the technology is not deployed at an agency (or location), or is deployed but configured in such a way as to be ineffective.

In general, Level 0 coverage is likely to be insufficient for agency compliance requirements.

Level 1: Low

Level 1 coverage indicates the technology is deployed at an agency (or location) in such a way as to achieve a minimal or low level of protection. A low level of coverage is substantially beneath the coverage needed to protect against most external threats.

In general, Level 1 coverage may be adequate for agencies that manage only Public data.

Level 2: Medium

Level 2 coverage indicates the technology is deployed at an agency (or location) in such a way as to achieve a medium level of protection. A medium level of coverage provides significant protection, but falls short of protecting against most external threats.

In general, Level 2 coverage may be adequate for agencies that manage only data classified as Public or Internal (no Confidential or Restricted data).

Level 3: High

Level 3 coverage indicates the technology is deployed at an agency (or location) in such a way as to achieve a high level of protection. A high level of coverage provides protection against most external threats.

In general, Level 3 coverage may be adequate for agencies that manage some types of Confidential or Restricted data.

Level 4: Advanced

Level 4 coverage indicates the technology is deployed at an agency (or location) in such a way as to achieve protection above and beyond Level 3. An advanced level of coverage provides above and beyond what is needed for most external threats.

Level 4 coverage may be required for some technologies for agencies that manage data with stringent compliance requirements (e.g. PCI DSS, IRS Pub 1075, MARS-E). Consult those specific standards to determine whether coverage extending into Level 4 is required for a given scope of your agency's systems or users.