State of California

Office of Information Security

Vulnerability Management Standard

SIMM 5345-A

April 2021

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**January 2021**	**Office of Information Security**	**New Standard in support of SAM Section 5345, Vulnerability And Threat Management**
Minor Update	**April 2021**	**Office of Information Security**	**Corrected name and reference to Security Event Notification and Response Protocols (SIMM 5335-A).**

TABLE OF CONTENTS

I. INTRODUCTION

The term "vulnerability" is framed within the concept of "susceptible to attack" or "assailable" (Gartner, 2018). State entities shall continuously identify, investigate reports of, and remediate vulnerabilities affecting their IT assets before they can be exploited. Vulnerability management are the processes by which the continuous identification, tracking, reporting, and remediation of vulnerabilities that exist within those IT assets are conducted. IT assets are physical and virtual, hardware and software, processing, networking, and storage in nature, and may exist either within a state entity's direct control or outside (e.g. cloud).

II. MINIMUM VULNERABILITY MANAGEMENT REQUIREMENTS

At a minimum the vulnerability management technologies and processes used by state entities must include the following protection, detection, investigative support, containment, and remediation capabilities.

A. Protection Capabilities

To protect assets that are under the control of a State entity, the vulnerability management technologies and processes used by a state entity shall (at a minimum):

- Be able to assign assets to groups.
- Be able to assign assets to multiple groups.
- Be able to generate reports based on asset groups.
- Be able to assign asset grouping automatically based on OS/application in addition to manual assignment.
- Support access controls to limit users' visibility and change privileges to specific groups of assets.

B. Detection Capabilities

The vulnerability management and scanning technologies and processes used by state entities shall (at a minimum):

- Be able to scan assets from inside the enterprise perimeter firewall.
- Be able to scan internet-facing assets from the internet.
- Indicate which vulnerabilities of an asset are exploitable from both outside and inside the network and which are only exploitable from the inside.
- Support credentialed and non-credentialed scanning.
- Support credentialed scanning for Windows, Linux, AIX, Solaris, and commonly used network devices.
- Support middleware vulnerability detection for products like Microsoft SQL, Oracle, WebSphere, Apache web services, IIS…
- Be able to perform Dynamic Application Security Testing (DAST) and scan web-based applications for Open Web Application Security Project (OWASP) Top Ten.
- Be able to scan web-based interfaces and Application Programming Interfaces (API), to include HTTP, WebSockets, JSON, XML, REST, SOAP.
- Be able to exchange vulnerability data with department Security Information and Event

Management system(s) using automated processes.

C. Investigative Support Capabilities

The investigate functions of the vulnerability management and scanning technologies and processes must include a historical timeline of all detections and apparent remediation of specific vulnerabilities and shall (at a minimum):

- Be able to search for specific vulnerabilities and retrieve a list of assets with those vulnerabilities.
- Be able to search for specific assets by hostname or IP and receive a list of all vulnerabilities on that asset.
- Be able to generate a report showing all vulnerabilities and assets within a specific user-defined or automated group.
- Be able to generate a report of the most critical external vulnerabilities, including the related assets that are vulnerable.
- Be able to limit reports to external vulnerabilities only, internal vulnerabilities only, or combined vulnerabilities
- Have clearly defined risk values for assets and vulnerabilities and be able to use those for reporting.
- Be able to generate a report of most critical vulnerabilities across the system or by user-defined or automated group.
- Be able to generate a report of most critical assets across the system or by user-defined or automated group.
- Be able to generate aging reports of open vulnerabilities.
- Be able to provide continuous real time results and reporting of existing and closed vulnerabilities.
- Be able to generate a risk state of the various asset groups as well as the entire enterprise.
- Be able to respond to vulnerability reports from the California Department of Technology, Office of Information Security, Security Operations Center and other external parties in accordance with the Security Event Notification and Response Protocols, SIMM 5335-A.

D. Containment Capabilities

There are no containment capabilities that are at a minimum required by the vulnerability management and scanning technologies and processes.

E. Remediation Capabilities

The remediation functions of the vulnerability management and scanning technologies and processes must (at a minimum):

- Maintain a registry of all detected and un-remediated vulnerabilities.
- Provide both automated and manual methods to show that vulnerabilities have been remediated.
- Allow for different groups to manage the vulnerabilities based on assigned groups.
- Integrate with bug tracking and configuration management platforms.
- Record how remediation of a vulnerability was affected.

F. QUESTIONS

Questions regarding this standard may be sent to:
California Department of Technology
Office of Information Security
Security@state.ca.gov