noblis

For the best of reasons

WHITE PAPER

Noblis ScanCenter - A Premier Continuous Monitoring Platform

noblis

WHITE PAPER

Table of Contents

Technical Points of Contact

Dale Roach
FedRAMP Program Manager
Dale.roach@noblis.org

Andrew Lins
FedRAMP Program Manager
Andrew.lins@noblis.org

Sam Aydlette
Continuous Monitoring Lead
samuel.aydlette@noblis.org

WHITE PAPER

Executive Summary

Maintaining the security of Federal computing environments, whether on government networks or in the cloud, is an increasingly high stakes challenge. Mandatory cybersecurity compliance standards and frameworks, such as those defined by the Federal Information Security Management Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP), include Continuous Monitoring (ConMon) as a key activity. To implement a successful ConMon program, agencies must typically define and implement an agency-specific process that satisfies the FISMA requirements in their unique environment, and then must capture, decipher, analyze, and store a myriad of ConMon data, often with limited automation. As a result, many agencies struggle to manage their ConMon efforts.

ScanCenter Continuous Monitoring as a Service (CMaaS) can improve the Continuous Monitoring process for federal agencies while maintaining alignment with cybersecurity compliance standards.

The Noblis ScanCenter is a dynamic, robust network intelligence platform for Continuous Monitoring. It significantly eases the burden faced by agencies in maintaining alignment with federal cybersecurity compliance standards. Its proven automation approach offers a fast, accurate view into the vulnerability and security posture of complex networked information systems, freeing cybersecurity professionals from mundane manual tasks and allowing them to focus on high-value threat assessment activities. ScanCenter can be implemented as a stand-alone solution or as Continuous Monitoring as a Service (CMaaS) and can be used by any agency that follows a Risk Management Framework such as FedRAMP to improve its Continuous Monitoring process.

ScanCenter is a proven, powerful, secure tool that allows agencies to meet the most stringent ConMon cybersecurity compliance requirements. It gives agencies the ability to optimize, automate, and streamline their ConMon efforts, minimizing risk of human error and reducing the level of effort and cost needed to implement a successful ConMon program. Its automated dashboards and reports increase network-wide visibility and facilitate effective threat detection. Because it accepts data feeds “as is” from 22 industry standard vulnerability scanning tools and leverages existing PIV and CAC cards for user authentication, it is easily integrated into existing operations. ScanCenter also simplifies and speeds achievement of FedRAMP Authorization and scales easily, without corresponding increases in staffing and cost. ScanCenter is a premier solution for low risk, high value automation of agency ConMon activities.

Introduction

Risk management programs that follow NIST 800-37 Rev 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, such as FedRAMP, require information systems to provide continuous monitoring data for agency review on a monthly or more frequent basis. This includes vulnerability scan data, current system inventory and a Plan of Action and Milestones (POA&M). Agency experts must pull down the ConMon data, and perform their own analysis, including:

WHITE PAPER

- Comparing vulnerability scan data against FedRAMP, FISMA, or agency-specific requirements
- Monitoring system architecture with the inventory
- Tracking closure progress of outstanding open vulnerabilities in the POA&M

This analysis is typically performed manually. Manual data processing is slow and costly, with a higher chance of human error. With multiple systems and environments, agencies cannot easily correlate ConMon data between reporting periods, or across different authorization boundaries to gain deeper insights into the data. Additionally, manual processing requires a greater level of effort as use of Cloud Service Providers (CSP) scales and becomes more complex. ScanCenter and ScanCenter Continuous Monitoring as a Service (CMaaS) were created to address these issues, and to provide a powerful, secure, automated tool that helps departments and agencies to simplify and speed their Continuous Monitoring analyses.

Automation decreases processing time and increases the overall amount of ConMon data that can be managed with the same personnel, reducing the cost and level of effort required to manage the same amount of data. ScanCenter automates the handling of structured data, minimizing the risk of human error. ScanCenter accomplishes this by using software “agents” to ingest and process monthly ConMon data from the vulnerability scanning tools associated with all information systems in all environments (site, data center, and cloud). ScanCenter agents identify and process the structured ConMon data, ensuring that manual handling of that data is limited. Use of agents that can be refreshed to process new data formats and collect data from new vulnerability scanning tools allows ScanCenter to grow to accommodate various types of structured data, ensuring that as an organization’s data requirements change, ScanCenter can accommodate those changes.

ScanCanter facilitates FedRAMP authorizations. When used within the FedRAMP context, ScanCenter ensures continuous data monitoring, recording, measuring, and tracking against FedRAMP requirements. Because ScanCenter leverages commonly used data formats, it easily ingests monthly ConMon deliverables, such as scan data from industry standard vulnerability scanning tools (e.g., Nessus, Retina, Qualys, etc.). Different types of alerts can be set to further track compliance, and to notify relevant stakeholders, resulting in increased situational awareness. Additionally, ScanCenter can correlate ConMon data from different reporting periods, and across different authorization boundaries, with the results displayed on a single security dashboard. This allows for a complete, organization-wide picture of an agency’s, or other organizations’, security posture, enabling early detection of and rapid reaction to trends and major events.

ScanCenter is the only product that supports 22 vulnerability scans out of the box. Additionally, there is no product that fully meets FedRAMP’s requirements for metric thresholds and reporting, nor is there another vendor with our unique FedRAMP positioning that enables multi-agency collaboration.

High Level Architecture

ScanCenter can be deployed as either a private, cloud-based solution, or as a stand-alone, client-based application, in order to support an organization’s unique deployment requirements. The technical details discussed below pertain to deployment options.

WHITE PAPER

ScanCenter ingests scan data obtained both from Authorization and ConMon processes, as well as from authorized users. All connections made to ScanCenter are secured via Transport Layer Security (TLS) version 1.2 or higher. Authentication security is bolstered by two-factor authentication, including PIV and CAC authentication, for which ScanCenter provides full support as specified by Homeland Security Presidential Directive 12 (HSPD-12).

As ScanCenter ingests and processes scan data, authorized users are notified of any resulting configuration, compliance or vulnerability alerts.

As ScanCenter ingests and processes scan data, authorized users are notified of any resulting configuration, compliance or vulnerability alerts. These authorized users can then access ScanCenter to view scan results and associated alerts, in order to determine the best course of action.

ScanCenter also supports role-based access control (RBAC). With RBAC, permissions to perform certain operations, such as uploading scan data, are assigned to specific roles. Roles are defined as either privileged or unprivileged. Privileged users can perform actions associated with a role, such as viewing data, uploading data within specific information system boundaries, and creating new deviation requests. Similarly, administrators can perform privileged user actions, as well as approve new users, set user privileges, and create and assign groups and boundaries. Unprivileged users, on the other hand, cannot perform these actions.

ScanCenter's reporting capability also provides summary views of an agency's portfolio of Cloud Service Offerings (CSOs), including detailed views of vulnerabilities, remediation activities, compliance issues, and trends analyses. Report generation capabilities and agency collaboration capabilities ensure that deviation requests, significant changes, and other risk management activities are effectively shared across all leveraging agencies for a given CSO.

ScanCenter Key Features

ScanCenter users have access to key features that provide stakeholders with insights into their security posture, helping them to make informed decisions. These include ScanCenter Vulnerability Management Dashboards, Consolidated Continuous Monitoring Reports, Performance Management Statuses, and Validated POA&Ms and Inventories. The ScanCenter workflow is illustrated in Figure 1.

WHITE PAPER

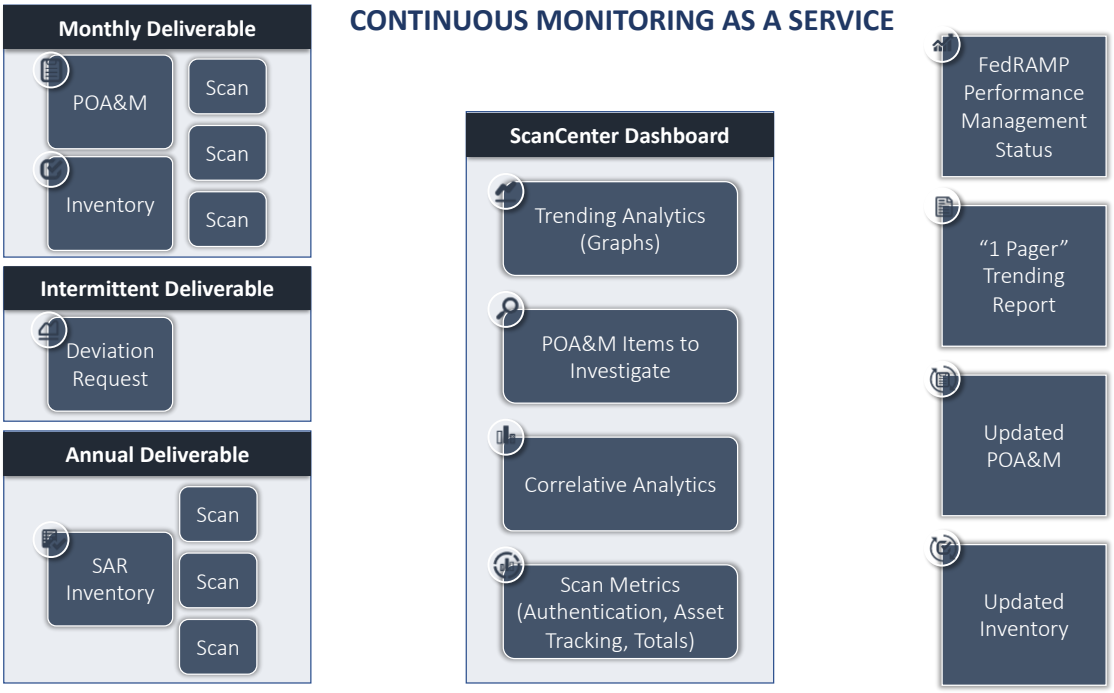

Figure 1: ScanCenter Workflow

ScanCenter Vulnerability Management Dashboards

The ScanCenter Live Dashboard is a management-friendly, live dashboard that enables system administrators, Information System Security Officers (ISSOs), Information Systems Security Managers (ISSMs), developers, and other key stakeholders to view the most critical information in their computing environments.

- **Environment Six Month Vulnerability Trends** – Tracks and measures changes in vulnerabilities
- **Top 10 Vulnerability Types (by Frequency)** – Identifies the most common problems across the computing environment
- **Top 10 Vulnerabilities (by Severity)** – Uses vulnerability risk and asset value/criticality to help determine which problems would have the greatest overall impact on the security posture of the computing environment
- **Top 10 Assets (by Severity)** – Identifies which assets have the most serious vulnerabilities
- **New Hosts (last 15 days)** – Identifies any undocumented/unauthorized hosts on the network
- **Trending Authentication Tracking** – Tracks percentage of authentication success rates during scan
- **Scan Correlation with Compliance Documentation –** Correlates scan vulnerabilities with associated POA&Ms and Inventory documentation, along with pending and active Deviation Requests

WHITE PAPER

Consolidated Continuous Monitoring Report

The ScanCenter Portfolio and Single System Dashboards are illustrated in Figures 2 and 3, respectively. The ScanCenter Portfolio Dashboard provides a “Chief Information Officer (CIO) View” of an organization’s risk posture by displaying metrics across the entire portfolio of systems that an organization leverages. Additionally, this dashboard provides in-depth reporting of high-risk vulnerabilities, insecure assets, and more, across the entire portfolio. The Single System Dashboard view displays meaningful analytics that capture metrics across each IT system. Examples of these metrics include performance management status, compliance with emerging security directives, the number of vulnerabilities (ranked by severity) that exceed a defined baseline, and the number of vulnerabilities that remain un-remediated or un-mitigated within a required timeframe.

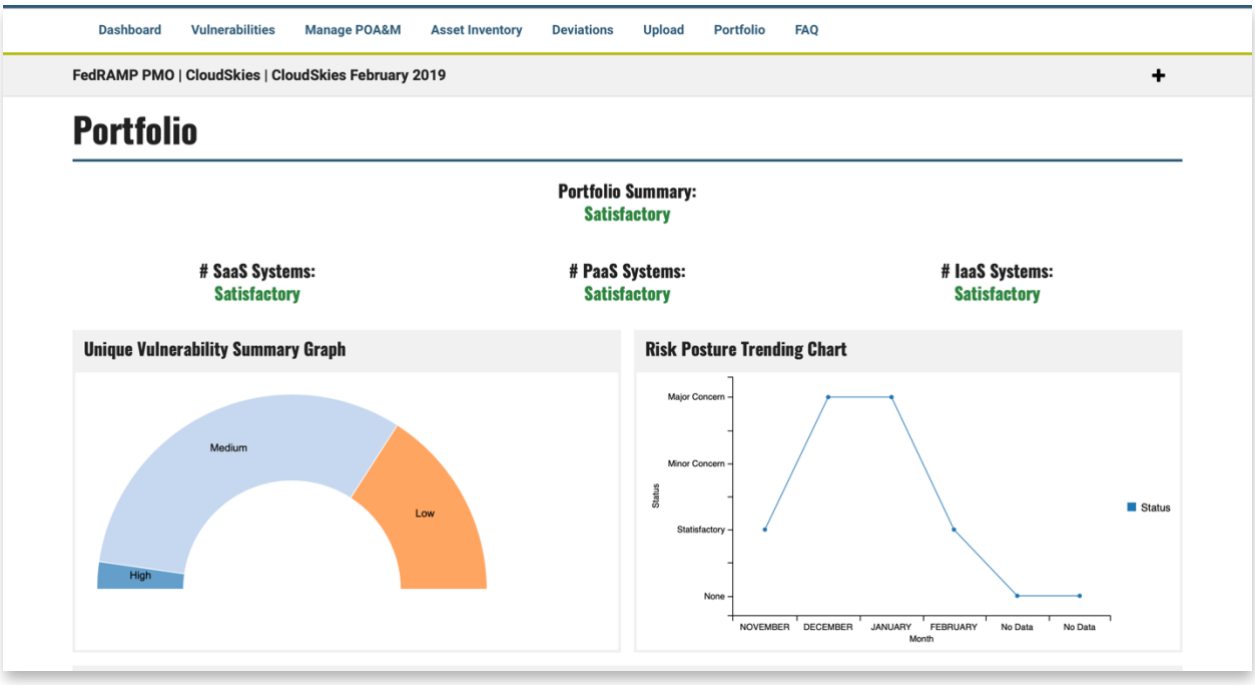

Figure 2: Portfolio Dashboard

WHITE PAPER

Figure 3: Single System Dashboard

Performance Management Status

ScanCenter automatically tracks security program metrics in near real-time, promoting a high degree of accountability and transparency for compliance achievement. Customizable, automated reports can be tailored to capture information considered most relevant to analyst or decision-maker needs and can be scheduled for delivery to key staff on a daily, weekly, quarterly, or other basis. Broad reporting highlights changes to the network, while demonstrating security program effectiveness. Monthly management statistic summaries enable more informed decision-making. Automated reporting supports platform and infrastructure scalability without proportionate staff and cost increases for ConMon activities.

Maintain Compliance with Emerging Security Directives

ScanCenter facilitates compliance with emerging and developing security directives. It:

- Enforces security workflow
- Assists compliance activities (FISMA, NIST SP 800-53, FedRAMP, etc.) by exporting required data into automated, usable tools, such as Microsoft Excel
- Fully supports PIV/CAC authentication per HSPD-12
- Can deliver alert messages to defined recipients in an encrypted and digitally-signed format
- Reduces staff burden while preparing agencies for emerging, automated reporting compliance standards

WHITE PAPER

Cloud Based Software Optimizes Availability and Security

ScanCenter provides a web-facing login portal that is accessible from anywhere. It offers secure, multi-factor authentication, and a tiered user schema that enables privileged or normal access to data.

Validated Inventory and POA&M Tracking

ScanCenter maintains a record of the approved security inventory baseline (Figure 4). After a vulnerability scan completes, algorithms compare scan results against the last approved security inventory baseline. This is known as a Positive Security Model. Any deviation from the approved baseline configuration is treated as a configuration vulnerability. Owners of non-compliant assets are notified of the discrepancy via the use of the ScanCenter Inventory Tab.

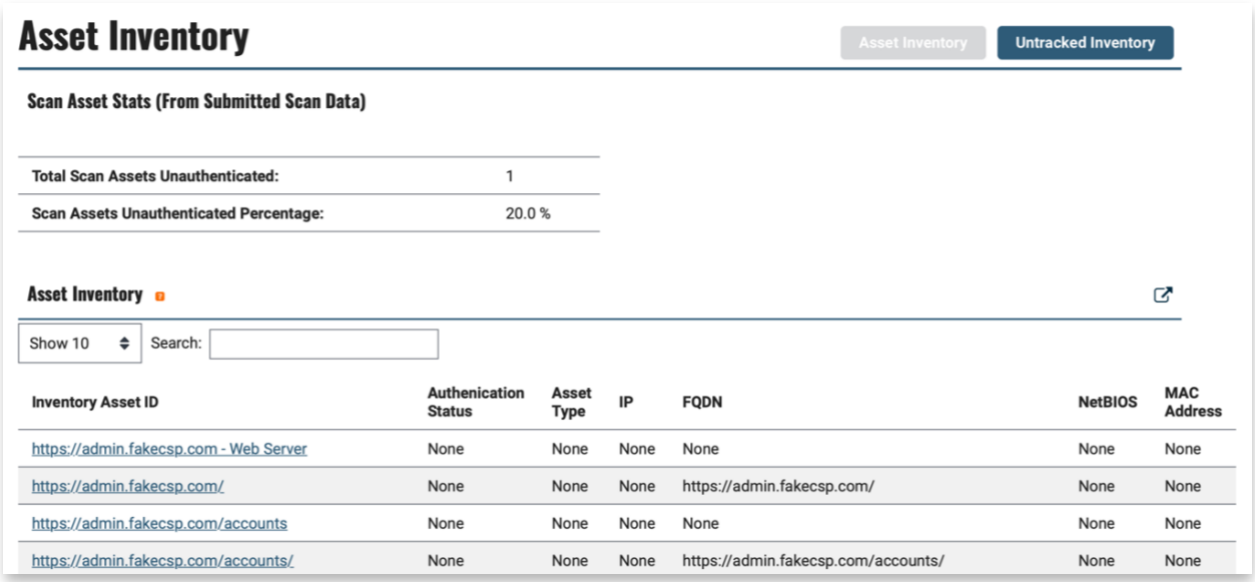

Figure 4: Asset Inventory

ScanCenter also facilitates convenient tracking of progress against the Plan of Action and Milestones, as shown in Figure 5. By correlating scan vulnerabilities with associated POA&Ms and Inventory documentation, along with pending and active Deviation Requests, ScanCenter enables managers to quickly and easily spot problems requiring attention.

WHITE PAPER

POA&M V-1

POA&M Item Details

Item Identifier	V-1
Weakness Name	Apache httpd remote denial of service
Weakness Description	This weakness is an Apache issue, it is something that is documented in the NVD database
Controls	RA-5
Original Source Detector - Identifier	Acunetix
Original Detection Date	2017-01-15
Asset Identifier	**Port** 80 **Protocol** HTTP **UID** 43125678 **FQDN** https://admin.fakecsp.com/

Scheduled Completion Date	2017-07-15
Scheduled Completion Date Change	2017-08-23
Milestones	The system administrator attempted to patch on 2017-07-01. Patch caused unanticipated problems so rollback occured. Investigating solution.
Status	open
Status Date	2017-07-15
Vendor Dependency	False
Last Vendor Check-in Date	2017-07-15
Original Risk Rating	medium

Figure 5: POA&M Details

Summary of ScanCenter Benefits

ScanCenter is a robust solution for government ConMon implementations, with more than a decade of proven performance monitoring the security of government computing and web environments. Its benefits include:

Time and Cost Savings

ScanCenter saves its users both time and money, allowing the same number of staff to manage more systems and data:

- Streamlines data comparison analysis across various FedRAMP authorization documents to ensure consistency
- Reduces time from development to a FedRAMP Authorization for agencies, CSPs, and Third-Party Assessment Organizations (3PAOs)
- Simplifies and speeds the process for managing thousands of information systems
- Automated reporting allows platform and infrastructure scalability without proportionate staff and cost increases
- Reduces cost by leveraging PIV and CAC card authentication

Integration with Popular Tools & Technology

ScanCenter leverages existing investments in vulnerability scanning tools:

WHITE PAPER

- Automatically ingests and processes data from 22 industry standard vulnerability scanning tools, the only product on the market with this capability. Additionally, ScanCenter software agents can be easily updated to consume data from updated and new scanning tools, keeping the platform evergreen.

Standardized Data Management

ScanCenter works with standardized and fixed data sets, allowing automation to be used to improve the user experience. Automation capabilities include:

- Dashboard views of high priority vulnerabilities that need attention or investigation
- Display of trend analyses of historical data gathered through continuous monitoring
- Management of continuous monitoring assessment and authorization documents, including POA&M and Security Assessment Report (SAR) artifacts
- Exportable table and graph data in common file formats, such as CSV.

Deployment Flexibility

ScanCenter can be deployed as a stand-alone solution or as a cloud-based software solution ScanCenter CMaaS. Both optimize availability and security using:

- A web-facing login portal that is accessible everywhere
- Multi-factor authentication
- A fixed user schema that enables privileged or normal access to data

These benfits make ScanCenter a unique and powerful platform for facilitating and increasing the value of the continuous monitoring activities required by government standards and frameworks. It can be easily integrated into exisiting operations environments and reporting structures, and updated quickly to take advantage of evolving tools and data streams. It improves decision support and saves scarce resources, with less risk, greater speed, and better confidence in results. ScanCenter is a premier continuous mnonitoring solution for government users.

Doing What's Right and What Works for Our Clients

Noblis fosters a culture of collaboration. Through our Centers of Excellence (COEs), we are connecting our staff so that they may better serve our clients. The COEs reach across domain areas and our three companies to ensure the right capabilities, people, tools, and expertise are applied to our work. This enables us to offer every client the best solutions to fit their needs and challenges.

About Noblis

Noblis is a nonprofit science, technology, and strategy organization that brings the best of scientific thought, management, and engineering expertise with a reputation for independence and objectivity. We work with a wide range of government and industry clients in the areas of national security, intelligence, transportation, healthcare, environmental sustainability, and enterprise engineering. Together with our wholly owned subsidiary, Noblis ESI, we solve difficult problems of national significance and support our clients' most critical missions.

Working with Us

Government agencies can access Noblis through a variety of contracting mechanisms. We have several IDIQ contracts in place and available to civilian and DoD agencies. We are also a GSA Schedule holder. For a full list of vehicles, visit noblis.org.

703.610.2000 answers@noblis.org