NIST SPECIAL PUBLICATION 1800-5

IT Asset Management

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Michael Stone
Chinedum Irrechukwu
Harry Perper
Devin Wynne
Leah Kauffman, Editor-in-Chief

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-5

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-5

IT Asset Management

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Michael Stone
National Cybersecurity Center of Excellence
Information Technology Laboratory

Chinedum Irrechukwu
Harry Perper
Devin Wynne
The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

September 2018

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-5A

IT Asset Management

Volume A:
Executive Summary

Michael Stone
Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

Chinedum Irrechukwu
Harry Perper
Devin Wynne
The MITRE Corporation
McLean, VA

September 2018

This publication is available free of charge from: http://doi.org/10.6028/NIST.SP.1800-5

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Executive Summary

- The National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example solution that financial services companies can use for a more secure and efficient way of monitoring and managing their many information technology (IT) hardware and software assets.
- The security characteristics in our IT asset management platform are derived from the best practices of standards organizations, including the Payment Card Industry Data Security Standard (PCI DSS).
- The NCCoE's approach uses open source and commercially available products that can be included alongside current products in your existing infrastructure. It provides a centralized, comprehensive view of networked hardware and software across an enterprise, reducing vulnerabilities and response time to security alerts, and increasing resilience.
- The example solution is packaged as a "How To" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. The guide helps organizations gain efficiencies in asset management, while saving them research and proof of concept costs.

CHALLENGE

Large financial services organizations employ tens or hundreds of thousands of individuals. At this scale, the technology base required to ensure smooth business operations (including computers, mobile devices, operating systems, applications, data, and network resources) is massive. To effectively manage, use, and secure each of those assets, you need to know their locations and functions. While physical assets can be labeled with bar codes and tracked in a database, this approach does not answer questions such as "What operating systems are our laptops running?" and "Which devices are vulnerable to the latest threat?"

Computer security professionals in the financial services sector told us they are challenged by the vast diversity of hardware and software they attempt to track, and by a lack of centralized control: A large financial services organization can include subsidiaries, branches, third-party partners, contractors, as well as temporary workers and guests. This complexity makes it difficult to assess vulnerabilities or to respond quickly to threats, and to accurately assess risk in the first place (by pinpointing the most business essential assets).

SOLUTION

The NIST Cybersecurity IT Asset Management Practice Guide is a proof-of-concept solution demonstrating commercially available technologies that can be implemented to track the location and configuration of networked devices and software across an enterprise. Our example solution spans traditional physical asset tracking, IT asset information, physical security, and vulnerability and compliance information. Users can now query one system and gain insight into their entire IT asset portfolio.

This guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations, including the PCI DSS
- provides:
  - a detailed example solution with capabilities that address security controls
  - instructions for implementers and security engineers, including examples of all the necessary components for installation, configuration, and integration
- is modular and uses products that are readily available and interoperable with your existing IT infrastructure and investments

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Our example solution has the following benefits:

- enables faster responses to security alerts by revealing the location, configuration, and owner of a device
- increases cybersecurity resilience: you can focus attention on the most valuable assets
- provides detailed system information to auditors
- determines how many software licenses are actually used in relation to how many have been paid for
- reduces help desk response times: staff will know what is installed and the latest pertinent errors and alerts
- reduces the attack surface of each device by ensuring that software is correctly patched

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/financial-services-sector/it-asset-management. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To learn more by arranging a demonstration of this example implementation, contact the NCCoE at financial_nccoe@nist.gov.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.