Continuous Diagnostics and Mitigation Learning Program

Benefits of Automating Security Control Assessments

Learning Community Event

January 21, 2016

Homeland Security

Federal Network Resilience

Table of Contents

I. Introduction

The automation of security control assessments is critical in today's fast paced security environment, where cyber threats are continually evolving to become more sophisticated and common. Departments and agencies (D/As) must know what they can automate to improve their cyber defenses and how to do it.

During this meeting, three experts (see Appendix C) answered questions about the benefits of automation, what D/As should do to prepare for automation, relevant material in the National Institute of Standards and Technology Internal Report (NISTIR) 8011 draft publication volumes, and next steps for automation. The panelists were:

- **Kelley Dempsey**, National Institute of Standards and Technology (NIST)
- **Paul Eavy**, Department of Homeland Security (DHS) Federal Network Resilience (FNR)
- **Greg Witte**, G2, Inc.

While there are many ways to automate the assessment of security controls, the Continuous Diagnostics and Mitigation (CDM) approach provides an acceptable method for automated security control assessments that is also consistent with NIST guidance.

II. Meeting Summary

A. Benefits of Automation

Automated assessments allow stakeholders to pull near real-time data about their current security posture. These assessments can help D/As quickly identify flaws, determine each defect's risk level, and better prioritize actions.

Automating security control assessments can potentially provide more complete and timely detection of defects or discrepancies between an organization's actual state—how its devices are configured at a specific point in time—and desired state—a specification for how an organization wants its devices to be configured, which will be compared to the actual state. Other benefits of automated assessments include:

- Finding and correcting vulnerabilities before attackers can exploit them.
- Automating manual checks.
- Reducing costs by reducing direct manual labor.
- Optimizing staff time.
- Reducing human error.
- Providing near real-time information to effectively identify risk factors that relate to specific threats.
- Exposing inadequacy of implementation of security controls
- Providing a consistent and standardized way for D/As to analyze their cybersecurity posture.
- Supporting security visualization.
- Improving the timeliness of information D/As share across agencies to adjust their networks and could help prevent attacks.

B. Preparing for Automation

D/As need to make sure they have the organizational structure in place to support the implementation of automated security controls assessment systems and CDM. This includes defining their actual and desired state, identifying assets, ensuring staff understand their roles and responsibilities, looking at timeliness of policy processes and how policy changes affect desired states, and providing training. D/As should also ensure they have established processes in place to support the application of the Risk Management Framework (RMF) to their Federal information system.

C. National Institute of Standards and Technology Internal Report 8011

NIST recently released the initial public draft of the NISTIR 8011, *Automation Support for Security Control Assessments,* Volumes 1 and 2. These documents represent a joint effort between NIST and DHS to provide an operational approach for automating security control assessments.

The first volume, *Overview*, introduces concepts to support automated assessments, while the second volume, *Hardware Asset Management*, focuses on how organizations can identify their assets. The panelists highlighted how these documents will be useful for D/As transitioning to automated assessments. The document:

- Provides the methodology and system elements associated with conducting automated assessments.
- Describes defect checks, actual states, and examples of how to group controls.
- Provides a mapping of security capabilities defined in the NISTIR to 800-53 r4 controls.
- Facilitates use of Open Checklist Interactive Language for security controls or capabilities that need to be checked manually.

Similar to how Volume 2 addresses on hardware asset management (HWAM), subsequent NISTIR volumes will be organized by CDM security capability. For example, Volume 3 will address the software asset management (SWAM) security capability.

D. Future Capabilities

The Federal government is developing United States Government Configuration Baselines (USGCB) for many platforms which can be leveraged to provide standardized secure configuration. Data exchange models such as the Security Content Automation Protocol (SCAP) (including Common Vulnerabilities and Exposures (CVE)) will help provide consistency in automated assessments while still giving organizations the flexibility to determine what and how to assess.

NIST is also collaborating with the United States Computer Emergency Readiness Team (US-CERT) to integrate information from indicators such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). This will allow users to feed their knowledge of system security flaws into scanners that consume Security Content Automation Protocol (SCAP) content, and will build community threat awareness across D/As. D/As are encouraged to engage with the CDM community to share and receive lessons learned and best practices.

E. Additional Resources

These resources will help D/As implement automated security control assessments:

- **CDM Bits and Bytes Email Newsletter.** Provides weekly CDM tips, information for upcoming CDM events, and updates on new CDM resources. Register here: https://www.us-cert.gov/cdm/home.
- **Federal Risk Scoring Sub-Working Group.** Develops risk scoring for CDM, and is looking for input from cybersecurity professionals. Contact cdm.fnr@hq.dhs.gov for more information.
- **National Cybersecurity Workforce Framework.** Provides educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize, think, and talk about cybersecurity work, including what is required of the cybersecurity workforce: https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework.
- **NIST Computer Security Resource Center.** Provides information on NIST publications: http://csrc.nist.gov/. Click here to view the initial public draft of NISTIR 8011: http://csrc.nist.gov/publications/PubsDrafts.html.
- **US-CERT Portal.** Helps government users share threat information: https://portal.us-cert.gov/.
- **US-CERT Website.** Provides additional CDM information, including CDM resources, event information, and meeting summaries: https://www.us-cert.gov/.

Submit any questions, ideas for future meetings, or comments to cdm.fnr@hq.dhs.gov.

III. Appendices

A. Meeting Agenda

TIME	ACTIVITY
12:30-1:00	**Registration**
1:00-1:15	**Introduction** • Welcome – ***Susan Hansche,*** *DHS Federal Network Resilience* • Meeting Purpose and Structure – ***Patrick White,*** *Nexight Group LLC*
1:15-1:20	**Panel Expert Introduction** ***Kelley Dempsey,*** *NIST* ***Paul Eavy,*** *DHS Federal Network Resilience* ***Greg Witte,*** *G2, Inc.*
1:20-2:20	**Panel Discussion –** Panel experts answer questions that will help the audience implement an automated assessment capability.
2:20-2:40	**Audience Q&A –** Panel experts answer questions from the audience, both in-person at the event and from the Webinar.
2:40-3:00	**Next Steps/Wrap-up –** Overview of resources for more information and future discussion topics. ***Patrick White,*** *Nexight Group LLC*

B. Panelist Biographies

Kelley Dempsey, NIST

Kelley Dempsey began her career in information technology (IT) in 1986 as an electronics technician repairing computer hardware before moving on to system administration, network management, and information security. In 2001, Kelley joined the NIST operational Information Security team, managing the NIST information system certification and accreditation program, and then joined the NIST Computer Security Division FISMA team in October 2008. Kelley has co-authored NIST SP 800-128, *Security-Focused Configuration Management*; NIST SP 800-137, *Information Security Continuous Monitoring*; NISTIR 8011, *Automating Ongoing Assessments*; and NISTIR 8023, *Risk Management for Replication Devices*. She is a major contributor to NIST SPs 800-30 Rev 1, 800-37 Rev 1, 800-53 Rev 3/Rev 4, 800-53A Rev 1/Rev 4, 800-39, 800-160, and 800-171. Kelley earned a B.S. in Management of Technical Operations, graduating *cum laude* in December 2003, and an M.S. in Information Security and Assurance in December 2014. Kelley also earned a certified information systems security professionals (CISSP) certification in June 2004, a certified authorization professional (CAP) certification in January 2013, and a Certified Ethical Hacker certification in November 2013.

Paul Eavy, DHS FNR

Paul Eavy is an IT Specialist with DHS. He is a co-author of NISTIR 8011, *Automation Support for Security Control Assessments, Volumes 1 and 2*. He began his professional career as a researcher on automobile accident prevention, doing some of the early research on predictors of automobile accidents and the effects of seatbelt legislation in Michigan. He moved to Washington, D.C., where he developed application systems, designed data models, and then managed software applications and database management systems worldwide for the U.S. Agency for International Development (USAID). In his current position, he explores ways that assessment data for security controls can be generated, prioritized, and made available for reporting and analysis to evaluate cybersecurity risk. He holds master's degrees in Public Policy Studies and Business Administration, both from the University of Michigan.

Greg Witte, G2, Inc.

Greg Witte is a Senior Security Engineer for G2, Inc., a security innovation firm in Maryland. Witte supports Federal and commercial clients, primarily the NIST IT Lab. He has been managing IT for over 30 years, including 20 in the information security arena. As part of his NIST support role, he has helped to focus on security automation (including SCAP), and he was one of several primary authors of the NIST Cybersecurity Framework (CSF). Additionally, Greg was the lead author for *Security Automation Essentials*, McGraw-Hill's textbook regarding the use of SCAP.