PROJECT DESCRIPTION

CONTINUOUS MONITORING FOR IT INFRASTRUCTURE

Techniques for auditing user activity and detecting irregular activity events within small and medium-size businesses

Karen Waltermire
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Kelley Burgin
Chinedum Irrechukwu
Harry Perper
Susan Prince
Devin Wynne
The MITRE Corporation

DRAFT

June 2019

smb_nccoe@nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit http://www.nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant across small- and medium-size businesses. NCCoE cybersecurity experts will address this challenge through collaboration with members of the small and medium-size business community and vendors of cybersecurity solutions. The resulting reference architecture will detail an approach that can be used by small and medium businesses.

ABSTRACT

Many organizations monitor business information technology (IT) infrastructure by manual inspection or computer-aided audits, which can result in after-the-fact detection of malicious-user access events.

This project explores continuous monitoring capabilities that can effectively, efficiently, and automatically detect when a malicious actor, be it an authorized user or an external actor, attempts to perform an action in an organization's IT infrastructure that could result in financial, reputational, and operational impacts to the organization by collecting appropriate log data from the IT infrastructure. Furthermore, the continuous monitoring capabilities can also be used to automate analysis and reporting of the log data to alert the proper personnel in the organization with actionable information and guidance so they may take measures toward resolving the detected issue.

This project will result in a freely available NIST Cybersecurity Practice Guide, which includes a reference architecture, a fully implemented example solution, and a detailed guide of practical steps needed to implement the solution.

KEYWORDS

Access management; compliance; continuous monitoring; medium business; small business; unauthorized access; user access control.

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

Comments on this publication may be submitted to smb_nccoe@nist.gov.

Public comment period: June 17, 2019 – July 26, 2019

TABLE OF CONTENTS

1 Executive Summary

Purpose

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) is interested in supporting small- and medium-size businesses by providing cybersecurity guidance to improve their continuous monitoring programs. This project will enhance an adopting organization's ability to detect out-of-policy access activity as well as reduce the resources required for compliance reporting, such as certification and recertification. The resulting publication can assist in evaluation or assessment, design, acquisition, and integration of a continuous monitoring effort at an adopting organization. Specifically, the NCCoE is requesting feedback on this project idea.

This project is the first in a series of continuous monitoring projects that cover a range of subjects, including networks, assets, and privileged user activity. The NCCoE intends that the project, via the resulting practice guide, will provide adopting organizations with the following potential benefits:

- detection of privilege escalation
- detection of unauthorized access to sensitive data
- detection of malicious system-access attempts
- detection of suspicious login events
- minimization of workload
- support of compliance and reporting efforts with real-time information

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge. The reference design describes a vendor/technology-agnostic approach that illustrates a solution. An example solution (proof of concept), included in the Practice Guide, will illustrate an integration of commercial and open-source products, which demonstrates an implementation based on the reference architecture and conforming to cybersecurity standards and best practices. The publication can be used to assist in design, acquisition, and integration of a continuous monitoring effort at an adopting organization.

Scope

The scope of this project includes continuous monitoring of an information technology (IT) infrastructure for user activity, such as normal and anomalous activity (malicious or not), and compliance support. The results will include a reference architecture and example implementation to enable the reader to understand and implement the proposed approach to monitoring user activity across an IT infrastructure. The logging and auditing functions associated with authorization, authentication, and system/application access processes are the primary sources of data to be monitored and analyzed.

The project will not address other aspects of identity and access management, such as vetting, credential management, rights management, and provisioning. Functions other than logging and auditing for authorization, authentication, and system/application access processes are not included in the project.

Assumptions

Continuous monitoring is a desirable outcome for an organization monitoring its IT infrastructure. In addition, the NCCoE assumes that an organization will perform a risk assessment to determine the value of an investment in one or more of the continuous monitoring capabilities included in the architecture. The NCCoE also assumes that all privacy, legal, and ethical issues of data collection for continuous monitoring will be considered.

Background

Malicious actors are known to exploit security vulnerabilities that enable access to sensitive data. Organizations understand that by continuously monitoring their IT, they can limit their exposure to operational and compliance risks by detecting malicious activity quickly. Many industries, such as the financial sector, must adhere to regulations that require monitoring. Also, most cybersecurity best practices and frameworks include monitoring as an enabling technique to detect incidents (both accidental and malicious).

2 Scenarios

The following scenarios have been used to develop this project description. They will become the use cases for the reference architecture in the practice guide. The scenarios focus on continuous monitoring of user access. Although not specifically mentioned in the scenarios, continuous monitoring can also assist with compliance by providing log management, access certification reporting, and audit support by using automation.

Scenario 1: Unauthorized Use of User Credentials

A system user—either an authorized insider or an unauthorized outsider—gains access to the network and steals the credentials of another user. The malicious user then accesses critical assets containing sensitive data that the user is not authorized to view, such as nonpublic personal information.

Continuous monitoring solutions can help detect such malicious behavior by monitoring user activity logs, including correlation and analytics based on known user access policies. Anomalies and suspicious activity such as accessing unusual data or systems, or writing and executing binaries, can be detected quickly.

Scenario 2: Malicious Access Attempts

A malicious actor gains access to a network to upload malware, access sensitive data, or move laterally or vertically within the network (e.g., using privilege escalation).

Collecting log data on login and access events, both successful and failed, can help detect such intrusion attempts, especially if a high number of failed authentication attempts is found or a user is logging in at unusual times or with unusual frequency.

Scenario 3: Simultaneous Logins

A user's credentials are used to log in on two devices on the network at the same time (e.g., a second login occurs while a first login is still active). Although there are legitimate use cases with system administrators and lab system users, one of the connections could have been made by a malicious actor who gained access to the credentials of the authorized user and has used them to connect to the network.

Monitoring for simultaneous usage of user accounts can be detected by collecting log data on the time, duration, and system associated with each user session. If simultaneous sessions are detected, IT personnel can communicate with the user (e.g., through the sessions or out-of-band methods) to determine if both sessions were made by the authorized user.

Scenario 4: Activity from Multiple Geographic Locations

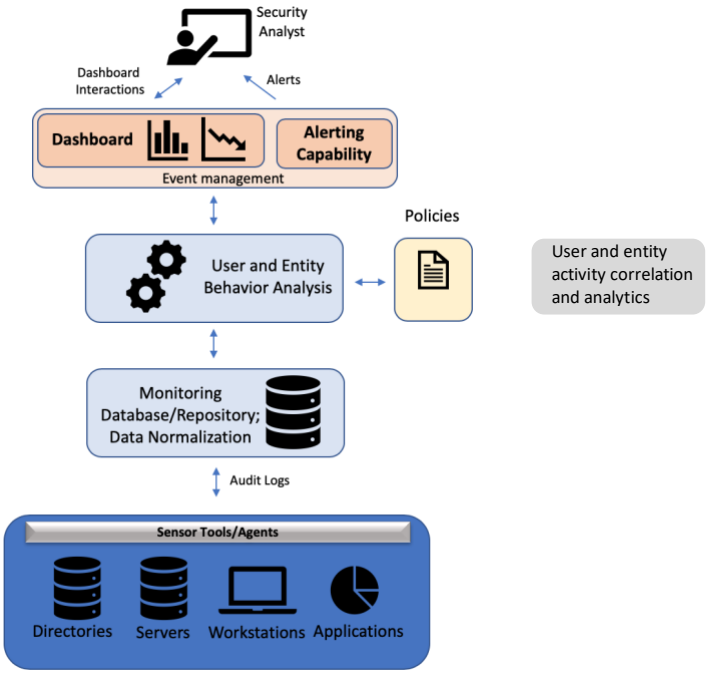
A user's credentials are used to log in, within a short period of time, from two different locations (simultaneously or subsequently) that are geographically far apart. This situation indicates the user has logged in by using different network connections such as Wi-Fi and virtual private network, or a second connection was made in the second location, possibly by a malicious actor who has gained access to the credentials of the authorized user and has used them to connect to the network.

Collecting and monitoring account logging data that contains internet protocol addresses paired with geo-location tagging (or other knowledge of the organization's network topography) will allow detection of this type of unauthorized user activity. If this activity is detected, IT personnel can communicate with the user to determine if both sessions were made by the authorized user.

3 High-Level Architecture

The high-level architecture diagram in Figure 1 introduces continuous monitoring into the IT infrastructure of an organization. The architecture and monitoring techniques could be applied to different types of accounts, such as normal user accounts, privileged user accounts, third-party accounts (business partners, contractors, etc.), and departing employee accounts. The high-level architecture addresses the scope noted in Section 1 and the desired requirements noted below.

Figure 1: High-Level Architecture



The above figure identifies a high-level architecture of the enterprise system and the associated components for this project. During development of the laboratory environment implementing this project, the figure will be refined to describe detailed components and to map the physical architecture in the lab environment for the specific scenario being implemented. A goal of this figure is to help spur identification of vendor participants and hardware and software components for collaborative use in a laboratory environment to build open, standards-based, modular, end-to-end example implementations.

Data to Be Collected

It is important to collect event data (containing when, where, who, and what information) from multiple sources, including firewalls, intrusion detection and intrusion prevention systems, end-point security sources, and application sources [1, 2]. A security information and event management system can process the log data and provide information on authentication and authorization failures, privilege escalation, and suspicious login events.

The logs generated by different operating systems, devices, and systems will likely contain information in different formats, which may require some transformation on the log data to normalize it for analysis. This document identifies some data at a high level that should be monitored to support improved security and compliance.

These are the types of log data that should be collected for monitoring and analysis:

- authentication and authorization failures and successes
- application errors and system events
- changes to privileges
- use of a system's administrative privileges
- access to sensitive data
- successful/unsuccessful logins

Component List

The NCCoE is seeking collaborating vendors to provide components to develop an example solution, including the following components that:

- collect and normalize user access activity data from
    - workstations and servers
    - directories and databases
    - operating systems and applications
    - devices that perform authentication or authorization
    - network and perimeter security devices
    - intrusion detection systems and intrusion prevention systems
    - host-based security software
- analyze user access activity data to identify suspicious/malicious activity
- provide alerts and information about suspicious/malicious access activity to cybersecurity analysts

Desired Capabilities

The desired security capabilities, behaviors, and life-cycle security requirements of the solution are identified in the following list:

- user access monitoring
- identification and analysis of user access behavior
- detection and alerting of malicious user access activity

4 Relevant Standards and Guidance

- NIST, *Framework for Improving Critical Infrastructure Cybersecurity v1.1*, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- R. Ross, M. McEvilley, and J. Oren, NIST Special Publication (SP) 800-160 Volume 1, *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* March 2018
- K. Kent and M. Souppaya, NIST SP 800-92, *Guide to Computer Security Log Management,* September 2006
- M. Souppaya and K. Scarfone, NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* July 2013

5 Security Control Map

The security control map in Table 2 lists the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (also known as NIST Cybersecurity Framework) Subcategories relevant to the desired solution.

Table 2: Security Control Map

Function	Category	Subcategory
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.

Function	Category	Subcategory
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
		DE.AE-5: Incident alert thresholds are established.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-2:** Detection activities comply with all applicable requirements.
		DE.DP-4: Event detection information is communicated.

Appendix A References

[1] The Open Web Application Security Project. Available: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.

[2] B. Todd, *Creating a Logging Infrastructure*, SANS Institute, Information Security Reading Room. Available: https://www.sans.org/reading-room/whitepapers/logging/creating-logging-infrastructure-38130.