Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 5: Monitoring User Activity on Classified Networks

Introduction

Objectives

The Minimum Standards require your program to include the capability to monitor user activity on classified networks. This is an essential component in combatting the insider threat.

In this lesson, you will learn about program strategies for such monitoring.

What to Monitor

Activities to Monitor

Monitoring activity on classified networks is essential for any insider threat program. Successful monitoring will involve several levels of activities.

The first aspect is governance – that is, the policies and procedures that an organization implements to protect their information systems and networks. These policies set the foundation for monitoring.

Once policies are in place, system activities, including network and computer system access, must also be considered and monitored.

Finally, an insider threat program must also monitor user activities so that user interactions on the network and information systems can be monitored.

Each level of activity is equally important and you should incorporate all of them into your insider threat program to best mitigate the risk of insider threats.

Governance

Governance, or the policies and procedures you enact for your insider threat program, will guide your efforts in monitoring user activity on your organization's networks.

These should include user and group management, use of privileged and special rights, and security and policy changes. Key components of governance include having employees sign agreements acknowledging monitoring and implementing banners informing users that their system and network activity is being monitored.

Monitoring these components ensures that users' access is limited to what is essential for their role. This allows you to then prioritize monitoring efforts.

It also allows you to identify users who are abusing their privileges.

System Activity Monitoring

Monitoring system activities will allow your program to identify possible system misuse.

Activities or events to monitor include logons and logoffs, system restarts and shutdowns, and root level access. Monitoring these activities identifies when the network is being accessed, any potential software installs, and whether someone is accessing or making changes to the root directory of a system or network.

User Activity Monitoring

Monitoring user activity helps identify users who are abusing their access and may be potential insider threats.

This includes monitoring file activities, such as downloads; print activities, such as files printed; and search activities. Monitoring these activities can identify abnormal user behaviors that may indicate a potential insider threat. While you cannot monitor every aspect of these activities, you can prioritize efforts as they relate to the systems and information that require the most protection.

How to Monitor

Monitoring Considerations

Once you determine what you are going to monitor, you must determine how you are going to monitor the activities and make sense of monitored activity.

First, there is an overarching consideration to take into account: Will your program monitor user activity in real time or will monitoring be event-triggered? Questions to ask include:

- How will data be integrated?
- How will data be analyzed?
- How will results be reported?

While some methods are preferable to others, budgets will likely be the determining factor of which methods are used.

Integration

In order to detect potential insider threats, your program needs to integrate the data it collects so it may be viewed as a whole. There are two common methods for integrating data – they are known as “push” and “pull.” Many programs use a combination of these two methods.

Using the push method, collected data is pushed to the central hub automatically. This streamlines the collection process and helps ensure the timely analysis of data. However, if too many requirements are programmed into the system, it may swamp the system with data.

With the pull method, an analyst retrieves data from several locations. This allows the analyst to request smaller and more specific queries. However, the timeliness and consistency of collection depends on the analyst’s workflow.

When determining how your program will integrate data, you will need to take into account your organization’s resources, staffing, and network setup.

Analysis

It is not enough to simply monitor and collect data. To be useful, the data must be analyzed to detect potential insider threats. Two common analysis methods are manual analysis and automatic analysis.

Manual analysis relies on analysts to review the data. It relies on the skills of the analysts involved and is often less expensive than automatic processing options, although the number of users and the amount of data being collected may require several analysts, resulting in higher costs.

Automatic analysis relies on algorithms to scan data, which streamlines the discovery of adverse information. However, this type of automatic processing is expensive to implement.

Reporting

Reporting is the culmination of the metrics and leads derived from integrating and analyzing collected data and is an essential component of any insider threat program. Reporting considerations include weighing the pros and cons of real-time versus event-triggered monitoring.

Real-time monitoring, while proactive, may become overwhelming if there are an insufficient number of analysts involved.

Event-triggered monitoring is more manageable because information is collected and reported only when a threshold is crossed. However, because event-triggered monitoring is reactive, it typically operates behind the threat, leaving open an opportunity for increased damage.

Review Activity

Which of the following best describes what your organization must do to meet the Minimum Standards in regards to classified network monitoring?

Select the correct response.

○ Develop policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.

○ Running audit logs will catch any system abnormalities and is sufficient to meet the Minimum Standards.

○ Establishing a system of policies and procedures, system activity monitoring, and user activity monitoring is needed to meet the Minimum Standards.

Answer Key

Review Activity

Which of the following best describes what your organization must do to meet the Minimum Standards in regards to classified network monitoring?

Select the correct response.

○ Develop policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.

○ Running audit logs will catch any system abnormalities and is sufficient to meet the Minimum Standards.

⦿ Establishing a system of policies and procedures, system activity monitoring, and user activity monitoring is needed to meet the Minimum Standards.

Establishing policies and procedures, system activity monitoring, and user activity monitoring are equally important and are all needed to meet the Minimum Standards.