Cybersecurity and Insider Threat Short

Student Guide

May 2026

Center for Development of Security Excellence

Contents

Welcome

Narrator: Welcome, and thank you for joining the Cybersecurity and Insider Threat Q&A session. Insider Threat Hub teams are made up of professionals from Cybersecurity along with:

- Security
- Human Resources
- Legal
- Counterintelligence
- Behavioral Science
- Law Enforcement

Each of these groups contributes important and unique information to the risk management process.

Insider Threat Hub teams exist to deter personnel from becoming an insider threat, detect existing insider threats, and analyze potential threats to validate reports and develop context on the subject and situation. Insider Threat Hub teams mitigate the risks personnel may pose and work to move them off the critical pathway through early intervention, proactive reporting, and referrals.

Cybersecurity professionals recognize the vulnerabilities of digital systems and communications to insider attacks. Because cybersecurity attacks are becoming increasingly impactful, common, and complex, Cybersecurity professionals stay current with changing threats and implement enhanced security requirements.

For these reasons and more, Cybersecurity professionals are essential to an effective Insider Threat Hub team. Today, you will hear from a Cybersecurity professional and have an opportunity to ask questions to understand the role Cybersecurity personnel play in deterring, detecting, analyzing, and mitigating potential insider threats.

Cybersecurity Representative Introduction

Narrator: I'd like to introduce our Cybersecurity representative, Ms. Catherine Mijango. As an Information Technology Specialist and DITMAC Cybersecurity Hub Representative, Ms. Mijango works to corroborate findings when assistance is needed on a case or referral. She has over 17 years of experience in the Information Technology (IT) field and has worked with DCSA since 2015 as both a contractor in the Cyber Division Operation team and as a civilian for the Insider Threat Program.

General Cybersecurity and Insider Threat

Narrator: Let’s first focus on establishing the basic relationship between Cybersecurity and insider threat.

What are the key elements of a successful cyber insider threat program?

Ms. Mijango: A successful Cyber Insider Threat program is a multi-faceted endeavor that combines technology, clear policies, and a strong security culture to protect an organization from the inside out. The primary goal of such a program is to detect, deter, and mitigate threats posed by individuals with authorized access, whether their actions are malicious or unintentional.

The key element of a successful Cyber Insider Threat program includes a clear definition of insider threat, a comprehensive risk assessment, and well-defined policies and procedures. It is also essential to have robust data collection and analysis capabilities using tools such as SIEM, UAM, and DLP. Incident response and remediation plans should be clearly defined and regularly tested. Employee training and awareness programs are critical, as it is a collaboration between Security, HR, and Legal departments. Leadership support and commitment are essential for ensuring that the program is adequately resourced and implemented effectively. Continuous monitoring improvements are also essential for adapting for changing threats and maintaining the effectiveness of the program.

What are the key differences between detecting external and insider threats?

Ms. Mijango: So, detecting external threats primarily relies on perimeter security measures and analyzing network traffic for anomalies, signatures of known malware, and suspicious connections originating from outside the organization.

Insider threat detection, however, focuses on analyzing user behavior, access patterns, and data usage within the organization's network, looking for deviations from established baselines and violations of security policies.

External threat detection typically involves known attack patterns and signatures, while insider threat detection relies on identifying unusual behavior patterns that may not immediately appear malicious. Insider threat detection requires understanding that context of user actions, the user's role, and the sensitivity of that data that they’re accessing.

While both external and insider threats pose significant risk to organizations, the methods for detecting them are fundamentally different. Detecting external threats often involves a more straightforward process of identifying and blocking known malicious actors and their tools. In contrast, detecting insider threats requires a more

sophisticated, context-aware approach that can distinguish between normal and abnormal behavior within a trusted environment.

What are some of the most effective data sources for detecting potential cyber insider threats?

Ms. Mijango: Effective data sources for detecting cyber insider threats include security information and event management, system logs, user activity monitoring data, network traffic analysis data, loss prevention alerts, and endpoint detection and response logs. Analyzing access control lists, active directory logs, and database audit logs is also very important. Human resource data such as employee departures, performance reviews, and disciplinary actions can provide a valuable context for identifying potential insider threat risk. Combining technical data sources with human factors can significantly improve the accuracy and effectiveness of the insider threat detection.

How do you balance security with user productivity when implementing insider threat detection measures?

Ms. Mijango: Balancing robust security with user productivity is a critical challenge when implementing insider threat detection measures. A heavy-handed approach can stifle productivity and create a culture of mistrust, while a lax approach can leave an organization vulnerable. The key is to strike a balance that protects the sensitive assets without unduly burdening employees. An effective insider threat program requires a holistic approach that involves collaboration across departments, which could include IT, HR, and Legal. Regular security awareness trainings are also essential to educate employees about insider threats and their role in preventing them. By combining technology, user centric policies, and a positive security culture, organizations can create a secure and productive environment where both the agency's assets and its employees are protected.

Cybersecurity's Role in the Insider Threat Hub

Narrator: Let's move on to a new topic: Cybersecurity's role in the Insider Threat Hub.

What is your understanding of the role of a cyber insider threat analyst or investigator?

Ms. Mijango: So, a cyber incident threat analyst investigator is responsible for identifying, assessing, and mitigating risk posed by individuals within an organization who have legitimate access to its systems and data, but may wittingly or unwittingly misuse that access to harm the organization. This would include preventing data breaches, intellectual property theft, sabotage and other malicious activities

originating from within the organization's trusted environment. The role requires a blend of technical skills, investigative skills, and an understanding of human behavior to proactively identify potential threats and respond effectively when incidents occur. Specifically, analysts work to prevent breaches, investigate suspicious behavior, and understand the scope and impact of threats. They also recommend security enhancements, develop and implement detective controls, and contribute to overall security awareness and training programs to prevent future incidents.

How do you handle false positives in insider threat detection?

Ms. Mijango: Handling false positives in insider threat detection is crucial for maintaining the efficiency and effectiveness of the security team. The first step is to thoroughly investigate each alert to determine whether it is a true positive or a false positive. If it is determined to be a false positive, I would analyze the reasons why the alert was triggered and identify any potential improvements to the detection rules or data sources. This may involve adjusting the thresholds for certain events, adding exceptions for specific users or devices, and/or improving the accuracy of the underlying data. It is also important to document all false positives and track frequency over time. This helps to identify the systematic issues within the detection rules and prioritize our efforts to improve their accuracy. Testing is key and always done to make sure we don't trigger false positives.

What steps would you take to contain and remediate a confirmed cyber insider threat incident?

Ms. Mijango: The first step would be detection and analysis of the threat, gathering information to determine its nature and scope. Next is to escalate and triage. Once a potential threat is detected, it must be escalated to the IRT for an initial assessment of its severity and potential impact. Last step is containment, eradication, and recovery. Once the threat is confirmed, the priority shifts to containing the damage and restoring normal operations. This phase should be handled with care to avoid alerting a malicious insider and ensure all legal and ethical considerations are met. Lastly, we would hold a debriefing with all relevant parties to discuss what worked, what didn't, and what could be improved. This is a crucial step for continuous improvement.

Cybersecurity Methods for Detection of Insider Threats

Narrator: It’s important to understand the methods Cybersecurity personnel employ to detect insider threats.

What are Security Information and Event Management (SIEM) systems?

Ms. Mijango: So, SIEM systems collects, aggregates, and analyzes security logs from various sources to identify potential insider threat indicators such as unauthorized access attempts, unusual data downloads, and policy violations. This involves building custom correlation rules and alerts that trigger when specific combinations of events occur.

SIEMs can be used to create dashboards and reports that provide a clear overview of insider threat activity within the organization. This data is then used to track key metrics and identify trends, and communicate findings to stakeholders as well as to conduct proactive threat-hunting exercises to uncover potential insider threats that may not be detected by automated alerts.

What is User and Entity Behavior Analytics (UEBA) and how does it enhance insider threat detection?

Ms. Mijango: User and Entity Behavior Analytics is a security technology that uses machine learning and statistical analysis to establish baselines of normal behavior for users and entities within an organization. UEBA then detects deviations from these baselines that may indicate suspicious or malicious activity. By analyzing a wide range of these data points, such as login times, access patterns, and data usage, UEBA can identify anomalies that may not be detected by traditional rule-based security systems. UEBA enhances insider threat detection by providing a more holistic and contextual view of user behavior. It can identify subtle changes in behavior that may be indicative of an insider threat, even if those changes do not trigger any specific security alerts. This helps improve the accuracy and effectiveness of the insider detection and reduce the number of false positives.

What are some common insider threat indicators that you would look for in network traffic analysis (NTA)?

Ms. Mijango: So, in network traffic analysis, we would look for several common insider threat indicators, including unusual data transfers to external destinations such as a use of USB or cloud storage, especially those involving sensitive data or large file sizes. Another indicator would be odd logins from strange locations as well as spikes in the network traffic. Lastly, a user who is trying to circumvent security, such as disabling security applications, or browsing malicious or inappropriate websites. Monitoring these deviations from normal behavior is key to detecting potential insider threats early.

Cybersecurity Mitigation Strategies

Narrator: After detecting potential insider threats, Cybersecurity personnel must act to mitigate those threats.

Describe your experience with Data Loss Prevention (DLP) technologies and how you've used them to prevent data exfiltration.

Ms. Mijango: We work with the CSOC* who creates the DLP policies which lets our UAM monitor user activity and generate alerts when users attempt to violate DLP policies. This assists the CSOC as well, so they can fine tune their own policies. Having their assistance to provide DLP logs corroborates user activity, providing a clear timeline of events and user actions. DLP helps security teams quickly understand the, "who, what, where and when" of a data-related incident. This information is invaluable for investigating insider threat incidents and can serve as evidence in legal proceedings.

**The Cyber Security Operations Center is also known as CSOC.*

What are some effective strategies for detecting credential theft and misuse?

Ms. Mijango: Effective strategies for detecting credential theft and misuse may include monitoring for unusual login patterns, such as logins from unfamiliar locations or devices, analyzing authentication logs for failed login attempts, and brute force attacks can help identify potential credential theft attempts. Monitoring for changes in user permissions and group memberships can also reveal unauthorized access to sensitive resources. Tools like firewalls and intrusion detection systems can block unauthorized access attempts. Additionally, a virtual private network, also known as a VPN, should be used on public Wi-Fi to encrypt traffic and prevent credential interception. Behavioral analytics tools can identify users who are accessing resources that they don't typically use or who are logging in at unusual times. Implementing multi-factor authentication can significantly reduce the risk of credential theft by requiring users to provide multiple forms of identification, as well as educating employees about phishing scams, social engineering, and the importance of good password hygiene, can significantly reduce the risk of credential theft.

Training and Competencies for Cybersecurity Insider Threat Hub Team Members

Narrator: You may still have additional questions about the training and competencies required of Cybersecurity members of the Insider Threat Hub Team.

How do you stay current with the latest trends and techniques in cyber insider threat detection?

Ms. Mijango: Staying current with the latest trends and techniques in cyber insider threat detection requires a proactive and ongoing effort. I regularly read security articles, industry publications, and research reports to stay informed about the latest threats and vulnerabilities. I also attend security conferences and webinars to learn from experts in the field, as well as network with other security professionals, participating in online communities and forums and other ways to stay up-to-date on the latest trends. I also engage in continuous learning by doing my continuous education credits for my certifications related to cybersecurity and insider threat detection.

What are some of the ethical considerations involved in monitoring user activity for insider threats?

Ms. Mijango: There are several ethical considerations involved in monitoring user activity for insider threats. It is important to be transparent with users about the fact that their activity is being monitored and the reasons why. It is important to have clear policies and procedures in place that govern the monitoring of user activity and ensure that those policies are followed consistently. Limiting the scope of monitoring of what is necessary to detect and prevent insider threat is crucial, as it is, ensuring the data is stored securely and the access of that data is restricted to authorized personnel. It is also important to protect the privacy of users by minimizing the collection of personally identifiable information and ensuring that that data is used only for legitimate security purposes.

Conclusion

Narrator: I'd like to wrap up this Cybersecurity Insider Threat information session by thanking our Cybersecurity representative for joining us today. She really helped us summarize the role Cybersecurity personnel, like herself, play in deterring, detecting, analyzing, and mitigating potential insider threats.

Ms. Mijango: Thank you so much for having me and allowing me to collaborate.

Narrator: We now know that Cybersecurity personnel provide support that is invaluable to Insider Threat Hub teams and greatly benefits risk mitigation efforts.