Establishing an Insider Threat Program for Your Organization

Course Overview

Narrator: Threats from insiders are serious and they are happening now. You and your organization are at risk. You already know what an insider threat is...but what can your organization do to combat it? As a federal agency, DoD Component, or Cleared Contract facility under the National Industrial Security Program, what must you do? Welcome to the Establishing an Insider Threat Program for Your Organization course.

Screen text: Establishing an Insider Threat Program for Your Organization

Course Objectives

Narrator: In this course you will learn about establishing an insider threat program and the role that it plays in protecting you, your organization, and the nation. You will learn the policies and standards that inform insider threat programs and the standards, resources, and strategies you will use to establish a program within your organization. Here are the course objectives. Take a moment to review them. When you're ready, select the forward arrow to go to the Course Menu.

Screen text: Course Objectives:

- Identify the policies and standards that inform the establishment of an insider threat program
- Identify key challenges to detecting the insider threat
- Identify key steps to establishing an insider threat program
- Identify the minimum standards for insider threat programs and key resources for implementation
- Identify program strategies for:
    - Monitoring user activity on classified networks
    - Evaluating personnel security information
    - Training cleared employees on the insider threat

Insider Threat Program Requirement

Introduction

Narrator: Who could become an insider threat? An insider is any person with authorized access to any United States government resource, such as personnel, facilities, information, equipment, networks or systems. An insider threat refers to an insider who wittingly or unwittingly does harm to their organization. This threat can include espionage, terrorism, sabotage, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Insider threat programs seek to mitigate the risk of insider threats. This lesson will review program policies and standards. It will also discuss some key challenges to detecting insider threats.

Screen text: Lesson Objectives:

- Identify the policies and standards that inform the establishment of an insider threat program
- Identify key challenges to detecting the insider threat

Background

Narrator: Insider incidents impact public and private organizations causing damage to national security, loss of life, the loss or compromise of classified information, and billions of dollars annually in lost revenue related to trade secret theft, fraud, sabotage, damage to an organization's reputation, acts of workplace violence, and more. Most insider threats exhibit risky behavior prior to committing negative events. If identified early, many risks can be mitigated before harm occurs. In order to manage risks associated with the insider threat, Federal and DoD policies require federal agencies, DoD components, and cleared industry under the National Industrial Security Program to establish Insider Threat Programs. Insider Threat Programs are multidisciplinary teams comprised of security, human resources, cybersecurity, legal, counterintelligence, mental health professionals and others who work together to proactively identify insiders who may pose a threat to the organization or its resources. Establishing your program is the first step toward developing this capability. Let's take a closer look at the policies and associated requirements.

Screen text: National insider threat policy applies only to classified information, but its principles may also be used as a good general practice to protect other information.

National Policy

Narration: Executive Order 13587 establishes the requirement for federal agencies to establish their own insider threat programs. DoDD 5205.16 establishes this requirement for DoD Components. Requirements for cleared industry are identified under DoDD 5220.20-M, the National Industrial Security Operating Manual, and associated Industrial Security Letters or ISL. These policies define the purpose of insider threat programs as deterring, detecting, and mitigating insider threats. Insider threat programs are intended to: Deter personnel from becoming insider threats; detect insiders who pose a risk to their organizations resources including classified information, personnel, and facilities and mitigate the risks through early intervention and proactive reporting and referral of information. The policies also includes general department and agency responsibilities that we will discuss throughout this course.

Minimum Standards

Narrator: The Presidential Memorandum "Minimum Standards for Executive Branch Insider Threat Programs" outlines the minimum requirements to which all executive branch agencies must adhere. These standards are also required of DoD Components under the DoDD 5205.16 and Industry under the NISPOM.

These elements include:

- The designation of a senior official
- Implementation of data sharing practices across an organization
- Capability to gather, integrate, centrally analyze, and respond to key threat-related information, monitor employee use of classified networks
- Provide the workforce with insider threat awareness training
- Train insider threat program personnel on specific topics
- Conduct self-assessments of insider threat programs
- Report and refer matters to law enforcement, counterintelligence, or other departments and agencies as required
- Protect the civil liberties and privacy of all personnel

While these standards provide the minimum elements needed for organizations to establish effective insider threat programs, mature programs often incorporate additional elements and best practices. Throughout this course, we will refer you to the course resources for additional information on implementing these minimum requirements and explore strategies for several areas in greater detail.

Why Do Insiders Go Undetected?

Narrator: Insider Threat policy was issued to address challenges in deterring, detecting, and mitigating risks associated with the insider threat. These challenges include insiders who operate over an extended period of time with access at different facilities and organizations. Employees may not be trained to recognize reportable suspicious activity or may not know how to report, and even when employees do recognize suspicious behaviors, they may be reluctant to report their co-workers. It is also important to note that the unwitting insider threat can be as much a threat as the malicious insider threat. Traditional access controls don't help - insiders already have access. Insiders can collect data from multiple systems and can tamper with logs and other audit controls. It can be difficult to distinguish malicious from legitimate transactions. The failure to share information with other organizations or even within an organization can prevent the early identification of insider risk indicators. Insider threat program requirements are designed to help address these challenges.

Screen text:
Challenges

- Insiders may operate over a long period of time with access at different facilities and organizations
- Potential Risk Indicators often go unreported
- Unwitting insiders can inflict serious harm but are often unacknowledged
- Information sharing is often limited

Review Activity

Narrator: Now check your knowledge.

Screen text:
The minimum standards for establishing an insider threat program include which of the following? Select the best responses; then select Submit.

- ☐ Designation of Senior Official
- ☐ Monitor employee classified network use
- ☐ Provide employee training
- ☐ Protect civil liberties and privacy

Conclusion
Narrator: You have completed the Insider Threat Program Requirement lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Insider Threat Program Requirement lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Setting Up an Insider Threat Program

Objectives

Narrator: Insider threat programs as outlined in policy and Minimum Standards seek to mitigate the risk of insider threats. This lesson provides guidance on how to set up an insider threat program in your agency or organization.

Screen text: Lesson Objective:

- Identify key steps to establishing an insider threat program

Roles and Responsibilities

Narrator: Each agency must establish its own capability to deter, detect, and respond to the insider threat. This centralized capability relies on several entities. There is a Senior Official who manages the program. In addition, in order to establish the program, key organization stakeholders must be involved. This can be thought of as a working group. Finally, establishing the program also includes putting in place the capability to execute the program. For ease of discussion, we'll describe this as the "hub." Let's take a closer look at each.

Screen text: Insider threat programs rely on involvement from several entities.
Senior Official – Manages program
Working Group – Establishes program
“Hub” – Executes program

The Senior Official

Narrator: Minimum Standards require an organization to designate a Senior Official. The Senior Official plays a vital role in establishing the process of gathering, integrating, analyzing, and responding to potential insider threat information. When establishing your own insider threat program, it is important to have the buy-in and continuing involvement of your agency’s Insider Threat Senior Official. The Senior Official is responsible for managing and overseeing the program and providing resource recommendations to the agency head, submitting the implementation plan and annual reports to the agency head, ensuring proper handling and use of records, consulting with legal, civil liberties, and privacy officials; establishing guidelines for record retention; and facilitating oversight reviews to ensure compliance with policy.

Screen text: Insider threat programs should have Senior Official buy-in and involvement. Responsibilities include:

- Manage the program
- Provide resource recommendations
- Submit the implementation plan and annual report
- Ensure proper handling and use of records
- Consult with legal counsel
- Establish guidelines for record retention
- Facilitate oversight reviews to ensure policy compliance

Establishing the Working Group

Narrator: When establishing your agency or organization's capability to deter, detect, and respond to the insider threat, you should establish a working group that includes representatives from key stakeholder offices within your organization. This includes those who can provide personnel-related information, such as counterintelligence, security, and human resources; those who can provide system monitoring, such as cybersecurity and information assurance; those who can provide legal guidance, such as the office of the General Counsel or privacy officials; and, finally, those who can provide response capabilities, such as the Inspector General and law enforcement. For more information, refer to the CDSE Course INT201 Developing a Multidisciplinary Insider Threat Capability. You can access this and other materials in the course resources.

Screen text: When setting up insider threat program, include representatives from agency's key stakeholder offices.

Personnel Information

- Counterintelligence
- Security
- Human Resources

Response Capabilities

- Inspector General

System Monitoring

- Cybersecurity
- Information Assurance

Legal Guidance

- General Counsel
- Privacy Officials

Identifying What Requires Protection

Narrator: One of the key activities when establishing an insider threat program is to identify and prioritize what requires protection. This may include people, facilities, technology, equipment, and information. However, with limited resources, you cannot protect all assets. Of the assets you do protect, you cannot protect them at the same level. To help in identifying and prioritizing, ask: Is the asset essential for the organization to accomplish its mission? Would loss of access to the asset disrupt time-sensitive processes? Would compromise or degradation of the asset damage national or economic security of the US or your company? Could an adversary exploit or manipulate this asset to harm the organization, U.S., or allied interests? Would an adversary gain advantage by acquiring, compromising, or disrupting the asset? The answers to these questions will guide you to identify and prioritize what requires protection.

Screen text: Insider threat programs must identify and prioritize assets requiring protection.

Protection Identification and Prioritization

Questions to ask:

- Is it essential to the mission?
- Would its loss disrupt time-sensitive processes?
- Would its compromise or degradation damage national or economic security?
- Could an adversary exploit it to cause harm?
- Would it help an adversary gain advantage?

Other Considerations

Narrator: When establishing the program, other considerations include: Who are our key agency stakeholders? What resources are available to us? What capabilities do we already have in place? How should we incorporate subordinate entities? How will we apply our program to contractors? The answers to these questions will guide you in setting up an insider threat program within your organization.

Screen text: Other considerations include:

- Key stakeholders
- Available resources
- Existing capabilities
- Incorporation of subordinate entities
- Applicability to contractors

Executing Program Capabilities

Narrator: Once the insider threat program is established in your organization, there needs to be a centralized capability in place to execute the program. This centralized capability can be thought of as a hub. Hub activities include: Accessing agency-internal information to detect and/or analyze potential insider threats, receiving insider threat reports from inside the agency, and developing informed responses to insider threat activity. For more information, refer to the CDSE Course INT240 Basic Insider Threat Hub Operations. You can access this and other materials in the course resources.

Screen text: Activities include:

- Detect and analyze potential threats
- Receive internal threat reports
- Develop responses to threat activity

Review Activity

Narrator: Now check your knowledge.

Screen text: Which of the following stakeholders should be involved in establishing an insider threat program in an agency? Submit all that apply; then select Submit.

☐Information Assurance
☐Security
☐Human Resources
☐Finance Officer

Conclusion

Narrator: You have completed the Setting Up an Insider Threat Program lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Setting Up an Insider Threat Program lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Minimum Standards for an Insider Threat Program

Objectives

Narrator: In this lesson, you will learn about Minimum Standards for implementing an insider threat program. As discussed in lesson one, these minimum standards include: Designation of Senior Official, Implementation of Data Sharing, Capability to Manage Threat Information, Monitoring of Employee Classified Network, Providing Employee Awareness Training and Specific Training for Insider Threat Program Personnel, Protecting Privacy and Civil Liberties, Conducting Self-Assessments and Reporting and Referral. We will explore a few of these items in more detail as we discuss how to establish an insider threat program.

Screen text: An agency's insider threat program must meet these minimum standards, but may go further.

Core Requirements

Narrator: How do you develop an insider threat program? The National Minimum Standards contain the core requirements you must fulfill. They center on establishing your program's capability to analyze and respond to a potential insider threat. The basic elements of these standards are replicated in policy requirements for both DoD Components and Industry. Regardless of the type of organization there are specific items to help develop an insider threat program. You must establish your program's ability to gather, integrate, review, assess, and respond to information derived from a variety of sources. You must also establish procedures for insider threat response actions to both clarify and resolve insider threat matters and to ensure that such response actions are centrally managed. Finally, you must develop procedures to document insider threat matters reported to the program and the response actions taken. These procedures must also ensure timely resolution of matters.

Screen text: Analysis and Response Capabilities
Sources include:

- Counterintelligence
- Security
- Human resources
- Law enforcement
- User activity monitoring

Procedures include:

- Threat matter clarification
- Central management of response actions

Documentation includes:

- Reported threats and response actions
- Timely resolution of matters

Ensure Program Access to Information

Narrator: In order for your program to have any effect against the insider threat, information must be shared across your organization. As part of your insider threat program, you must direct all relevant organizational components to securely provide program personnel with the information needed to identify, analyze, and resolve insider threat matters. You must establish procedures for program requests to access sensitive information, such as special access programs. Ensuring such information will be adequately protected will facilitate cooperation by components. Minimum Standards also direct you to establish guidelines for reporting information to the program. This will help your workforce understand what and how to report. Finally, as part of establishing an insider threat program, you must ensure timely access to available intelligence and counterintelligence threat-related information.

Screen text: Information sharing is key to mitigating the risk of insider threats.

Minimum standards:

- Direct components to provide insider threat-related information
- Establish procedures for accessing sensitive information
- Establish reporting guidelines
- Ensure access to relevant intelligence and counterintelligence information

Establish User Activity Monitoring Capability

Narrator: Minimum Standards also require you to develop a user activity monitoring capability for your organization's classified networks. When establishing your organization's user activity monitoring capability, you will need to enact policies and procedures that determine the scope of the effort. Depending on the type of organization, you may need to coordinate with external elements, such as the Defense Information Systems Agency for DoD components, to provide the monitoring capability. You will need to execute interagency Service Level Agreements, where appropriate.

Screen text: Information threat programs must include the capability to monitor user activity on classified networks.

Minimum standards:

- Establish user monitoring policies and procedures
- May use another agency to provide the monitoring capability
- Execute interagency Service Level Agreements, where applicable

Personnel Training

Narrator: Minimum Standards require training for both insider threat program personnel and for cleared employees of your organization. Minimum Standards designate specific areas in which insider threat program personnel must receive training. In addition, all cleared employees must receive training in insider threat awareness and reporting procedures.

Screen text: Insider threat programs must include training for insider threat program personnel and cleared employees.

Minimum standards require:

- Specific training for insider threat program personnel
- Awareness and reporting training for all cleared employees

Review Activity

Narrator: Now check your knowledge.

Screen text: When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include? Select all that apply; then select Submit.

- ☐ Ensure access to insider threat-related information
- ☐ Establish analysis and response capabilities
- ☐ Establish user monitoring on classified networks
- ☐ Ensure personnel are trained

Conclusion

Narrator: You have completed the Minimum Standards for an Insider Threat Program lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Minimum Standards for an Insider Threat Program lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Evaluating Personnel Security Information

Objectives

Narrator: Minimum Standards require your program to ensure access to relevant personnel security information in order to effectively combat the insider threat. In this lesson, you will review strategies for collecting personnel security information and see how information drawn from multiple sources can be beneficial in identifying potential insider threats.

Screen text: Lesson Objective

- Identify program strategies for evaluating personnel security information

Information Sources

Narrator: In order to create a comprehensive picture of potential risk, you must gather information from multiple sources. Minimum standards require that privacy and civil liberties of all individuals be respected in the gathering, reviewing, retaining, and sharing of this information. For more information, you can refer to the CDSE Course INT260 Privacy and Civil Liberties in Insider Threat. You can access this and other materials in the course resource page. Ensuring that properly acquired personnel security information is accessible to stakeholders in a timely manner first requires organizational components to share information. In doing this, you need to gather information from a variety of sources that includes, but is not limited to: Counterintelligence, security, human resources, and cybersecurity. Information collected from multiple sources assists your program in creating a comprehensive picture of a potential insider threat. Select each personnel security information source for more information.

Screen text: In order to create a comprehensive picture, you must gather information from multiple sources.

Counterintelligence

Narrator: Information from counterintelligence includes, but may not be limited to counterintelligence files, foreign travel, and foreign contacts.

Popup Text:

Information includes, but it not limited to:

- *Counterintelligence files*
- *Foreign travel*
- *Foreign contacts*

Security

Narrator: Information from security should include, but may not be limited to: a variety of records and reports, security clearance adjudications, as well as information security clearance adjudications. Take a moment to review this list of possible security information sources.

Popup Text:

Information includes, but it not limited to:

- *Facility access records*
- *Financial disclosure filings*
- *Security incident files*
- *Serious incident reports*
- *Inspector General reports*
- *Security clearance adjudications*
- *Polygraph results*
- *Foreign travel*
- *Foreign contacts*

Human Resources

Narrator: Information from human resources may include personnel files, payroll information, and other files. Take a moment to review this list of possible human resources information sources.

Popup Text:

Information includes, but it not limited to:

- *Personnel files*
- *Payroll and voucher files*
- *Outside work/activities requests*
- *Disciplinary files*

Cybersecurity

Narrator: Possible information from cybersecurity might include different types of network access information and logs. Take a moment to review this list of possible cybersecurity information sources.

Popup Text:

Information includes, but it not limited to:

- *Personnel usernames and aliases*
- *Levels of network access*
- *Unauthorized use of removable media*
- *Print logs*
- *IT audit logs*

Evaluating Information

Narrator: Collecting information from multiple sources will assist your program in creating a comprehensive picture of an individual. Evaluated as a whole, this picture may help determine the risk posed by a potential insider threat. For example, a print log might show that an individual has been printing an unusually large amount of documents. On its own, this might not raise any flags – there could be a reasonable explanation for the printing. However, combining it with additional pieces of information might change how you see the situation. Select View to explore how.

Example

Narrator: Notice the information from the employee's disciplinary file: Her performance has dropped and it's noted that she is hostile toward coworkers and managers. Also note times listed in the Facility Access Records. This is outside of regular duty hours and, as it turns out, some of these times coincide with the increased print activity previously noted. Viewed together, this information should raise some concerns. For more information, refer to the CDSE Courses INT201 Developing a Multidisciplinary Insider Threat Capability and INT210 Insider Threat Mitigation Response Options. These courses can be accessed from the resource page.

Review Activity

Narrator: Now check your knowledge.

Screen text: An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened. Select the files you may want to review concerning the potential insider threat; then select Submit.

- ☐ IT audit logs
- ☐ Levels of network access
- ☐ Personnel files
- ☐ Security incident files

Conclusion

Narrator: You have completed the Evaluating Personnel Security Information lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Evaluating Personnel Security Information lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Monitoring User Activity on Classified Networks

Objectives

Narrator: 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.

Screen text: Lesson Objective

- Identify program strategies for monitoring user activity on classified networks

Activities to Monitor

Narrator: Monitoring activity on classified networks is required for insider threat programs. While not required, many organizations have found that monitoring of unclassified networks also provides valuable information for managing risk. 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. Select each level to learn more.

Screen text: Insider threat programs must operate at different levels to mitigate the risk of insider threats.

User Activity Monitoring

Narrator: 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. For more information, see the UAM in Insider Threat Job aid available in the course resources.

Screen text: Monitoring user activity allows you to flag users who are abusing system and network access and may be potential insider threats.

Includes:

- *File activities*
- *Print activities*
- *Search activities*

Importance: Identify abnormal behaviors indicative of a potential insider threat.

Systems Activity Monitoring

Narrator: 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.

Screen text: Monitoring system activities allows you to flag possible system misuse.

Includes:

- *Logons/Logoffs*
- *System restarts/shutdowns*
- *Root level access*

Importance:

- *Identify when network is accessed*
- *Detect software installs*
- *Detect root directory access and changes*

Governance

Narrator: 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.

Screen text: The policies and procedures you enact will guide your monitoring efforts.

Includes:

- *User and group management*
- *Use of privileged/special rights*
- *Security and policy changes*
- *User monitoring acknowledgement agreements*
- *Monitoring banners*

Importance:

- *Limits users' access*
- *Helps identify users abusing their privileges*

Monitoring Considerations

Narrator: 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, and how will results be reported? While some methods are preferable to others, budgets will likely be the determining factor of which methods are used. Let's take a closer look.

Screen text: Insider threat programs must both consider what activities are monitored and how they are monitored.

What

- File access
- System restarts/ shutdowns
- User/group management
- Logons and log offs
- Printer activity
- Root level access
- Search activity

How
Is user monitoring real time or event-triggered?

- How is data integrated?
- How is data analyzed?
- How are results reported?

Integrating

Narrator: 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.

Screen text: Data integration allows disparate pieces of information to be analyzed and viewed as a whole and is key to detecting potential insider risks. How is data integrated?

Push
Data automatically sent

- Less time spent collecting data
- Leads to timely data analysis
- Relies on careful programming of requirements

Pull
Data manually retrieved

- May retrieve smaller, more focused queries
- Relies on analyst for timely and consistent data collection

Analysis

Narrator: 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.

Screen text: Data analysis is critical to detecting potential insider threats. How is data analyzed?

Manual

- Relies on skills of analysts
- May be less expensive option, depending on number of analysts needed

Automatic

- Relies on algorithms
- Expensive to implement

Reporting

Narrator: 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. Remember that data from User Activity Monitoring must be gathered, stored, retained, and shared with the same respect to privacy and civil liberties as all other information in your program. See the course resources for additional information on Privacy and Civil Liberties.

Screen text: Sharing and reporting information is essential to detecting potential insider threats. How are results reported?

Real Time

- Depending on number of analysts, may become overwhelming
- Proactive solution

Event Triggered

- More manageable because information is collected only when a threshold is crossed
- Reactive solution

Review Activity

Narrator: Now check your knowledge.

Screen text: 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(s); then select Submit.

- o Developing policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.
- o Running audit logs will catch any system abnormalities and is sufficient to meet the Minimum Standards.
- o Establishing a system of policies and procedures, system activity monitoring, and user activity monitoring is needed to meet the Minimum Standards.

Conclusion

Narrator: You have completed the Monitoring User Activity on Classified Networks lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Monitoring User Activity on Classified Networks lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Training Employees on the Insider Threat

Objectives

Narrator: Your program is required to provide insider threat training to insider threat program personnel and the cleared employees of your organization. In this lesson, you will review the requirements for training both insider threat program personnel and cleared employees in your organization.

Screen text: Lesson Objective
- Identify program strategies for training cleared employees on the insider threat and specialized training for insider threat program personnel

Insider Threat Program Personnel

Narrator: The Minimum Standards require individuals assigned to the insider threat program to be fully trained in the following areas: Counterintelligence and security fundamentals; agency procedures for conducting insider threat response actions; applicable laws and regulations on gathering, integrating, retaining, safeguarding, and using records and data; applicable civil liberties and privacy laws, regulations, and policies; and applicable investigative referral requirements.

Screen text: Program Personnel Training Requirements
- Fundamentals of Counterintelligence and Security
- Conducting Insider Threat Response Actions
- Records & Data and Applicable Laws & Regulations
- Civil Liberties & Privacy: Laws, Regulations, & Policies
- Requirements for Investigative Referrals

Cleared Employees

Narrator: In addition to the training requirement for insider threat program personnel, Minimum Standards also require your organization's cleared employees to complete insider threat awareness and reporting training. Though not required, most programs find it effective to train all personnel – whether cleared or not – to increase awareness of the insider threat, identify potential risk indicators, and ensure timely reporting. Individuals must complete training within 30 days of hire, assignment, or access to classified information. They must complete annual refresher training thereafter. As with insider threat personnel training, cleared employee training must cover certain topics that include: Current and potential threats in the work and personal environments, the importance of detection and reporting to proper authorities, methods used by adversaries to recruit insiders and/or collect information, behavioral indicators and reporting procedures, and counterintelligence and security reporting requirements.

Screen text: Personnel must complete training within 30 days of hire/assignment or access to classified information. All cleared personnel must complete annual refresher training.

Cleared Personnel Training Requirements
- Current and Potential Threats
- Detecting and Reporting
- Recruitment and Information Collection Methodologies
- Behavior Indicators and Reporting Procedures
- Counterintelligence and Security Reporting Procedures

Obstacles

Narrator: Despite the great emphasis training places on the importance of the threat, recognizing indicators, and reporting procedures, employees may have reservations about reporting a coworker. How, then, do you overcome this obstacle? One successful strategy is to keep the focus on the welfare of the individuals involved. Odd or concerning behaviors are often associated with life crises, such as work stress, financial pressure, divorce, and death. By reporting a coworker displaying odd or concerning behaviors, that person may get help to resolve a life crisis. Alternatively, reporting may prevent a crime that could have far reaching consequences for the employees of an organization and the citizens of the United States. If employees understand that reporting may help an individual and prevent them from taking harmful actions they might later regret and/or reduce harm to the organization and national security, they may be more inclined to report what they observe. Often annual training is not enough to instill this mindset in the workforce. The CDSE Insider Threat Vigilance Campaign provides resources for your organization to keep the message fresh year round. Access to both required annual training and vigilance materials is provided in the resource page.

Screen text:
Displaying concerning behaviors following a death in the family.

Received counseling after a coworker reported him.

After concerning behavior reported, was found to be taking classified documents home with the intent to sell to a foreign country.

Was referred to appropriate authorities for further investigation. Loss of classified information prevented.

Review Activity

Narrator: Now check your knowledge.

Screen text: It's now time to put together the training for the cleared employees of your organization. Select the topics that are required to be included in the training for cleared employees; then select Submit.

- Behavioral indicators and reporting procedures
- Methods used by adversaries to recruit insiders
- Risk management for the insider threat
- Current and potential threats in the work and personal environment

Conclusion

Narrator: You have completed the Training Employees on the Insider Threat lesson. Select the Student Guide to review, or select the forward arrow to move on.

Screen text: You have completed the Training Employees on the Insider Threat lesson. To review, select the Student Guide, or select the forward arrow to choose your next lesson.

Course Conclusion

Course Summary

Narrator: Insider threat programs seek to deter, detect, and mitigate the risk of insider threats. In this course, you learned about the minimum requirements and strategies needed to establish such a program for your organization.

Screen text: Lesson Objective

- Identify program strategies for training cleared employees on the insider threat and specialized training for insider threat program personnel

Lesson Review

Narrator: Here is a list of the lessons in the course. Select Student Guides to review any lesson.

Screen text:

- Course Introduction
- Lesson 1: Insider Threat Program Requirement
- Lesson 2: Setting Up an Insider Threat Program
- Lesson 3: Minimum Standards for an Insider Threat Program
- Lesson 4: Evaluating Personnel Security Information
- Lesson 5: Monitoring User Activity on Classified Networks
- Lesson 6: Training Employees on the Insider Threat

Select Student Guides to review any lesson.

Course Objectives

Narrator: Congratulations. You have completed the Establishing an Insider Threat Program for Your Organization course. You should now be able to perform all of the listed activities. Please consult the course resources for additional information and consider these additional CDSE Courses to support program implementation. To receive course credit, you MUST take the Establishing an Insider Threat Program for Your Organization examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Screen text:

Establishing an Insider Threat Program for Your Organization

You should now be able to:

- ✓ Identify the policies and standards that inform the establishment of an insider threat program
- ✓ Identify key challenges to detecting the insider threat
- ✓ Identify key steps to establishing an insider threat program

- ✓ Identify the minimum standards for insider threat programs and associated resources for implementation
- ✓ Identify program strategies for:
  - Monitoring user activity on classified networks
  - Evaluating personnel security information

Additional CDSE Courses:

- INT201 Developing a Multidisciplinary Insider Threat Capability
- INT210 Insider Threat Mitigation Response
- INT220 Preserving Investigative and Operational Viability in Insider Threat
- INT240 Basic Insider Threat Hub Operations
- INT260 Privacy and Civil Liberties in Insider Threat

To receive course credit, you must take the Establishing an Insider Threat Program for Your Organization examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

Answer Key

The minimum standards for establishing an insider threat program include which of the following? Select the best responses; then select Submit.

- ☑ Designation of Senior Official
- ☑ Monitor employee classified network use
- ☑ Provide employee training
- ☑ Protect civil liberties and privacy

Which of the following stakeholders should be involved in establishing an insider threat program in an agency? Submit all that apply; then select Submit.

- ☑ Information Assurance
- ☑ Security
- ☑ Human Resources
- ☐ Finance Officer

When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include? Select all that apply; then select Submit.

- ☑ Ensure access to insider threat-related information
- ☑ Establish analysis and response capabilities
- ☑ Establish user monitoring on classified networks
- ☑ Ensure personnel are trained

An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened. Select the files you may want to review concerning the potential insider threat; then select Submit.

- ☑ IT audit logs
- ☑ Levels of network access
- ☑ Personnel files
- ☑ Security incident files

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(s); then select Submit.

- o Developing policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.
- o 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.

It's now time to put together the training for the cleared employees of your organization. Select the topics that are required to be included in the training for cleared employees; then select Submit.

- o Behavioral indicators and reporting procedures
- o Methods used by adversaries to recruit insiders
- o Risk management for the insider threat
- • Current and potential threats in the work and personal environment