Insider Threat Basic Hub Operations

Student Guide

September 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Course Welcome

Welcome to the Insider Threat Basic Hub Operations course. This course will provide you with the knowledge and resources needed to support you in your role as a member of the Insider Threat Hub. Listed below are the course objectives.

- Explain the role and purpose of an Insider Threat Program and Hub.
- Given a scenario, apply the principles of Insider Threat Hub operations.
- Given a scenario, apply Insider Threat Hub management protocols.

Why an Insider Threat Hub?

Our organizations are always susceptible to risks posed by trusted insiders. In the past, insider threats were addressed retroactively, through siloed compilation and analysis of pertinent threat information discovered by security, law enforcement, Human Resources, or counterintelligence. In other words, we responded, or reacted after we discovered a concerning event or identified a potential foreign nexus.

Today insider threat policy requires a more comprehensive and collaborative approach to how insider risk is managed. Insider Threat Programs establish hubs or teams of personnel from multiple disciplines.

Insider Threat Hub Purpose

Insider Threat Hubs are designed to put processes in place to examine and assess concerning behaviors with a holistic perspective with the intent of preventing, deterring, detecting, and mitigating risks associated with insiders. This proactive strategy often identifies and resolves issues before a potential insider becomes a threat to themselves or protected resources such as personnel, information, and property. Conducting Insider Threat Hub operations requires development of a carefully planned and managed program that considers more than just the minimum standards.

The Challenge

Your Challenge

You just heard that Insider Threat Hubs need a comprehensive and collaborative approach to managing insider risk and conducting Insider Threat Hub operations is critical to an effective program. This is where you come in. You have been volunteered by your supervisor to lead your organization's Insider Threat Program. Unfortunately, you are not sure senior leadership is on board due to a multitude of pressing priorities currently taking place within the organization. Are you ready for a challenge?

Challenge Rules

Welcome to the newest Federal agency – the Defense eLearning Activity (DeLA). You were volunteered by your supervisor to lead its Insider Threat Program. Your auxiliary duty begins today!

As the program manager, you will need to ensure hub operations comply with policy and run effectively. First, an operations plan needs to be approved by senior leadership. Senior leadership is open to hearing a proposal for operations, but they will need to be persuaded during your interactions with them throughout the week.

Use your knowledge of Insider Threat Hub Operations to impress and persuade senior leadership to buy into the idea of executing a robust Insider Threat Program that executes prevention, deterrence, detection, and mitigation strategies. If you garner enough support, then senior leadership will deliver the Insider Threat Program operations plan up to the Director for endorsement. Here is a short introduction from your senior executive, Claire.

> *Hi. I'm Claire, and I understand you want to set up an Insider Threat Program. I have to admit, I'm skeptical about putting a lot of resources behind it—but I'm willing to hear you out. I'll be around all week if you need to reach out.*

Throughout the week you will have numerous opportunities to interact with Claire to gain her buy in for implementing the Insider Threat Hub Operations Program. You will earn points by providing Claire with accurate information on the program and by correctly answering her questions. There will be 14 questions and you will earn 1 point for each correct answer. You will track your progress throughout the challenge to gauge your success. The number of correct answers at the end of the challenge corresponds to the level of support you will receive from Claire. Good luck on the challenge!

Lesson 2: Functions of an Insider Threat Hub

Introduction

Agenda for the Day

Happy Monday! Today is the first day of the challenge.

Looks like you have a meeting this afternoon with Claire to explain the functions and requirements of an Insider Threat Hub. You will need to take some time to prepare for this afternoon's meeting. Let's get started!

Functions of an Insider Threat Hub

What is an Insider Threat?

You never know what questions Claire will have for you later today. You may want to start by brushing up on your knowledge of what an insider threat is.

Definition – What is an Insider Threat?

An insider threat is someone with authorized access who uses that access, wittingly or unwittingly, to either harm or degrade organizational resources. This can include, but is not limited to:

- The loss, compromise, or unauthorized disclosure of protected classified or unclassified information;
- Kinetic threats to include violent events against self or others; and
- Threats to Government installations, facilities, personnel, missions, or resources.

Policy Documents – What is an Insider Threat?

Executive Order (E.O.) 13587; Department of Defense Directive (DODD) 5205.16; and Title 32 of the Code of Federal Regulations (CFR) Part 117 contain definitions of an insider threat.

Executive Order 13587

Insider Threat means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

DODD 5205.16

The threat insiders may pose to DOD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage,

terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

32 CFR Part 117 (NISPOM Rule)

The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

What is an Insider Threat Hub?

Claire may also have some questions on what an Insider Threat Hub is and its purpose. Be prepared.

Email – What is the Insider Threat Hub?

Take a moment to review the email that explains what an Insider Threat Hub is.

Email
To: Program Manager From: Supervisor Subject: What is an Insider Threat Hub? The Minimum Standards requires that DOD components and Federal Agencies accessing classified information develop "…effective Insider Threat Programs within departments and agencies to deter, detect, and mitigate actions by employees who may represent a threat to national security." An Insider Threat Hub is a multi-disciplinary staff element or activity established by an organization that possesses an integrated capability to monitor, audit, fuse, and analyze incoming information for insider threat detection and mitigation. Hub personnel will be able to analyze information and activity indicative of an insider risk and refer that data to the appropriate officials for investigation and/or resolution.

Whiteboard – What is the Insider Threat Hub?

Part of the requirement from the National Threat Policy is to establish a team or Hub. To effectively counter insider threats to our national security, best practices dictate that the Hub include:

- Program manager
- Legal counsel
- Law enforcement
- Security
- Counterintelligence
- Cybersecurity
- Mental health and behavioral science, and

- Human resources or human capital disciplines.

Industry requirements, as identified under the NISPOM rule, require facilities to establish an Insider Threat Program group consisting of program personnel from offices across the contractor's facility, based on the organization's size and operation. The size and complexity of your organization will determine the exact makeup of your insider threat team or Hub.

Regardless, all actions undertaken by the Insider Threat Hub must respect the privacy and civil liberties of the workforce.

Training Icon – What is the Purpose of an Insider Threat Hub?

Insider Threat Hubs take proactive measures to prevent, deter, detect, mitigate, and report the threats associated with trusted insiders. The Hub identifies anomalous behaviors that may indicate an individual poses a risk. Early identification allows Insider Threat Program personnel to focus on an individual's issues of concern or stressors and deploy appropriate mitigation responses.

When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and reports information outside the organization as required by policy or regulation. Measures taken by the Insider Threat Hubs are listed below.

Prevent

Insider Threat Hubs prevent potential insider threats by providing leadership with threat information that may help to shape decisions about managing insider risk and building resiliency throughout the workforce.

Deter

Insider Threat Hubs deter potential insider threats by instituting appropriate security countermeasures, including awareness programs.

Detect

Insider Threat Hubs detect individuals at risk of becoming insider threats by identifying potential risk indicators. These observable and reportable behaviors or activities may indicate an individual is at greater risk of becoming a threat.

Mitigate

Insider Threat Hubs mitigate the risks potential insider threats pose. One of the goals of the Insider Threat Hub is to identify and mitigate issues before they escalate, but sometimes programs become involved in the middle of an incident or event or even after the fact.

Report

Insider Threat Hubs are required to report information about actual or potential insider threats and can refer insider threat data to the appropriate officials to investigate or otherwise resolve.

Insider Threat Hub Requirements

What are the Insider Threat Hub Requirements?

There is one last topic you need to be prepared to share with Claire during your meeting this afternoon. You need to be well versed in the Insider Threat Hub Requirements.

Computer Screen – What are the Insider Threat Hub Requirements?

Policy requirements for the Insider Threat Program articulate minimum standards for establishing a program.

First, E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the responsible Sharing and Safeguarding of Classified Information. It outlines the establishment of the National Insider Threat Task Force, which assists with implementation of agency insider threat programs.

Next, the Presidential Memorandum, National Insider Threat Policy and Minimum Standards (Nov 21, 2012), lays the foundation for your program. It outlines the policy and general responsibilities.

For the DOD, DODD 5205.16, The DOD Insider Threat Program, establishes policy and assigns responsibilities within DOD to develop and maintain an Insider Threat Program.

In addition, DOD Instruction (DODI) 5205.83 establishes the DOD Insider Threat Management and Analysis Center, also known as the "DITMAC," and requires DOD Hubs to report insider threat matters meeting certain thresholds to the DITMAC in a timely manner.

Lastly, 32 CFR Part 117 NISPOM rule prescribes the requirements for industry Insider Threat Programs.

These are the minimum standards. To be truly effective, Insider Threat Hubs must:

- Designate a senior official,
- Develop guidelines and procedures for information, integration, analysis, and response,
- Ensure insider threat program personnel are trained,
- Provide access to information,
- Ensure monitoring of user activity on networks,
- Ensure employees are provided awareness training on insider threats, and
- Perform independent and self-assessments of compliance with insider threat policies and standards.

You can view these requirements on the Center for Development of Security Excellence (CDSE) Insider Threat Toolkit Policy/Legal page.

Meeting with Senior Leadership

Knowledge Check – 1

Now that you are up to speed with the functions and requirements of an Insider Threat Hub, you now need to prepare a short brief to provide to Claire prior to your meeting this afternoon. You want to make sure the brief is factual.

Which of the following statements are true about Insider Threat Hubs and should be shared with Claire prior to your meeting?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Insider Threat Hubs implement proactive strategies to help identify and resolve issues before an insider threat becomes a reality.
- ☐ Insider Threat Hubs implement strategies to help prevent, deter, detect, and mitigate insider threats.
- ☐ Insider Threat Hubs are required to report information about actual or potential insider threats.
- ☐ Insider Threat Hubs are created to prevent, deter, detect, and mitigate actions by external threats.

Knowledge Check – 2

It's now time to meet with Claire to answer questions on the functions and requirements of Insider Threat Hubs.

> *Claire: Thanks for the brief, that was very helpful. However, I still have a few logistical questions pertaining to the Hub. There are a lot of key resources that are all part of the Hub. Does every Insider Threat Hub team include the same positions and the same number of people?*

Does every Insider Threat Hub team include the same positions and the same number of people?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

- ○ Yes. All Insider Threat Hub teams are made up of the same type of personnel and the same number of people.
- ○ No. All Insider Threat Hub teams are made up of the same types of personnel; however, the number of people on the Hub will vary.
- ○ No. There are best practices that dictate who should be included on the Hub. However, the size and complexity of the organization will determine the makeup of the Hub.
- ○ No. The number of people on the Hub is the same; however, the type of personnel will vary.

Knowledge Check – 3

> *Claire: There appears to be a lot of resources and policies pertaining to the Insider Threat Program. If I need to determine the requirements for establishing a program, what document should I refer to?*

If I need to determine the requirements for establishing a DOD insider threat program, what document should I refer to?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

- ○ DODI 5205.83
- ○ DODD 5205.16
- ○ 32 CFR Part 117

Conclusion

Day 1 Score

Claire: Congratulations on completing Day 1 of the challenge! Have you gotten my support?

Note: In the Appendix A: Answer Key, indicate any points earned for each Knowledge Check question.

Lesson 3: Insider Threat Hub Operations

Introduction

Lesson Overview

Yesterday you explained the functions and requirements of an Insider Threat Hub to Claire. But there is more information you will need to share to get her on board. Specifically, she will need to understand the requirements for establishing an Insider Threat Hub and how to implement insider threat strategies.

According to your calendar, it looks like you have a follow up meeting with Claire this afternoon to discuss these specific items. You will need to take some time to prepare for this meeting.

Requirements for Establishing a Hub

Requirements

If the organization is new to the Insider Threat program, establishing an Insider Threat Hub will be one of the first actions taken. The responsibility for establishing a Hub belongs to the Insider Threat Senior Official and/or Program Manager. However, the entire team will be involved as the program's policy and procedures are developed. There are seven components to establishing an Insider Threat Hub.

1. Identify Program Office

The first item on the list is to identify the program office. What really needs to be determined is how the team will be structured and where it will be located. Does your organization have the ability to house the team in a single location? Or, are the team members geographically separated and reliant on virtual communications to conduct operations? This, of course, depends on how the organization is structured and what works best for the team.

2. Staffing and Resources

Staffing and resources are the second item on the list. An organization selects the Insider Threat Program Senior Leader or official. In some cases, this person may also serve as the Hub Program Manager that oversees day-to-day operations. They will work with the organization's senior leadership to determine resource and staffing needs.

Once established, it is the Hub Program Manager's responsibility to train, exercise, and equip the Hub team with the knowledge, skills, abilities, and resources to conduct counter-insider threat duties. The National Insider Threat Policy and Minimum Standards identify the minimum training requirements for federal Insider Threat Program personnel. The NISPOM rule identifies these requirements for industry programs.

3. Establish Organization Rules and Policy

Looks like you have a message. Take a moment to review the message.

Message
Claire: Hello – I just read a news story about the after effects of a security program's failure to remove a problematic employee because the security official did not document and report several incidents. How would one account for policy violations? Or address the workforce at large? What if you are unavailable -- how will the program remain effective? You: Hello, Claire. Thank you for the questions. I am more than happy to elaborate on program efficiency and continuity in our next meeting. Claire: 

Now, continue to review the seven components to establishing an Insider Threat Hub.

The third item on the list is to establish organization rules for how the Hub operates within the organization and how it coordinates its activities within the organization. These rules and policies will be specific to your organization. National, DOD, and industry policies and guidance can only go so far. Every agency or organization will have functions and activities that are specific to them. It is up to the Hub team to develop policy and procedures that meet the minimum standards and are detailed enough to be effective for their organization.

4. Institute Consequence for Established Rule/Policy Violations

As part of rule and policy development, the Hub team must also identify consequences for violations of internal rules committed by Hub team members. Insider Threat team members must maintain standards of professional conduct like any other personnel. However, because you're dealing with extremely sensitive information it's important that you clarify these responsibilities up front.

5. Continuity of Operations Planning

As a best practice, you may want to establish a continuity of operations plan (COOP). This plan will lay out your team's strategies for continuing the program's operations in the event of disruptions related to natural disasters, terror attacks, cyber-attacks, or equipment failures.

FEMA has developed a useful template for these types of plans. When your team is ready to start building this plan, you can start with the template or develop your own. You can access this template in the Course Resources, as needed.

6. Communicate Program Requirements to Staff and Contractors

Once the training is complete, policies are in place, and plans are established, the team needs to ensure that all Insider Threat Program personnel are trained to prevent, deter, detect, mitigate, and respond to insider threats. Insider Threat Program personnel must be able to appropriately respond to incident reporting, protect privacy and civil liberties, support mitigation options, and refer matters as required.

7. Conduct Internal Spot Checks

Once the staff is aware of the requirements, you must ensure policies and procedures are being followed by conducting self-assessments. Self-assessments help you determine whether your program is meeting requirements and operating effectively. This information can guide performance measures that lead to more efficient and effective programs.

You've Got Email

Looks like you've got an email! Take a moment to review the email from Claire.

Email
To: Program Manager From: Claire Subject: Setting up the Hub I'm reviewing my notes from yesterday's meeting and I realize we didn't discuss what needs to take place to set up the Hub. I just received a call from my leadership asking for this information. If we were to establish an Insider Threat Hub at our organization, what would be one of the first things we would need to do once the hub is established? Claire

Knowledge Check – 1

If we were to establish an Insider Threat Hub at our organization, what would be one of the first things we would need to do once the hub is established?

Select the best response; then check your answer in the Answer Key at the end of this Student Guide.

- ○ We would communicate the program requirements to the staff and contractors.
- ○ We would identify consequences for violations of internal rules committed by hub team members.
- ○ We would identify the program office.
- ○ We would determine resources and staffing needs for the hub.

Implementing Insider Threat Operations

Implementing Insider Threat Operations – Overview

Now let's get back to work and prepare for this afternoon's meeting with Claire. The purpose of the Insider Threat Program is to proactively prevent, deter, detect, and mitigate threats associated with trusted insiders. These actions make up the daily operations of your Insider Threat Hub. Let's look at each of these individually.

Prevent

Prevent is one of the actions that make up the daily operations of your Insider Threat Hub. Preparing leadership and following general best practices are just two key components of prevention.

Preparing Leadership

Prevention of insider threat actions typically is enabled by ensuring leaders are aware of the current threat landscape, including pertinent insider threat information, activities, and behaviors. This is supported by providing reports and recommendations for threat management and ensuring the workforce understands available resources. Prevention activities complement deterrence.

Insider threat professionals must be able to understand risk perception, communicate risk to organizational leaders, and leverage risk and crisis communications principles. While every situation is unique, ensuring leadership is aware of indicators of a re-emergent concern is key to preventing threats.

For more information on risk communication consider reviewing, "The Art and Science of Being Heard: A Risk Communication Playbook for Insider Threat Professionals," developed by the Defense Personnel and Security Research Center (PERSEREC).

General Best Practices for Prevention

As a best practice, pace the decision-making process. If there is not an imminent physical threat, then reconsider taking immediate action and allow more time to evaluate options before making a final decision.

In addition, avoid judgment. Offer guidance based upon current circumstances and where the leader wants to be in the future. Focusing on how the leader could have avoided the present situation is not productive for insider threat strategy.

Finally, facts matter. Discuss the facts of an incident, to include any unknowns, and explain how the facts contributed to both assessment and recommendations.

Deter

Deterrence efforts are designed to prevent insider threats from manifesting in the first place. Deterrence occurs through strategic communications, ensuring personnel are aware of punitive actions that potential offenders may face, and promoting a security posture that detects malicious insider threats. These deterrents support detection. Deterrence programs are more than just general awareness. They should take into account multiple facets of your organization and Hub activities.

Integrate Personnel Security

Integrating personnel security is a great first step in deterring insider threats. Building a good working relationship with the personnel security team is vital. They can help the Hub team understand pre-employment vetting activities and define their role in mitigating risk prior to human capital or human resources on-boarding personnel.

Train/Exercise the Workforce

You must train and exercise the organization's workforce. Covered employees must complete initial and annual Insider Threat Awareness training.

You may also be responsible for maintaining workforce awareness of insider threats and employee reporting responsibilities. As an aid, CDSE has instituted a year-round vigilance campaign.

Lastly, you will conduct internal evaluations. These are small exercises used to test your workforce's knowledge of insider threat indicators and reporting requirements. These exercises do not have to be elaborate but should help you gauge the effectiveness of your program. You may use information from these evaluations to adjust your training and awareness program to ensure effectiveness.

Develop "Normal Activity" Baseline and Institute Internal/Security Controls

Having a day-to-day operating baseline will make deviations or anomalies stand out from normal activities. It will also help determine what your user activity monitoring triggers should be.

Once a "Normal Activity" baseline is established, internal and security controls help us identify deviations from the baseline. For example, user activity monitoring could help identify a rash of IT system misuses that may suggest an employee needs some re-training. Another example would be access control logs indicating an employee is working irregular hours or has unexplained absences from work. You would want to look into this further. Internal and security controls can help identify important risk factors.

Encourage Reporting

Individuals should be encouraged to report on issues they may have or the actions of others. One of the goals of an Insider Threat Hub is to deter adverse actions by pointing those asking for assistance to resources that can help them. The challenge is to have people see the Insider Threat Program as a resource rather than a punitive element.

You can build this rapport by informing the workforce of your program, the mission, and its goals; by respecting privacy and civil liberties, and by deploying appropriate insider threat mitigation responses.

Your program must establish reporting procedures for the general workforce. Those that witness potential indicators should know exactly, when, where, and how they can report the information.

Prepare procedures for "walk-ins" or those that may want to report their information face to face. Procedures should also include hotlines or dedicated email addresses.

Finally, your Hub must consider the concept of organizational justice. Organizational justice refers to employee perceptions of fairness in the workplace. Labor relations can have an overall effect on the number of insider threat incidents you see.

The worse the labor relations are, the more incidents you may encounter. Counterproductive workplace environments have consequences that can lead to disgruntlement. Organizational leadership that develops a positive workplace environment keeps the workforce engaged and productive.

This same concept applies to the Insider Threat Program. Ensuring appropriate mitigation response options and the protection of privacy and civil liberties in the conduct of your duties will minimize negative outcomes from maladaptive responses. Being responsive to workforce concerns is a great way to build rapport with personnel; encourage future reporting; and ultimately mitigate risk.

Detect

Insider threat detection is another essential daily Insider Threat Hub Operation activity.

Ensure Cross-Function Coordination

Cross function coordination is the key to effective detection. You must determine who will lead the team; how the team will communicate; and how the team will integrate contributors who are not part of the organization's Insider Threat Program. The team must decide the role that each of these external partners will play. For example, they may serve as a reviewer of the team's work, or a consultant that is used on an as-needed basis.

Monitor Activity

User Activity Monitoring (UAM) is the technical capability to observe and record the actions and activities of an individual operating on your computer networks, in order to detect potential risk indicators and to support mitigation responses.

For additional information on developing UAM, refer to the Insider Threat Indicators in User Activity Monitoring Job Aid in the Course Resources.

Perform Risk-based Analytics

Risk based analytics allow Insider Threat Hubs to manage risk in complex threat environments. The process of identifying assets, assessing threats and vulnerabilities, evaluating risk, and identifying countermeasures can help determine the risks most closely associated with trusted insiders and the best methods to deter and mitigate them.

It also allows your organization to differentiate between exigent threats to your enterprise and less pressing matters. Exigent threats, such as those related to interpersonal violence, can be managed by utilizing a structured professional judgement (SPJ) approach. This approach is an analytical method used to understand and mitigate risk posed by individuals that is discretionary, but reliant on evidence-based guidelines to formalize the exercise of discretion. Data-driven SPJ tools include a set of validated risk factors that when combined result in a risk category of high, medium, or low.

For more information on SPJ tools, consider reviewing "Structured Professional Judgment Tools: A Reference Guide for Counter Insider Threat Hubs," developed by PERSEREC.

Gather, Integrate, Review, Assess, and Respond to Indicators

Your Hub will need to gather, integrate, review, assess, and respond to threat indicators. To do that, you need to establish data collection protocols. Indicators provide a gauge to measure the state of a situation.

To be effective, indicators must meet several criteria. First, they should be observable, from a reliable source, and be gathered in accordance with laws and regulations. Next, indicators should be valid, reliable, relevant, and considered in context. Insider Threat Programs must use consistent data collection methods, or the data will be unreliable.

All data collection protocols must be developed in coordination with legal counsel and any applicable systems of records notice. Prohibited actions must be clearly identified to ensure that you protect the privacy and civil liberties of the workforce in the conduct of your duties. This clarity can also prevent Insider Threat team members from inadvertently overstepping their bounds.

Create Auditable Records of Actions Taken

The actions performed by your program may come under scrutiny and having a clear record of program actions may protect you and your organization from legal repercussions and help external agencies when you refer incidents. They also help ensure you follow the established guidelines and identify criteria that need to be adjusted. For instance, you may review a memorandum of action and discover one of your threat indicator triggers are not set properly and needs to be adjusted.

Please check out the Insider Threat Program Memorandum of Activity template located in the Course Resources. It may be helpful when developing your record keeping methods.

Share Information as Appropriate

Responsible information sharing is critical to the success of your program. Developing protocols – such as when to report or refer matters, approved methods for information transmittal, and the identification of authorized recipients – is an essential function of the program and one that will require close coordination with your legal team.

No matter how your Hub decides to do this, you must ensure that you consider the privacy and civil liberties of your employees as part of your processes and practices.

Mitigate

To be effective, Insider Threat Programs must be on the lookout for potential issues before they pose a threat, have a risk assessment process in place, address identified issues adequately, and take actions that minimize risk while avoiding those that escalate risk.

In most cases, proactive mitigation responses provide positive outcomes for both the organization and the individual. This allows you to protect information, facilities, and personnel, retain valuable employees, and offer intervention to help alleviate the individual's stressors.

Conduct Hub Team Case Review

Developing a case review process will help your Hub review incidents and conduct analysis on insider threat matters. The case review process includes:

- Receiving the report,
- Reviewing and gathering additional information,
- Assessing the situation, and
- Responding to the situation.

Determine and Implement Appropriate Response

Your Hub's responses are situationally dependent but may include recommendations such as:

- Suspending access to information.
- Taking personnel actions such as counseling, referral, or termination.
- Organizational responses that may require changes to policy or procedures.
- Increased or additional training.

Produce Insider Threat Incident Outcome Report

Your Hub should create a record of the incident outcome. There is no standard form for this, so you could incorporate this information in your Records of Actions form or create a new format. You may also create or coordinate with other elements to develop a "Damage Assessment" or "After Action Report" that explains the damage to national security, personnel, facilities, or other resources.

The Hub will need to work with the legal team and any other contributing elements to ensure the report is stored and retained appropriately.

Execute Insider Threat Incident Report Referral Actions

Once your report is complete, or sometime while you are working on it, you may need to execute referral actions. The Insider Threat Hub may refer the matter internally to its agency's security office, cybersecurity, or human resources for action to mitigate risks. It may also be referred elsewhere in the agency, if appropriate.

Human Resource and mental health team members can assist with counseling referrals or prescribed human resource interventions which may be corrective in nature. They deal with Employee Assistance Programs for resources in financial counseling, lending programs, mental health, and other well-being programs.

Hub members from the various security disciplines, whether cyber, personnel, information, or physical, can assist with mitigation response options such as updating security protocols, adjusting UAM or other inspections, and providing basic security training and awareness to the workforce.

Some insider threat incidents may warrant external referrals to counterintelligence or law enforcement authorities. For DOD component insider threats, this includes referral of certain threshold level events to the DITMAC.

Not all incidents will meet reporting thresholds or result in an arrest. However, you must still work with the referral agency and your organization's legal counsel to ensure that any information gathered during the incident is handled properly in case it is determined to be evidence in subsequent actions.

Meeting with Senior Leadership

Knowledge Check – 2

Now that you are up to speed with the requirements for establishing an Insider Threat Hub, you now need to prepare a short brief to provide to Claire prior to your meeting this afternoon.

Which of the following statements are true about the requirements for establishing an Insider Threat Hub and should be shared with Claire prior to your meeting?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ We will need to work together to determine resources and staffing needs for the hub. As the Hub Program Manager, I can take the lead to train the team to conduct counter-insider threat duties.
- ☐ For operating the hub, we will need to implement rules and policies from National, DOD, and industry policies and procedures. We do not need to include policies specific to our organization.
- ☐ As a best practice, our Hub team will need to establish a continuity of operations plan. Our team can use a template when we start building this plan.
- ☐ We must perform self-assessments to help determine whether our program is meeting requirements and operating effectively.

Knowledge Check – 3

It's 3:00; time to meet with Claire to answer any questions she has on applying requirements for establishing an Insider Threat Hub and implementing insider threat strategies.

Claire: I received the brief you emailed me earlier today. It was helpful to understand the requirements for establishing an Insider Threat Hub. I still have a couple of questions though. Can you give me examples of some actions that make up the daily operations of the Insider Threat Hub?

Can you give me examples of some actions that make up the daily operations of the Insider Threat Hub?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Detect insider threat actions by using User Activity Monitoring to observe and record the actions and activities of an individual operating on your computer networks.

- ☐ Manage insider threat actions by being transparent on all the specific details on how systems/people are being monitored.
- ☐ Mitigate insider threat actions by developing a case review process that will help your Hub review incidents and conduct analysis on insider threat matters.
- ☐ Prevent insider threat actions by ensuring leaders are aware of the current threat landscape including pertinent insider threat information, activities, and behaviors.

Knowledge Check – 4

Claire: What about deterrence? What are some of the activities our Insider Threat Hub team will need to do if we want to deter threats associated with trusted insiders?

What are some of the activities our Insider Threat Hub team will need to do if we want to deter threats associated with trusted insiders?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Our team will need to produce insider threat incident outcome reports.
- ☐ Our team will need to ensure personnel are aware of punitive actions that potential offenders may face.
- ☐ Our team will need to promote a security posture that detects malicious insider threats.
- ☐ Our team will need to encourage individuals to report on issues they may have or the actions of others.

Conclusion

Day 2 Score

Claire: Congratulations on completing Day 2 of the challenge! Have you gotten my support?

Note: In the Appendix A: Answer Key, indicate any points earned for each Knowledge Check question.

Lesson 4: Insider Threat Hub Management Protocols

Introduction

Agenda for the Day

This week you explained to Claire the functions and requirements of an Insider Threat Hub, the requirements for establishing an Insider Threat Hub, as well as strategies for implementing insider threat hub operations.

Today's focus is to educate Claire on applying the Insider Threat Hub management protocols and hopefully gain her support. These protocols are in place to ensure your Insider Theat Hub is ready to handle situations when they arise.

After viewing the calendar for the day it appears you have one more day to get Claire's buy in to the Insider Threat Hub. You will need to take some time to prepare for this afternoon's meeting.

Management Protocols

Overview

So, what protocols should you have in place to ensure your Insider Threat Hub can respond quickly and consistently? It would be nearly impossible to write a protocol for every situation that you could encounter as a Hub member. However, you should standardize some procedures to ensure the members of the Insider Threat team are not reinventing the wheel each time those situations arise. Some of the basic protocols to consider developing for your Hub include procedures for:

- Tracking and implementing policy;
- Formal and informal agreements;
- Developing Standard Operating Procedures (SOPs);
- Integrating the program into the organizational mission; and
- A program evaluation plan.

These topics are addressed in more detail in the CDSE course: Preserving Investigative and Operational Viability.

Protocol 1 – Tracking and Implementing Policy

You've got email! Take a moment to review the email about Protocol 1 – Tracking and Implementing Policy.

Email
To: Program Manager From: Daily Insider Threat Hub Tips

Subject: Protocol 1 - Tracking and Implementing Policy

All Insider Threat Hubs should have something in writing designating responsibility for keeping up to date with policy changes. Follow policy releases, updates, and modifications to incorporate new requirements and ensure you are always acting under proper legal authority.

Stay up to date with the policy issuers.

- Many policy issuers offer email services that notify you when they post policy updates.
- Regularly check policy issuers websites for updates. Refer to the:
  - Defense Counterintelligence and Security Agency for industry programs.
  - Defense Technical Information Center for DOD programs.
  - National Insider Threat Task Force for Federal Programs.

Access CDSE Insider Threat Toolkit, working groups, and forums.

- The CDSE's Insider Threat Toolkit also lists the latest policies.
- Can refer to your colleagues and working groups for tracking policy issuances.
- Stay connected to the larger community and attend Insider Threat working groups or forums.

Engage your legal team when new releases are issued.

- Anytime you receive new policy information, you need to run it past your Hub's legal team. The legal team must be aware of any changes to policy, so they can assess possible implications for your program.

You've Got Email

You've got email! Take a moment to review the email from Claire.

Email
To: Program Manager From: Claire (Senior Executive) Subject: Staying up to date As a team, I'm sure there are always new policies coming out all the time to improve Insider Threat Hubs. What can the team do to stay up-to-date with the new policies that are released? Claire

Knowledge Check 1

As a team, I'm sure there are always new policies coming out all the time to improve Insider Threat Hubs. What can the team do to stay up-to-date with new policies that are released?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Team members can check social media for updates to important policies.
- ☐ Team members can access the CDSE Insider Threat Toolkit that will list the latest policies.
- ☐ Team members can regularly check policy issuers websites for updates.
- ☐ Team members can see if the policy issuers offer email services that notify you when they post policy updates.

Protocol 2 – Formal and Informal Agreements

Let's take a look at the second management protocol.

Developing protocols for formal and informal agreements is critical to the success of your Insider Threat Program. These agreements lay the groundwork for conducting business with internal and external organizational elements your Hub will need to work with. They include Law Enforcement (LE) and Counterintelligence (CI).

Coordinate with your legal team when developing relationships with these outside agencies. Some laws, policies, and directives require an Insider Threat Hub to refer certain insider threat matters to external CI and/or LE entities. Your legal team's expertise and assistance will be necessary to develop your policy, procedures, and agreements.

Industry programs under 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM Rule) may be required to inform their senior leadership and/or consult with Defense Counterintelligence and Security Agency (DCSA) for guidance on any further actions. Planning this coordination in advance can make for a more effective incident response and mitigation. Ensure that you have a communication method for your internal leadership as well as your DCSA Industrial Security Representative and/or CI Special Agent.

Insider threat matters that require referral to LE and/or CI include:

- Threats and acts of violence,
- Loss or compromise of classified information,
- Physical or cyber breaches,
- Foreign intelligence entity activity, and
- Criminal activity.

It's important to remember that most incidents handled by your program will not result in the apprehension of a spy or even identify someone committing a crime. The main goal of the program is to detect potential risk indicators, determine whether a threat exists, and if so, mitigate it appropriately.

You've Got Email

You've got email! Take a moment to review the email from Claire.

Email
To: Program Manager From: Claire (Senior Executive) Subject: Conducting Business with Organizational Elements I imagine that there will need to be protocols in place indicating how and when to conduct business with internal and external organizational elements such as Law Enforcement and Counterintelligence. Are there certain insider threat matters that require referral to law enforcement and counterintelligence?

Claire

Knowledge Check 2

Are there certain insider threat matters that require referral to law enforcement and counterintelligence?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Threats or acts of violence
- ☐ Loss or compromise of classified information
- ☐ Disagreement between two employees
- ☐ Criminal activity

Protocol 3 – Developing Standard Operating Procedures Overview

Now let's focus on Protocol 3 – Developing Standard Operating Procedures.

Insider Threat Hubs can handle most matters internally, but some incidents require reporting and referral actions that may result in law enforcement or counterintelligence investigations, inquiries, operations, and/or legal proceedings.

Your actions can affect the outcome of cases. Develop your internal policies, procedures, and authorities in a way that ensures your activities do not produce negative impacts on cases. All Insider Threat Hub team members should understand how to preserve investigative and operational viability.

There are four best practices for developing SOPs for the Insider Threat Hubs:

- Communication plan
- Non-alerting protocol
- Reporting and referral timelines
- Handling and seizure of information of potential evidentiary value

Protocol 3 – Developing Standard Operating Procedures

Communication Plan

Develop a communications plan that describes the protocol for discussing insider threat matters with the media and other external elements. Your Insider Threat Program Manager will work with the public affairs office and legal counsel to develop your communications plan and establish guidelines for what information is releasable to the public and by whom.

Follow the guidance provided by the communications plan and your public affairs office. The things you say may have far-reaching impacts on potential operations or investigations, individuals, and ultimately the effectiveness of Insider Threat Hub Operations.

Non-alerting Protocol

Take steps to avoid alerting subjects of a potential inquiry, investigation, or operation whenever your program conducts its internal situational assessment. Insider Threat Hub protocols should determine how and when you limit or prohibit interviews of subjects or checks of certain data sets that have alert capabilities.

Also, consider incorporating non-alerting protocols that may limit the Hub's internal distribution of information. A non-alerting protocol limits the number of program personnel who have knowledge of the most sensitive matters.

Reporting and Referral Timelines

Delayed reporting or failure to make timely referrals may increase your organization's insider threat risk. Delayed reporting or referral may negatively impact investigations, inquiries, or operations carried out by CI or LE. Significant time lapses between suspected activities may impede the ability to successfully investigate or prosecute wrongdoing. You can mitigate that risk by incorporating timelines for reporting and referrals in SOPs. That's why it's important to work with your General Counsel to determine the best course of action during each referral process.

Handling and Seizure of Information of Potential Evidentiary Value

There may be rare instances when the Program must take possession of and/or transmit physical or digital information of potential evidentiary value associated with a potential insider threat. While Insider Threat Hubs do not conduct investigations, your program's standard operating procedures should include provisions for proper handling and documentation of any items seized in the course of your actions that may have evidentiary value. Your Hub's legal team can tell you, there are many legal rules to follow when seizing, handling, and storing information.

When developing procedures involving information with potential evidentiary value, it's a best practice to coordinate with the Inspector General and/or your General Counsel.

Voicemail

Before learning about the next protocol, you notice you have a voice mail on your cell phone.

"Hey, I was in a meeting this morning with Claire, and she voiced some doubts about establishing Insider Threat Program Standard Operating Procedures. I know you have been meeting with her this week and just wanted to give you a heads up."

Knowledge Check 3

To address Claire's concerns, you decide to send her an email.

You start by explaining that the Hub's actions, or inactions, can affect the outcome of cases. It is important to develop internal policies, procedures, and authorities in a way that ensures your activities do not produce negative impacts on cases. You finish the email by sharing some best practices.

Which of the following are best practices for establishing Insider Threat Program Standard Operating Procedures that you should share with Claire?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Develop a communication plan that describes the protocol for discussing insider threat matters with the media and other external elements.
- ☐ Determine appropriate response when mitigating insider threats.
- ☐ Determine how and when you limit or prohibit interviews of subjects or checks of certain data sets that have alert capabilities.
- ☐ Incorporate timelines for reporting and referrals.

Protocol 4 – Integrating the Program into the Organizational Mission

Time to get back to work. You've got email! Take a moment to review the email about Protocol 4 – Integrating the Program into the Organizational Mission.

Email
To: Program Manager From: Insider Threat Hub Tips Subject: Protocol 4 – Integrating the Program into the Organizational Mission Insider Threat Hub operations require integration within your organization to succeed. The Program Manager must work with the organizational leadership to ensure the program has top-down support. However, the entire team needs to advocate for the program. Highlighting the Insider Threat Hub's role in mission assurance and risk management can engender support needed from the entire organization. This requires Insider Threat Hub team members to adopt a cohesive message. Help team members deliver the same message by putting together talking points that explain the program's role. Participate in internal working groups and meetings to understand changes in the organization that may affect your ability to deter, prevent, detect, and or mitigate a threat. Organizational activities that may increase the risk of an insider threat incident include hiring waves, layoffs, pay freezes, deployments, new computer software/systems, new security protocols, and program funding issues.

You've Got a Message

Looks like you have a message from your supervisor. Take a moment to review the message.

Message
Supervisor: I received a message from Claire today. She mentioned that you two met the last two days about the Hub and she is questioning whether you both need to meet this afternoon. What should I tell her? *You: Yes, we have a meeting this afternoon. We are going to discuss how to apply the Insider Threat Hub management protocols. These are in place to ensure the Hub is ready to handle situations when they arise. It's important that she is aware of these protocols.*

Supervisor: Sounds good! I'll let her know.

Knowledge Check 4

Fortunately, you were able to provide input to your supervisor explaining the importance of your meeting today with Claire; however, you recognize that you will need to work with the organizational leadership to ensure the program has top-down support. This underscores the importance of integrating the program into the organizational mission.

What can you and your team do to integrate the program into the organizational mission?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Keep up to date with policy changes pertaining to insider threats.
- ☐ Adopt a cohesive message and provide talking points to the team that explain the program's role.
- ☐ Participate in internal working groups and meetings to understand changes in the organization that may affect ability to handle threats.
- ☐ Be in the know of organizational activities that may increase the risk of insider threats.

Protocol 5 – Program Evaluation Plan – Internal Audits

There is one more management protocol that you need to be prepared to discuss with Claire: Protocol 5 – Program Evaluation Plan. Though they vary slightly, all insider threat policies require that you perform self-assessments of compliance with insider threat policies and standards.

To meet that requirement, you need to develop an Insider Threat Program Evaluation Plan. A good program evaluation plan helps your program focus on meeting the requirements applicable to your organization and promotes continuous improvement.

Do this by evaluating the program's plan, policies, procedures, and metrics. Metrics can document everything from the number of general workforce personnel training on insider threat awareness, the number of reports or indicators received, the number of incidents handled or mitigated, or the number of external referrals. These metrics help you both evaluate the effectiveness of Hub operations and advocate for resources to ensure the success of your program.

Listed below are some policy documents to help you learn more about internal audits of evaluation plans.

National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

These are the general responsibilities of departments and agencies. Take a moment to review.

B. General Responsibilities of Departments and Agencies

7) Perform self-assessment of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee.

DODD 5205.16

Take a moment to review part of Enclosure 2 of this document.

Enclosure 2

For DOD components and federal agencies, program self-assessments must be completed in accordance with National Minimum Standards and other appropriate policy and memoranda. DOD components can work with the DOD Insider Threat Enterprise Program Management Office for specific guidance. Federal programs should contact the National Insider Threat Task Force for additional information.

32 CFR Part 117

Take a moment to review information on contractor reviews in this document.

117.7 Procedures

(2) Contractor Reviews - Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.

(i) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the Insider Threat Program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable.

(ii) The contractor will prepare a formal report describing the self-inspection, its findings, and its resolution of issues discovered during the self-inspection. The contractor will retain the formal report for CSA review until after the next CSA security review is completed.

(iii) The SMO at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.

Resource: You can find more information on Pages 11-21 of the Self-Inspection Handbook for NISP Contractors (dcsa.mil) located in the Course Resources.

Protocol 5 – Program Evaluation Plan – External Audits and Auditable Records

Now, let's change the focus from internal audits to external audits and auditable records.

You've got email! Take a moment to review the email about the importance of external audits and auditable records.

Email
To: Program Manager From: Insider Threat Hub Tips Subject: External Audits and Auditable Records Self-inspections help you identify and correct program issues. Staying current is important because processes, policy, and guidance are subject to change. In addition, the government retains some level of oversight to ensure Insider Threat Programs keep up with the latest insider threat requirements. External audits verify that your program maintains its effectiveness. It is in your best interest to cooperate with and facilitate these audits to ensure that your program meets all the requirements and acquires assistance in areas where the program is lacking.

Claire may also have some questions this afternoon on external audits and auditable records. Take a few minutes to prepare.

Creating and Maintaining Auditable Records

One of the best ways to prepare for external audits is to create and maintain auditable records of your actions. Work with your legal team to ensure that these items are created, stored, and retained in accordance with privacy and civil liberties regulations.

Keeping good program records has several other benefits for your program as well. They become a consolidated repository of data used to measure the effectiveness of your program. This information can be used to:

- Demonstrate compliance with Insider Threat Policy,
- Develop metrics,
- Gain top-down support from your organization,
- Help with risk management by identifying areas at risk, and
- Help justify funding for your program.

Program Evaluation Tools

No specific format has been identified for program evaluation. Depending on your organization, you may be able to utilize resources from the DOD, National Insider Threat Task Force (NITTF) or DCSA.

One such tool is the Defense Personnel and Security Research Center (PERSEREC) Insider Risk Evaluation and Audit Tool. While developed for DOD, it can be applied to most organizations and helps to gauge relative vulnerability to insider threats and adverse behavior.

DOD Insider Threat Programs may also have access to the Enterprise Program Risk Management (EPRM) tool. Contact the DITMAC Enterprise Program Management Office to learn more.

Best Practices

While meeting the minimum standards and policy requirements are essential, truly effective programs also incorporate the lessons of past program best practices and lessons learned.

Best practices include:

- Staying connected with the larger insider threat community to ensure that you are aware of the latest best practices. (You can consult with DCSA, DOD, or NITTF depending on your type of organization.)
- Joining working groups and staying up to date with the latest research and publications;
- Consulting with your legal team before implementing new practices, to ensure that they are within your authority and are appropriate relative to privacy or civil liberties concerns;
- Engaging with executive leadership so they understand, advocate for your program, and determine when and how significant activities should be reported to senior management in advance;
- Appropriately sharing insider threat information, both internally and externally, when warranted or required; and
- Working with your Public Affairs office prior to disseminating information about the program, its activities, awareness efforts, or training materials developed by the program.

Meeting with Senior Leadership

Now that you are up to speed with the Insider Threat Hub management protocols, you now need to prepare a short brief to provide to Claire prior to your meeting this afternoon.

Knowledge Check 5

Which of the following statements are true about establishing an Insider Threat Program Evaluation Plan, specifically internal audits, and should be shared with Claire prior to your meeting?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ All insider threat policies require that you perform self-assessments of compliance with insider threat policies and standards.
- ☐ Program evaluation plan helps the program focus on meeting the requirements applicable to the organization.
- ☐ Program evaluation includes evaluating the program's plan, policies, procedures, and metrics.
- ☐ Program evaluation is conducted by the team on a bi-monthly basis.

Knowledge Check 6

It's time for your meeting with Claire. You have one more opportunity to meet with her and answer any remaining questions she may have on the Insider Threat Hub. Good luck on your last meeting!

Claire: I do have a couple more questions I was hoping you could answer. Specifically having to do with the Insider Threat Program Evaluation Plan. It sounds like preparing for the evaluation plan is key. What does the team need to do to create and maintain auditable records in preparation for an external audit of the Hub's evaluation plan?

What does the team need to do to create and maintain auditable records in preparation for an external audit of the Hub's evaluation plan?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ The team needs to prepare for external audits by creating and maintaining auditable records of its actions.
- ☐ The team doesn't need to do anything since this is an external audit conducted by resources outside of the team.
- ☐ The team needs to work with the legal team to ensure items are created, stored, and retained in accordance with privacy and civil liberties regulations.
- ☐ The team needs to keep program records that can be used to measure the effectiveness of the program.

Knowledge Check 7

Claire: So, if we continue to move forward and implement the Insider Threat Hub at our facility, are there some best practices that we should implement as it relates to the evaluation plan?

So, if we continue to move forward and implement the Insider Threat Hub at our facility, are there some best practices that we should implement as it relates to the evaluation plan?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Stay connected with the larger insider threat community to keep up to date with the latest best practices.
- ☐ Consult with legal team before implementing new practices to ensure they are within your authority.
- ☐ Share insider threat information with subjects of a potential inquiry when requested.
- ☐ Join working groups and stay up-to-date with latest research and publications.

Conclusion

Day 3 Score

Claire: You've completed the final day of the challenge! How did you do?

Note: In the Appendix A: Answer Key, indicate any points earned for each Knowledge Check question. Once complete, add up your points to determine your final score.

Lesson 5: Course Conclusion

Course Conclusion

Challenge Results

Claire: Congratulations on completing the challenge!

Do you have my support? Did you score 9-14 points? If so, I am ready to move forward and support the Insider Threat Hub? I am on board.

Or did you score 1-8 points? If so, I'm afraid I may require more convincing before I can put my support behind it?

If Claire needs more convincing, and you would like to improve your score, you may go back and complete the challenge again.

Course Review

Here is a list of lessons in the course:

- Lesson 1: Course Introduction
- Lesson 2: Functions and Requirements of an Insider Threat Hub
- Lesson 3: Insider Threat Hub Operations
- Lesson 4: Insider Threat Hub Management Protocols
- Lesson 5: Course Conclusion

Lesson Summary

Congratulations. You have completed the Insider Threat Basic Hub Operations course.

You should now be able to perform all of the listed activities:

- Explain the role and purpose of an Insider Threat Program and Hub.
- Given a scenario, apply the principles of Insider Threat Hub operations.
- Given a scenario, apply Insider Threat Hub management protocols.

To receive course credit, you must take the Insider Threat Basic Hub Operations examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check – 1

Which of the following statements are true about Insider Threat Hubs and should be shared with Claire prior to your meeting?

- ☑ Insider Threat Hubs implement proactive strategies to help identify and resolve issues before an insider threat becomes a reality. (correct response)
- ☑ Insider Threat Hubs implement strategies to help prevent, deter, detect, and mitigate insider threats. (correct response)
- ☑ Insider Threat Hubs are required to report information about actual or potential insider threats. (correct response)
- ☐ Insider Threat Hubs are created to prevent, deter, detect, and mitigate actions by external threats.

Feedback: *Insider Threat Hubs implement proactive strategies that help prevent, deter, detect, and mitigate insider threats. These hubs are required to report information about actual or potential insider threats.*

Points Earned (0 for incorrect and 1 for correct): _____

Knowledge Check – 2

Does every Insider Threat Hub team include the same positions and the same number of people?

- ○ Yes. All Insider Threat Hub teams are made up of the same type of personnel and the same number of people.
- ○ No. All Insider Threat Hub teams are made up of the same types of personnel; however, the number of people on the Hub will vary.
- ⦿ No. There are best practices that dictate who should be included on the Hub. However, the size and complexity of the organization will determine the makeup of the Hub. (correct response)
- ○ No. The number of people on the Hub is the same; however, the type of personnel will vary.

Feedback*: There are best practices that dictate who should be included on the Hub. However, the size and complexity of the organization will determine the makeup of the Hub.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check – 3

If I need to determine the requirements for establishing a DOD insider threat program, what document should I refer to?

- ○ DODI 5205.83
- ⦿ DODD 5205.16 (correct response)
- ○ 32 CFR Part 117

***Feedback**: You will refer to DODD 5205.16, The DOD Insider Threat Program, if you need to determine the requirements for establishing one.*

Points (0 for incorrect and 1 for correct): _____

Lesson 3 Review Activities

Knowledge Check – 1

If we were to establish an Insider Threat Hub at our organization, what would be one of the first things we would need to do once the hub is established?

- ○ We would communicate the program requirements to the staff and contractors.
- ○ We would identify consequences for violations of internal rules committed by hub team members.
- ⦿ We would identify the program office. (correct response)
- ○ We would determine resources and staffing needs for the hub.

***Feedback**: Identifying the program office is one of the first things you would need to do once the hub is established.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check – 2

Which of the following statements are true about the requirements for establishing an Insider Threat Hub and should be shared with Claire prior to your meeting?

- ☑ We will need to work together to determine resources and staffing needs for the hub. As the Hub Program Manager, I can take the lead to train the team to conduct counter-insider threat duties. (correct response)
- ☐ For operating the hub, we will need to implement rules and policies from National, DOD, and industry policies and procedures. We do not need to include policies specific to our organization.
- ☑ As a best practice, our Hub team will need to establish a continuity of operations plan. Our team can use a template when we start building this plan. (correct response)
- ☑ We must perform self-assessments to help determine whether our program is meeting requirements and operating effectively. (correct response)

***Feedback**: Requirements for establishing a Hub include determining resources and staffing needs, establishing a continuity of operations plan, and performing self-assessments.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check – 3

Can you give me examples of some actions that make up the daily operations of the Insider Threat Hub?

- ☑ Detect insider threat actions by using User Activity Monitoring to observe and record the actions and activities of an individual operating on your computer networks. (correct response)
- ☐ Manage insider threat actions by being transparent on all the specific details on how systems/people are being monitored.
- ☑ Mitigate insider threat actions by developing a case review process that will help your Hub review incidents and conduct analysis on insider threat matters. (correct response)
- ☑ Prevent insider threat actions by ensuring leaders are aware of the current threat landscape including pertinent insider threat information, activities, and behaviors. (correct response)

***Feedback**: Daily operations include detecting insider threat actions by using User Activity Monitoring to observe and record the actions and activities of an individual operating on your computer networks, mitigating insider threat actions by developing a case review process that will help your Hub review incidents and conduct analysis on insider threat matters, and preventing insider threat actions by ensuring leaders are aware of the current threat landscape.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check – 4

What are some of the activities our Insider Threat Hub team will need to do if we want to deter threats associated with trusted insiders?

- ☐ Our team will need to produce insider threat incident outcome report.
- ☑ Our team will need to ensure personnel are aware of punitive actions that potential offenders may face. (correct response)
- ☑ Our team will need to promote a security posture that detects malicious insider threats. (correct response)
- ☑ Our team will need to encourage individuals to report on issues they may have or the actions of others. (correct response)

***Feedback**: Ensuring personnel are aware of punitive actions that potential offenders may face, promoting a security posture that detects malicious insider threats, and encouraging individuals to report on issues they may have or the actions of others can all help to deter threats.*

Points (0 for incorrect and 1 for correct): _____

Lesson 4 Review Activities

Knowledge Check 1

As a team, I'm sure there are always new policies coming out all the time to improve Insider Threat Hubs. What can the team do to stay up-to-date with new policies that are released?

- ☐ Team members can check social media for updates to important policies.
- ☑ Team members can access the CDSE Insider Threat Toolkit that will list the latest policies. (correct response)
- ☑ Team members can regularly check policy issuers websites for updates. (correct response)
- ☑ Team members can see if the policy issuers offer email services that notify you when they post policy updates. (correct response)

Feedback*: Team members can access the CDSE Insider Threat Toolkit that will list the latest policies, they can regularly check policy issuers websites for updates, and they can see if the policy issuers offer email services that notify you when they post policy updates.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 2

Are there certain insider threat matters that require referral to law enforcement and counterintelligence?

- ☑ Threats or acts of violence (correct response)
- ☑ Loss or compromise of classified information (correct response)
- ☐ Disagreement between two employees
- ☑ Criminal activity (correct response)

Feedback*: Threats or acts of violence, loss or compromise of classified information, and criminal activity are insider threat matters that require referral to law enforcement and counterintelligence.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 3

Which of the following are best practices for establishing Insider Threat Program Standard Operating Procedures that you should share with Claire?

- ☑ Develop a communication plan that describes the protocol for discussing insider threat matters with the media and other external elements. (correct response)
- ☐ Determine appropriate response when mitigating insider threats.
- ☑ Determine how and when you limit or prohibit interviews of subjects or checks of certain data sets that have alert capabilities. (correct response)
- ☑ Incorporate timelines for reporting and referrals. (correct response)

***Feedback**: Best practices for establishing Insider Threat Program Standard Operating Procedures include developing a communication plan that describes the protocol for discussing insider threat matters with the media and other external elements, determining how and when you limit or prohibit interviews of subjects or checks of certain data sets that have alert capabilities, and incorporating timelines for reporting and referrals.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 4

What can you and your team do to integrate the program into the organizational mission?

- ☐ Keep up to date with policy changes pertaining to insider threats.
- ☑ Adopt a cohesive message and provide talking points to the team that explain the program's role. (correct response)
- ☑ Participate in internal working groups and meetings to understand changes in the organization that may affect ability to handle threats. (correct response)
- ☑ Be in the know of organizational activities that may increase the risk of insider threats. (correct response)

***Feedback**: Adopting a cohesive message and providing talking points to the team that explain the program's role, participating in internal working groups and meetings to understand changes in the organization that may affect ability to handle threats, and being in the know of organizational activities that may increase the risk of insider threats can help integrate the program into the organizational mission.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 5

Which of the following statements are true about establishing an Insider Threat Program Evaluation Plan, specifically internal audits, and should be shared with Claire prior to your meeting?

- ☑ All insider threat policies require that you perform self-assessments of compliance with insider threat policies and standards. (correct response)
- ☑ Program evaluation plan helps the program focus on meeting the requirements applicable to the organization. (correct response)
- ☑ Program evaluation includes evaluating the program's plan, policies, procedures, and metrics. (correct response)
- ☐ Program evaluation is conducted by the team on a bi-monthly basis.

***Feedback**: All insider threat policies require that you perform self-assessments of compliance with insider threat policies and standards, program evaluation plan helps the program focus on meeting the requirements applicable to the organization, and program evaluation includes evaluating the program's plan, policies, procedures, and metrics.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 6

What does the team need to do to create and maintain auditable records in preparation for an external audit of the Hub's evaluation plan?

- ☑ The team needs to prepare for external audits by creating and maintaining auditable records of its actions. (correct response)
- ☐ The team doesn't need to do anything since this is an external audit conducted by resources outside of the team.
- ☑ The team needs to work with the legal team to ensure items are created, stored, and retained in accordance with privacy and civil liberties regulations. (correct response)
- ☑ The team needs to keep program records that can be used to measure the effectiveness of the program. (correct response)

Feedback*: The team needs to prepare for external audits by creating and maintaining auditable records of its actions, work with the legal team to ensure items are created, stored, and retained in accordance with privacy and civil liberties regulations, and keep program records that can be used to measure the effectiveness of the program.*

Points (0 for incorrect and 1 for correct): _____

Knowledge Check 7

So, if we continue to move forward and implement the Insider Threat Hub at our facility, are there some best practices that we should implement as it relates to the evaluation plan?

- ☑ Stay connected with the larger insider threat community to keep up to date with the latest best practices. (correct response)
- ☑ Consult with legal team before implementing new practices to ensure they are within your authority. (correct response)
- ☐ Share insider threat information with subjects of a potential inquiry when requested.
- ☑ Join working groups and stay up-to-date with latest research and publications. (correct response)

Feedback*: Best practices include staying connected with the larger insider threat community to keep up to date with the latest best practices, consult with legal team before implementing new practices to ensure they are within your authority, and join working groups and stay up-to-date with latest research and publications.*

Points (0 for incorrect and 1 for correct): _____

Total Points: _____