Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

INSIDER THREAT JOB AID

FACILITATION GUIDE

Insider Threat Vigilance Series Episode One: An Odd Encounter With Tim

Overview: The Insider Threat Vigilance Series aids the workforce in understanding how to identify and report insider threat indicators. The series also provides an overview of how Insider Threat Programs (also known as Insider Threat HUBs) take a multi-disciplinary staff approach towards analyzing information and activity indicative of an insider threat and referring that data to the appropriate officials to investigate or otherwise resolve. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://www.youtube.com/watch?v=Kr2QAdHBMB4&feature=youtu.be

Micro Learn Location: https://www.cdse.edu/micro/vigilance-episode1/vigilance-episode1.html

Instructions

Video Segment 1: Play video and then pause it at 3:30, after the narrator says "What would you do?" Consider asking the students the following questions.

Question 1: What potential risk indicators did Susan see in Tim's behavior?

Desired Responses:

- Tim was talking on his phone in a muffled voice
- Tim was working late and by himself at the office
- Tim quickly minimized his computer screen and shut down his computer
- Tim placed folders in his briefcase and rushed out of the office and left a sandwich and hot cup of coffee at his desk

Question 2: What Should Susan do?

Desired Response: Report Tim to the Insider Threat Program

Additional Comment: Correct students if they recommend taking matters into their own hands in conducting investigative activity, such as: going through his desk drawers, trying to follow him, questioning other employees about Tim's behavior, etc.

Video Segment 2: Un-pause the video and watch Susan's interaction with the Insider Threat POC (Beth Sloan).

Question 3: Did Beth take any immediate adverse actions against Tim?

Desired Responses: No, she realized Tim's behavior was suspicious and outside of the norm. However, she does not have enough information to understand why Tim is acting abnormally. Her main concern was understanding what happened and sharing the information with the other members of the Insider Threat Program. By alerting the other Insider Threat Team Members (HR, Cyber, LE, CI, etc.), she may be able to get additional information that sheds light on why Tim is behaving oddly.

She didn't have enough information to warrant suspending a clearance, firing, or reprimanding him in anyway.

Question 4: Was Tim's privacy protected?

Desired Responses: Yes, Beth informed Susan not to tell anyone about Tim's behavior. Beth did not jump to any conclusions or take any overly intrusive actions against Tim.

Susan reported what she observed but **did not** take steps towards conducting an investigation of her own. If Susan would have searched through Tim's desk, followed him, conducted surveillance, or questioned other employees about Tim's behavior, her activities might have been inappropriate, a violation of policy/regulation, and/or potentially illegal.

Question 5: Do you know where and how to report potential threat Indicators?

Possible Discussion: Please take the opportunity to discuss your organization's Insider Threat Program and reporting procedures.

Additional Facilitator Resources

Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php

Counterintelligence Toolkit: https://www.cdse.edu/toolkits/ci/index.php

DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf

Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html

Security Briefing Templates: https://www.cdse.edu/toolkits/fsos/security-education.html

Security Posters: https://www.cdse.edu/resources/posters.html

Potential Espionage Indicators (PEI) Detecting Actions Outside the Norm Webinar (30 minutes):

https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html

Adverse Information Reporting Webinar (30 Minutes):

https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html

Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes):

https://www.cdse.edu/catalog/elearning/INT220.html