



FACILITATION GUIDE

Insider Threat Vigilance Series Episode Two: “Check Out My New Ride”

Overview:

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options all while protecting the privacy and civil liberties of the workforce. 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://youtu.be/E9w9bDyH1rU>

Micro-Learning Location: <https://www.cdse.edu/micro/vigilance-episode2/vigilance-episode2.html>

Instructions

Play the video for your group and consider asking the following questions.

Question 1: What potential risk indicators did MAJ Montenegro see in Tim’s behavior?

Desired Responses:

- Splitting up with his girlfriend and calling off their engagement
- Purchase of expensive car
- Mentioned having financial difficulties
- Put in his two week notice
- Discouraged because he didn’t get the lead programmer position

Question 2: Why could Tim’s behavior be considered suspicious?

Desired Responses:

- Financial Considerations: Tim is discouraged because he didn’t get the promotion. During his conversation with MAJ Montenegro, he said, “I really needed the money.” He then mentioned that he had purchased an expensive car. It’s odd that Tim needed the promotion for “the money” but was then able to purchase an expensive vehicle. Tim also mentioned planning to put in his two



week notice and leave his job. Tim's purchase of the vehicle could be an example of unexplained affluence.

- **Personal Conduct:** Tim split up with his girlfriend, and they have called off their engagement. The ending of a serious relationship is a difficult life situation. When combined with not getting the promotion and possibly having some financial difficulties, Tim could be going through a life crisis. Tim's personal predispositions will determine how he handles the crisis.

Additional Comment: If the group has watched episode 1, "An Odd Encounter with Tim," you may ask them to discuss some of the potential risk indicators he displayed in episode 1.

- 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

In episode 1, Tim displayed some suspicious personal conduct. Mark Smith and MAJ Montenegro were probably unaware of Tim's previous suspicious behavior reported by Susan in episode 1. In this episode, Tim displays some potentially risky financial indicators and personal conduct. MAJ Montenegro and Mark Smith's reporting will help the Insider Threat Program gain additional context on Tim's situation.

Question 3: What did MAJ Montenegro do?

Desired Response: MAJ Montenegro was concerned about Tim's behavior. He decided to discuss his concerns with Tim's supervisor, Mark Smith. Mark was also concerned about Tim's behavior and decided to contact the organization's Insider Threat Program.

Question 4: What is an Insider Threat Program?

- Designed to identify "at risk" individuals and help them off this pathway and toward more positive outcomes.
- Insider Threat Programs often assist with solutions that focus on providing help and resources for those in need.
- Insider Threat Programs are multidisciplinary. They typically include representatives from CI, Law Enforcement, Cyber, behavioral health, and legal. As a team, the group can look at Tim's situation and best determine how to mitigate risk to the organization – including options that would help Tim onto the right path.

Additional Comment: This is a good point to ask the group if they know how to report information to their Insider Threat Program. The facilitator should provide contact information for their organizational Insider Threat Program.



Question 5: Why was it important for MAJ Montenegro and Mark to report Tim's behavior?

Desired Responses: Mark and MAJ Montenegro are concerned about Tim. They didn't jump to any conclusions, but it is possible that Tim is involved in espionage or other criminal or harmful activity. Ultimately, they really don't know what is going on with Tim. They are concerned about Tim's behavior and want to get him help if it is needed.

Insider Threat Programs have access to many resources including the Employee Assistance Program that can help Tim. If Tim is having trouble, the Insider Threat Team wants to get him the help he needs before he becomes an insider threat.

It's possible that other co-workers have concerns about Tim's behavior. Maybe they reported him as well (see episode 1). Mark and the MAJ's reporting could give the Insider Threat Team additional context into Tim's situation. More importantly, what if Mark and the MAJ are the only ones to notice Tim's suspicious behavior, or are the only ones that knew to report it? Mark and MAJ Montenegro could be the Insider Threat Team's only opportunity to know Tim is struggling.

Additional Facilitator Resources

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

Counterintelligence Awareness 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>

Customizable DoD Command Briefing: <https://www.cdse.edu/documents/cdse/customizable-dod-command-brief-for-insider-threat-awareness.pdf>

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>