LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

SEPTEMBER 2024

INSIDER THREAT AWARENESS MONTH

Do you know how to identify an Insider Threat and the associated indicators?

It is not a frequent occurrence when individuals intentionally betray their company, harm their fellow colleagues, or sell our national security secrets. In fact, studies show that malicious acts are rarely conducted by insider threats, but rather by trusted employees who are triggered by previous or current life crises. When the reactions to these stressors are not addressed, they could influence a person to commit espionage, leak information, engage in targeted violence, or contemplate self-harm.

It is important to remember that just because personnel in our workforce have received a favorable eligibility determination of trustworthiness, it does not make them immune to human condition. Life circumstances do happen and are unavoidable. We all have to deal with challenges, crises, and the obstacles that life will inevitably present. While we understand these "life circumstances" occur to all of us, we are reluctant to report suspicious behavior, even when there is reasonable evidence that something is not right. We do not pry into other people's business, or we are afraid of making false accusations. It is natural to want to give someone the "benefit of the doubt," especially when it's someone in a position of authority, a colleague, or a friend. Unfortunately, the stakes are too high not to report incidents of possible insider threats. As a result, it is a requirement to report indicators as soon as they occur.

IDENTIFYING INSIDER THREAT INDICATORS

Most insider threats exhibit risky behavior prior to committing negative workplace events. Not all of these potential risk indicators will be evident in every insider threat, and not everyone who exhibits these behaviors is doing something wrong. However, most insider threats have displayed at least some of these potential risk indicators. If identified early, many risks can be mitigated before harm to the organization can occur. Here are some indicator examples.

- Access Attributes
- Criminal/Violent Conduct
- Financial Considerations
- Foreign Considerations
- Professional Performance
- Psychological Conditions
- Security/Compliance Incidents
- Substance Abuse
- Technical Activity
- Violent Extremist Mobilization

At your leisure, explore Insider Threat Case Studies at: https://securityawareness.usalearning.gov/cdse/case-studies/index.php

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

WHAT AN INSIDER THREATS DIGITAL FOOTPRINT LOOKS LIKE

What is a Digital Footprint? A digital footprint is the unique trail of data pertaining to a user's activities, actions, communications, and transactions on the internet.

Examples:

- Websites visited
- Emails or messages sent
- Information submitted in online forums
- Reviews or comments posted
- Photos and status updates posted

There are two types of digital footprints: active and passive. Let's take a closer look.

Active Digital Footprint: The user has intentionally shared information about themselves either by using social media sites or other websites. For example, a user might log into a site to comment on an online forum like Reddit or Yelp, or on social media platforms like Instagram or Twitter (X).

Passive Digital Footprint: Information is collected from the user without their knowledge or awareness of it happening. For example, a user visits multiple websites, leaving their IP address behind.

A digital footprint, whether passive or active, may put an insider at-risk of being targeted for malicious actions such as identity theft, financial scams, or social engineering ploys. An insider's digital footprint may also reveal susceptibility to misinformation or disinformation campaigns designed to sow discord, and potentially compromise an insider's allegiance to their organization. For insiders with security clearances, this is uniquely important because it may reveal information that might put one's trustworthiness, loyalty, reliability, and overall ability to safeguard information into question.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com