



Insider Risk Investigative Response

Corporations that invest significant resources to improve their insider risk programs may often find themselves unprepared to deal with a suspicious incident.

Whether it is gathering data for law enforcement or legal action, the response activities must be thorough but conducted expeditiously and judiciously. – Insider Threat Task Force Whitepaper¹

If your security team suspects an insider incident has occurred, do they have the resources and expertise to investigate the incident; determine if the nature of the event was malicious, negligent, or inadvertent; and then respond effectively?

RESPONDING TO AN INSIDER THREAT

When there is concern of potential insider activity within your organization, Leidos works with you to resolve the matter successfully. Our team of former law enforcement, counterintelligence, and industry professionals has extensive experience conducting complex investigations, collecting evidence, determining intent, and testifying in legal proceedings.

WHAT DOES THE ENGAGEMENT ENTAIL?

The Investigative Response Service is customized to your organization's specific needs but typically involves our consultants working with you to develop an investigative plan, gather facts, collect evidence, and guide the investigation's detailed day-to-day execution related to the insider incident.

INSIDER RISK PROGRAM BENEFITS

- ▶ Protect critical assets and prevent loss of intellectual and proprietary property, confidential data, or customer information
- ▶ Ensure regulatory compliance, specifically for those in defense, healthcare, and financial services
- ▶ Avoid immediate or future loss of revenue
- ▶ Maintain customer and shareholder confidence
- ▶ Avert critical system or service availability disruption
- ▶ Prevent overall harm to an organization's brand image and reputation
- ▶ Deter potential insiders

Our investigative team has the knowledge, experience, and resources to guide and direct all aspects of the internal investigation. Depending on the nature of the investigation, we can:

- ▶ Provide subject matter expertise and instruction
- ▶ Gather all relevant facts
- ▶ Ensure the proper collection and storage of electronic evidence
- ▶ Conduct cyber forensic analysis
- ▶ Facilitate the sharing of information between your organization, Leidos Cyber, and law enforcement, when appropriate
- ▶ Compile investigative facts and document findings
- ▶ Identify procedural gaps and make recommendations to prevent future occurrences

WHY PARTNER WITH LEIDOS?

As a comprehensive insider solutions provider, we offer a suite of cyber products to address insider threat issues along with in-house analytical resources and highly-skilled cyber forensic experts to support the needs of any investigative effort. Our expert practitioners leverage their decades of counterintelligence and forensic investigation expertise to help you assess anomalies and other indicators of insider threats and respond accordingly.

Having worked with organizations across both government and private sectors from multiple industries, each team member keenly understands the sensitivity of internal investigations and can be trusted to maintain the highest level of discretion.

NEXT STEPS:

Responding to an insider incident requires more than just detection. If you suspect your organization is the victim of an insider breach, bring the focus back to the individual by conducting a proper investigation. After all, not all threats are malicious – training or counseling may be the answer to remediate the conduct. Talk to a cybersecurity expert today.

TRUST LEIDOS TO HELP SAFEGUARD YOUR MOST IMPORTANT ASSETS.

Intelligence and National Security Alliance (INSA), Cyber Council: Insider Threat Task Force. A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector. (INSA, 2013).

FOR MORE INFORMATION

855-56-CYBER | cyber.security@leidos.com

Visit us online: cyber.leidos.com

