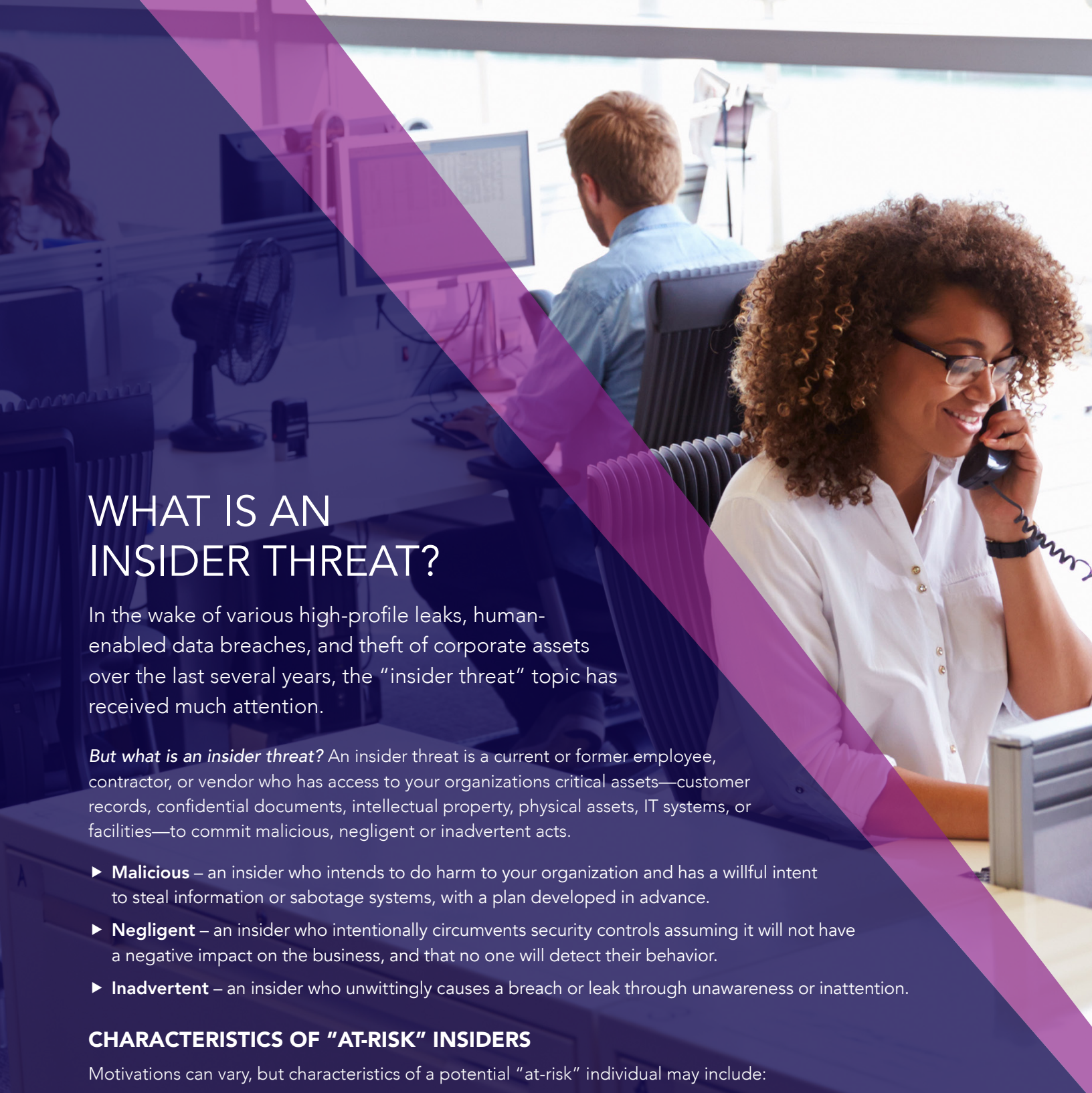
leidos

Insider Risk Solutions

DEVELOP A SUCCESSFUL INSIDER RISK PROGRAM



WHAT IS AN INSIDER THREAT?

In the wake of various high-profile leaks, human-enabled data breaches, and theft of corporate assets over the last several years, the "insider threat" topic has received much attention.

But what is an insider threat? An insider threat is a current or former employee, contractor, or vendor who has access to your organizations critical assets—customer records, confidential documents, intellectual property, physical assets, IT systems, or facilities—to commit malicious, negligent or inadvertent acts.

- **Malicious** – an insider who intends to do harm to your organization and has a willful intent to steal information or sabotage systems, with a plan developed in advance.
- **Negligent** – an insider who intentionally circumvents security controls assuming it will not have a negative impact on the business, and that no one will detect their behavior.
- **Inadvertent** – an insider who unwittingly causes a breach or leak through unawareness or inattention.

CHARACTERISTICS OF "AT-RISK" INSIDERS

Motivations can vary, but characteristics of a potential "at-risk" individual may include:

- Ethical flexibility
- Greed or financial distress
- Susceptibility to blackmail
- Intolerant of criticism
- Lack of empathy
- Self-entitlement
- Debilitating introversion
- Passive-aggressive
- Extreme compulsiveness

A SHIFTING THREAT LANDSCAPE

The global workforce has evolved. As retiring baby boomers leave the workforce, Generation-Y Millennials, raised on the internet and social networks, fill those gaps with the expectation – and even demand – for constant and immediate access to information, wherever they are on any and every device of their choice.

Generation-Y are accustomed to evolving technology, possessing greater levels of technical expertise previously held primarily by engineers and IT professionals. They also have an increased expectation for connectedness and access.

Another factor, how simple it is to take anything stored electronically. Consider the volumes of sensitive data your organization has stored on your network. If a malicious insider wants to exfiltrate proprietary information from your network, it can be accomplished in a matter of minutes – if not less!

Finally, economic pressure. Certain nation states, companies and even people are in a financial crisis. Obtaining trade secrets and intellectual property can be used to their economic advantage – selling it to the highest bidder and helping alleviate their financial stress.

As the workplace becomes more complex and insider risks increase, organizations must ensure they can detect anomalies and prevent incidents before they happen. This requires continuous monitoring, continuous evaluation of both human and IT-centric behavioral indicators and evaluation of individual attributes. Leidos is your trusted partner to ensure the protection of your company's critical assets and help you prevent an insider incident before it occurs.

SAFEGUARDING YOUR MOST IMPORTANT ASSETS

Today's organizations often struggle to manage complex insider risk challenges independently. Although most cyber and risk professionals are well aware of the detrimental impacts an insider can have on their organization, many often lack the internal resources or expertise to develop a comprehensive insider risk management plan, or effectively respond to alleged or suspected insider activity.

Many corporations invest significant resources to improve their defenses against external threats but too often fail to adequately protect themselves from internal risks—risks created by insiders with direct access to critical corporate assets. Neutralizing internal threats is as important to strengthening overall security and reducing organizational risk as protecting against external attacks.

OBSTACLES LAUNCHING AN INSIDER RISK PROGRAM

- Convince executive leaders to invest in an insider risk program
- Create a powerful business case to fund and source the project properly
- Lack of internal resources or lack of the 'right' resources to build a strategic vision and deliver a holistic insider risk program
- Understand the essential components of an insider risk program
- Apprehensions employees will feel untrusted and that 'Big Brother' is watching
- Concerns over data privacy – especially for multinationals with stricter privacy laws or work councils (i.e. Europe)

Are you confident your current insider risk program is comprehensive enough to protect your critical assets, and prevent loss of intellectual and proprietary property, confidential data, or customer information? Can you effectively thwart an insider threat at your organization? Are you willing to risk loss of revenue, customer or shareholder confidence, or harm to your organization's brand image and reputation?

THE TECHNOLOGY

Traditionally, organizations believe that network monitoring tools were sufficient to detect an insider threat. But network monitoring only captures the individuals' virtual data or digital trail – what systems an individual accesses, when they view and download files, send emails, access the web, and log on and off the corporate network. Many times these activities are not found early enough or simply not identified at all.

Organizations must also take into account non-virtual risk indicators to develop a proactive and effective insider risk program. For example, the individuals' role, access and clearance levels, work habits (i.e. what hours do they 'normally' start/stop work), compliance to corporate policies, and even their performance rating (have they received a reprimand, are they at risk for termination).

Can your organization correlate this virtual and non-virtual data? More importantly, if for example, an individual downloaded a large number of proprietary files, outside of their normal working hours, and also had just received a poor performance review, would this collective activity generate an alert and trigger an internal analyst to take a closer look at that individual?

LEIDOS' APPROACH TO MANAGING INSIDER RISK

Providing a holistic, proactive, and risk-based approach through strong and effective policies, business processes, technical controls, and training.

Establishing a holistic, proactive insider risk program is essential to any organization that wants to manage insider risk effectively. However, many organizations think they need to attack the problem solely from a technical perspective and push it to the Chief Information Security Officer (CISO) or Chief Information Officer (CIO), but this may not be the most effective approach.

A comprehensive insider risk program requires people, processes, and tools, acting collectively to achieve the greatest benefit and return on investment. Therefore, Leidos' preference is for the insider risk program to be led by a Chief Security Officer (CSO), or perhaps even the Chief Risk Officer (CRO).

When implementing an insider risk program, it is necessary to take foundational measures to integrate both technical and non-technical elements for a truly holistic defense. Some steps include constructing proper governance and documentation, defining critical assets vital to business operations, establishing processes for implementation and execution, and ensuring transparent communication with ongoing training for employees.

Our array of insider risk solutions and team of insider risk experts are ready to assist you through all phases of assessing your current risk profile, creating and administering a comprehensive insider risk management program – including the best technology for your specific needs – and helping you to respond to insider incidents if they do occur properly.

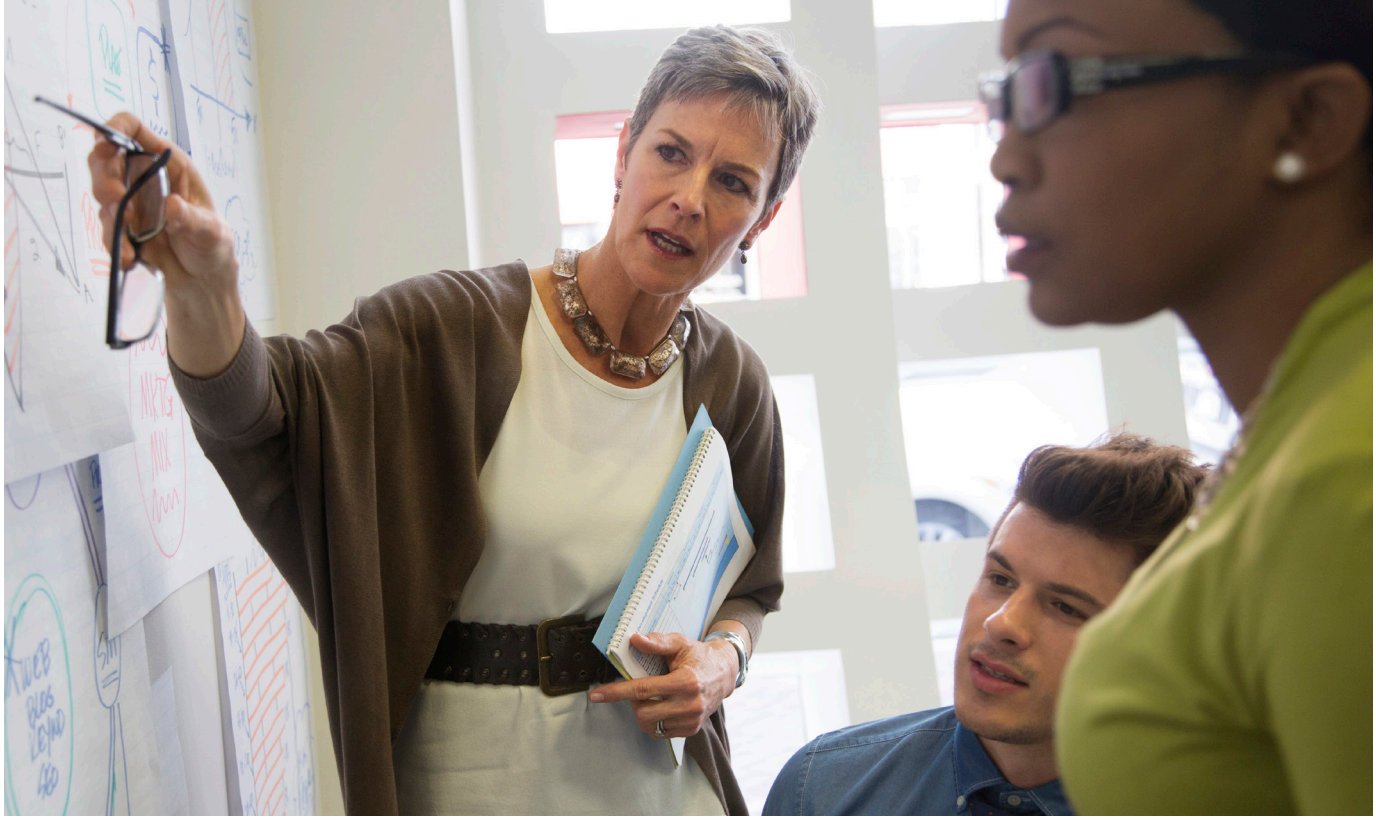
INSIDER RISK PROGRAM BENEFITS

- 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
- Deter potential insiders
- Avoid immediate or future loss of revenue and maintain customer and shareholder confidence
- Avert critical system or service availability disruption
- Prevent overall harm to an organization's brand image and reputation

INSIDER RISK SOLUTIONS AT A GLANCE

Leidos insider risk services can complement existing technical tools or may be employed independently, and include Insider Risk Quick Start, Insider Risk Assessment, Insider Risk Training, Insider Risk Program Design and Implementation, and Insider Risk Investigative Response offerings.

- Identify existing Insider Risk components and capabilities, identify gaps, and help you begin developing a holistic Insider Risk Program
- Evaluate and measure your organization's existing capabilities to prevent, detect, and respond to an insider threat with our Insider Risk Assessment
- Educate stakeholders and Insider Risk Program personnel with our Insider Risk Management course
- Develop a vision for your insider risk program and initial framework to drive your program toward optimization with our Insider Risk Program Design and Implementation Services
- Incorporate technology with Arena Insider Threat Identification™ (ITI) seamlessly integrating structured and unstructured contextual information, as well as data from cyber monitoring applications to provide a highly robust and effective insider threat detection solution
- Leverage investigative experience with our in-house analytical resources and highly-skilled cyber forensic experts with our Investigative Response Service



Uncover Program Gaps

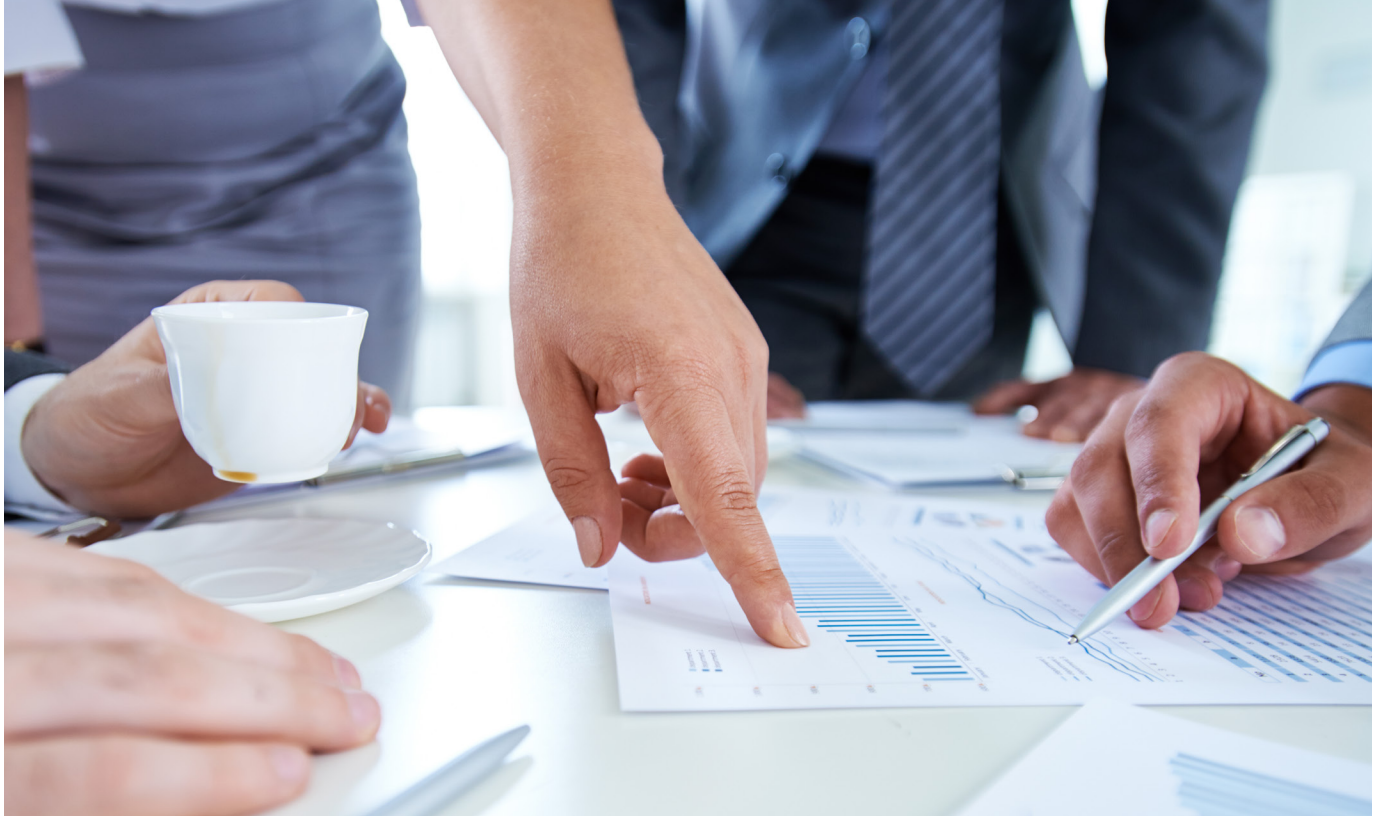
INSIDER RISK QUICK START

The Insider Risk Quick Start is an abbreviated assessment and an excellent way to evaluate existing organizational capabilities, identify gaps, introduce industry best practices, and provide high-level recommendations to help you get your Insider Risk Program started.

Our Insider Risk Quick Start service can also be used to evaluate one aspect of your Insider Risk Program in more depth and provide recommendations for developing and maturing that specific area.

Conducted by Leidos' team of insider risk experts, the Quick Start utilizes document reviews, direct observations, and personal interviews, to gain insight into your organization's current insider risk posture. The Leidos team will work with you to determine the Quick Start scope and review related artifacts. We then conduct an on-site evaluation, typically two days, and educate the program manager, stakeholders, and executives about insider risk and the organization's preparedness to address insider-related threats. Following the on-site evaluation, Leidos will provide a short (i.e., two-page) report documenting the findings and high-level recommendations for initiating and developing your organization's Insider Risk Program.

- Gain insight into your organization's current risk posture
- Identify gaps and the most critical areas of concern
- Propose risk treatment recommendations to help inform decision makers on next steps



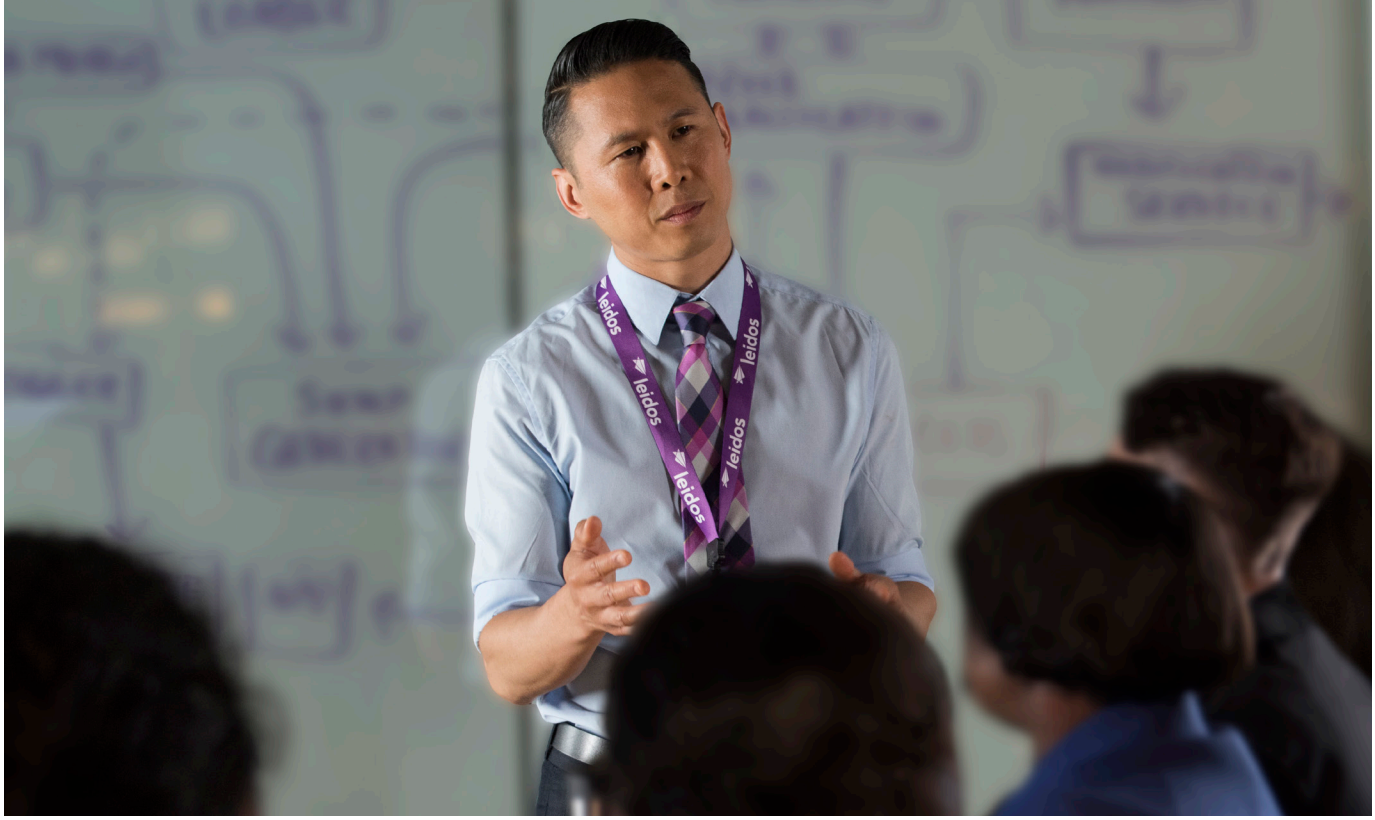
Evaluate And Measure Your Current State

INSIDER RISK ASSESSMENT

The Insider Risk Assessment evaluates and measures your organization's existing capabilities to prevent, detect, and respond to insider threats by following a structured insider risk assessment process aligned with NIST, ISO, NISPOM, and other industry best practices and standards. It includes a thorough review of administrative, technical, and physical controls that may be exploited by an insider to harm your organization and its critical assets, and provides a complete current state evaluation of your organization's insider risk security posture.

The assessment involves merging information from key stakeholders to form a comprehensive depiction of the company's level of preparedness to address insider-related threats. The assessment utilizes document reviews, direct observations, and personal interviews, including cross-functional areas of the business, to gain insight into organizational silos where relevant program information may reside. After each assessment, you will receive a detailed report that outlines the findings of your insider risk security posture, including risk treatment recommendations.

- Identify core strengths and vulnerabilities associated with managing insider threats
- Determine if you meet applicable compliance requirements, such as NIST, ISO, NISPOM, and other industry best practices and standards
- Provide a gap analysis to identify the most critical areas of concern
- Propose risk treatment recommendations to help inform decision makers on next steps



Insider Risk Training

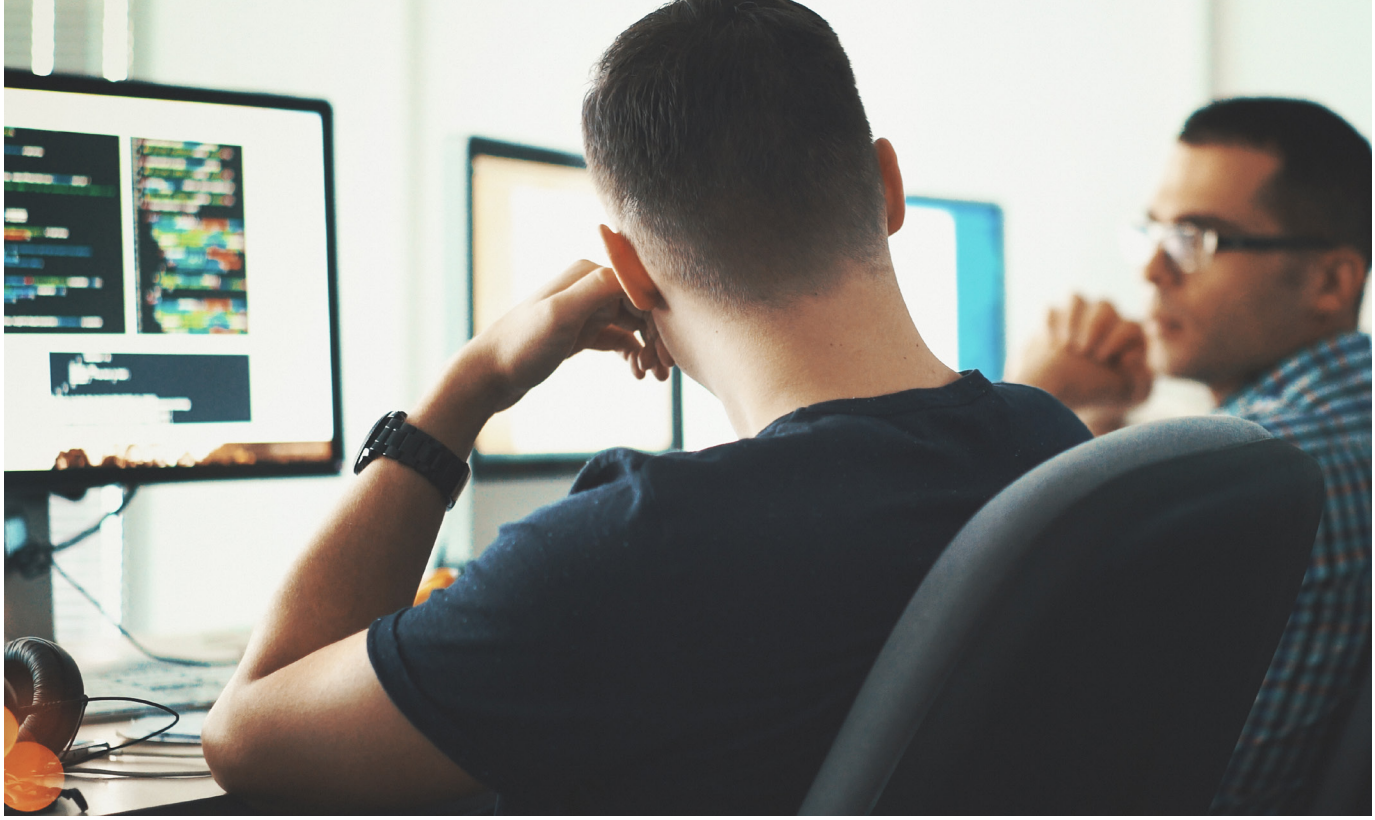
INSIDER RISK MANAGEMENT COURSE

This eight-hour course introduces your Insider Risk Program stakeholders, program personnel, and security professionals to the complexities of insider risk. Participants will learn how an Insider Risk Program is essential to protecting an organization from intellectual property theft, sabotage, and even workplace violence by employees and Trusted Business Partners. This course will focus on how aggregated Key Risk Indicators (KRIs) collected from technical, behavioral, and third-party data sources enable an organization to forecast and, ideally, interrupt the idea-to-action continuum that may lead to detrimental events.

Instruction on the appropriate management of privacy and legal issues and their impact on an Insider Risk Program are also covered. The course culminates with the participants examining realistic scenarios to evaluate and triage KRIs leading to the escalation decision-making paradigm.

Leidos' Insider Risk Services team anticipates developing additional Insider Risk Program training courses. If your organization has an Insider Risk Program training need, we can develop an ad-hoc course to meet your requirements.

- Eight-hour course introduces insider risk program complexities
- Focuses on aggregated Key Risk Indicators and the management of privacy and legal issues
- Examines realistic scenarios to evaluate and triage KRIs



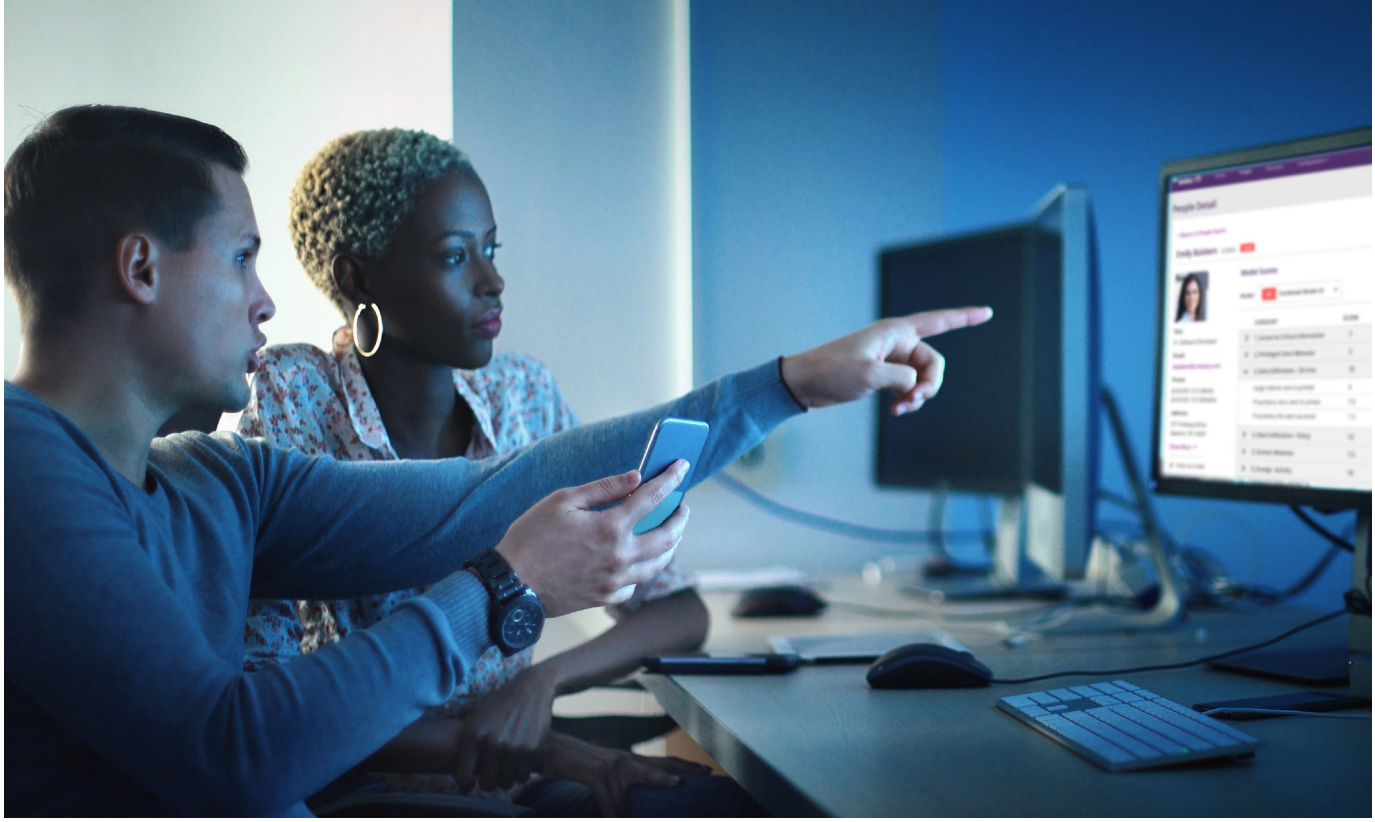
Develop a Vision

INSIDER RISK PROGRAM DESIGN AND IMPLEMENTATION

Leidos will work with you to develop a vision for your insider risk program and initial framework to drive your program toward optimization. Our Insider Risk Program Design and Implementation Service is a natural next step following an Insider Risk Assessment (but can be offered independently). Once an assessment of your current state is complete, the desired goals for a successful insider risk program are defined and risk treatment recommendations identified, organizations use these actionable recommendations to design and implement a program.

Leidos' team of insider risk experts can augment your existing internal resources to design a holistic insider risk program that incorporates all the components for an effective program. Our consultants work with you to develop or modify relevant business processes, organizational policies, and security awareness training, as well as integrate appropriate technology to enable your organization to counter threats while minimizing business disruption.

- Develop strategic vision roadmap
- Provide a holistic approach integrating data across the entire enterprise
- Resource, implement and execute the strategic vision roadmap
- Augment existing internal resources during the program build or implementation phase



Incorporate Technology

ARENA INSIDER THREAT IDENTIFICATION™

The Arena ITI™ solution provides organizations of any size with proactive identification of potential insider threat activity, built on industry-leading experience in counterintelligence.

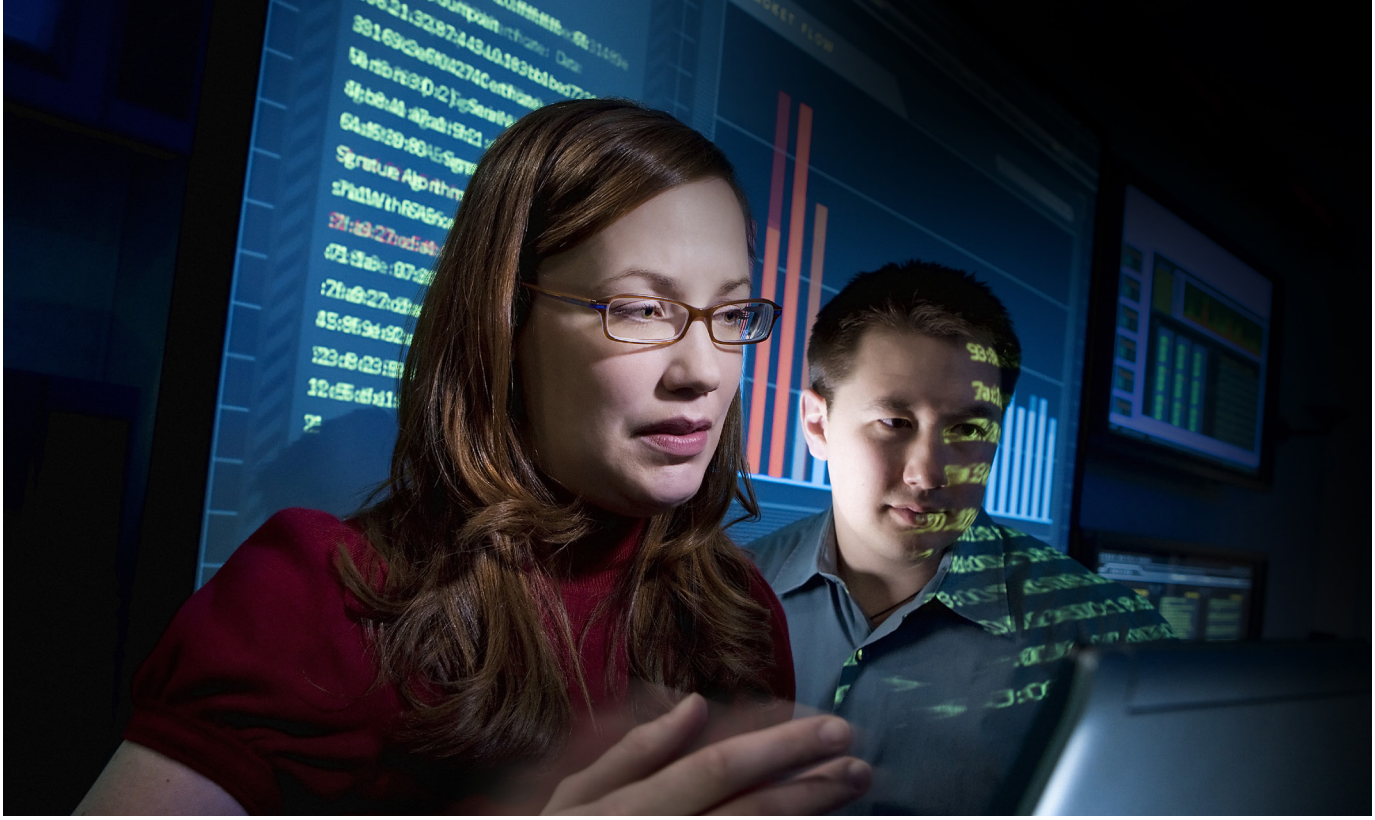
This solution takes a holistic approach to detecting insider threats, seamlessly integrating structured and unstructured contextual information, such as performance reviews or employee information access, as well as data from cyber monitoring applications to provide a highly robust and effective insider threat detection solution.

Arena ITI analyzes individuals' anomalous IT activities with their non-IT behaviors in a single platform to produce faster, highly accurate, insider threat detection by:

- Continuously ingesting intelligence from disparate company data sources
- Aggregating data through predefined models and scoring
- Drilling down for advanced analysis and further investigation

To complement the advanced Leidos Arena ITI data and analytic models, Leidos also offers clients a solution for User and Entity Behavior Analytics (UEBA). UEBA software integrates raw log type data sources and analyzes unusual behavior using machine learning models. UEBA software provides a clear picture of threats across IT systems by tracking the relationship between, and risks associated with, users, machines, applications, and files. When Arena ITI is complemented with a UEBA application, it offers clients the most robust insider threat solution available.

- Protect critical assets and prevent loss of intellectual and proprietary property, confidential data or customer information
- Ensure regulatory compliance, specifically for those in the defense industrial base, financial, and healthcare industries
- Avoid immediate or future loss of revenue



Leverage Investigative Experience

INSIDER RISK INVESTIGATIVE RESPONSE

When there is concern of potential insider activity within your organization, Leidos works with you to resolve the matter successfully. 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.

Leidos in-house analytical resources and highly-skilled cyber forensic experts can 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. Each team member keenly understands the sensitivity of internal investigations and can be trusted to maintain the highest level of discretion.

- Provide subject matter expertise and instruction
- Ensure the proper collection and storage of electronic evidence
- Conduct cyber forensic analysis
- Compile investigative facts and document findings
- Identify procedural gaps and make recommendations to prevent future occurrences

WHY PARTNER WITH LEIDOS?

OUR DEFENDER DNA

Successful cyber programs require great people with 'defender DNA.' Defending against sophisticated cyber threats takes more than technology. It takes people. People with skills and innate qualities to outpace today's evolving threat landscape. Qualities we call 'defender DNA.' We see these qualities in successful client teams and in our own team.

Our consultants leverage their defender DNA. Their many years of counterintelligence, investigative, and industry experience and expertise help our customers develop, implement and manage an end-to-end, holistic, insider risk program.

Organizations across both government and private sectors as well as multiple industries rely on our team to help them understand and evaluate their current state, flush out vulnerabilities and gaps, develop their strategic vision, evaluate which technology is best suited to their needs, and design and implement their insider risk solution.

Our mastery of insider risk program best practices will help inform and influence your decision makers on the most effective risk treatment recommendations and include the optimum risk treatment solutions for your organization. We provide a comprehensive, holistic, and product agnostic view.

Leidos is a total insider solutions provider, coupling an entire suite of cyber products to address technical insider threat issues.

NEXT STEPS

Don't wait to be a victim of an insider threat. Find out how your organization measures up, what steps you can take to improve your insider risk profile, and how to respond when an incident occurs. Talk to a cybersecurity expert today.

TRUST LEIDOS TO HELP SAFEGUARD YOUR MOST IMPORTANT ASSETS.

FOR MORE INFORMATION

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

Visit us online: **cyber.leidos.com**

LinkedIn: Leidos
Facebook: Leidosinc
YouTube: Leidosinc
Twitter: @Leidosinc

leidos

© Leidos. All rights reserved. | 17-Leidos-0427-1716 | 17-0166-Leidos Creative