Arena Insider Threat Identification™

PROTECT YOUR ORGANIZATION FROM THE INSIDE OUT

Growing use of personal devices, email, and cloud storage drives, as well as an evolving global workforce, is increasing the risk of information intentionally or unknowingly leaked.

An employee, contractor, supplier, or business partner who has access to your critical assets — customer records, confidential documents, intellectual property, physical assets, and IT systems — all have the opportunity to do irrevocable harm to your company and your brand.

In a report by Juniper Research, data breach losses are estimated to reach $2.1 trillion globally by 2019, with an average cost per incident to exceed $150 million by 2020.

What are the implications to your company if such information fell into the wrong hands?

PROTECT YOUR BUSINESS WITH ARENA INSIDER THREAT IDENTIFICATION™ (ITI)

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.

WHY INVEST IN AN INSIDER RISK SOLUTION?

- 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
- 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

leidos

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).

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 award-winning 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.

THE ARENA ITI™ ADVANTAGE

- Integrates existing enterprise data with behavioral models, and continually analyzes the data for indicators that an individual may be putting the company at risk
- Proactively alerts your team of at-risk individuals to protect the organization
- Combines an individual's cyber footprint with non-cyber behavioral data for an accurate risk profile
- Gives analysts the ability to evaluate relationships between all data sets through a built-in link analysis tool
- Provides an easy-to-use interface and threat modeling capability customized to your specific industry, organization, and employee demographics
- Delivers multi-dimensional views of data, in a variety of graphical and statistical outputs, easily assessed in minutes

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.

ABOUT LEIDOS

Leidos is a global science and technology solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, homeland security, civil, and health markets. The company's 32,000 employees support vital missions for government and commercial customers. Headquartered in Reston, Virginia, Leidos reported annual revenues of approximately $7.04 billion for the fiscal year ended December 30, 2016.

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**

17-0165 | Leidos Creative