Capgemini

Insider Threat Identification
Protect Your Organization From The Inside Out

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

A recent Ponemon Institute study identified over 3,000 insider incidents over a 12 month period averaging $8.76M of damage per incident.

What are the implications to your organization if critical information fell into the wrong hands? Or a critical facility or application was sabotaged? Or led to a workplace violence incident?

MITIGATE YOUR RISK WITH INSIDER THREAT INTELLIGENCE (ITI) FROM CAPGEMINI

Traditionally, organizations believed that IT monitoring tools were sufficient to detect an insider threat. But IT monitoring only captures the individuals' 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 property and mitigate cases of sabotage or the potential for workplace violence.

- Ensure regulatory compliance, specifically for those in the defense, transportation, financial, and healthcare industries

- Avoid immediate or future loss of revenue

- Maintain customer, shareholder and board confidence

- Avert critical system or service availability disruption

- Prevent overall harm to an organization's brand image and reputation

- Deter potential insiders

Trust Capgemini to Help Safeguard Your Most Important Assets.

ITI is a software application that provides organizations of any size the ability to cost effectively mature their Insider Threat Program. It empowers insider risk analysts with robust and proven automation and analytics that leads to a significant improvement in their ability to **proactively** identify high risk employees and contractors. ITI is built on decades of experience in counterintelligence and best practices of some of the world's most mature insider risk organizations.

The ITI solution takes a holistic approach to detecting insider threats, seamlessly integrating human behavioral indicators, such as poor performance, disciplinary actions, employee access to critical assets, life stressors as well as data from IT security monitoring applications to provide a highly accurate insider threat detection solution.

ITI significantly streamlines the insider analyst escalation and triage process through automation:

- Ingesting intelligence from company and third-party data sources
- Aggregating data through predefined models and scoring
- Drilling down for advanced analysis and further investigation
- Reporting of organizational metrics and risk indicator trends

ITI provides continuous context and insight for the complete population and alerts security teams to high-risk individuals.

ITI is a complement to your existing IT monitoring solutions, such as a SIEM, DLP, User and Entity Behavior Analytics (UEBA) or User Activity Monitoring (UAM) application.

THE ITI ADVANTAGE

- Proven successes in preventing insider and workplace incidents
- Earlier identification of persons of interest than sole reliance on IT monitoring only solutions
- Productivity enabler requiring only a very small insider threat analyst team
- Only product on the market developed for and by insider threat security analysts
- Used by some of the most effective insider threat programs in industry
- Data and risk model flexibility to meet client evolving use-cases and priorities
- User interface, analysis, reporting, alerts and metrics designed specifically for insider threat analysts
- Supports over 150 insider threat risk indicators

As the workplace becomes more complex and insider risks increase, organizations must ensure they can detect and prevent incidents before they happen. This requires continuous monitoring, continuous evaluation of both human and IT system behavioral indicators. Capgemini 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
Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Learn more about us at

www.capgemini.com/cyber

People matter, results count.

Capgemini