Mitigating Insider Threats:

Latest Trends, Best Practices and AI Automation

Sep 9, 2019

Insider threat incidents range from data security breaches, which have cost firms like Capital One as much as $100—$150 million to violent threats from disgruntled employees, like the case of Coast Guard Lieutenant Christopher Hassan who was arrested after a joint Coast Guard and FBI investigation found he was stockpiling weapons and seeking to launch a major attack.

Every Organization is Vulnerable

While these high-profile incidents grab international headlines, the reality is that every organization is vulnerable to insider threats. On average, insider threats cost almost $9 million, take more than two months to contain and include issues related to careless workers, disgruntled employees, workplace violence and malicious insiders.

Consider that between January and June 2019, the healthcare industry had already disclosed 285 incidents of patient privacy breaches, with hospital insiders responsible for 20 percent of the incidents. Similarly, the Verizon 2019 Data Breach Investigations Report, found that 34 percent of all breaches were caused by insiders.

Companies are Building Insider Threat Programs, But Want to Invest More

Some 90 percent of organizations feel vulnerable to insider attacks and 86 percent have or are building an insider threat program. Still, nearly 75 percent of C-level executives do not feel they are invested enough to mitigate the risks associated with an insider threat.

As part of National Insider Threat Awareness Month this September, the National Counterintelligence and Security Center (NCSC) is reminding companies of the need for strong insider threat protection programs and the signs to look for with existing employees.

Look for These Concerning Behaviors

William Evanina, who heads up NCSC, shares that those individuals engaged or contemplating insider threats display "concerning behaviors" before engaging in these events.

The CERT National Insider Threat Center in the latest edition of its Common Sense Guide to Mitigating Insider Threats, identifies these behaviors as including:

- repeated policy violations;
- disruptive behavior;
- financial difficulty or unexplained; extreme change in finances; and
- job performance problems.

Early Detection Technologies

The Center suggests deploying solutions for monitoring employee actions, correlating information from multiple data sources, having tools for employees to report concerning or disruptive behavior, and monitoring social media.

Surveys like the one conducted by Crowd Research Partners show more and more organizations are increasingly using behavior monitoring and similar methods to help with early detection of insider threats.

And, a report from Accenture found that while advanced identification, security intelligence and threat sharing technologies are widely adopted, automation, AI and machine learning are now being used by about 40 percent of companies.

Costs Savings from AI Automation

According to the same report, once investment costs are considered, AI automation could offer the highest net savings of about $2 million and begin to address the shortage in skilled security staff.

AI can help detect the risk indicators displayed by those who want to defraud organizations but without the inherent human bias. Additionally, AI can help manage the incredible volume of data that must be collected, aggregated, correlated, analyzed and fused across disparate sources.

Following the Common Sense Guide to Mitigating Insider Threats

Companies looking to follow the CERT National Insider Threat Center's guidelines, should consider how the Radiance platform can help with monitoring social media, correlating disparate information, and providing a tool for employees to report concerning behaviors.

Radiance OS-INT monitors all publicly available information across the entire deep web, not only social media. And, it can ingest massive amounts of unstructured content from disparate internal data sources for further correlation and verification.

Radiance's HUM-INT platform, known as S4, is a mobile application that allows users to confidentially report concerns in real time. It can be configured as a workplace tool, with a centralized management portal to allow clients to access real-time threats to geo-fenced facility locations.