SAS for Insider Threat

Early, auditable warning system to improve organizational security

SAS Facts

SAS is ranked as a leader in advanced analytics and artificial intelligence.

SAS software is open, cloud-based, unified and powerful.

SAS has customers in 147 countries

SAS software is installed at more than 83,000 customer sites.

Trusted insiders are your best asset or greatest risk

When considering insider threats, organizations need to look to current employees, suppliers, contractors, partners, and former employees. Whether done unintentionally or maliciously, insider threats can harm organizational information assets through theft, sabotage, fraud, leaking and other means.

Traditional insider threat programs have not adequately identified the risks. Programs have focused on tip lines, infrequent sampling, and investigator knowledge. Additionally, organizational security professionals often concentrate on external threats to the exclusion of internal ones.

To proactively detect insider threats and prevent costly losses, organizations are turning to advanced technologies. These technologies help identify individuals who might need retraining, reassignment, or intervention.

Challenges

Insider threats are difficult to detect.

- **Trusted access.** Insiders can use their access to and knowledge of computing and physical resources to exploit social engineering, physical security, and other areas to access sensitive assets. In some cases, insiders may be privileged users, system administrators or have access to sensitive assets not available to average users.
- **Unique indicators and warnings.** Insiders typically do not follow the same kill chain or attack progression methodologies as cyberattackers because their motivations are different. Insiders can be spurred to act as a result of financial distress, work conflicts, outside influences, being disgruntled, and other drivers.
- **Dependence on institutional knowledge.** The background of the investigator often determines the threat classification. As people leave the organization or move to other positions, the institutional knowledge is lost. Without a long series of data, organizations do not have useful records that can be validated if legally challenged.
- **Multiple data silos.** The volume and data types available to investigators varies. Without thorough insights, organizations cannot identify the indicators of an insider threat in time to trigger a response.

Our Approach

SAS helps organizations improve security outcomes with a continuous, early warning system that identifies fraud, abuse, sabotage, and espionage by trusted internal users. SAS provides organizations with proactive, precise, and timely information about individual users and overall user risk.

We approach the problem by providing you software and services to help you:

- **Access all relevant data**. Get a single, clean, and consistent data set for analysis and insight generation.
- **Identify risky business.** See individual risk scores, compared to peer groups and dynamic threshold baselines. This risk score and the data used to generate it are the result of SAS' hybrid analytic approach combining anomaly scenarios, network linking, text, and predictive analytics. Both are available to investigators to speed time-to-decision.
- **Explore and visualize networks in the data.** Improve awareness of relationships and interactions among the data.
- **Improve investigator efficiency.** Launch, manage, prioritize, and assign governed and compliant investigations within the software using embedded workflow capabilities.

Business Impact

US federal government agency and Department of Defense contractors are required to have an insider threat program in place (NISPOM Conforming Change 2). Yet, private sector organizations are realizing they too cannot afford to ignore the costly and disruptive nature of these potential risks.

SAS can help by providing:

- Improved security outcomes through better understanding of user behavior; faster identification of individuals who might need retraining, reassignment, or other security actions than through a manual data review.
- Consistent insider threat determinations through a repeatable decision process using AI to examine suspicious actions and potential motives in all available data.
- Reduced costs by identifying areas of overlap and/or inefficiency to streamline insider threat review and investigation processes.