Solution Brief

Insider Risk Management

thalestct.com

THALES
Building a future we can all trust

THALES

Insider attacks are on the rise. According to a recent study, 83% of organizations have experienced at least one insider attack in the past year. And, 85% of cybersecurity leaders expect data loss from insider incidents to escalate in the next 12 months.

The U.S. Federal Government is not exempt from this trend. Insider threats come in a variety of forms—everything from malicious, covert actions of individuals within or connected to an agency to the unintentional loss or theft of data or end-user devices. Any actors with administrative privileges, whether legitimately provisioned or maliciously obtained, have the potential to inflict severe damage and present significant risks to an agency's mission and national security.

Types of Insider Threats

Malicious Insider—someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. Malicious insiders have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

Careless Insider—a negligent employee or contractor who unknowingly exposes the system to outside threats. This is the most common type of insider threat, resulting from mistakes, such as leaving a device exposed or falling victim to a scam. For example, an employee who intends no harm may click on an insecure link, infecting the system with malware.

Mole—an imposter who is technically an outsider but has managed to gain otherwise valid insider credentials in order to access a privileged network, posing as an employee or contractor.

Identifying Insider Threats is Harder Than Ever

Authorized users have legitimate access to valuable information—bad actors often leverage valid accounts through exploitation of system weaknesses, misconfiguration, and vulnerabilities. Threats can come from anywhere and organizations must be prepared to respond.

- **Privilege misuse** is common to successful attacks. Adversaries abuse credentials of existing accounts to bypass access controls.
- **Threat context is important.** Overwhelmed by excessive alerts, incident response teams require intelligent tools to aid the manual evaluation of low severity events and prioritize response efforts.
- **IT security teams need force multipliers.** Organizations need to differentiate between appropriate data access and an insider threat incident. Capable automation enables focus on events that require human interpretation.
- **More applications, more paths to data.** Organizations struggle with solutions that don't allow for an increased number of applications and the exponential growth of data found in most organizations.

Risk-Based Analytics and Automation Increase Accuracy

Adopting a risk-based methodology allows for the evaluation of data according to an organization's risk profile and priorities, reducing the likelihood of a breach. User data access activity should be consistent across all environments.

- **Trust, but verify and track.** Database activity monitoring detects suspicious commands and access patterns. Organizations need to log historical records for future evaluation and auditing.
- **Prioritizing the handling of incidents is critical.** Even small improvements in accuracy can multiply incident response effectiveness. Automated prioritization of high-risk incidents allows security teams to stay focused.
- **Less noise, for more signal.** Context is essential to decision making. Effective data risk mitigation requires advanced security analytics to help security staff pivot from one issue to the next.
- **What happened and was it important?** 44% of organizations are blind to data activity and need to see data across the entire enterprise to monitor which sensitive data is being used and accessed, and by whom.

Automate Discovery of Non-Compliant, Risky, and Malicious Data Access Behavior Anywhere

Organizations must analyze user behavior and data access activities to accurately identify threats. It is essential to quickly understand critical, high, medium and low incidents; the users associated with them; and the data accessed. Organizations can boost the effectiveness of incident response teams through the use of strong tools that reduce repetitive tasks. Incidents should automatically be assigned a risk score that incorporates the sensitivity of the data, the privilege required for access, and the prevalence of the event. And, threat intelligence platforms and SEIMs should leverage new data access behavior context during event enrichment.

Insider Risk Management Through Thales Imperva Solutions

User behavior analysis is key to protecting against insider threats, but is not enough. Thales Trusted Cyber Technologies (TCT) can help U.S. Federal agencies reduce insider threats through Imperva Data Security Fabric (DSF). Imperva DSF protects your organization from data breaches and compliance incidents by augmenting traditional enterprise security approaches with controls for the data itself to drive policy-compliant data handling behavior and help security staff pinpoint and mitigate data threats before they become damaging events. The solution monitors how users move through the network while protecting assets on a data level, ensuring that whatever a malicious insider touches, you are in control.

Database Risk and Compliance

Imperva DSF's data risk analytics capability reduces exposure to insider threats by remediating vulnerabilities and protecting sensitive data. Organizations can:

- Identify the most significant data risks by severity and likelihood to prioritize risk mitigation.
- Gain specialized insights derived by fusing together a comprehensive range of data risk indicators and an overall organizational risk factor.
- Drill down for guidance and recommendations for appropriate action to mitigate gaps in risk protection.

Data User Behavior Analytics

Imperva DSF data risk analytics capability detects compromised accounts and malicious insiders as soon as behavior changes. The solution automates the detection of non-compliant, risky, or suspicious data access behavior of an organization's data repositories to determine if the behavior is an actual security incident. It provides visibility into a broad range of events from accidental exposures to persistent attacks by an evasive exploit for quick evaluation.

- Faster problem resolution times
- Categorize and prioritize by real risks, rather than anomalies
- Spot bad actors before they cause damage
- Correct non-compliance issues before audit failures
- Get clear summaries that explain complex issues in plain language
- Eliminate false positives, and enable SOC teams to focus on the critical issues

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com