OBSIDIAN

SOLUTION BRIEF

Uncover SaaS Insider Threats with Obsidian

Keep sanctioned users from engaging in unsafe or malicious activity across your applications and putting sensitive data at risk.

Understanding SaaS Insider Risk

The migration of important workflows and sensitive data to SaaS has driven attackers to target business applications more intently, as evidenced by several high profile breaches over the last few years. In response, security leaders have explored a number of proactive and reactive measures meant to minimize opportunities for adversaries and manage compromises when they do occur. As teams formulate their approaches to SaaS security, it's important to remember that threats to their environment are not exclusively external.

Whether purposely malicious or unintentionally careless, your sanctioned users can just as easily engage in unsafe behaviors and jeopardize sensitive internal data. Insider threats can be easy to overlook and difficult to address, especially for security teams with limited visibility into their SaaS environment. Roles, permissions, user activities—these crucial details play a role in measuring and managing insider risk.

Insider threat detection necessitates that security teams have clear insight into how their users are behaving and an immediate understanding of when this activity is unusual or unsafe. Moreover, ensuring users have access to only the permissions they need to do their job—and nothing more—upholds the principle of least privilege and reduces the likelihood and impact of insider threats.

Prevent and Mitigate Insider Threats with Obsidian

As the industry's most advanced SaaS security platform, Obsidian Security doesn't just enable teams to detect and mitigate compromises and insider threats—it also helps them understand and address the posture vulnerabilities that make these incidents more likely in the first place.

The platform continuously collects and normalizes activity data from every connected application to define a baseline of typical user behavior. This baseline informs Obsidian's cutting-edge machine learning models to detect incidents with unmatched speed and accuracy. These early indicators make it possible for security teams to investigate and mitigate insider threats in a timely manner, limiting data exfiltration and ultimately preventing sanctioned users from undermining the security of your SaaS applications.

Identify users who present a greater risk to your SaaS security.

Detect insider activity with threat models driven by machine learning.

Investigate incidents precisely with clear timelines of malicious activity.

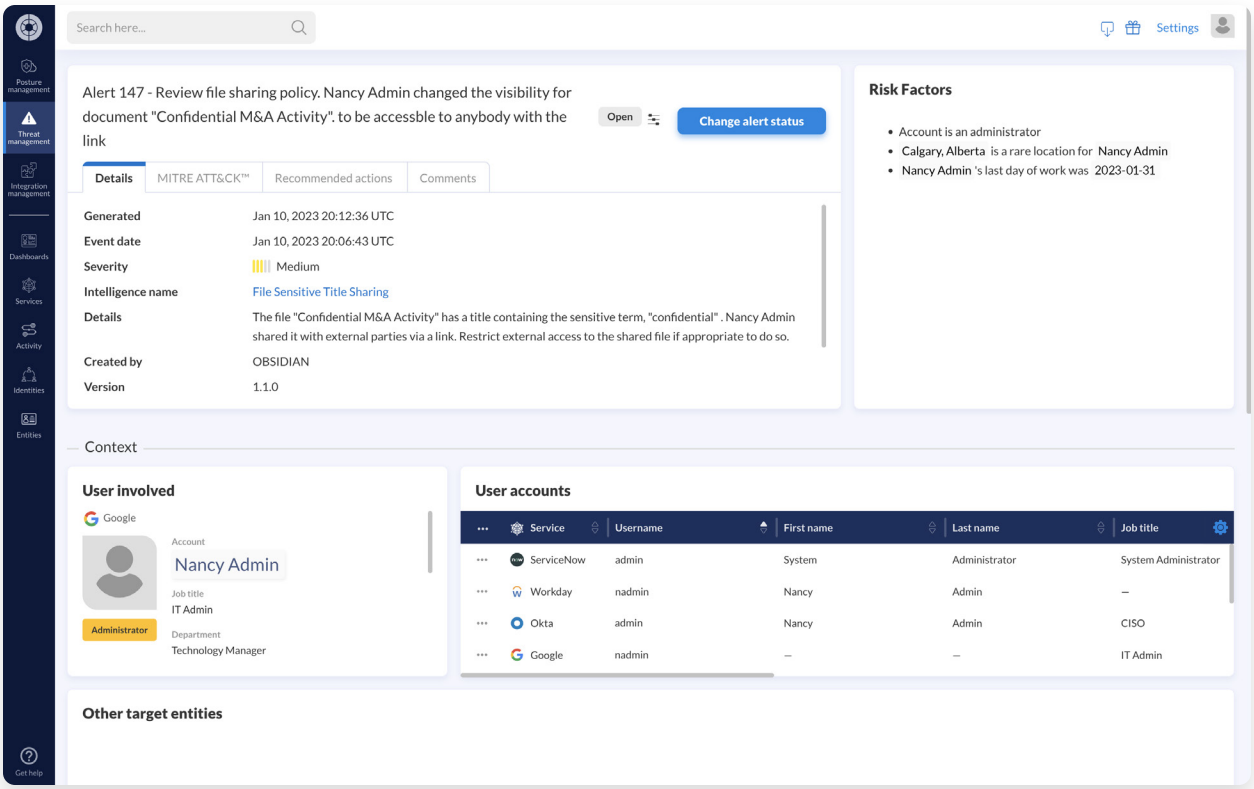
Tighten permissions and application controls to prevent future incidents.

Recognize users who pose a greater risk

Especially in larger organizations where SaaS applications are accessed by thousands of users every day, monitoring for insider threats can be a significant challenge. Obsidian helps teams prioritize and scale their detection capabilities by determining which users pose a greater potential risk to organizational security. This involves correlating cross-application context to identify users with administrator privileges or users with upcoming termination dates in Workday, for example.

Identify and investigate insider activity promptly

With a baseline of normal user behavior, Obsidian can promptly detect and notify your team when a user is acting in an unusually risky or malicious manner. A sudden spike in file downloads or the forwarding of business emails to an external inbox are two such examples of behaviors that may indicate the exfiltration of internal data. These detections are further refined as Obsidian cross-correlates this unusual activity with employment details in HR systems like Workday.



Minimize risk by tightening privileges and controls

The potential impact of an insider threat scenario is defined by the privileges entrusted to a given user. Obsidian helps teams manage user permissions and SaaS configurations to minimize opportunities for incidents to occur. Tighten controls to prevent broad file sharing, limit data exporting, block external email forwarding, and minimize other forms of risky behavior. Obsidian also highlights users with excessive or unused privileges to ensure these elevated permissions are delegated securely.