semperis

IDENTITY-FIRST SECURITY BRIEFING:

How to Protect Your Organization from Insider Threats

IGOR BAIKALOV
Semperis Chief Scientist and former SVP of global information security at Bank of America, with 20 years' experience in insider threat and risk monitoring

Insider threats—cyber incidents carried out by trusted actors—are increasing sharply. As with all cyberattacks, most breaches committed by inside threat actors involve access abuse, whether the compromise was the result of negligence or malicious intent. The global economic slowdown has resulted in layoffs and general uncertainty, creating conditions that raise the risk of insider threat attacks, whether they stem from decreased resources for training or security policy enforcement or from lower job satisfaction among employees—which can lead to retaliatory behavior.

Insider threats are particularly dangerous because they involve access abuse by trusted actors who, in order to do their jobs, have access to critical assets and sensitive data across the organization. But most security solutions focus on detecting illegitimate access. To adequately address insider threats, organizations need solutions that protect the core identity system itself by scanning for identity system vulnerabilites that insiders can abuse, detecting and automatically remediating risky changes, shining a light on attack paths into critical assets, and providing post-breach forensics to close backdoors left by malicious insiders. In particular, organizations in the midst of major transitions, such as consolidating business offices or reducing the overall workforce, need the ability to take action on suspicious activity from high-risk users—such as employees who are flagged as a flight risk or are slated for upcoming termination.

Insider threats are on the rise—again

Although external malicious actors receive most of the media attention, insider threats—stemming both from negligence and from malicious intent—are on the rise. According to the Ponemon Institute's *2022 Cost of Insider Threats Global Report*, 67% of companies experience 21 to 40 insider-related incidents per year—up from 60% in 2020—with each incident incurring an average cost of $484,931. Insider threats are notoriously difficult to eradicate: It takes victim organizations an average of 85 days to contain an insider-related incident.

Insider threats can come from malicious intent or negligence

56%

of insider-threat attacks are caused by ***employee or contractor negligence***

26%

of insider-threat attacks are caused by ***malicious insiders***

Source: *Ponemon Institute 2022 Cost of Insider Threats Global Report*

Access abuse underlies internal threat incidents

Anyone who has permission to access critical business assets can potentially abuse that privilege, either through negligence or malicious intent. Negligence can lead to system compromise in several ways, but the result is the same: Because of a mistake someone made—for example, an end user who left their laptop unlocked or an Active Directory admin who failed to follow defined employee off-boarding policies—privileged credentials are easy picking for malicious actors. An inside threat actor with malicious intent can use privileged access to compromise the organization's system for a variety of reasons, from monetary gain to revenge. Regardless of the intent, access abuse underlies insider threats. An identity-first security strategy that addresses every phase of the cyberattack lifecycle—including recovering from an insider attack if the worst happens—is critical to protecting organizations from insider threats.

"Based on my experience addressing insider threat and risk monitoring at Bank of America, I can attest that the stark increase in inside threat incidents is a warning to organizations that haven't yet implemented a comprehensive identity threat detection and response solution. Access abuse is the common element in insider attacks. Employees, contractors, vendors, and partners can inflict devastating damage on organizations, either out of carelessness or malice. ***Protecting against insider threats requires a concerted effort***—a comprehensive strategy that addresses every phase of the attack lifecycle, including prevention, remediation, and recovery."

— **Igor Baikalov**, *Semperis Chief Scientist and former SVP of global information security at Bank of America*

How Semperis Protects Organizations from Insider Threats

Semperis has specific capabilities for detecting and remediating insider threats stemming from access abuse to the identity system by trusted actors (employees, contractors, partners, or vendors), whether the activity is motivated by negligence or malice. Semperis protects organizations' core identity system—which is Active Directory (AD) and Azure Active Directory for 90% of businesses—before, during, and after attacks by inside threat actors:

- **Before attack:** Uncovers security vulnerabilities that could pave the way to access abuse by trusted actors (for example, accounts with expired passwords and inactive accounts), enables deployment of an **identity freeze**—preventing certain changes by a defined set of users—in advance of terminations to forestall malicious changes by disgruntled employees, and provides visibility into attack paths to critical Tier 0 assets
- **During attack**—Continuously monitors for indicators of compromise (IOCs), tracking risky changes to on-prem AD and Azure AD, and automatically rolls back specific changes that could signal an attack—for example, unexplained additions to the Domain Admins group
- **After attack**—Provides post-breach forensics capabilities to uncover attack techniques used by insiders and close backdoors into AD and Azure AD

Attack technique	Example scenario	How Semperis addresses
Privilege escalation	Because of inadequate controls, an IT helpdesk employee discovers the ability to create an account for himself with elevated privileges	Monitors for new accounts created with elevated privileges, automatically rolls back account creation, and sends an alert
Logon/access abuse	Active Directory administrator who discovers he'll soon be terminated makes changes to the identity system to leave a backdoor into the system	Allows deployment of an identity freeze—immediately detecting, automatically rolling back, and alerting on any changes made by or to a defined list of employees, vendors, or contractors
Access privilege misconfiguration	Active Directory admin mistakenly gives access to signing keys to the entire development group, enabling a vindictive developer to write and deploy malware	Detects risky changes to permissions and flags entire attack paths to critical assets
Excessive/unused privilege exploit	Former employee with knowledge of an enabled but inactive admin account uses credentials to steal sensitive data	Monitors and reports on indicators of exposure and compromise, including enabled admin accounts that are inactive
Abusing account with expired password	Unhappy IT department employee conducting an AD hygiene exercise uncovers a highly privileged account with an expired password and resets the password with the intent to steal sensitive data	Monitors and automatically rolls back password reset
Remote access software configuration	An organization with a complex network of third-party vendors discovers malware propagating through the system, causing system failures throughout the supply chain	Monitors permissions that are allocated to specific groups of software users (for example, a vendor group), automatically rolls back changes that indicate vendor identity permission escalation into critical systems, and monitors for changes in attack paths to critical assets
Backdoor user creation	An AD admin who discovers she's on a list for termination exploits the SMTP Matching Abuse in Azure AD to set up a backdoor to the system that goes undetected by the organization's SIEM system	Detects attacks that bypass traditional log- and event-based systems such as SIEM by monitoring changes in the identity system

Identity-First Security Steps to Guard Against Insider Threats

Action steps organizations can take now to shore up defenses against insider threats:

1. Download **Purple Knight**, a free community AD security assessment tool, to scan the environment for indicators of exposure (IOEs) or compromise (IOCs)
2. Download **Forest Druid**, a free Tier 0 attack path discovery tool that helps defenders quickly close attack paths to the organization's most sensitive assets
3. Use **Directory Services Protector (DSP)** to continuously monitor and automatically remediate unwanted changes across both on-prem AD and Azure AD
4. Use **Active Directory Forest Recovery (ADFR)** to ensure fast, malware-free AD forest recovery in the case of an insider attack

semperis