Case Study

Insider Threat

Insider Data Leaks to Unauthorized Third-Parties

Safeguarding the tech industry **from insider data leaks to unauthorized third-parties**

SITUATION

Insiders leaking sensitive information to third-parties can severely impact organizations. When employees with authorized access misuse their privileges to share sensitive information, it exposes the organization to financial losses, potential legal repercussions, and operational disruptions. Because of these risks, it is essential for organizations to implement robust security measures to detect and prevent insider threats.

A technology company discovered that proprietary information was being leaked to unauthorized third-parties. The leak threatened the company's competitive position and raised serious concerns about potential ongoing breaches. Suspicion soon centered on a disgruntled employee with access to the compromised data.

To address these risks, the Client sought assistance from Nisos to confirm whether this individual was responsible for the leaks and to explore solutions for preventing future incidents. The Client required a thorough investigation and effective mitigation controls to protect their sensitive information and secure their internal environment.

INVESTIGATION

This investigation began with a targeted review of leaked content and Human Resource (HR) records to identify potential suspects. A review of firewall and VPN logs identified one individual who used their personal third-party file share to violate corporate policy, exfiltrate the sensitive data, and provide unauthorized access to a third-party.

Nisos worked with the Client's IT team to implement a device check at the suspect's work location, allowing us to isolate the employee's device for forensic analysis.

Our findings provided conclusive evidence of collusion with external parties. In coordination with physical security, we matched digital logs to surveillance footage, confirming that the employee had been taking photos of sensitive data on their phone and sending it through encrypted chat to unauthorized third-parties.

IMPACT

Our investigation empowered the Client to act decisively by collaborating with their HR and legal teams to terminate the insider without further incident. In addition to identifying and addressing the leak, Nisos provided strategic guidance to strengthen the Client's security posture, including configuring monitoring systems to detect unauthorized file-sharing activity and refining bring your own device (BYOD) policies to enforce device security.

The Client acknowledged that Nisos' intervention not only prevented additional leaks, saving significant resources, but also laid the groundwork for a robust insider threat program that involves engineering, legal, and HR in a coordinated defense against internal risks.

Nisos brought a multifaceted approach to the investigation, seamlessly blending digital forensics with discrete physical security data-gathering techniques that allowed us to collect evidence without alerting the employee.

Let's **Connect**

Nisos is the human risk management company specializing in unmasking threats before they escalate. We are a trusted advisor who operates as an extension of security, intelligence, legal, and human resource teams to protect their people and business. Our intelligence-led solutions help enterprises make critical decisions, manage human risk, and drive real world consequences for digital threats. For more information, visit **nisos.com**.

For more information:

visit: www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn