NUIX NEO INVESTIGATIONS FOR INSIDER THREATS

Nuix Neo Investigations redefines insider threat management with advanced AI, forensic-grade processing, automation, and behavioral analytics, enabling teams to swiftly detect, investigate, and mitigate risks. By uncovering hidden patterns, automating workflows, and providing proactive threat detection, Nuix allows organizations to act decisively to protect critical assets, fast.

Insider threats are an evolving and increasingly pervasive challenge for organizations. Whether resulting from malicious intent or employee negligence, these threats can lead to devastating financial, operational, and reputational consequences.

Effectively addressing these risks and incidents requires the ability to swiftly identify suspicious behaviors and emerging risks within vast volumes of data. This includes proactively uncovering suspicious activity, accelerating risk detection, and recognizing subtle cues and patterns that may indicate intellectual property theft, malicious intent, or policy violations.

According to the 2024 Insider Threat Report[1] 83% of organizations experienced at least one insider attack in the past year. With incidents averaging over $15 million in damages, and containment of insider incidents stretching to 85 days on average.

Insider threats can quickly spiral from internal issues to public crises. Failure to mitigate insider threats can result in substantial economic losses, stolen intellectual property, regulatory fines, customer attrition and loss of trust.

> **The adoption of Nuix Neo Investigations has revolutionized our investigation process. The system now flags matters involving intellectual property, trade secrets, and confidential information, ensuring high-risk cases receive immediate attention. This shift has cut incident evaluation and response time from an average of 7 ½ days to less than 24 hours."**
>
> Large Global Pharmaceutical Corporation.

HARNESS DATA. HALT RISKS.

Nuix Neo Investigations ingests and analyzes terabytes of data from emails, file systems, endpoints and more, using proactive scanning and real-time monitoring to detect insider threats at speed and scale. With responsible and tuneable AI, behavioral mapping, and automation, it streamlines detection to investigation so teams can act decisively before risks escalate.

With Nuix Neo Investigations, investigators can:

◎ **DETECT EMERGING THREATS**
Identify suspicious behavior patterns, exfiltration attempts, and insider misconduct with advanced user and entity behavior analytics.

🔍 **UNCOVER HIDDEN CONNECTIONS**
Correlate data from multiple sources including endpoints, sharepoint, user activity logs, and external communications to reveal previously undetected relationships and activities of concern.

🔳 **ACCELERATE FORENSIC INVESTIGATIONS**
Quickly build comprehensive activity analysis, automate case workflows, and simplify evidence review for faster resolutions.

🔄 **STREAMLINE COLLABORATION**
Consolidate disparate data into a unified view, making real-time collaboration seamless across teams.

◎ **ACT FAST**
Detect anomalies, automate responses, and tailor detection policies to prioritize the highest-risk indicators before damage occurs.

1. 2024 Insider Threat Report, by Cybersecurity Insiders

ADVANTAGES OF NUIX NEO INVESTIGATIONS

Nuix Neo Investigations empowers Security and Investigative teams to manage insider threats with greater efficiency and forensic precision. Unlock powerful insights, gain operational clarity, and drive insider risk monitoring with Nuix.

Responsible AI

Deploy Nuix's responsible Cognitive AI (CogAI) alongside its ability to ingest and understand data at a binary level, enabling the analysis of over 1,000 file types. With hundreds of easily tuneable out of the box AI models, Nuix CogAI automates the interpretation, classification, categorization, and enrichment of your data, to surface critical insights with defensible results.

Industry-Leading Processing

Harness Nuix's patented processing capabilities to sift through multi-terabyte datasets with forensic precision, speed and scale. Reduce false positives and unnecessary alerts to focus on real threats.

Advanced Automation

Process data 24/7/365, and operate investigations at scale with flexible, transparent, repeatable and automated workflows. Quickly identify insider threats and save time and resources by streamlining repetitive tasks and enabling analysts to quickly concentrate on what matters most.

Proactive Defense

Continuously monitor for threats with real-time detection, deploy automated responses to evolving risks, and isolate compromised endpoints instantly. Anticipate and counteract emerging threats with a unified view of live and historical activities.

Customizable Dashboards

Craft personalized views to spotlight the most relevant insider threat indicators. Surface tailored insights based on your role or investigative focus to identify risks faster and more effectively.

Enhanced Analytics and Visualization

Leverage relationship mapping, deep-link analysis, and visual timelines to spot patterns and extract meaning from complex insider threat scenarios.

Scalable and Secure

Designed to fit organizations of any size, Nuix Neo Investigations scales to meet the demands of hundreds of users. Achieve regulatory compliance and manage your most pressing inside risk exposures, with user-specific views for secure, role-specific access, and regulatory compliance.

WHO NEEDS NUIX NEO INVESTIGATIONS FOR INSIDER THREATS?

Ask yourself these questions to determine if your organization could benefit from Nuix Neo Investigations:

> Are decentralized or siloed data systems creating blind spots in addressing insider threats?

> Are you struggling to differentiate between malicious actions and benign activity?

> Do you have a full understanding of your organization's data and potential vulnerabilities that insiders could exploit?

> Do you know precisely who has accessed your intellectual property, trade secrets, and confidential information in the last 24 hours, and why?

> Can you trace insider activities across email logs, endpoints, and cloud repositories at speed and scale?

> Is your current insider threat incident evaluation time longer than 24 hours?

> Do false positives waste your team's time and delay critical investigations?

> Are you concerned that external actors are using stolen credentials to appear as insiders, making detection harder?

GET STARTED TODAY

Take the first step in revolutionizing the way your organization handles insider threats. Nuix Neo Investigations turns your data into actionable intelligence, helping you detect risks early, investigate efficiently, and act decisively. Contact us for a demonstration to see how you can equip your Security and Investigations Teams with cutting-edge collaboration, advanced automation and responsible AI to swiftly spot and stop insider threats. Speak with Nuix today.

Speak to us today to find out more
nuix.com/contact-us