



Proactive Threat Detection and Vendor Monitoring: An MAMAA Success Story

CASE STUDY



Introduction

In the rapidly evolving world of cybersecurity, HackNotice stands out for its cutting-edge, tailored monitoring and alert services. With real-time, actionable threat intel, HackNotice has redefined how businesses approach digital security. Moreover, our commitment to customizing our services to each client's unique needs sets us apart in a crowded field.

The Challenge

A prominent MAMAA company, with its vast digital assets and global footprint, faced significant challenges in rapidly monitoring threats and managing third-party vendor risks. In an environment where digital threats are increasingly sophisticated, and where time is of the essence, the company sought a partner capable of providing advanced, instant threat intelligence and independent vendor monitoring – functions that other and tech stacks had proven unable to provide. Threat intel companies and tech stacks had proven unable to provide.

Solution

HackNotice's real-time, detailed monitoring service, tailored to the company's specific security environment, provided powerful solutions:

Immediate, API-Configured Threat Detection:

We provided the MAMAA company with targeted alerts specific to their digital landscape, sent instantly, plus a robust API to automate ingestion into their internal systems, effectively creating a real-time pager system of vendor security incidents.

Superior, Scaled Vendor Monitoring:

Uniquely, our service offered independent third-party vendor monitoring, enabling the company to maintain a vigilant eye on thousands of vendors across a dauntingly complex, vast supply chain, and freeing the company from reliance on vendor disclosures. The economic, flexible addition and removal of vendors added further benefit.



Results

“We’ve been really happy with the service. Last month alone you provided us with 12 actionable alerts.”

Enhanced Security Posture

The 12 actionable alerts provided by HackNotice (in a single month) exemplify the proactive stance we enabled the company to take against potential digital threats. Moreover, detection and response times were dramatically shortened via HackNotice’s real-time alerts.

Independent Oversight

Our third-party vendor monitoring allowed the company to strengthen its defenses without relying on vendor disclosures, empowering them to take quicker and more effective remedial actions.

Customized, Immediate Intelligence

Each alert delivered was tailored, sent in real-time, and relevant, significantly reducing the time to remediation and enhancing overall security resilience.



About HackNotice

HackNotice is the leader in dark web intelligence and breach monitoring, helping organizations around the world reduce risk from credential exposure, data leaks, and supply chain threats. Our platform continuously monitors the global dark web—including criminal forums, Telegram, marketplaces, and breach archives—for stolen credentials, infostealer logs, and leaked corporate data.

HackNotice provides real-time alerts for ransomware events, data breaches, and account exposures, empowering security teams to take immediate action. From individual employee protection to comprehensive vendor monitoring, we help enterprises detect and mitigate risk before it becomes a compromise.

Our services include:

Credential and Session Exposure Monitoring

Discover when your employees, customers, or systems appear in infostealer logs or breach dumps.

Third Party and Supply Chain Risk Intelligence

Track vendors and partners for breaches, ransomware attacks, or data leaks that may put your business at risk.

Ransomware & Data Breach Alerts

Get real-time, actionable notifications about new attacks across your ecosystem.

Dark Web Incident Analysis

Receive deep-dive investigations into specific dark web data incidents, including attribution, scope, and remediation guidance.

With HackNotice, your team gains early visibility into attacker data and behavior—enabling you to respond quickly, protect identities, and minimize business disruption. [Learn more at hacknotice.com](https://hacknotice.com) or [contact us](#) to schedule a tailored threat briefing.