



Enhancing Vendor Risk Monitoring with Dark Web Intelligence:

A Success Story in the Educational Services Sector



CASE STUDY





Introduction

In today's threat landscape, educational institutions are increasingly targeted by attackers seeking to exploit third-party weaknesses. While many rely on traditional security ratings services to evaluate vendor risk, these tools often miss the exposure indicators that matter most: breached credentials and social engineering pathways. HackNotice equips organizations with real-time visibility into dark web threats, helping teams identify vendor vulnerabilities that traditional tools overlook.

For this small but security-conscious educational services company, HackNotice's Third Party Monitoring transformed how they approach vendor risk management.

The Challenge

The organization needed a way to assess and continuously monitor the dark web exposure of their third-party vendors. While they were using a traditional third-party risk ratings platform focused on SSL misconfigurations, vulnerability scans, and public posture, it wasn't surfacing the data they felt was most closely tied to real-world compromise.

With phishing and credential theft among the leading causes of breaches, the network admin sought a solution that would highlight which vendors had actual leaked data circulating on the dark web, and whether threat actor targeting was increasing.



Solution

HackNotice's **Third Party Monitoring** provided a powerful new lens into vendor risk by offering dynamic tracking of breaches, infostealer data, and dark web activity tied to their supply chain.

Continuous Threat Factor Scoring

Each vendor was assigned a dynamic Threat Factor score based on historical breach/ransomware incidents and their presence in dark web leak files—providing an attacker-centric view of vendor risk.

Complement to Traditional Ratings

HackNotice served as a complementary source of intelligence to their existing Security Ratings Service (SRS), offering insights that focus on **real threat actor data**, rather than just surface-level posture.

Cost-Effective Supply Chain Visibility

With the ability to monitor a broad vendor set without incurring prohibitive costs, the organization expanded its coverage and immediately began surfacing high-risk partners that warranted deeper scrutiny.



Results

A Network Admin in the education sector shared that HackNotice's Threat Factor ratings revealed high-risk vendors with dark web exposure that would have otherwise gone undetected.

More Effective Risk Decisions

Vendors flagged by HackNotice's Threat Factor score led to immediate reviews and follow-up actions, enabling the team to take a more proactive and data-driven approach to vendor oversight.

Improved Supply Chain Coverage

Unlike legacy SRS tools that limited the number of vendors they could afford to monitor, HackNotice's flexible model allowed them to scale visibility across the full supply chain.

Real-World Attack Surface Awareness

By focusing on data actually trafficked and weaponized by attackers—such as stolen credentials and infostealer logs—the organization aligned their third-party monitoring efforts with real-world threats.



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.