Use Case: Third-Party Risk Monitoring

THIRD-PARTY VULNERABILITY MONITORING

PROBLEM:

DON'T LET THREAT ACTORS IN THROUGH THE SIDE DOOR!

Your organization doesn't go it alone; it's common to use third parties to tap into specialized skills and enhance efficiency. Yet, this collaboration can also introduce significant cyber risk. Third parties are increasingly interconnected with the organizations they serve. They often sharing access to their systems and data but, as a result, your organization is subject to your third parties' vulnerability management policies, which may vary in strength from your own.

Threat actors search for the weakest point in your attack surface to gain access, which may be via a vulnerability in third-party infrastructure or the products they have supplied. Once they've gained access to a third-party, they can move laterally to target connected organizations, including your own. Real-time visibility of the risks arising from these vulnerabilities is crucial for stopping cybercriminalsfrom entering through the side door, before it is too late.

INTEL 471 SOLUTION:

ACHIEVE VISIBILITY OF THIRD-PARTY VULNERABILITY THREATS

Intel 471 provides you with a window into the vulnerabilities affecting your third parties and the goods they supply. Its comprehensive monitoring of the cyber underground provides near-real-time intelligence about vulnerability life cycles, active threats, and threat actors who may be exploiting them. By tracking precursors to exploitation, such as increasing interest levels among threat actors or proofs of concept (PoCs) being developed, you can track threats as they evolve. Customers can seamlessly pivot to analyst-driven assessments and related intelligence reports which offer expert contextualization of the risk associated with the vulnerability, and consequently, your own organization. Intel 471 empowers you to deploy early defensive action to safeguard your assets against threats via third-party vulnerabilities.

© Intel 471 Inc. All rights reserved.

KEY FEATURES:

- **Continuous monitoring of cyber underground,** including exclusive forums and instant messaging platforms, for the early detection of vulnerabilities in third-party infrastructure and products, and emerging threats to them that may impact your own organization.
- **Live vulnerabilities dashboard** continuously tracks precursors to exploitation and delivers timely alerts when changes are identified.
- **Pivot to analyst-driven intelligence reports** on vulnerabilities, including proof of concept and exploitation code analysis, and the threat actors targeting them.
- **Map the external attack surface of third parties** to identify misconfigured ports, unpatched applications, shadow IT and more within third parties.

KEY BENEFITS:

- **More effective threat mitigation** with the early detection of threats to third-party vulnerabilities enabling a proactive response.
- **Strategically allocate resources** to address critical areas of risk from third-party vulnerabilities.
- **Aid third-party patch prioritization** with real-time, contextualized vulnerability intelligence.
- **Improve risk management** by using Intel 471 intelligence to better assess and manage threats extending from third-party relationships.

MONITOR THIRD-PARTY VULNERABILITIES WITH INTEL 471

Third-party vulnerability monitoring is part of Intel 471's Third-Party Risk Monitoring set of capabilities. It is designed for organizations who want to reduce risks associated with third-party interactions, products, and services. Third-Party Risk Monitoring solutions provide customers with threat intelligence and information to assist with the identification and remediation of risks introduced by interconnected vendors, customers and other third-party entities, and includes:

- Third-party vulnerability monitoring
- Third-party breach monitoring
- Third-party compromised credentials monitoring
- Supply chain risk monitoring

Limit the potential entry points for threat actors seeking to exploit an organization through its third-party relationships and ensure an agile threat response with the close monitoring of vulnerability lifecycles and best-in-class cyber threat intelligence.

ABOUT INTEL 471

Intel 471 arms enterprises and government agencies to win the cybersecurity war using real-time insights from the cyber underground. Organizations leverage our cyber intelligence platform to protect from costly security breaches and cyber incidents by solving real-world use cases, including third-party risk management, security operations, attack surface protection, fraud and more. Learn more at www.intel471.com.

Your Voice of Reason and Truth.

SALES@INTEL471.COM

© Intel 471 Inc. All rights reserved.