INTEL471

Use Case: Third-Party Risk Monitoring

THIRD-PARTY BREACH MONITORING

PROBLEM:

YOUR ORGANIZATION IS ONLY AS SAFE AS YOUR THIRD PARTIES

Your third parties can open up even the most security-conscious organizations to severe cyber security threats: Cyber attackers sniff out your connections that have less robust cybersecurity protocols. Credentials, banking details, patents; once inside, they can enjoy access to any of the sensitive and confidential data that you have shared and use it for their own illicit ends. No matter how the threat actors got their hands on your information, it is you who must withstand the consequences of your data being breached. Enduring legal implications, the erosion of stakeholder trust, and devastating blows to finances can undermine even the most resilient. As organizations continue to transform to rely on third parties, it's vital you prepare against the looming threat of third-party data breach.

INTEL 471 SOLUTION:

REAL-TIME VISIBILITY FOR A RAPID REACTION TO THREATS

Intel 471 provides you with the means to proactively track the threat of data breaches across your third-party ecosystems. Its sophisticated malware systems, automated collection, and research teams provide unparalleled visibility of the spaces where cybercriminals offer goods for sale and communicate plans so that you can quickly identify when a third-party has potentially been breached or is in an attacker's crosshairs. Intel 471 empowers you to stay ahead of the attackers and mitigate the repercussions of a third-party breach.

KEY FEATURES:

- **Advanced detection of potential third-party breaches** from sources exclusive to Intel 471's collection capabilities, including access to closed sources and sophisticated malware systems.
- **Near real-time monitoring and alerting** of potential and successful breaches of third-party companies and their own organizations.
- **API Integration** with internal tooling, SOAR platforms, and third-party databases.
- **Map third-party internal attack surfaces** to pinpoint vulnerabilities attackers may exploit as a stepping stone.
- **Gain technical malware intelligence**, such as indicators of compromise, to identify intrusion attempts and malware infections more readily.
- **Access to adversary linked insights,** including actor tactics, techniques, and procedures (TTPs), to support incident response and further threat research.

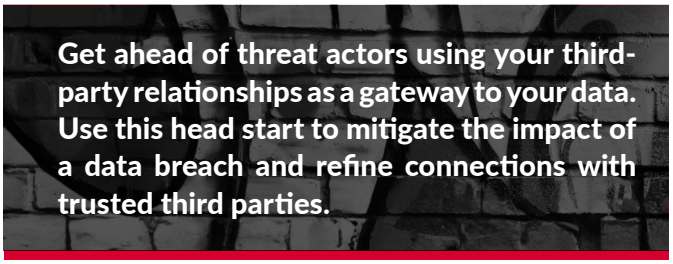
KEY BENEFITS:

- **Proactive prevention and mitigation of third-party data breaches** through early detection of possible incidents.
- **Inform business strategy** by evaluating third-party relationships against the risk they bring to a company.
- **Improve orchestration and automation of incident response,** in the event of a third-party data breach through API integration.

MONITOR THIRD-PARTY BREACHES WITH INTEL 471

Third-party breach 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. Our 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



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