

# L SUPPLY CHAIN RISK MONITORING



**PROBLEM:**

## **YOU'RE ONLY AS STRONG AS THE WEAKEST LINK IN YOUR SUPPLY CHAIN**

Your organization doesn't go it alone. Globalization has ensured dependence on an intricate supply chain of third parties to facilitate the production and distribution of your goods and services. Although they bring business benefits, each organizational link in a supply chain also increases your attack surface, resulting in a struggle to maintain visibility of each entity in order to defend it from cyber threats. As a result, you don't often see the risk of third-party compromised credentials, data breaches, and critical vulnerabilities until it's too late. Maintaining comprehensive visibility of your supply chain risk is not only a regulatory necessity for many, but paramount if you are to proactively mitigate its impact and avoid ensuing business disruption, legal implications, erosion of stakeholder trust, and ultimately revenue decline.

**INTEL 471 SOLUTION:**

### **COMPLETE DIGITAL SUPPLY CHAIN RISK VISIBILITY**

Intel 471 reduces digital supply chain risk by providing continuous monitoring, alerting, and full contextualization of cyber threats to your supply chain. This involves tracking the life cycles of vulnerabilities that may be potentially exploited, near-real-time alerting to potential breaches, and monitoring the sale of third-party compromised credentials to prevent a cyber incident within your organization's own walls. Leveraging insight into exclusive sources, Intel 471 provides both awareness of pre-indicators of attack and early detection of compromised entities to empower you to take control of your supply chain risk.



## KEY FEATURES:

- **Early detection of supply chain risk** via the continuous monitoring of the cyber underground.
- **Unique visibility** into spaces, such as exclusive forums and instant messaging platforms, where threat actors communicate.
- **Live vulnerabilities dashboard** continuously tracks precursors to exploitation and delivers timely alerts when changes are identified.
- **Live credentials dashboard** ensures easy monitoring and assessment of key information relevant to compromised credentials of supply chain entities, including date ranges, occurrence across other data sets, and links to related intelligence reports.
- **Timely breach reports** alert of an imminent or potential breach of a supply chain entity.
- **Swiftly pivot to related analyst-driven intelligence reports** and other key information.

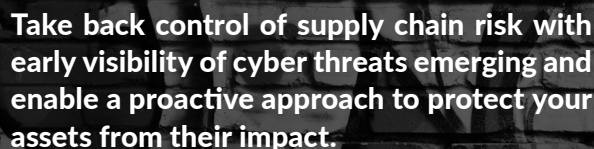
## KEY BENEFITS:

- **Enable a proactive response to supply chain risk** to ensure effective mitigation of its effects.
- **Strategically allocate resources** to address critical areas under threat from supply chain risk.
- **Act decisively** with fully contextualized threat intelligence.
- **Support strategic business decisions** by using Intel 471 intelligence to better evaluate supply chain relationships.

## MONITOR THIRD-PARTY VULNERABILITIES WITH INTEL 471

Supply chain risk monitoring is part of Intel 471's Third-Party Risk Monitoring. This set of capabilities 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



Take back control of supply chain risk with early visibility of cyber threats emerging and enable a proactive approach to protect your assets from their impact.

### 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](http://www.intel471.com).

**Your Voice of Reason and Truth.**

**SALES@INTEL471.COM**

