EXIGER

THIRD-PARTY AND SUPPLY CHAIN RISK MANAGEMENT

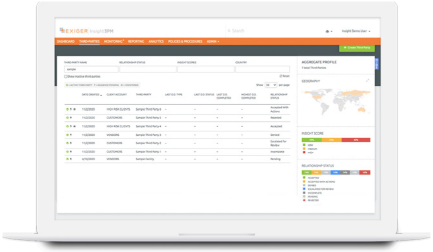
Cyber Vulnerability Detection & Mitigation

Now more than ever, cybersecurity is a key part of supply chain risk. Wide-ranging vulnerabilities—like we see with Log4j—and recent breaches such as SolarWinds and Accellion have demonstrated how software itself can become the Trojan horse, turning the products that protect us into an ecosystem-wide threat. The cyber hygiene and risk management practices of the third parties we rely on can help us assess how susceptible they are to our own ecosystem or external breaches that could change or modify code.

Cyber risk is an indicator of overall operational resilience; not just a question of who you are giving your data to. The Apache Log4j vulnerability is an exemplar that today's cyber risks require a cyber risk assessment that fits seamlessly into your comprehensive vendor risk management program, including real-time threat and vulnerability analysis to inform immediate mitigation at the speed of relevancy.

THREAT VECTORS

!
Supply Chain Risk
!
Cyber Vulnerabilities
!
Threat Actors



DID YOU KNOW?

Exiger's third-party risk management tools can assess, detect and mitigate Log4j and other similar vulnerabilities?

EXIGER
Governance. Risk. Compliance.

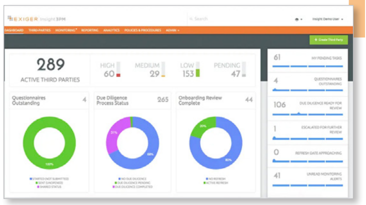
> “We were able to change the game on supply chain using commercially available tools, and one of them for the trusted capital program is called **Exiger DDIQ**. We run companies through, and we can look at their financials for anything on the company, from who is on the board, to where their financing has come from, legal issues etc.”

PENTAGON BRIEFING 2020
Under Secretary of Defense for Acquisition and Sustainment
& Chief Information Security Officer for DoD Acquisition and Sustainment

EXIGER SOLUTIONS

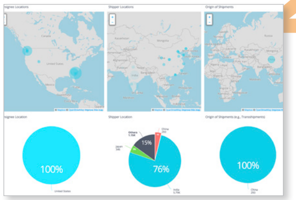
How We Can Help

1



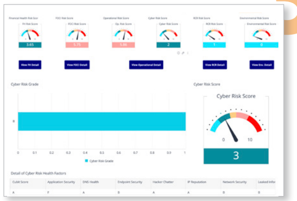
Survey Entities and Collect Data to Establish Risk and Criticality

2



Discover your Supply Chain and Supplier Network

3



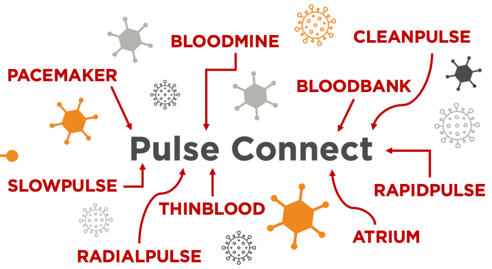
Analyze Risk

4

Comprehensive Due Diligence & Risk Mitigation

CASE STUDY

How Leading Companies and Government Agencies are Mitigating Risk in Their Supply Chains



THE CHALLENGE

As vulnerabilities and threats collide, Exiger clients use DDIQ Analytics to navigate their physical and cyber supply chains to create immediate actionable insight.

THE SOLUTION

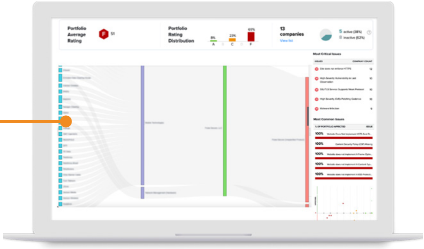
In the last three years, our clients have seen over **30** severe vulnerabilities targeted by hackers, often linked with powerful nation-state actors. In 2021, two cyber espionage groups, believed to be affiliated with the Chinese government, created over **16** different malware families just to target Pulse Secure VPN.

Total Software Being Tracked
36
Location of Companies Using Software
Top-Level Industry Software Usage
Sub-Level Industry Software Usage
58%

THE IMPACT

Utilizing DDIQ Analytics, Exiger clients are able to instantaneously identify and assess the criticality of threat in their environment.

DDIQ Cyber Analysis combined with SecurityScorecard creates a real-time view of the threat and the vulnerabilities to allow for risk-based mitigation, stopping the threat where it matters most.



2019 Canadian FinTech & AI Awards WINNER

Regulation Asia Awards for Excellence 2021
Winner
Exiger
Best Solution
Due Diligence
& Third Party Risk

REGTECH100 2020

SUPPLYCHAINBRAIN GREAT SUPPLY CHAIN PARTNER 2021

Top 100 Financial Technology Company 2021

CENTRAL BANKING FINTECH REGTECH Global Awards 2020
ANTI-MONEY LAUNDERING PARTNER

THE 10 BEST SUPPLY CHAIN SOLUTION PROVIDERS, 2021

ALM Intelligence
Vanguard Leader
in FCC Solutions

Gartner
COOL VENDOR
2020

MAKING
THE WORLD A
SAFER PLACE
TO DO BUSINESS

For more information, contact:

Daniel Banes
President, Commercial Technology
dbanes@exiger.com

Erika Peters
Managing Director, Global Head of SCRM and TPRM
epeters@exiger.com

Skyler Chi
Associate Director, Deputy Global Head of SCRM and TPRM
schi@exiger.com

exiger.com