Panorays

Risk Insights and Response Portal

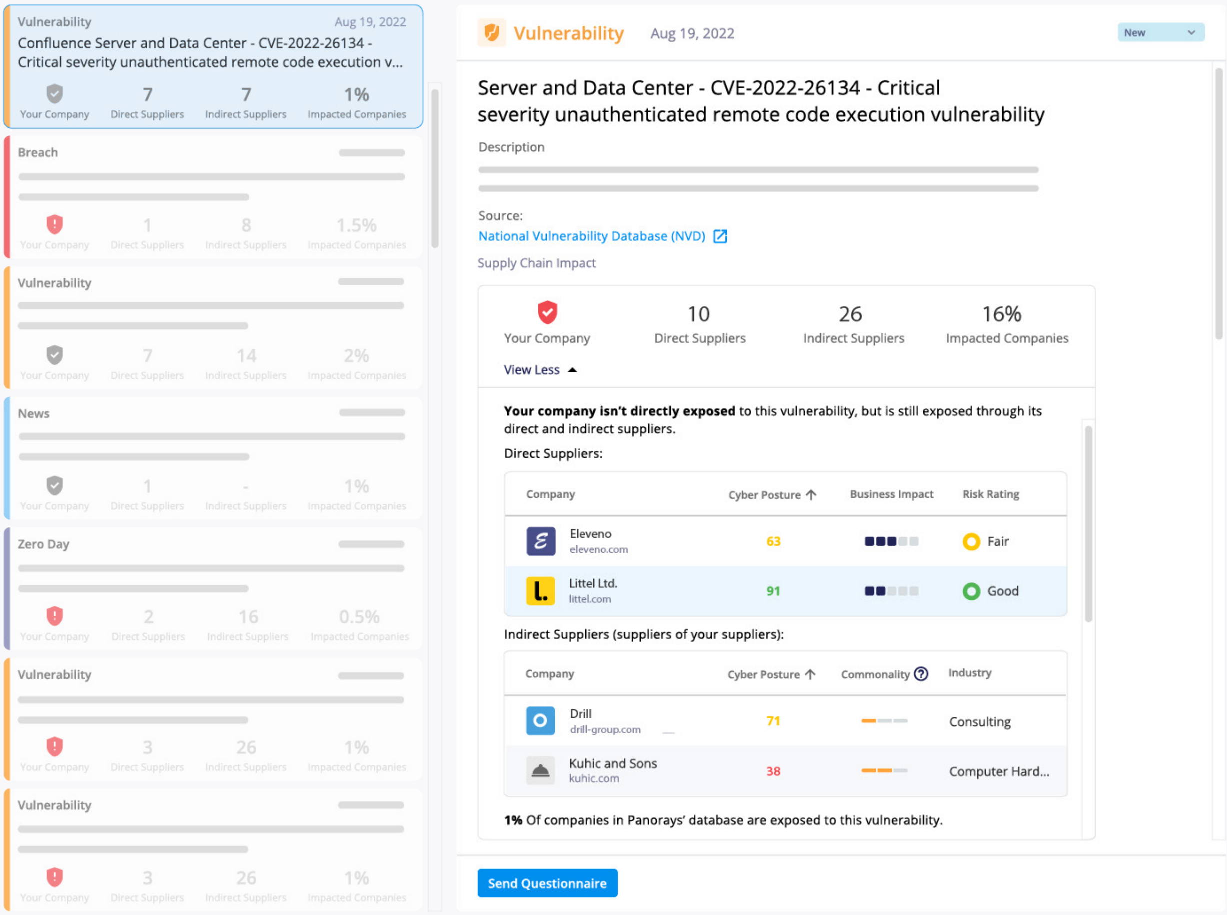
Today’s Challenges in Responding to Third-Party Risks

The rise of third-party breaches continues to pose one of the biggest threats to cybersecurity across the globe. Organizations are investing in third-party security risk management now more than ever, with the implementation of continuous monitoring and threat detection becoming essential to ensure the security of the entire supply chain.

As the number of third parties per company grows, security teams struggle to navigate a complex threat landscape and an increasingly intertwined third-party supply chain. In the event of third-party breaches, the process of mapping out threats and communicating with each party can be tedious and slow, delaying necessary response and mitigation steps. On top of that, meeting regulations and compliance laws can be difficult without proper visibility across your entire attack surface that enables you to publicly notify any breaches or risks. That’s why it is necessary to have complete visibility and first-hand alerts in order to respond immediately to any risks facing your organization.

Stay One Step Ahead With the Risk Insights and Response Portal

Panorays’ industry first Risk Insights and Response Portal provides first hand alerts on cyber risks impacting your supply chain. The portal reports an overview of several types of risks: vulnerabilities, including known exploited vulnerabilities (KEVs), breaches, news updates and zero-day attacks, and reveals your exposure to the event whether directly or indirectly. You’ll also see a detailed view of your entire attack surface, with automated mapping of the affected parties along your entire supply chain. Most importantly, the portal allows you to manage all threat responses immediately from within the platform until mitigations are assured, and provides all the details needed to comply with today’s regulations.



Vulnerability Aug 19, 2022
Confluence Server and Data Center - CVE-2022-26134 - Critical severity unauthenticated remote code execution v...

Your Company	7 Direct Suppliers	7 Indirect Suppliers	1% Impacted Companies

Breach

Your Company	1 Direct Suppliers	8 Indirect Suppliers	1.5% Impacted Companies

Vulnerability

Your Company	7 Direct Suppliers	14 Indirect Suppliers	2% Impacted Companies

News

Your Company	1 Direct Suppliers	- Indirect Suppliers	1% Impacted Companies

Zero Day

Your Company	2 Direct Suppliers	16 Indirect Suppliers	0.5% Impacted Companies

Vulnerability

Your Company	3 Direct Suppliers	26 Indirect Suppliers	1% Impacted Companies

Vulnerability

Your Company	3 Direct Suppliers	26 Indirect Suppliers	1% Impacted Companies

Vulnerability Aug 19, 2022 New

Server and Data Center - CVE-2022-26134 - Critical severity unauthenticated remote code execution vulnerability

Description

Source:
National Vulnerability Database (NVD)

Supply Chain Impact

Your Company	10 Direct Suppliers	26 Indirect Suppliers	16% Impacted Companies

View Less ▲

Your company isn't directly exposed to this vulnerability, but is still exposed through its direct and indirect suppliers.

Direct Suppliers:

Company	Cyber Posture ↑	Business Impact	Risk Rating
Eleveno eleveno.com	63	■■■□□	○ Fair
Littel Ltd. littel.com	91	■■□□□	○ Good

Indirect Suppliers (suppliers of your suppliers):

Company	Cyber Posture ↑	Commonality ?	Industry
Drill drill-group.com	71	■□□	Consulting
Kuhic and Sons kuhic.com	38	■■□	Computer Hard...

1% Of companies in Panorays' database are exposed to this vulnerability.

Key Benefits

Identify Risks with Complete Visibility

Having high visibility into your supply chain risks lets you react to breaches in a timely manner. It also prevents your organization from being exposed to attacks that can result in associated fines, lawsuits, loss of reputation and customer trust. The Risk Insights and Response Portal updates you of a cyber event and outlines all levels of exposure to your organization.

With the new Portal, security teams can quickly review which of their third and Nth parties were affected by the risk, seeing not just their own company's exposure but also a percentage score of how widespread the issue was for other Panorays users. Events are also easily filtered by supplier, making it simple to prioritize risks and report critical information to your team.

Immediately Respond to Threats

The Risk Insights and Response Portal allows you to manage all risks directly from the Panorays platform. In the event of a breach, you can confidently reach out to your third parties, gather critical information and take necessary action without the overwhelming process of emails, presentations and calls. By seeing the complete impact of a risk inside the Risk Portal, you understand exactly which third parties to collaborate with for quick and responsible mitigation. From within the platform, you can start a dialog with your third parties, share a security event questionnaire with all affected vendors, and send a remediation request for a new vulnerability if needed. These steps are tracked in the portal with a risk status so you are always aware of which events are "New", "In Progress" and "Done".

Document and Report Responsibly

With all of the information you need in one portal, it's easy to document the latest breaches and vulnerabilities. Whether it's internal presentations to your board or externally reporting the event, it's easy to communicate new breaches just moments after they happen. By quickly filtering through event types or third parties, you have all the information you need readily available, making it simpler to comply with cyber regulations requiring you to report a third party breach.

> Mitigating and responding to cyber risks is an essential part of managing your third-party security. With the Risk Insights and Response Portal, you gain complete visibility into cyber events impacting your supply chain and react immediately, keeping your entire organization safe from cyber threats.
>
> - Dov Goldman, VP Risk Strategy -

Ready to take your third-party security to the next level?

Schedule a demo today >

Panorays