SecurityScorecard

The Definitive Guide to Building a Supply Chain Incident Response Team

EBOOK

As organizations build increasingly complex supply chains and exchange digital information with a growing number of third parties, their cybersecurity threat surfaces increase dramatically. This growing reliance on external vendors — while fostering agility and innovation — introduces significant security risks that can reduce an organization's cyber resilience.

For this reason, there is a critical need for robust security measures that extend beyond traditional third-party risk management (TPRM). Recognizing that a purely prevention-focused security posture is no longer sufficient, organizations must adopt a more realistic approach built on the understanding that security incidents will occur across their supply chain.

In this guide, we'll show you step by step how to assemble a high-performing supply chain incident response team to effectively mitigate and respond to these evolving threats, ensuring business continuity and improving resilience.

Understanding the landscape of supply chain risk

Today's cyber criminals increasingly exploit the interconnected nature of today's world by targeting organizations with numerous relationships, but potentially weaker security cultures within their supply chain. In fact, 35.5% of all breaches in 2024 were third-party related, a 6.5% increase from 2023. This number is likely conservative, as many third-party breaches go unreported or are mistakenly assumed to be internal incidents. It's like playing "Spot the Breach Origin"— harder than you'd think and nobody wins.[1] Understanding the common supply chain attack vectors — where vulnerabilities are a significant and fast-growing entry point — is crucial for developing effective defense strategies.

Traditional TPRM, often characterized by infrequent assessments and limited visibility into vendor security posture, is no longer adequate in the face of escalating cyber threats. It is essential for organizations to evolve beyond this reactive approach and incorporate continuous monitoring, proactive threat hunting, and rapid response capabilities to identify and address vulnerabilities before bad actors can exploit them.

In addition, they must have a clear understanding of which vendors are critical to business continuity and categorize or tier vendors in terms of the potential impact on the business if they are breached.

35.5%

of all breaches in 2024 were third-party related

6.5%

increase in third-party related breaches from 2023

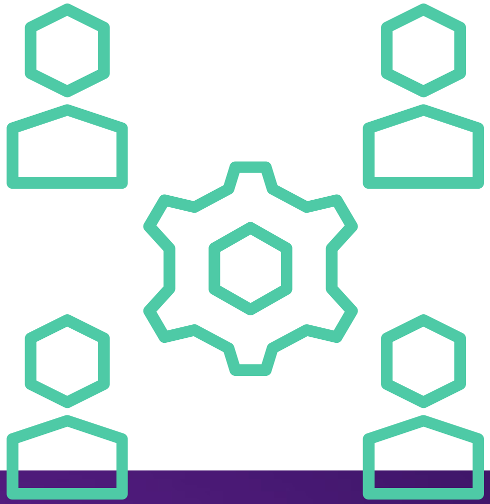
[1] Verizon, Data Breach Investigations Report, 2024

Why your organization needs a dedicated supply chain incident response team

Traditional TPRM programs and even security operations center (SOC) teams often fail to effectively address supply chain incidents. For one thing, responsibility for responding to a supply chain threat can often fall between these two groups, which can delay or even obstruct adequate response.

There is a clear need to move beyond solely identifying risks within the supply chain to focus on actionable resolution and significantly reducing the time it takes to remediate incidents. What's more, organizations must address the security risks posed not only by critical vendors, but also by the "long tail" of suppliers, as these less-scrutinized entities can still create meaningful attack vectors for threat actors.

Establishing a dedicated supply chain incident response team ensures focused attention and expertise in managing these unique challenges. The size of this team depends on the size and complexity of the organization's supply chain. It could be a single person within the SOC team, or for larger organizations, it might be an independent Vendor Risk Operations Center (VROC). Justifying the investment in such a team requires highlighting the potential for costly supply chain breaches and demonstrating the need for efficient processes to manage the expanding vendor ecosystem.



Establishing a dedicated supply chain incident response team ensures focused attention and expertise in managing these unique challenges.

Core functions and objectives of the supply chain incident response team

A robust supply chain incident response team takes a multi-layered approach to risk management, encompassing several core functions, including:

Continuous assessment of vendor risk via regular and comprehensive evaluations that leverage real-time monitoring tools to gain ongoing visibility into vendor security posture

Rapid response following incident detection to limit the initial damage, which might include cutting off access, stopping a process, or isolating a system

Proactive threat hunting within the supply chain, utilizing threat intelligence feeds and security analytics

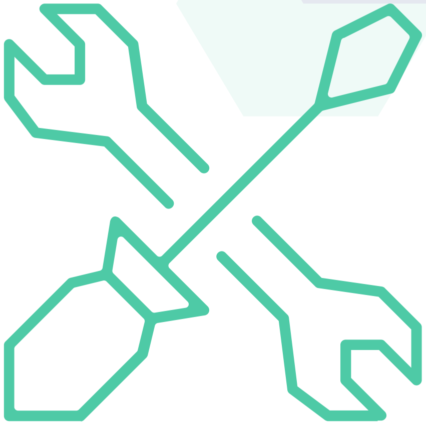
Post-incident analysis following the initial response to investigate the root cause of the incident, fix vulnerabilities, and prevent similar incidents from happening again

Supply chain incident response planning, including the development and implementation of well-defined incident response plans and effective collaboration with vendors to remediate issues and minimize the impact of incidents

Vendor engagement to address breaches or incidents and fix the underlying vulnerability, which also includes providing vendors with action plans and remediation requirements based on incident response principles

Assembling your supply chain incident response dream team: Skills and structure

A successful supply chain incident response team can often leverage existing resources within departments such as risk, compliance, procurement, or the current IT/security teams. Key skills for team members include:



- **Communication**, including the ability to communicate effectively and convey technical information clearly to both technical and non-technical stakeholders
- **Strong collaboration skills** that support working seamlessly with both external vendors and internal teams
- **Positive interpersonal skills,** such as building trust and fostering proactive cooperation with vendors
- **Foundational technical understanding,** including a firm grasp on the intricacies of vulnerabilities and remediation efforts across various security domains
- **Ability to perform threat hunting** by actively seeking out and analyzing potential threats
- **Digital forensics skills**, such as analyzing compromised systems, tracing attack origins, and building forensic evidence to support investigations
- **Incident response planning,** including the development and implementation of effective strategies
- **Project management skills,** such as initiating, organizing, and managing tasks toward timely incident resolution

Given this skill set, the ideal candidate for the supply chain incident response team would likely come from a SOC and/or TPRM team. Individuals from the SOC possess the necessary expertise in cybersecurity, threat-hunting, incident response, and digital forensics while TPRM team members likely have useful experience in managing vendor relationships and understanding operational, financial, and reputational risks.

When defining the team structure, organizations can opt for a separate, dedicated team or designate dedicated individuals within existing teams like the SOC or TPRM. The key is to foster cross-functional collaboration (potentially by establishing dotted communication lines) and ensure seamless communication and coordination across departments involved in supply chain risk management. Regardless of the model, make sure to clearly define reporting lines and support the increasing responsibilities CISOs have to report on supply chain risk to the board.

Learn more about incident response planning

VIDEO
A CISO's Guide to Mastering Cyber Incident Response

PLAYBOOK
Third-Party Cyber Incident Response

How to develop effective supply chain incident response plans

A key function of the supply chain incident response team is developing effective response plans specifically tailored to the unique scenarios you're likely to encounter within your supply chain. Adapting fundamental incident response principles to the supply chain context is crucial for effective management. Organizations should:

Define different severity levels of incidents that can occur within the supply chain to ensure appropriate responses

Develop playbooks and pre-defined workflows for common incident scenarios to streamline the response process

Consider the consequences of response actions, including cutting off access for compromised vendors as an immediate containment measure

Integrate supply chain incident response plans with existing first-party incident response protocols to ensure a cohesive and coordinated approach to security incidents

Leveraging technology for supply chain detection and response (SCDR)

Supply Chain Detection and Response (SCDR) is a new category of cybersecurity technology that can play a critical role in modern supply chain cybersecurity by extending the principles of XDR and CDR to the vendor ecosystem. These platforms offer key capabilities, including:

Supplier lifecycle management features to enable organizations to effectively manage vendor-related data, track engagement, and consolidate crucial evidence and documentation

Continuous threat and risk monitoring, providing instant and ongoing visibility into security issues, threat actor behavior, and active incidents impacting suppliers

Supplier collaboration and remediation tools and workflows that empower organizations and their suppliers to efficiently resolve identified issues with the highest criticality

By leveraging these capabilities, SCDR facilitates a shift from risk identification to proactive issue resolution, leading to faster response times and improved collaboration with vendors to enhance their overall security posture.

Introducing Supply Chain Detection and Response (SCDR)

SCDR is a solution for supply chain incident responders that drives critical issue identification, vendor responsiveness, and time to incident resolution.

SCDR capabilities are strongly aligned with the best practices of a high-performing supply chain incident response team. By leveraging risk intelligence, AI-driven workflows, and incident response capabilities, SCDR enables organizations to:

- Detect zero days and active infections in your supply chain and remediate them within **48 hours**
- Remove friction in the vendor collaboration process and reduce issue resolution time **by 90%**
- Reduce third-party breaches **by 75%** and elevate supply chain cybersecurity posture

Measuring success and continuous improvement

To ensure the effectiveness of a supply chain incident response team, it is crucial to establish methods for measuring success by tracking key metrics such as:

- Number or % of vendors assessed
- Number or % of vendors monitored
- Number or % of critical vendors monitored
- Quantity of critical risks identified
- Average incident response times
- Mean time to remediate (MTTR)

Organizations should regularly review and refine processes based on performance data, lessons learned from past incidents, and evolving threat landscapes. The goal should be to standardize processes across the entire vendor ecosystem and progressively expand the coverage of the supply chain incident response program to include a broader range of vendors. Finally, it is essential to regularly report the status and outcomes of the supply chain incident response program to relevant stakeholders, including the SOC and business leadership, to ensure transparency and demonstrate the value of the initiative.

> *Organizations should regularly review and refine processes based on performance data, lessons learned from past incidents, and evolving threat landscapes.*

The way forward

Building a high-performing supply chain incident response team requires a comprehensive approach encompassing proactive monitoring, robust planning, skilled personnel, and effective technology. Embracing a proactive, collaborative, and adaptive stance is paramount for navigating the complexities of supply chain security and mitigating the risks posed by third-party vendors.

Strong leadership and cross-functional buy-in are essential for fostering a culture of preparedness and building a truly resilient supply chain in the face of ever-evolving cyber threats. By prioritizing supply chain cybersecurity, organizations can safeguard their operations, protect sensitive data, and ensure long-term business success.

Take control of your supply chain risk with SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, Security Scorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, Security Scorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

Security Scorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. Security Scorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant Security Scorecard rating.

For more information, visit securityscorecard.com
or connect with us on Linkedin.

SecurityScorecard