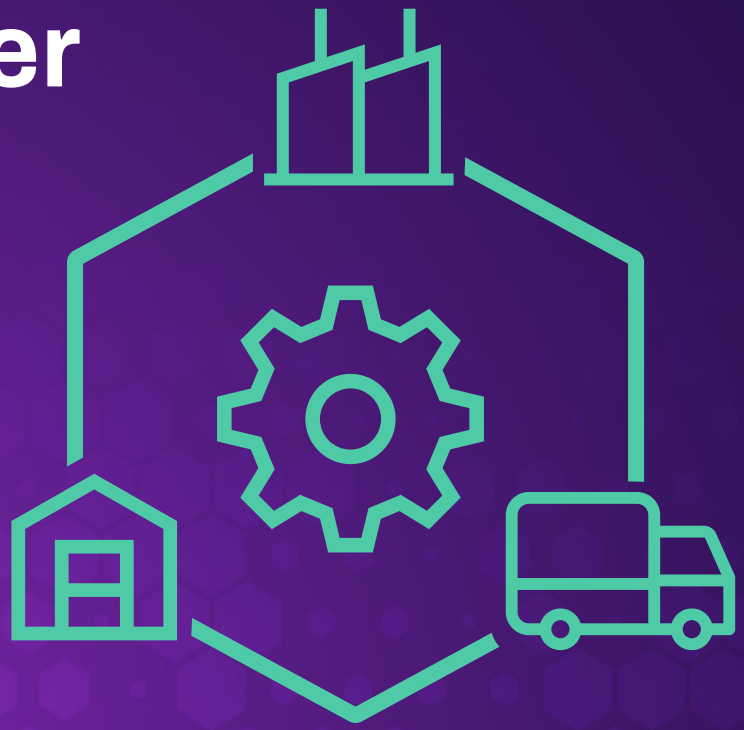
SecurityScorecard

Securing the Supply Chain: Building Cyber Resilience in the Modern Era



EBOOK

Third-party risk management (TPRM) programs — while crucial for establishing security controls — have limited ability to fully address the evolving landscape of cyber threats within supply chains. Relying as they do on periodic assessment, many TPRM programs not only lack the continuous visibility and actionability required in today's dynamic cyber threat environment, but they also rarely address what happens should an incident along the supply chain threaten business continuity.

So, augmenting TPRM with effective supply chain incident response is critical to attaining organizational resilience. Supply Chain Detection and Response (SCDR) is a new technology category designed to support incident response and operationalize supply chain cybersecurity. SCDR extends the principles of detection and response — similar to Extended Detection and Response (XDR) and Cloud Detection and Response (CDR) — into the supply chain ecosystem.

In this guide, we'll walk you through the process of building out your organization's supply chain incident response capabilities with SCDR to enhance its supply chain cyber resilience.

Third-party risk management (TPRM) programs — while crucial for establishing security controls — have limited ability to fully address the evolving landscape of cyber threats within supply chains.

How SCDR takes TPRM to the next level

Traditional TPRM programs focus on preventative controls to follow regulatory, industry, or organizational requirements. They typically rely on periodic assessments (often self-reported by vendors) and have limited incident response capabilities. This can lead to a lack of clear ownership and accountability between the Risk Management function and the Security Operations Center (SOC) for responding to supply chain incidents.

In addition, managing a large volume of vendors with varying levels of criticality can be challenging for TPRM programs, especially those that rely on manual processes like spreadsheets for risk assessment. If a TPRM program does have continuous monitoring, it is likely passive, involving the collection of data without active investigation and response to identified issues.

SCDR technology overcomes these limitations in several ways:

Shifting focus to proactive detection and incident response: SCDR transforms vendor risk managers into supply chain incident responders. It emphasizes proactive identification of critical vulnerabilities and issues, along with robust response capabilities to drive collaborative remediation.

Improving vendor risk management efficiency: SCDR solutions can help identify unreported vendors, streamline vendor communication, and provide a common risk management platform between organizations and their suppliers. This helps manage the volume and diversity of vendors more effectively.

Providing continuous and holistic visibility: SCDR offers continuous threat and risk monitoring, providing real-time visibility into the security posture of suppliers, including the detection of zero-day vulnerabilities and active incidents. It aggregates data about supplier ecosystems, external attack surfaces, and internal security controls to provide a holistic view.

Addressing ownership and skill gaps: SCDR supports the creation of dedicated supply chain incident response teams — potentially within a Vendor Risk Operations Center (vROC) — to take ownership of third-party risk response. These teams should be skilled in threat intelligence, incident response, and vendor communication.

Leveraging AI and automation for actionable insights: SCDR utilizes AI and data analytics to make sense of the vast amounts of data collected, prioritize risks based on business impact and likelihood of incident, and streamline identification and remediation workflows. This helps overcome the “analysis paralysis” often experienced with raw data from traditional TPRM tools.

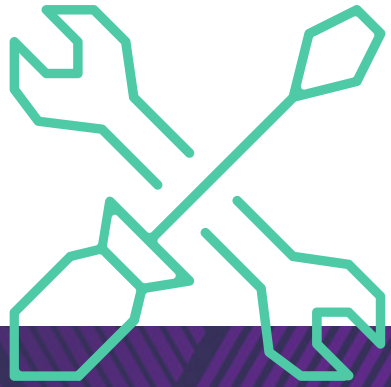
Enabling active collaboration and remediation: A key aspect of SCDR is facilitating supplier collaboration and remediation. It provides tools and workflows that enable organizations to alert vendors about security incidents, deliver recommended remediation actions, request evidence of resolution, and track progress. This active engagement goes beyond the passive monitoring of traditional TPRM.

How to build out a supply chain incident response program to support organizational resilience

Now that you understand the value of an effective supply chain incident response program, it's time to take a look at how to build one out.

This involves a 10-step process, beginning with understanding supply chain dependencies and identifying critical vendors. It progresses through establishing risk management mechanisms, addressing shadow IT, building real-time visibility, fostering collaborative relationships, and developing incident response capabilities. This comprehensive approach ensures a proactive and resilient defense against supply chain cyber risks.

Here's how it breaks down:



10 steps to building out a supply chain incident response program

1. **Know your supply chain (KYSC)**
2. **Identify critical vendors with a tiered approach**
3. **Identify and address shadow IT**
4. **Build out real-time visibility**
5. **Establish and consistently implement a comprehensive risk management framework**
6. **Foster strong, collaborative relationships with vendors**
7. **Clearly define the roles and responsibilities of individuals and teams involved in supply chain incident response**
8. **Develop specific incident response plans tailored to address the unique challenges of supply chain cyber threats**
9. **Develop after-incident processes**
10. **Conduct tabletop exercises**

1

Know your supply chain (KYSC)

Modern supply chains are a complex web of interconnected organizations that make the term “supply chain” almost quaint. You may be familiar with your suppliers, and even your suppliers’ suppliers, but a breach even at an “nth-party” vendor — one you’ve never even heard of — could disrupt your business. Organizations need to begin by thoroughly mapping their extended supply chain ecosystem and identifying all vendors, suppliers, contractors, and other external entities involved in their operations. A crucial aspect of this process is understanding the data access granted to each entity and the potential impact on the organization’s systems and overall operations.

2

Identify critical vendors with a tiered approach

Given the complexity of modern supply chains, it is imperative to identify and categorize critical vendors based on their significance to the business and the potential impact of a disruption involving them. You should prioritize vendors according to the types of data they are permitted to access — whether it is critical, high, medium, or low risk. You should also understand the potential ramifications if a critical vendor were to experience an operational outage due to a cyber incident. The result of this analysis is a tiered approach to a supply chain cybersecurity strategy that helps you prioritize vendors and response.

3

Identify and address shadow IT

A significant challenge for organizations is often the lack of complete knowledge regarding all their vendors, including instances of “shadow IT” where vendors are procured without the security team’s awareness. You will need the ability to identify these vendors independently of reporting structures.

4

Build out real-time visibility

Understanding the overall security hygiene of your suppliers is crucial for assessing the risk to your organization. Any solution you implement must include continuous monitoring for both non-exploited and actively exploited vulnerabilities — including emerging zero-day vulnerabilities — to maintain an accurate risk assessment of the supply chain.

Given the complexity of modern supply chains, it is imperative to identify and categorize critical vendors based on their significance to the business and the potential impact of a disruption involving them.

5

Establish and consistently implement a comprehensive risk management framework

The right risk management framework provides a structured and systematic approach to managing the complex and evolving cyber risks associated with your organization's supply chain and can help your organization move beyond reactive measures to a proactive and resilient security posture. An "Assess, Monitor, Respond, and Contextualize" cycle, for example, provides a comprehensive framework for operationalizing supply chain incident response.

6

Foster strong, collaborative relationships with vendors

Effective collaboration with procurement and legal teams is essential for achieving efficient and comprehensive vendor management. Your organization should work collaboratively with its suppliers to effectively remediate any identified security issues in a timely manner. Make sure you have strategies in place to address instances where vendors may push back on findings or be slow to respond to critical security concerns, and when necessary, there should be a clear process for escalating critical, unresolved issues to executive leadership within both the organization and the vendor.

7

Clearly define the roles and responsibilities of individuals and teams involved in supply chain incident response

Traditional TPRM teams are evolving to incorporate incident response activities as a core function. The relationship between TPRM teams, SOC, and a dedicated supply chain incident response team needs to be well-defined to ensure seamless coordination. Integrating supply chain incident response capabilities as a natural extension of the existing SOC functions can lead to greater efficiency and a more unified security posture. To learn more, read "The Definitive Guide to Building a Supply Chain Incident Response Team."

Effective collaboration with procurement and legal teams is essential for achieving efficient and comprehensive vendor management.

8

Develop specific incident response plans tailored to address the unique challenges of supply chain cyber threats

These third-party incident response plans differ significantly from traditional first-party (internal) incident response plans due to the external nature of vendor relationships. Each plan should clearly identify the types of data potentially impacted by a vendor incident. It should also provide up-to-date vendor contact information, a clear mapping of the architectural integration between the organization and the vendor, and a thorough business impact analysis to assess the potential consequences. Incident response plans should also consider the different criticality tiers of vendors, allowing for a tailored approach based on the potential impact of a compromise at each tier.

9

Develop after-incident processes

After an incident, it is essential to validate that the necessary remediation actions have been completed effectively and to review evidence confirming the successful execution of the incident response plans. Regularly communicate the status and overall outcomes of the supply chain incident response program to key stakeholders within the SOC and the broader business, and continue to monitor and evaluate the effectiveness of the response. The program should adapt to evolving cyber threats and changes in industry best practices to maintain its relevance and effectiveness.

10

Conduct tabletop exercises

The benefits of tabletop exercises and simulated incident response scenarios extend to identifying potential vulnerabilities and uncovering gaps in existing response plans. You should even consider conducting joint exercises with your most critical vendors. Regularly engaging in such exercises helps to foster a strong culture of preparedness and overall resilience across the supply chain.

After an incident, it is essential to validate that the necessary remediation actions have been completed effectively and to review evidence confirming the successful execution of the incident response plans.

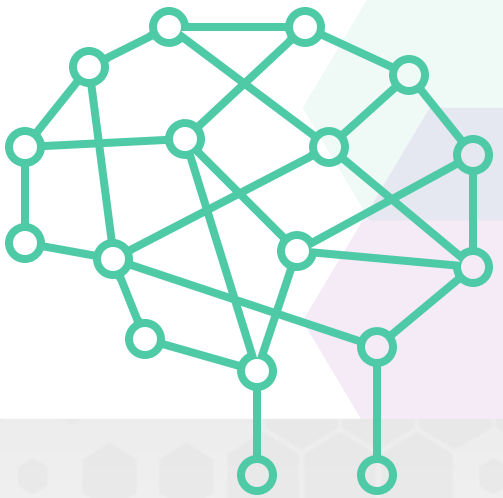
The role of technology and innovation in supply chain resilience

As we've seen, effective supply chain incident response capabilities aren't exclusively about technology. However, modern SCDR solutions are critical to operationalizing cybersecurity within the supply chain. They are specifically engineered to drive the identification of critical security issues, improve vendor responsiveness to these issues, and significantly reduce the time required for incident resolution. These solutions extend the fundamental principles of threat detection and incident response beyond the organization's internal network to encompass the entire supply chain ecosystem — providing continuous monitoring of threats and risks, efficient supplier lifecycle management, and robust supplier collaboration and remediation capabilities.

The integration of AI improves the accuracy, efficiency, and speed of both risk identification and subsequent mitigation efforts. AI can automate the often time-consuming process of assessing vendor risks by detecting anomalies in vendor behavior and predicting potential security threats before they can escalate. This enables organizations to anticipate potential disruptions to their supply chain and implement preventive measures proactively.

Organizations have several deployment options for SCDR capabilities, including fully managing the process internally ("do-it-yourself"), completely outsourcing these functions to a managed service provider, or adopting a collaborative ("co-manage") approach. In reality, managed services play an increasingly important role in providing comprehensive risk management for the complexities of the modern supply chain. These services can help organizations overcome challenges such as a lack of specific skills required or budgetary constraints by providing expert assistance on a 24/7 basis. SecurityScorecard MAX, for example, leverages the power of AI, extensive risk and threat telemetry, and the expertise of seasoned cybersecurity professionals to enhance an organization's security posture.

AI can automate the often time-consuming process of assessing vendor risks by detecting anomalies in vendor behavior and predicting potential security threats before they can escalate.



The future of supply chain resilience

The landscape of cyber threats continues to evolve rapidly, underscoring the ongoing and critical priority of ensuring resilience across the supply chain.

According to the 2025 SecurityScorecard Global Third-Party Breach Report, at least 35.5% of all data breaches in 2024 originated from third-party compromises, up 6.5% from the previous year. The report went on to say that even as security teams work to secure their own networks, attackers are already finding ways in through the back door-exploiting vendors, suppliers, and software providers to infiltrate organizations without ever touching their carefully monitored perimeters.

Supply chain attacks are increasing as hackers exploit the weakest links in security. As organizations strengthen their internal defenses, attackers bypass them by targeting less secure vendors, suppliers, and service providers.

Supply Chain Detection and Response (SCDR) enables organizations to proactively reduce the risk of costly supply chain breaches by providing continuous and comprehensive visibility into vendor security. This leads to improved operational efficiency through streamlined vendor communication and automated workflows, potentially reducing the time to resolve issues by 90%. In addition, SCDR helps organizations improve their overall cybersecurity posture and strengthen relationships with vendors through collaborative risk management and a shared commitment to security.

35.5%

of all data breaches in 2024 originated from third-party compromises, up 6.5% from the previous year.

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