SecurityScorecard

BUYER'S GUIDE

Supply Chain Detection and Response

How to choose the right solution to operationalize supply chain cybersecurity

Table of Contents

Executive Summary

Supply chain risks have grown in complexity and impact, yet most organizations are struggling to operationalize this aspect of their security programs. There are foundational gaps like poor visibility of suppliers, incomplete incident response plans, or lack of skills and accountability for driving supply chain issue resolutions.

Supply Chain Detection and Response (SCDR) has emerged as a category of solutions for operationalizing the cybersecurity of your organization's vendors or partners. It's a transformative technology that enables third-party risk management teams to evolve into supply chain incident responders.

A new category of security solutions naturally raises questions like: What is it? How does it work? How do I know if it's needed? This guide helps you make a more informed decision about evaluating the purchase of an SCDR solution.

What is SCDR?

Supply Chain Detection and Response (SCDR) is a solution for supply chain incident responders that drives critical issue identification, vendor responsiveness, and time to incident resolution. SCDR solutions provide risk intelligence, AI-driven workflows, and collaboration capabilities to improve the security posture of your organization and your suppliers.

SCDR shares principles from other detection and response approaches like Extended Detection and Response (XDR) and Cloud Detection and Response (CDR). Shared principles between SCDR and other detection and response products include:

Holistic visibility: SCDR aggregates data about supplier ecosystems, external attack surfaces, and internal security controls

Data correlation and contextual analysis: SCDR prioritizes suppliers by risk and business impact while identifying the most impactful remediation actions

Automation and orchestration: SCDR streamlines detection and incident response by using artificial intelligence and logic-driven rules

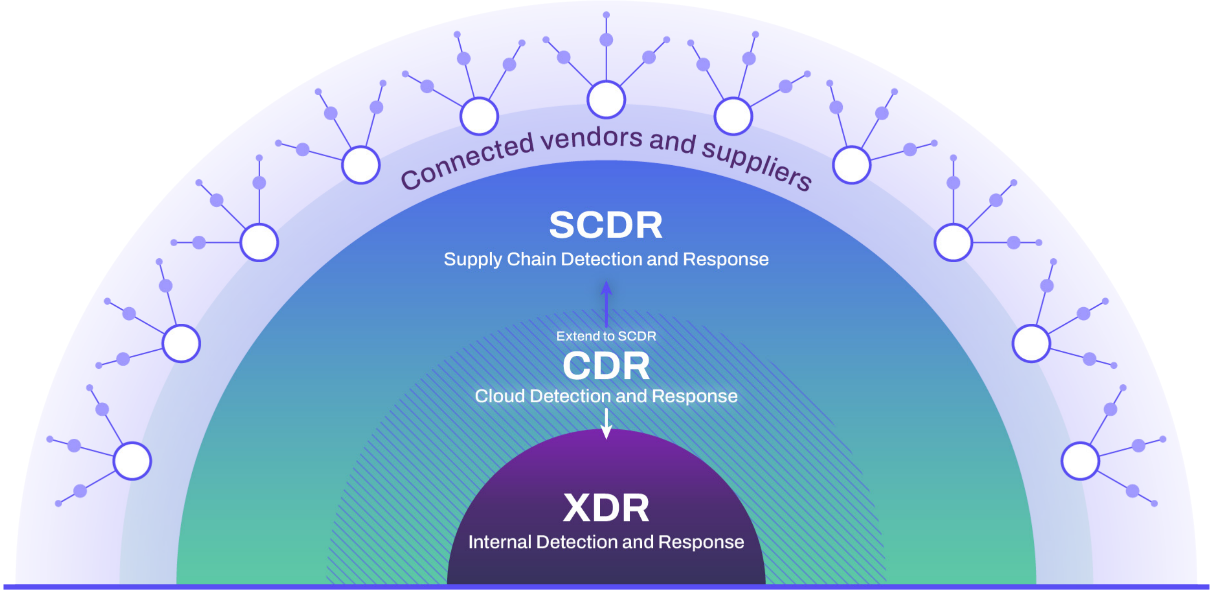
Centralized detection and response: SCDR provides a unified view of supply chains, supplier contacts, and tools for driving remediation

The need for SCDR stems from the evolution of an organization's attack surface. At its core, every organization's attack surface begins with its owned endpoints, servers, and networks. As more organizations move their assets to the cloud, their attack surface expands into that space. That is why XDR and CDR solutions have become core elements in an organization's security tech stack.

Today, most organizations depend on services from other firms, or they allow partners to access their systems and data. This dynamic exponentially increases an organization's attack surface. As a result, SCDR solutions have an equally important role in an organization's security tech stack.

Reasons to consider an SCDR purchase:

- You've experienced a costly supply chain breach
- Regulators require enhanced risk management processes
- A business strategy change increases external dependencies


Connected vendors and suppliers
SCDR
Supply Chain Detection and Response
Extend to SCDR
CDR
Cloud Detection and Response
XDR
Internal Detection and Response

Justifying SCDR Investment

Building a comprehensive business case for investing in new solutions can be challenging, especially when security budgets are flat or declining. Justifying investments often requires developing a narrative about where you are today, where you want to be tomorrow, and how that change will impact the organization.

Highlight organizational challenges

Today, very few organizations have a supply chain incident response team because operationalizing supply chain cybersecurity is challenging.

Who has the skills and time to respond to alerts related to third-party platforms? What data is shared with vendors, and how critical is it to the business? What is the plan for responding to the different types of third-party breaches? These questions are not clearly answered, leading to increased exposure to supply chain risks.

Here are the obstacles to operationalizing supply chain security:

1

Incomplete view of supply chain risks

The proliferation and specialization of software tools, direct marketing to users, and the search for cutting-edge technologies have helped skyrocket the number of vendors typical organizations depend on. There is also a dependency on questionnaires, which are single-point-in-time assessments that don't capture the necessary nuances or maintain visibility of active threats and emerging vulnerabilities.

2

Lack of actionable processes

Most incident response plans do not effectively consider what to do when a supplier is high risk or has been breached. Risk managers either have too much data or not the right data. External scanning tools create mounds of information without context, creating analysis paralysis. Security questionnaires are self-attestations that are time-consuming to analyze. If a supplier is unaware of issues that can lead to incidents, their responses aren't adding value.

3

Unclear ownership of supply chain incident response

Risk management teams focus on establishing preventative third-party breach controls, while security operations teams focus on containing the impact after a breach. That leaves a gap in the day-to-day response to supply chain incidents that can lead to a breach. Risk managers who continually monitor the suppliers can only inform their SOC of supply chain issues. SOCs are often overwhelmed by internal alerts and cannot work directly with suppliers to resolve issues.

4

Inefficient risk management processes

Many risk management programs only focus on a relatively small number of critical vendors. Yet organizations also have a long tail of suppliers who provide more services but can create meaningful attack vectors for threat actors. This long tail is often not considered because of the need to prioritize, given the limited time required to conduct reviews or monitor suppliers. This issue is compounded in organizations that rely on labor-intensive spreadsheet management and other manual risk assessment processes.

5

Lack of cybersecurity expertise

Risk management tends to be driven by business professionals with skill sets better suited to manage financial, operational, compliance, strategic, and reputational risks. They rely on IT or security professionals when in-depth assessments or incident response plan execution is required. Given the dynamic nature of cyber risk, the lack of security expertise can hinder the mitigation or response to active threats or novel vulnerabilities.

Questions to ask yourself:

- How much oversight do you have over your supplier ecosystem?
- What are your supply chain incident response plans?
- How are you detecting incidents that can turn into supply chain breaches?

Identify expected benefits

An organization that has successfully operationalized supply chain cybersecurity can consistently perform activities that an organization that is lower in the supply chain cybersecurity maturity curve cannot.

Identify unreported vendors

Use transaction data or integrations with internal systems to ensure supply chain dependencies are accounted for.

Assess a vendor's security posture:

Determine a vendor's potential for harmful security events with attack surface issue data and evidence of security control implementation.

Monitor supply chain risks:

Detect critical issues, zero-day vulnerabilities, and indicators of compromise like malware infections or leaked credentials.

Prioritize risk management efforts:

Categorize vendors according to their business impact and incident likelihood to create focused engagement and response actions.

Engage high-risk vendors:

Alert vendors about their exposure to security incidents, deliver recommended remediation actions, and request evidence of issue resolution.

Validate incident resolution:

Track the progress of remediation actions and review evidence that incident response plans were completed.

Regularly report to stakeholders:

Communicate the status and outcomes of the supply chain incident response program with stakeholders in the SOC or business.

Questions to ask yourself:

- What is your vision for supply chain cybersecurity?
- What are the obstacles to achieving that vision?
- What are the supply chain incident response tasks you want to achieve?

Estimate return on investment

Operationalizing supply chain cybersecurity with an SCDR solution will bring intangible business value and measurable risk reduction outcomes.

The primary tangible benefit of an SCDR solution is reducing the number of supply chain incidents and the financial impact of breaches or regulatory action. This can be challenging to measure since the goal is to prevent something bad from happening. If nothing bad happens, is it because of actions taken, or was it never going to happen? Despite this characteristic of risk, the performance of a supply chain cybersecurity program can be effectively measured through metrics that are proxies for risk reduction.

Vendor response rate:

Percentage of suppliers who accept the supply chain cybersecurity program onboarding invitation and commit to the program's expectations.

High-risk vendor decrease rate:

Percentage of vendors that move from high to low or medium risk.

Supply chain security improvement:

Percentage reduction in the number of issues across the entire supply chain.

Supplier remediation compliance:

Percentage of suppliers who resolve issues after notification.

Supplier remediation speed:

Time between a supplier being notified of an issue and reported resolution.

Intangible business benefits are also essential when evaluating ROI because they contribute significant, often long-term, value that might not be immediately reflected in performance or financial metrics. Factoring in these benefits gives a more holistic picture of the true return on investment.

1

Increased customer trust

Improved supply chain cybersecurity controls show customers you're proactively reducing vulnerabilities from suppliers, keeping their data and operations safe. This dedication to security fosters trust, making customers more confident in your brand's reliability.

2

Augment the skills and capacity of security and risk teams

Creating operational efficiencies allows your risk and security team to automate routine tasks, freeing up time to focus on more complex, skill-building activities. This shift increases their capacity to handle strategic projects and enhances their expertise and adaptability.

3

Build better relationships with suppliers

Helping suppliers resolve their security issues demonstrates a commitment to their success and a proactive approach to shared security, which builds trust and deepens collaboration. It shows that you value the partnership and are willing to invest in their resilience, creating a stronger, more cooperative relationship.

Questions to ask yourself:

- What are your goals for your supply chain cybersecurity program?
- How are you measuring success?

DETERMINING SCDR CRITERIA

Once you've realized that SCDR is a solution worth exploring, the next step is to figure out what exactly you need from this type of solution. There are two questions to consider: How would this solution fit within my organization? Does the solution have the required tooling to achieve my desired outcomes?

Align organizational fit

Every organization is on a journey toward operationalizing supply chain cybersecurity. That journey can be described as a maturity curve where effectiveness and business value increase throughput at each stage. As you consider SCDR solutions, it's worth reflecting on which stage of the maturity curve you are in, where you want to be, and how fast you want to get there.

Stage 1: Basic due diligence

This is the most basic stage of a supply chain cybersecurity journey where you are only performing single-point-in-time security reviews during key points in the relationship lifecycle, like onboarding or ahead of compliance assessments. These types of reviews rarely produce actionable insights, so the reality is that they are primarily done to "check the box" from a relationship management perspective. They still need to be performed to identify security red flags, but risk reduction value is limited once they are complete.

Stage 2: Ad-hoc TPRM

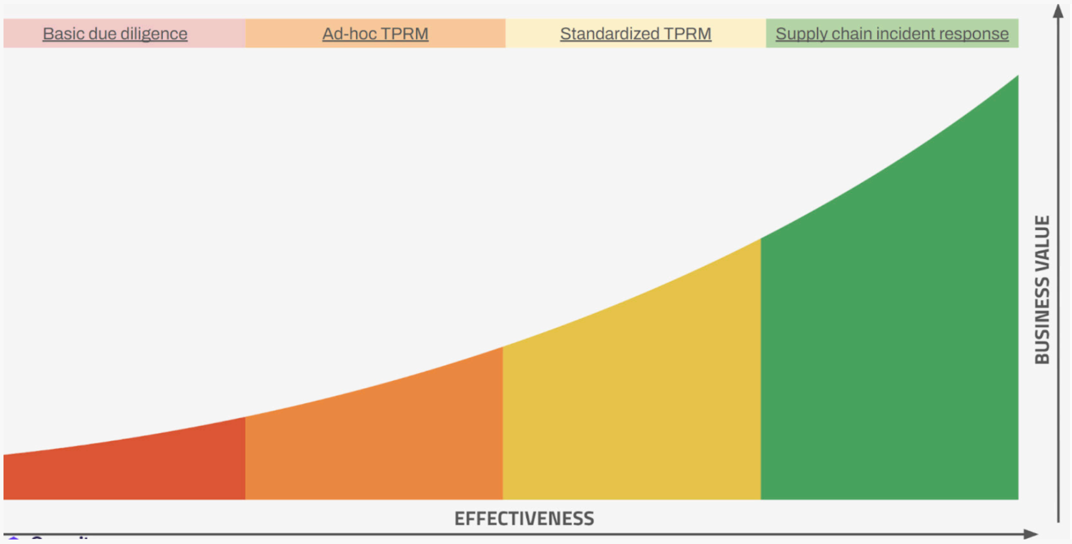
Organizations in this stage start monitoring their suppliers continuously, but their risk management policies and workflows remain relatively informal. They have better capabilities to detect risks, yet outcomes aren't necessarily better. At this point, the organization has a reactive approach that relies on heroic efforts to contain supply chain incidents. Manual processes and an inability to scale risk management across all suppliers means that supply chain incidents still fall through the cracks, and only the most serious incidents are handled at significant cost.

Stage 3: Standardized TPRM

Proactive and consistent implementation of breach prevention controls is the hallmark of a standardized TPRM program. Questionnaires are sent out on time, policies are enforced across all onboarded suppliers, and business stakeholders understand the impact of supply chain risks. This stage falls short because TPRM only focuses on implementing breach prevention controls, and there are challenges in directly engaging suppliers to fix issues before they lead to breaches.

Stage 4: Supply chain incident response

This is the highest-performing stage of supply chain cybersecurity because your organization has mastered rapid remediation of supply chain security issues. Whereas TPRM teams tend to delegate supply chain incident response to an overwhelmed SOC, a supply chain incident response team takes ownership of response plan development and execution. Having a tight integration with the SOC, supply chain incident response teams communicate findings with their suppliers, explain remediation strategies, and follow through with the SOC to contain any impact.



The other organizational consideration is related to your cybersecurity strategy and how you would prioritize supply chain risks. Supply chain risks can be tiered according to the relationship you have with a supplier and the impact a breach on their end would have on your organization. An SCDR solution can support a tiered prioritization to allocate attention and resources to suppliers across all tiers appropriately.

Tier 1: Critical suppliers

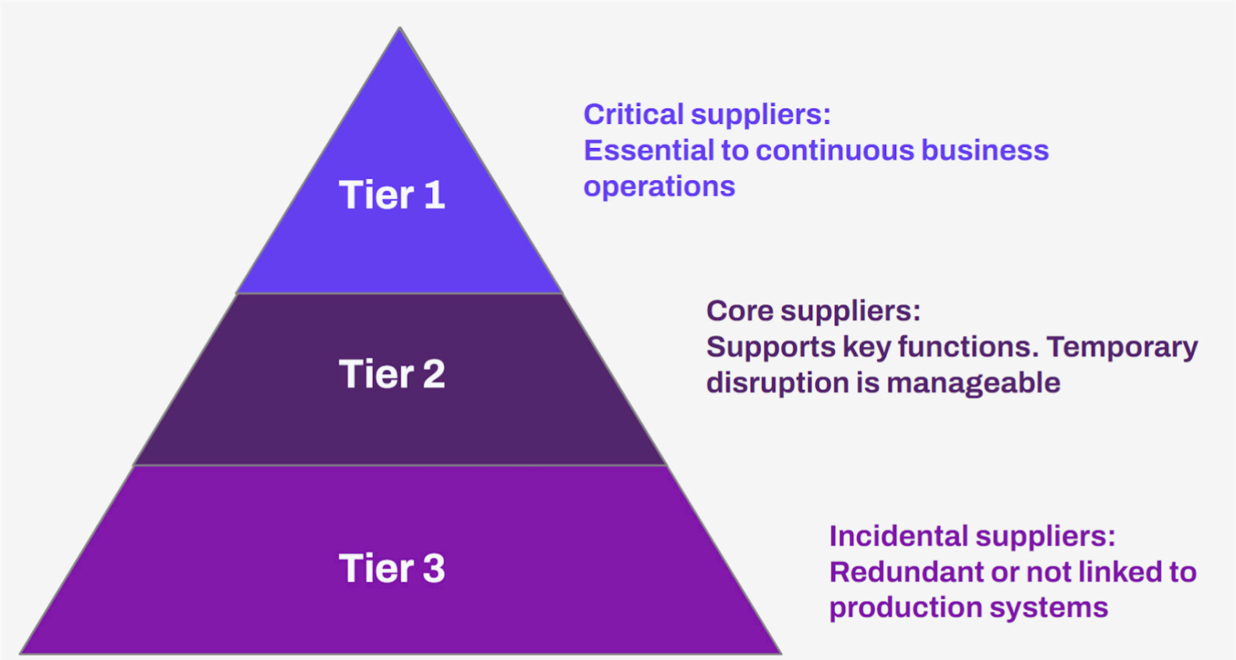
Any supplier that is essential to continuous business operations is classified as critical. Critical suppliers require the most stringent security and compliance requirements since you may give them access to your systems or data. Significant due diligence and continuous monitoring are required. Relationships with these suppliers should be active so that there is immediate engagement with them to drive remediation when incidents occur.

Tier 2: Core suppliers

Suppliers who provide key functions but where temporary disruption is manageable if they were to have an incident. They may not have access to critical systems or data, but the business teams rely on them. As a result, core suppliers should be aware of the security expectations you place on them so that when a critical incident occurs, they know you will follow up to verify remediations have been completed.

Tier 3: Incidental suppliers

Suppliers that are redundant or not linked to production systems are classified as incidental. The organizational impact would be minimal if any of these were to be breached. Due diligence at onboarding or every year is required to identify security red flags. Automation of risk management activities is ideal for this cohort, with intervention only for unexpected scenarios.


Tier 1
Critical suppliers:
Essential to continuous business operations
Tier 2
Core suppliers:
Supports key functions. Temporary disruption is manageable
Tier 3
Incidental suppliers:
Redundant or not linked to production systems

Identify required capabilities

Criteria selection often narrows down a necessary solution feature and its ability to help a supply chain incident responder complete a task.

A comprehensive supply chain detection and response solution has three critical pillars.

Continuous risk monitoring:

Instant and continuous identification of security issues, threat actor behavior, and active incidents that impact an organization and its suppliers.

Supplier lifecycle management:

Manage vendor-related data, track vendor engagement, and consolidate vendor-provided evidence and documentation to help streamline risk reduction and oversight.

Supplier collaboration and remediation:

Turns supply chain risk insights into action with tools and workflows that enable suppliers to efficiently resolve the issues identified and prioritized with the highest criticality.

Continuous risk monitoring represents the "detection" in SCDR.

What to look for	Why it's needed
Non-intrusive and automated evidence collection from vendors	Supplier may not be available or willing to complete questionnaires
Use of incident likelihood model to identify the specific issues that drive risk	Perfect supplier security hygiene is not possible, and remediation should be focused on the most impactful issues
Ability to monitor an organization's entire supply chain ecosystem at the same time	Security issues can emerge at any time for any supplier
Detection and alert security incidents and breaches within the supply chain	Meet regulatory or internal incident response requirements
Proactive discovery of unknown vendors within the organization's supply chain	Vendors can be adopted without consent from IT or security, which creates visibility gaps
Early warning and detection of exposure to zero-day vulnerabilities	Zero-day vulnerabilities can be exploited quickly, and immediate attention is required to remediate
Visibility of threat actor behavior across deep and dark web	Prevent incidents by identifying which vendors are being actively targeted
Contextualization of evidence via cross-reference of industry standards or compliance frameworks	Provides another lens of issue prioritization based on commonly accepted criteria
Financial impact analysis of the first-party costs incurred from a supply chain incident or breach	Communicates the impact of supply chain risks and the performance of supply chain incident response investments with business audiences

Supplier collaboration and remediation is the “response” in SCDR.

What to look for	Why it’s needed
Vendor invitation and onboarding	Suppliers need to understand their customer’s security needs and the supply chain cybersecurity program’s expectations
Questionnaire creation, delivery, and management	Some information that cannot be collected independently is still needed in a rapid and efficient manner
Targeted cyber incident alerting	Notifies supply chain incident response and supplier teams of incidents impacting their organization
Automated supply chain incident exposure analysis and response tracking	Accelerates follow-up, remediation, and business impact reporting
Integration with internal security controls systems	Enables rapid containment of supply chain risks
Attack surface management for suppliers	Empowers suppliers to remediate issues identified by a supply chain cybersecurity program
Prioritization of supply chain risks by business impact and incident likelihood	There is no one-size-fits-all approach to supply chain risks, and response resource allocation needs to be efficient
Supplier communications sorting and triage	Prevents redundant outreach when multiple organizations can have the same supplier
Common risk management platform between organizations and their suppliers	Streamlines the process of agreeing on the impact of security risks and communications to drive resolution

Supplier lifecycle management is the underlying organizational context that combines detection and response capabilities.

What to look for	Why it’s needed
System of record for capturing a supplier’s organizational attributes	Allows for business impact tiering and execution of incident response plans
Supply chain incident response backlog management	Helps teams stay focused, organized, and aligned while managing multiple supply chain incidents
Implementation of supply chain cybersecurity policies	Drives automated incident response plans and ensures a consistent risk management approach
Supply chain cyber risk management reporting	Monitor the impact of risk management strategies and report performance to executives

Evaluating SCDR alternatives

As discussed, SCDR solutions offer multiple value propositions. Given the pace of innovation and investment in the security industry, other solutions may provide overlapping capabilities. It's important to be mindful of alternatives that seem like a good fit but are not.

Security ratings platforms

A security ratings platform is a tool or service that assesses and scores the cybersecurity posture of organizations based on various external factors. These platforms gather data from public and proprietary sources, analyze it, and generate ratings that reflect an organization's level of cybersecurity risk.

Security ratings have strong detection capabilities, but lack the tooling or context needed to respond to incidents or manage the supplier lifecycle. Despite detection strengths, the findings are delivered in a manner that can be overwhelming.

Questionnaire management services

Specialized firms can handle the creation, distribution, collection, and analysis of risk assessment questionnaires sent to suppliers. However, these only gather evidence using questionnaires, so their supply chain detection capabilities are only as good as their ability to drive timely and complete response.

SCDR goes beyond these services since the solution reviews attack surface data that can't be captured in questionnaires, and it enables direct engagement with vendors to explain findings and drive remediation.

Third-party risk management systems

A TPRM system provides a framework for managing and mitigating various risks associated with third-party vendors, partners, and suppliers. TPRM systems usually cover the entire lifecycle of third-party relationships, from onboarding and risk assessment to continuous monitoring, remediation, and reporting.

These systems have no detection and limited response capabilities. They can ingest data from security ratings or SCDR platforms as input for the relationship management workflows they orchestrate.

SCDR capability	Security ratings	Questionnaire management services	TPRM systems	SCDR
Continuous risk monitoring	Strong	Weak	Weak	Strong
Supplier lifecycle management	Weak	Weak	Strong	Strong
Supplier collaboration and remediation	Moderate	Moderate	Weak	Strong

Implementing SCDR

The final consideration for an SCDR solution purchase is related to implementation, specifically, how much effort your team puts in to manage and administer the SCDR solution. There are three typical implementation options for SCDR solutions.

Do it yourself

This option is ideal for organizations that want to build an in-house supply chain incident response team with minimal ongoing assistance from the SCDR solution provider. Implementing this option requires an intuitive SCDR solution, the skills to review findings and work with suppliers to remediate, and the capacity to complete necessary tasks for all suppliers.

Outsource

This option is ideal for organizations who want to realize the outcomes of a high-performing supply chain incident response team without deploying dedicated resources. This option is typically delivered as a managed service from the SCDR provider. In this option, the SCDR provider has their team of supply chain incident responders who work on behalf of clients to administer a supply chain cybersecurity program.

Co-manage

This is a blend of the do-it-yourself and outsourcing options. The typical deployment approach for this option involves the SCDR buyer having a team that owns the engagement of high-risk suppliers. The SCDR solution provider manages the platform configuration and administration to inform supply chain incident response activities.

Implementation considerations:

- Is supply chain incident response a core competency that your organization needs to own and nurture?
- Cybersecurity evolves at a fast rate. How confident are you in your organization’s ability to keep up?
- Supply chain incident response requires a blend of cybersecurity, threat intelligence, TPRM, and soft interpersonal skills. Can you build a team like that?
- High-performing supply chain incident response teams typically review one alert per supplier daily. Is there capacity for that level of activity in the team?

Take control of your supply chain risk

Learn more today at securityscorecard.com/scdr

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard 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, SecurityScorecard'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.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard 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 SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io