

Supply Chain und die Risiken, die durch Unwissenheit im Lieferantennetzwerk entstehen

Kontrolle von Cyber Security-Risiken und Transparenz sind entscheidend



Thomas de Raaf
Senior Sales Director DACH/CEE
tderaaf@securityscorecard.io





To make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risks to their Boards, employees, and vendors.

Unsere Mission

NIS2 Anforderungen & Herausforderungen im Bereich Supply Chain



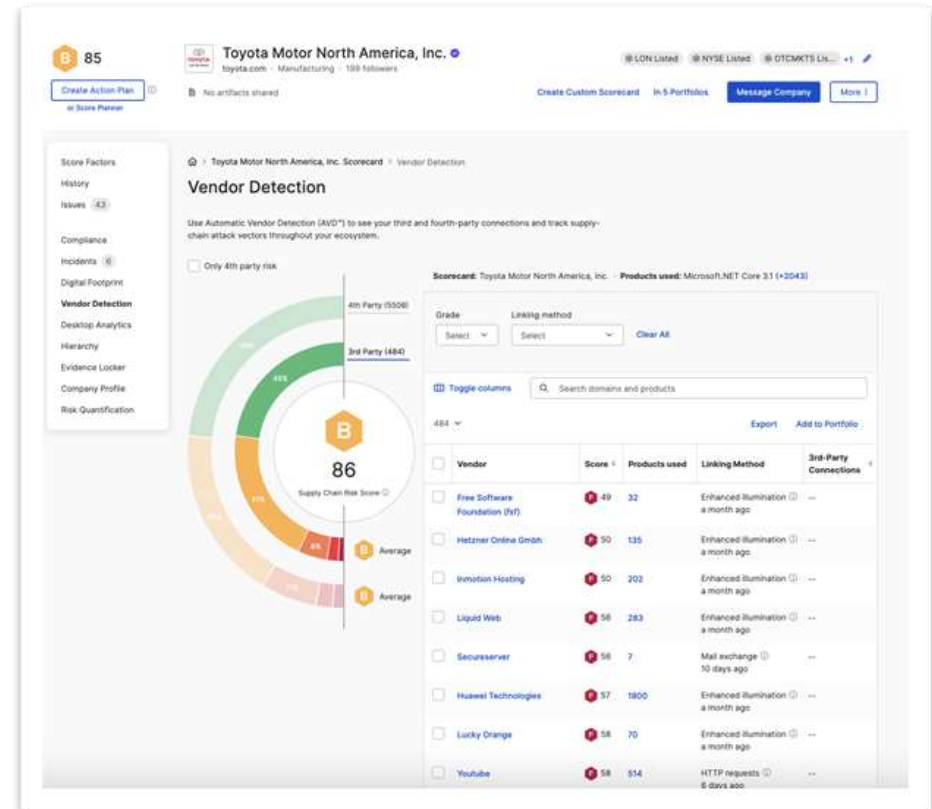
Eine umfassende Lösung zur Erfüllung aller obligatorischen Aspekte von NIS2, einschließlich: Supply Chain Risk, Incident Reporting und Management, Asset Management sowie Dienstleistungen zur Unterstützung technischer und organisatorischer Maßnahmen.

NIS2 Requirement	What is it?	How can we help?
Third-Party Risk Management	NIS2 requires measures to ensure the security of the supply chain, including third-party suppliers and contractors.	<ul style="list-style-type: none"> Gain continuous visibility of your entire third-party ecosystem Quickly validate a vendor's adherence to security standards Prioritise where you need to mitigate risks with your third parties
Asset Management	NIS2 requires complete visibility over the Information asset inventory and effective management.	<ul style="list-style-type: none"> Gain a complete view of how the adversary sees you Investigate vulnerabilities further to drive actionable next steps Prioritise remediation by the biggest impact to your business
Incident Reporting	Under NIS2, the notification requirement has been broken down into phases, with an initial notification to the relevant competent authority required within 24 hours.	<ul style="list-style-type: none"> Discover indicators of compromise that can trigger reporting requirement Quickly identify the cause of incidents to prevent further loss Collect, analyse, and preserve evidence to document the events that led to the incident
Technical and Organisational Measures & Incident Management	This includes measures such as access controls, encryption, monitoring systems and customised incident response plans.	<ul style="list-style-type: none"> Test the effectiveness of your security controls while achieving compliance and protecting your brand Practice your incident response skills and identify gaps in your incident response plan Perform simulated real-life cyber attacks against your own organisation



1. Third-Party Risk Management

- Verschaffen Sie sich einen kontinuierlichen Überblick über Ihr gesamtes Drittanbieter-Ökosystem
- Welche Lieferanten sind kritisch?
- Welche Lieferanten beeinflussen mein Business?
- Welche Lieferanten waren von einem Data-Breach betroffen?
- Kenne ich meine 3rd und 4th Parties?
- Haben wir einen Assessment Prozess?
- Haben wir ausreichende Reports bzw. Dokumentationen von unseren "3rd Parties"?





1. Third-Party Risk Management

- Schnelles Überprüfen der Einhaltung von Sicherheitsstandards durch einen Anbieter
- Welche Schwachstellen haben unsere Lieferanten?
- Sind diese Schwachstellen ein Angriffspunkt für mein Unternehmen
- Gibt es Breaches bei meinen Lieferanten
- Sind meine Lieferanten von Events wie MoveIT, Log4j etc. betroffen?

The screenshot displays the SecurityScorecard interface for a vendor named Nissan. The top navigation bar includes a score of 85, the vendor name 'Nissan', and various action buttons like 'Add Tag', 'Message Company', and 'View'. Below this, there's a section for 'Issues' with a filter for 'Open' issues. A table lists several issues, each with a severity score, a description, and a status. The issues include 'Self-Hosted Without Documented Controls', 'T13 Service Support to Host External Data', 'Certificate is Self-Signed', 'Certificate is Expired', 'Credentials at Risk For Up to Two Years', 'Credentials at Risk For Up to 180 Days', 'Low severity CVE patching delayed', 'Medium severity CVE patching delayed', 'High severity CVE patching delayed', and 'Provider Typo-squat Domain Detected'.

Issue ID	Score	Issue Description	Data Ingested	# of Records	Severity	Action
104	3.2	Self-Hosted Without Documented Controls	Yes	0	Medium Severity	
104	3.2	T13 Service Support to Host External Data	Yes	0	Medium Severity	
104	3.2	Certificate is Self-Signed	Yes	0	Medium Severity	
104	3.2	Certificate is Expired	Yes	0	Medium Severity	
105	3.2	Credentials at Risk For up to Two Years	Yes	0	Information Leak	
105	3.2	Credentials at Risk For Up to 180 Days	Yes	0	Information Leak	
105	3.2	Low severity CVE patching delayed	Yes	0	Missing Evidence	
105	3.2	Medium severity CVE patching delayed	Yes	0	Missing Evidence	
105	3.2	High severity CVE patching delayed	Yes	0	Missing Evidence	
105	3.2	Provider Typo-squat Domain Detected	Yes	10	Asset Engineering	



1. Third-Party Risk Management

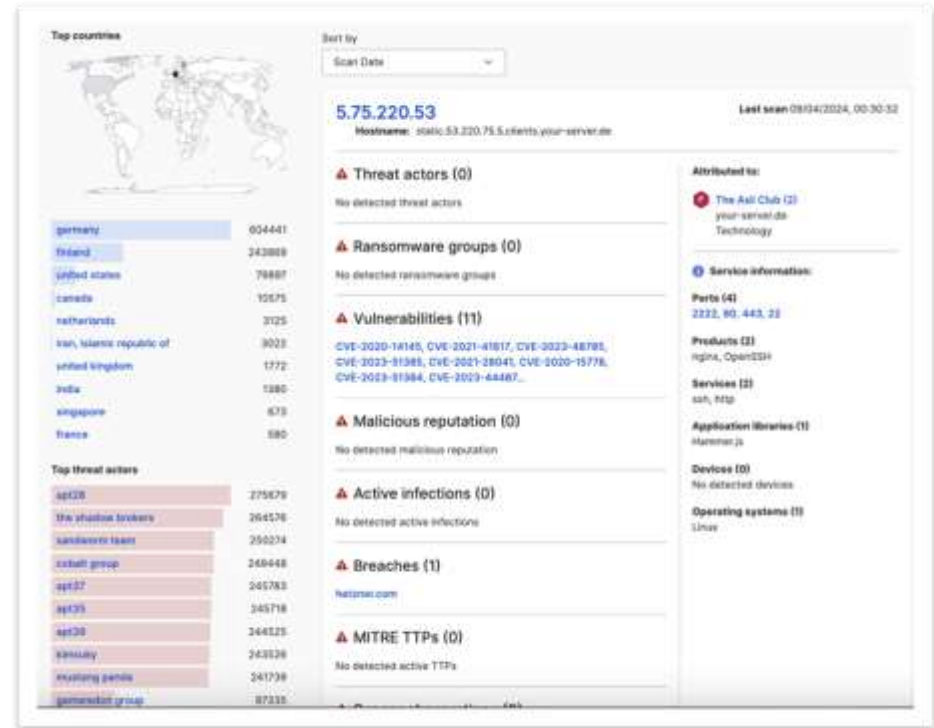
- Legen Sie Prioritäten fest, wo Sie die Risiken bei Ihren Dritten abmildern müssen.
- Treten Sie an Ihre Lieferanten mithilfe unserer Reports heran um auf Schwachstellen aufmerksam zu machen
- Liefern Sie Details zu einzelnen Schwachstellen und stellen Sie Hintergründe zur Verfügung

The screenshot displays a detailed report for the company 'Nissan' (Industry: Manufacturing, 18 followers). The report highlights a finding titled 'Certificate Without Revocation Control' under the category 'Network Security' with a 'Low severity' rating. The finding is mapped to standards including CWE, CSA-DCM, ISO27001/3, MITRE, NISTCSF, and SOC2. The 'DESCRIPTION' explains that certificates issued by a Certificate Authority (CA) should be checked for revocation, and the 'RISK' section notes that certificates without revocation controls are a violation of best practices. The 'RECOMMENDATION' suggests decommissioning or contacting the CA for replacement. The 'REFERENCES' section provides links to related resources. A 'COMPARISON TO SIMILAR COMPANIES' section includes a pie chart showing that 36% of similar companies have this issue, while 64% do not. A bar chart indicates that there are 3 findings for this company, compared to an average of 4 findings. The report also shows a '3.5' overall score impact and provides options to 'IMPROVE YOUR SCORE', 'CONTACT COMPANY', and 'DOWNLOAD AS CSV'.



2. Attack Surface verstehen

- Verschaffen Sie sich einen vollständigen Überblick darüber, wie ein Angreifer Ihr Unternehmen sieht
- Untersuchen Sie die Schwachstellen im Detail, um die nächsten Schritte festzulegen um sich zu schützen
- Priorisierung der Abhilfemaßnahmen nach den größten Auswirkungen auf Ihr Unternehmen





3. Incident Management

Können Sie eine Sicherheitsverletzung innerhalb von 24 Stunden erkennen und darauf reagieren?

Die folgenden Details sollten gemeldet werden:

- Anzahl der betroffenen Nutzer
- Menge der verlorenen Daten
- Geografische Ausbreitung
- Wirtschaftliche Auswirkungen und mehr
- Wie wird Ihr Betrieb wiederhergestellt, wenn es zu einer Sicherheitsverletzung kommt?

Wie wird diese Information aktuell eingeholt?

- Fragebogen workflow via Excel?

The screenshot shows the Nissan profile page in SecurityScorecard. At the top, there is a score of 85 and a 'Create Action Plan' button. The main content area is titled 'Incidents' and displays a table with the following data:

Published Date	Description	Source
Dec 7, 2023	Breach Nissan is investigating a cyberattack that targeted its systems in Australia and New Zealand, with no specific details mentioned, potentially leading to the exposure of personal information and posing a risk of scams to customers.	Go to source

On the left side, there is a navigation menu with options like 'Score Factors', 'History', 'Insights', 'Compliance', 'Incidents', 'Digital Postcard', 'Vendor Detection', 'Security Analytics', 'Hierarchy', 'External Links', 'Company Profile', and 'Risk Quantification'.



4. Prepare from Boardroom to Basement

Testen Sie regelmäßig Ihre Cyber-Resilienz:

- Schwachstellenanalysen
- Penetration Tests
- Red Teaming
- Tabletop-Übungen und mehr
- Proaktives Handeln hilft dabei, potenzielle Risiken zu erkennen und zu mindern und gleichzeitig die Geschäftskontinuität im Falle eines Cybervorfalls sicherzustellen.

Managed Service für 3rd und 4th Party Überblick:

- Lassen Sie “breach likelihood reports” erstellen um Schwachstellen zu verstehen
- Erkennen Sie “Zero-Days” in Ihrer Supply-Chain um Angriffen zuvor zu kommen
- etc.

SecurityScorecard ISAC Partner Program



SecurityScorecard ist stolz darauf, die ISACs der Industrie durch unser ISAC-Partnerprogramm zu unterstützen und damit unsere Mission zu fördern, die Welt sicherer zu machen, indem wir die Branchen unterstützen, die unser tägliches Leben ermöglichen.





Vielen Dank!

Thomas de Raaf
Senior Sales Director DACH/CEE
tderaaf@securityscorecard.io

