SecurityScorecard

EXPECT the UNEXPECTED

Security from A to F

Your digital guide to the Q4 ‘23 Release

What’s included?

Security from A to F is your guide to the Q4 2023 Release.

Q4 2023 Release Deck

An overview of the 30+ new innovations, services, and integrations, including screenshots and release notes.

Additional Resources

At the end of this deck, we provide you with additional guides, education and videos that will help you operationalize the Q4 ‘23 Release.

The traditional enterprise risk model has changed.

There is no perimeter

Your attack surface is not limited to your organization, making securing it more challenging.

Regulatory scrutiny

Regulators around the world are putting a microscope on third-party risk management.

Expanded view of risk

Security teams' scope is expanding and they are being asked to do more with less.

Are you prepared to...

Operationalize your vendor risk management program?

Accept the risk of a vendor falling below your risk appetite?

Respond to a third-party breach?

Comply with regulation that demands a quick response to a third-party breach?

Support a sales procurement process to close a deal at the last hour of the quarter?

Speak to the board about how your VRM program is driving your business forward?

Respond to a zero-day with a team of experts on hand?

Third-party risk is a business risk. Expect the unexpected.

SecurityScorecard empowers you to build a resilient third-party risk management program and expect the unexpected with complete visibility of your supply chain, the ability to take instant action, and increase collaboration across your entire ecosystem.

GAIN COMPLETE VISIBILITY

TAKE PROACTIVE ACTION

INCREASE COLLABORATION

Stay one step ahead of adversaries with a complete picture of your supply chain.

Be prepared to quickly respond to emerging threats with a trusted team of experts at your side.

Clearly communicate and partner with stakeholders, partners, and regulatory bodies.

One Platform, Multiple Use Cases

Enterprise Cyber Risk Management

Executive-Level Reporting

Service Providers

Compliance

Third-Party Risk Management

Cyber Insurance

M&A Cyber Due Diligence

Threat Intelligence

We've consolidated multiple data feeds into a single analytics platform that gives you insight into your own attack surface as well as your entire ecosystem.

SINKHOLE 2B+

malware requests per day – one of the world's largest malware DNS sinkhole

100B+

daily signals.. **analyzed** and **crowd-sourced** with **AI-Powered processing**

99%

of data is **collected and curated** by SecurityScorecard

1,500+ PORTS

scanned across the **entire internet** every 7 days

7B+

leaked credential/PII databases in-house from across dark web and forums

TOP 20M

websites crawled every week using full browsers imitating real users

Comprehensive solution for detecting and collaborating to eliminate supply chain cyber risk.

External Risk

- Security Ratings
- Security Data API
- Attack Surface Intelligence
- Automatic Vendor Detection

Continuous Compliance

- Questionnaires
- Evidence Locker
- Regulatory Compliance
- Cloud Compliance

SecurityScorecard Platform

Marketplace of Integrations & Apps

Professional Services

- Managed Cyber Risk Services
- Digital Forensics & Incident Response
- Proactive Security Services
- Cyber Risk Intelligence

Board Reporting

- Cyber Risk Quantification
- Reporting Center

What’s new in the Q4’23 Release?

Third-Party Cyber Risk Management

Action Plans

Integrated Questionnaires

ESG Data

Natural Language Search

Expanded Vendor Intelligence

Vendor Collaboration Invites

4th Party Vendor Detection in Portfolios

Invited Contact manager

Platform

Data Residency Compliance

Audit Log

Global Navigation

Enterprise Cyber Risk Management

Evidence & Events in the Digital Footprint

Automated Board Reports

Compliance Readiness Assessment

Asset Categories

Custom Scorecard Filters

Subsidiary Scorecards Issue View

Professional Services

Managed Cyber Risk Services *Soft-launch*

Zero-Day-as-a-Service *Soft-launch*

Request Services in Platform

Threat Intelligence

BreachDetails

Visual Search in Attack Surface Intelligence

Table view in Attack Surface Intelligence

CVEDetails.com *Beta*

Marketplace

S&P Risk Indicator

ProcessUnity

Jira On-Demand Ticket Creation

Cybersecurity Risk Insights

Salesforce Scorecard IMporter

Threat Quotient

Netskole CCI Integration

Third-Party Cyber Risk Management

- Action Plans
- Integrated Questionnaires
- ESG Data
- Natural Language Search
- Expanded Vendor Intelligence
- Vendor Collaboration Invites
- 4th Party Vendor Detection in Portfolios
- Invited Contact manager

Action Plans

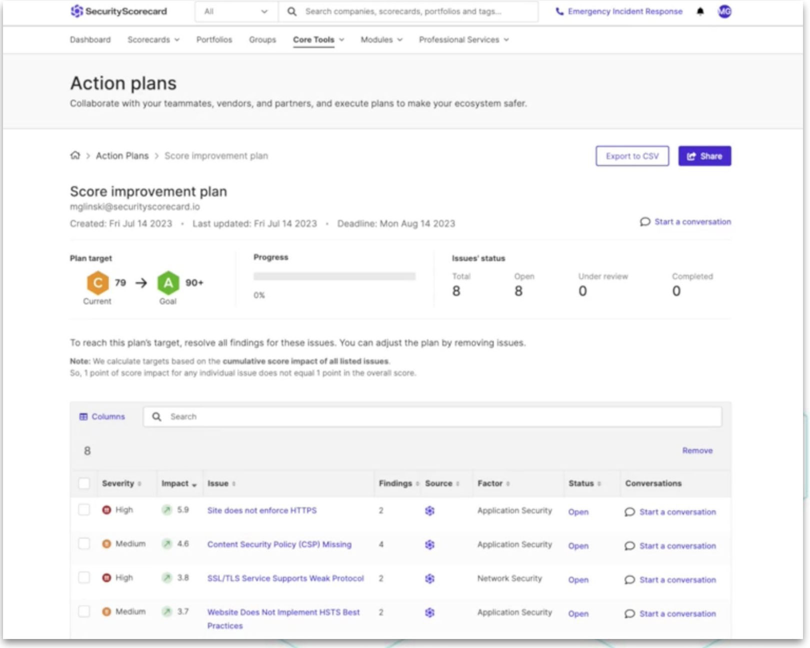
Collaborate and improve your ecosystem’s security posture with confidence.

Streamline collaboration with third-parties and key stakeholders in one dashboard.

How this helps you: Generate dynamic remediation plans, prioritize critical vulnerabilities, assign specific people to fix issues, and see progress in real time, saving you hours and reducing ecosystem risk.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Ensure that your vendors meet your risk appetite and work collectively to improve their security posture.
- **Enterprise-Cyber RIsk Management:** Collaborate with internal stakeholders to assign and prioritize security issues.
- **Cyber Insurance:** Accelerate the application process by eliminating subjectivity and collaborating with applicants at scale.



Action plans

Collaborate with your teammates, vendors, and partners, and execute plans to make your ecosystem safer.

Score improvement plan

mglinski@securityscorecard.io

Created: Fri Jul 14 2023 · Last updated: Fri Jul 14 2023 · Deadline: Mon Aug 14 2023

Plan target: C 79 Current → A 90+ Goal

Progress: 0%

Issues' status: Total 8 · Open 8 · Under review 0 · Completed 0

To reach this plan's target, resolve all findings for these issues. You can adjust the plan by removing issues.

Note: We calculate targets based on the **cumulative score impact of all listed issues**.
So, 1 point of score impact for any individual issue does not equal 1 point in the overall score.

8

	Severity	Impact	Issue	Findings	Source	Factor	Status	Conversations
□	High	5.9	Site does not enforce HTTPS	2		Application Security	Open	Start a conversation
□	Medium	4.6	Content Security Policy (CSP) Missing	4		Application Security	Open	Start a conversation
□	High	3.8	SSL/TLS Service Supports Weak Protocol	2		Network Security	Open	Start a conversation
□	Medium	3.7	Website Does Not Implement HSTS Best Practices	2		Application Security	Open	Start a conversation

LEARN MORE

Integrated Questionnaires

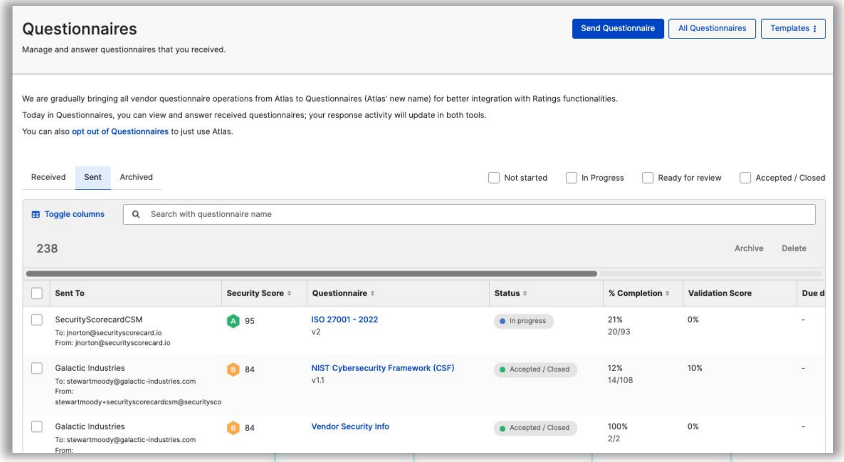
Automatically send and validate vendor questionnaires at scale.

Effectively assess your vendors with smart questionnaires integrated into our ratings platform

How this helps you: Use automation and machine learning to validate vendor responses and shorten the questionnaire process by as much as 83%.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Send, track, and validate questionnaires to your third and fourth parties.
- **Enterprise-Cyber RIsk Management:** Conduct internal security assessments with automated questionnaires.
- **M&A Due Diligence:** Assess the cybersecurity risk of a potential acquisition target with security questionnaires.



Questionnaires

Manage and answer questionnaires that you received.

We are gradually bringing all vendor questionnaire operations from Atlas to Questionnaires (Atlas' new name) for better integration with Ratings functionalities.

Today in Questionnaires, you can view and answer received questionnaires; your response activity will update in both tools.

You can also opt out of Questionnaires to just use Atlas.

□ Not started □ In Progress □ Ready for review □ Accepted / Closed

238

□	Sent To	Security Score	Questionnaire	Status	% Completion	Validation Score	Due d
□	SecurityScorecardCSM To: jnorton@securityscorecard.io From: jnorton@securityscorecard.io	A 95	ISO 27001 - 2022 v2	● In progress	21% 20/93	0%	-
□	Galactic Industries To: stewartmoody@galactic-industries.com From: stewartmoody+securityscorecardcsm@securitysco	B 84	NIST Cybersecurity Framework (CSF) v1.1	● Accepted / Closed	12% 14/108	10%	-
□	Galactic Industries To: stewartmoody@galactic-industries.com From:	B 84	Vendor Security Info	● Accepted / Closed	100% 2/2	0%	-

LEARN MORE

ESG Data

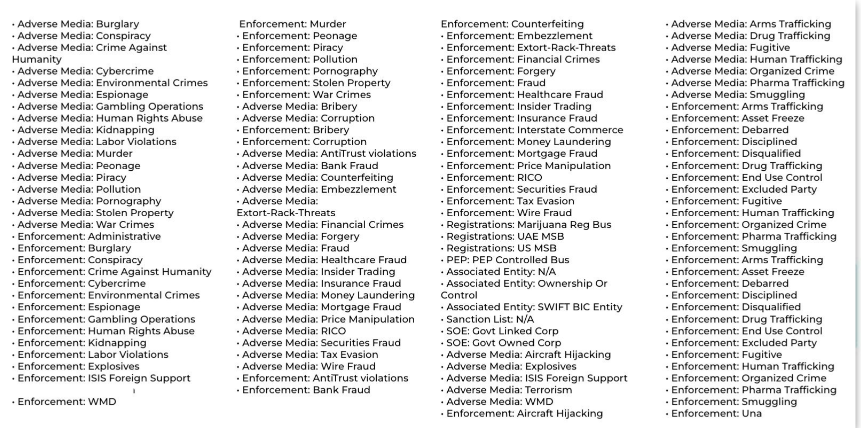
Get critical data for evaluating Environmental, Social, and Corporate Governance (ESG) risk

Get vendor risk data from one trusted source delivered through a customer-facing API.

How this helps you: Stay ahead of regulatory activity and investor pressure by adding additional ESG risks to monitor for in your third-party ecosystem.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Continuously monitor your entire third-party ecosystem for economic, political, environmental, and ethical risks.
- **Insurance Underwriting:** Integrate ESG risk into your assessment framework for underwriting decisions.
- **Investment Banking:** Consider ESG risk alongside financial and cyber risk.
- **Procurement:** Evaluate current and future suppliers' ESG risk before procuring products and services or renewing.



- Adverse Media: Burglary
- Adverse Media: Conspiracy
- Adverse Media: Crime Against Humanity
- Adverse Media: Cybercrime
- Adverse Media: Environmental Crimes
- Adverse Media: Espionage
- Adverse Media: Gambling Operations
- Adverse Media: Human Rights Abuse
- Adverse Media: Kidnapping
- Adverse Media: Labor Violations
- Adverse Media: Murder
- Adverse Media: Peonage
- Adverse Media: Piracy
- Adverse Media: Pollution
- Adverse Media: Pornography
- Adverse Media: Stolen Property
- Adverse Media: War Crimes
- Enforcement: Administrative
- Enforcement: Burglary
- Enforcement: Conspiracy
- Enforcement: Crime Against Humanity
- Enforcement: Cybercrime
- Enforcement: Environmental Crimes
- Enforcement: Espionage
- Enforcement: Gambling Operations
- Enforcement: Human Rights Abuse
- Enforcement: Kidnapping
- Enforcement: Labor Violations
- Enforcement: Explosives
- Enforcement: ISIS Foreign Support
- Enforcement: WMD

Enforcement: Murder

- Enforcement: Peonage
- Enforcement: Piracy
- Enforcement: Pollution
- Enforcement: Pornography
- Enforcement: Stolen Property
- Enforcement: War Crimes
- Adverse Media: Bribery
- Adverse Media: Corruption
- Enforcement: Bribery
- Enforcement: Corruption
- Adverse Media: AntiTrust violations
- Adverse Media: Bank Fraud
- Adverse Media: Counterfeiting
- Adverse Media: Embezzlement
- Adverse Media: Extort-Rack-Threats
- Adverse Media: Financial Crimes
- Adverse Media: Forgery
- Adverse Media: Fraud
- Adverse Media: Healthcare Fraud
- Adverse Media: Insider Trading
- Adverse Media: Insurance Fraud
- Adverse Media: Money Laundering
- Adverse Media: Mortgage Fraud
- Adverse Media: Price Manipulation
- Adverse Media: RICO
- Adverse Media: Securities Fraud
- Adverse Media: Tax Evasion
- Adverse Media: Wire Fraud
- Enforcement: AntiTrust violations
- Enforcement: Bank Fraud

Enforcement: Counterfeiting

- Enforcement: Embezzlement
- Enforcement: Extort-Rack-Threats
- Enforcement: Financial Crimes
- Enforcement: Forgery
- Enforcement: Fraud
- Enforcement: Healthcare Fraud
- Enforcement: Insider Trading
- Enforcement: Insurance Fraud
- Enforcement: Interstate Commerce
- Enforcement: Money Laundering
- Enforcement: Mortgage Fraud
- Enforcement: Price Manipulation
- Enforcement: RICO
- Enforcement: Securities Fraud
- Enforcement: Tax Evasion
- Enforcement: Wire Fraud
- Registrations: Marijuana Reg Bus
- Registrations: UAE MSB
- Registrations: US MSB
- PEP: PEP Controlled Bus
- Associated Entity: N/A
- Associated Entity: Ownership Or Control
- Associated Entity: SWIFT BIC Entity
- Sanction List: N/A
- SOE: Govt Linked Corp
- SOE: Govt Owned Corp
- Adverse Media: Aircraft Hijacking
- Adverse Media: Explosives
- Adverse Media: ISIS Foreign Support
- Adverse Media: Terrorism
- Adverse Media: WMD
- Enforcement: Aircraft Hijacking

- Adverse Media: Arms Trafficking
- Adverse Media: Drug Trafficking
- Adverse Media: Fugitive
- Adverse Media: Human Trafficking
- Adverse Media: Organized Crime
- Adverse Media: Pharma Trafficking
- Adverse Media: Smuggling
- Enforcement: Arms Trafficking
- Enforcement: Asset Freeze
- Enforcement: Debarred
- Enforcement: Disciplined
- Enforcement: Disqualified
- Enforcement: Drug Trafficking
- Enforcement: End Use Control
- Enforcement: Excluded Party
- Enforcement: Fugitive
- Enforcement: Human Trafficking
- Enforcement: Organized Crime
- Enforcement: Pharma Trafficking
- Enforcement: Smuggling
- Enforcement: Arms Trafficking
- Enforcement: Asset Freeze
- Enforcement: Debarred
- Enforcement: Disciplined
- Enforcement: Disqualified
- Enforcement: Drug Trafficking
- Enforcement: End Use Control
- Enforcement: Excluded Party
- Enforcement: Fugitive
- Enforcement: Human Trafficking
- Enforcement: Organized Crime
- Enforcement: Pharma Trafficking
- Enforcement: Smuggling
- Enforcement: Una

Natural Language Global Search

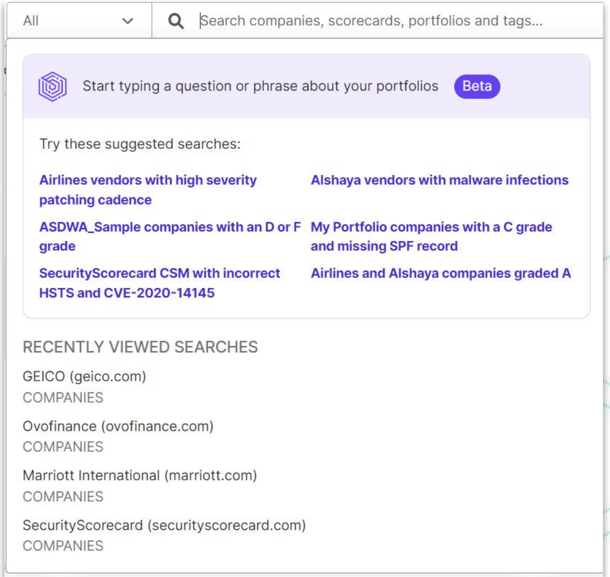
Accelerate risk analysis simply by asking questions that are top of mind

Identify which vendors have critical issues by leveraging AI and asking direct and intuitive questions.

How this helps you: Spend less time figuring out how to filter through a portfolio by typing for what you are looking for.

Other Use Cases this Enables:

- **Third-party Risk Management:** Identify which vendors have critical issues
- **Cyber insurance:** Determine a portfolio's exposure to specific security issues



Start typing a question or phrase about your portfolios Beta

Try these suggested searches:

Airlines vendors with high severity patching cadence

Alshaya vendors with malware infections

ASDWA_Sample companies with an D or F grade

My Portfolio companies with a C grade and missing SPF record

SecurityScorecard CSM with incorrect HSTS and CVE-2020-14145

Airlines and Alshaya companies graded A

RECENTLY VIEWED SEARCHES

GEICO (geico.com)
COMPANIES

Ovofinance (ovofinance.com)
COMPANIES

Marriott International (marriott.com)
COMPANIES

SecurityScorecard (securityscorecard.com)
COMPANIES

Vendor Collaboration Invites

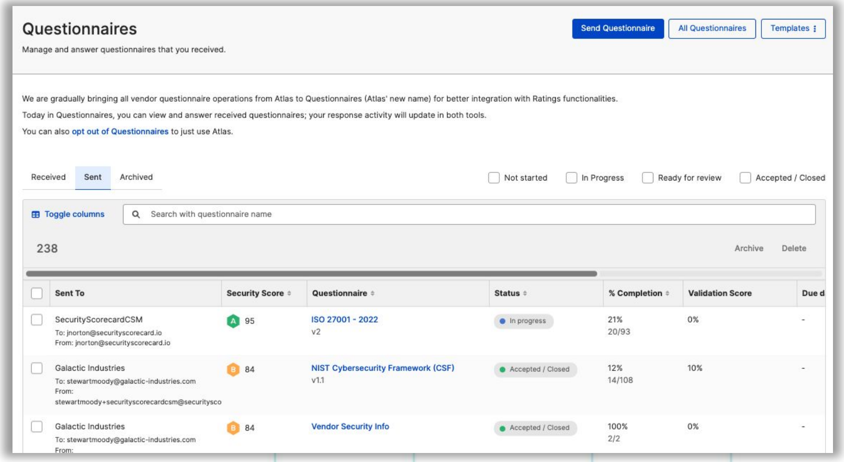
Increase response rates and customize requests when inviting your vendors to SecurityScorecard

A seamless invite flow for both the recipient and the sender.

How this helps you: When requesting evidence from the Evidence Locker, personalize your invite to familiar contacts using the Contact Manager. As a recipient of a request, respond to requests quicker without being interrupted and asked to create a SecurityScorecard account.

Use Cases this Enables:

- **Third-Party Risk Management:** Improve collaboration with your vendors and partners by inviting them onto the platform through a personalized invite and allow them to quickly fulfill the request
- **Compliance:** Requesting evidence from the evidence locker ensures your vendors are complying with standards and regulations.



Questionnaires

Manage and answer questionnaires that you received.

We are gradually bringing all vendor questionnaire operations from Atlas to Questionnaires (Atlas' new name) for better integration with Ratings functionalities.

Today in Questionnaires, you can view and answer received questionnaires; your response activity will update in both tools.

You can also opt out of Questionnaires to just use Atlas.

238

☐	Sent To	Security Score	Questionnaire	Status	% Completion	Validation Score	Due d
☐	SecurityScorecardCSM To: jnorton@securityscorecard.io From: jnorton@securityscorecard.io	A 95	ISO 27001 - 2022 v2	● In progress	21% 20/93	0%	-
☐	Galactic Industries To: stewartmoody@galactic-industries.com From: stewartmoody+securityscorecardcsm@securitysco	B 84	NIST Cybersecurity Framework (CSF) v1.1	● Accepted / Closed	12% 14/108	10%	-
☐	Galactic Industries To: stewartmoody@galactic-industries.com From:	B 84	Vendor Security Info	● Accepted / Closed	100% 2/2	0%	-

4th Party Vendor Detection in Portfolios

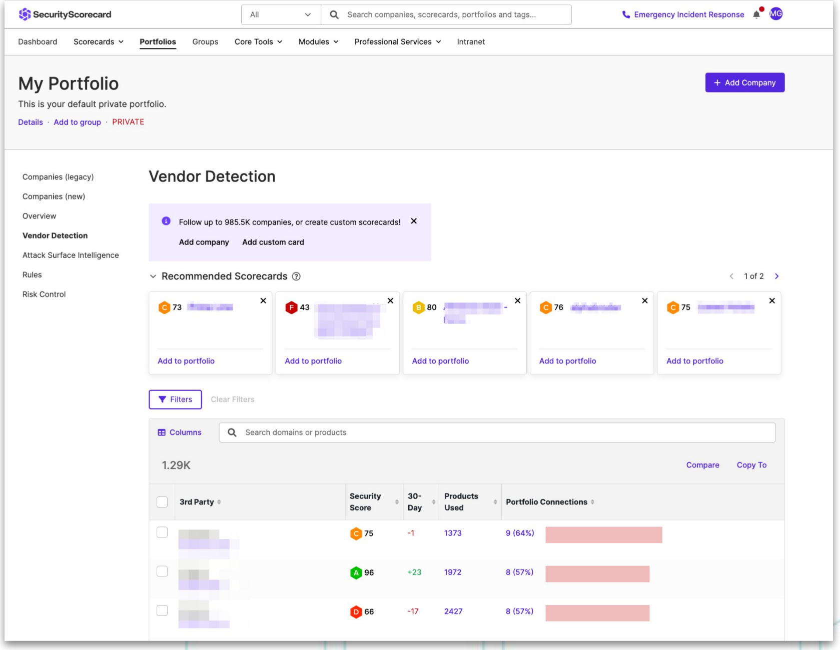
Instantly assess concentration risk within your Portfolios

Gain visibility into what vendors and products your third parties in a Portfolio rely on to get ahead of concentration risk.

How this helps you: When looking at a Portfolio, you can now see your fourth parties connected to the vendors, how they are connected, and their security risk.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Evaluate the concentration risk posed to your organization by your most critical vendors.
- **Enterprise-Cyber RIsk Management:** Protect your organization against potential third and fourth party breaches by getting ahead of concentration risk.
- **M&A Due Diligence:** Stay ahead of threats in your investments or M&A prospects with insight into the organizations and products they rely on.



My Portfolio

This is your default private portfolio.

Vendor Detection

Follow up to 985.5K companies, or create custom scorecards!

Recommended Scorecards

C	73	[redacted]
F	43	[redacted]
B	80	[redacted]
C	76	[redacted]
C	75	[redacted]

1.29K

□	3rd Party	Security Score	30-Day	Products Used	Portfolio Connections
□	[redacted]	C 75	-1	1373	9 (64%)
□	[redacted]	A 96	+23	1972	8 (57%)
□	[redacted]	D 66	-17	2427	8 (57%)

Invited Contact Manager

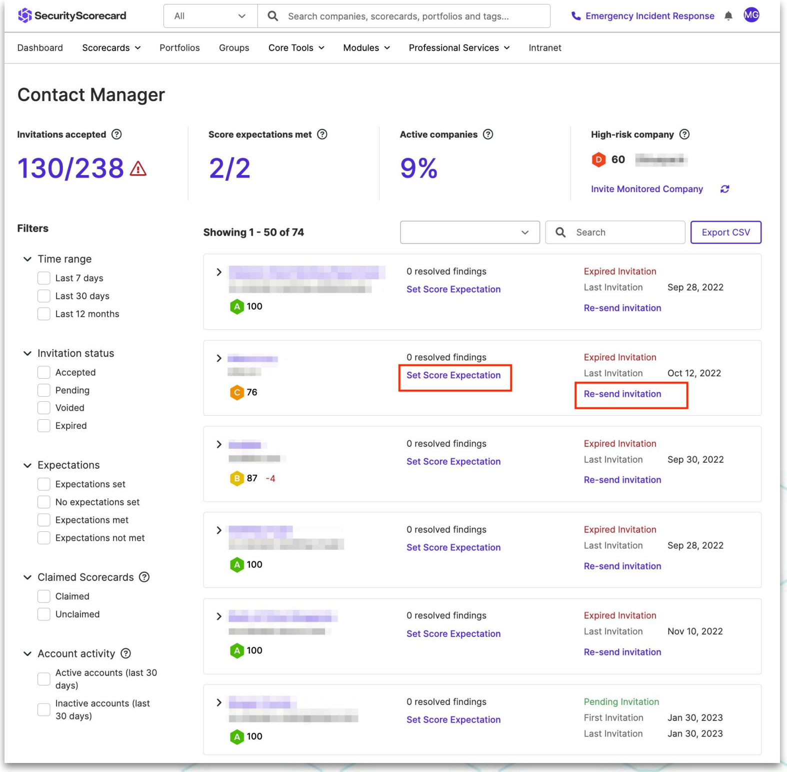
Easily collaborate with key partners to get ahead of ecosystem risk.

Gain visibility into the status of all of your invited vendors and their progress on improving their security posture.

How this helps you: Eliminate the need for email back and forth with instant visibility into the status of every vendor you've invited and their progress so you can prioritize next steps.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Partner with your vendors to improve ecosystem risk with visibility into every step.
- **Cyber Insurance:** Monitor the adoption of security ratings as a policyholder benefit amongst your insureds
- **M&A Due Diligence:** Stay ahead of risk within your Portfolio companies by easily inviting them to improve their security posture with visibility into their progress.



Contact Manager

Invitations accepted: 130/238 ⚠
Score expectations met: 2/2
Active companies: 9%
High-risk company: D 60 [redacted]
Invite Monitored Company

Filters

Time range
□ Last 7 days
□ Last 30 days
□ Last 12 months

Invitation status
□ Accepted
□ Pending
□ Voided
□ Expired

Expectations
□ Expectations set
□ No expectations set
□ Expectations met
□ Expectations not met

Claimed Scorecards
□ Claimed
□ Unclaimed

Account activity
□ Active accounts (last 30 days)
□ Inactive accounts (last 30 days)

Showing 1 - 50 of 74 | Search | Export CSV

Company	Findings	Status
[redacted] A 100	0 resolved findings Set Score Expectation	Expired Invitation Last Invitation Sep 28, 2022 Re-send invitation
[redacted] C 76	0 resolved findings Set Score Expectation	Expired Invitation Last Invitation Oct 12, 2022 Re-send invitation
[redacted] B 87 -4	0 resolved findings Set Score Expectation	Expired Invitation Last Invitation Sep 30, 2022 Re-send invitation
[redacted] A 100	0 resolved findings Set Score Expectation	Expired Invitation Last Invitation Sep 28, 2022 Re-send invitation
[redacted] A 100	0 resolved findings Set Score Expectation	Expired Invitation Last Invitation Nov 10, 2022 Re-send invitation
[redacted] A 100	0 resolved findings Set Score Expectation	Pending Invitation First Invitation Jan 30, 2023 Last Invitation Jan 30, 2023

LEARN MORE

Enterprise Cyber Risk Management

- Evidence & Events in the Digital Footprint
- Automated Board Reports
- Compliance Readiness Assessment
- Asset Categories
- Custom Scorecard Filters
- Subsidiary Scorecards Issue View

Evidence & Events in the Digital Footprint

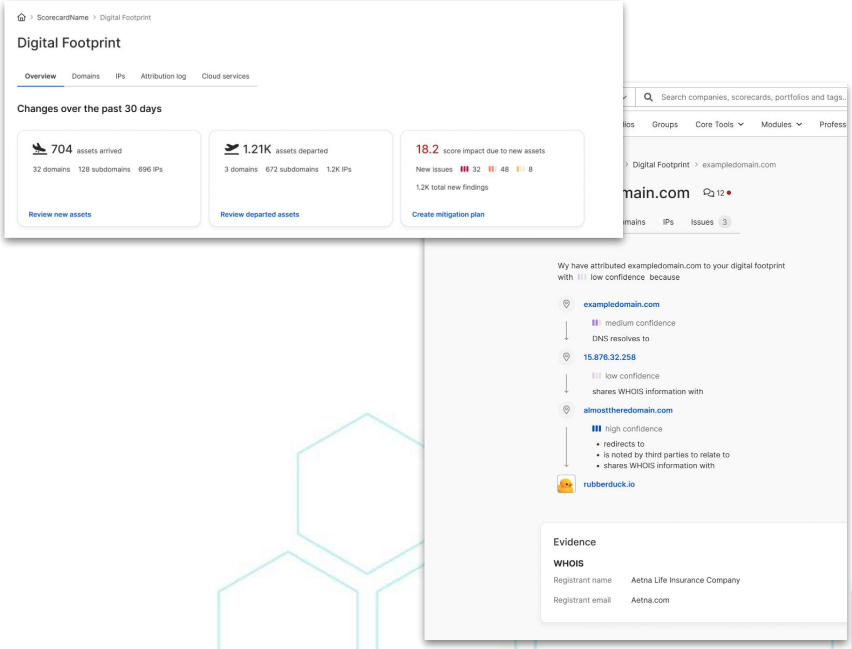
Clearly identify evidence of attributed domains in your Digital Footprint

Actively assess how assets relate to your organization

How this helps you: Clear communication of attribution sources and any underlying evidence for Digital Footprint assets. Easily understand what assets have been discovered and/or decommissioned, providing a clear picture on how those assets relate to their organization.

Other Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Verify if asset is attributed correctly to your scorecard, before reviewing the associated issues and accordingly allocating internal resources to remediate them.
- **Third-Party Risk Management:** While reviewing issues (that matter to you) on your vendor's scorecard , verify whether corresponding assets are attributed correctly.


ScorecardName > Digital Footprint
Overview
Domains
IPs
Attribution log
Cloud services
Search companies, scorecards, portfolios and tags..
lios
Groups
Core Tools
Modules
Profess
Digital Footprint > exampledomain.com
main.com
12
mains
IPs
Issues 3

Digital Footprint

Changes over the past 30 days

704 assets arrived
32 domains 128 subdomains 696 IPs
Review new assets

1.21K assets departed
3 domains 672 subdomains 1.2K IPs
Review departed assets

18.2 score impact due to new assets
New issues 32 48 8
1.2K total new findings
Create mitigation plan

Wy have attributed exampledomain.com to your digital footprint with low confidence because

exampledomain.com
medium confidence
DNS resolves to
15.876.32.258
low confidence
shares WHOIS information with
almosttheredomain.com
high confidence
- redirects to
- is noted by third parties to relate to
- shares WHOIS information with

rubberduck.io

Evidence

WHOIS

Registrant name	Aetna Life Insurance Company
Registrant email	Aetna.com

LEARN MORE

Automated Board Reports

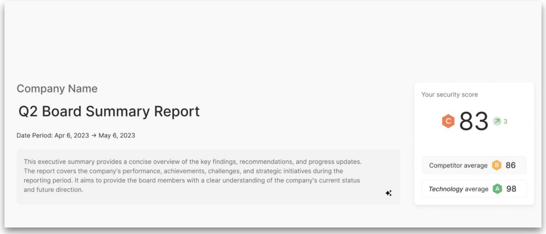
Clearly articulate the work done to improve your organization's score

Contextualize security risks with business risks.

How this helps you: Better communicate the most important high-level metrics across a Scorecard. Summarize key information on your organization's self-monitoring, vendor risk management, industry peers, and the competition.

Other Use Cases this Enables:

- **Executive Level Reporting:** Easily report on your cybersecurity posture, benchmarked against peers and in time, so that I can assess our top priorities and determine if the investments are aligned with the business priorities and risks



Company Name

Q2 Board Summary Report

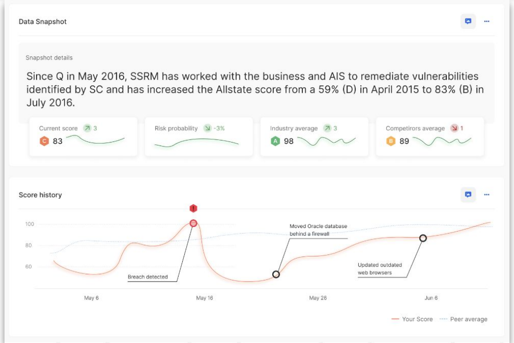
Date Period: Apr 6, 2023 → May 6, 2023

This executive summary provides a concise overview of the key findings, recommendations, and progress updates. The report covers the company's performance, achievements, challenges, and strategic initiatives during the reporting period. It aims to provide the board members with a clear understanding of the company's current status and future direction.

Your security score: C 83 ↗ 3

Competitor average B 86

Technology average A 98



Data Snapshot

Snapshot details

Since Q in May 2016, SSRM has worked with the business and AIS to remediate vulnerabilities identified by SC and has increased the Allstate score from a 59% (D) in April 2015 to 83% (B) in July 2016.

Current score ↗ 3: C 83

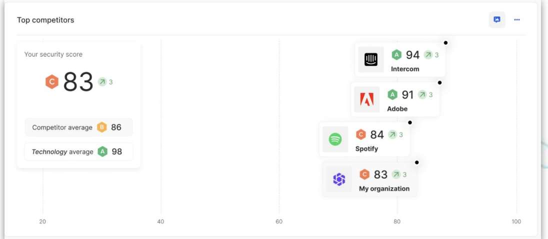
Risk probability ↘ -3%

Industry average ↗ 3: A 98

Competirors average ↘ 1: B 89

Score history

100
80
60
Breach detected
Moved Oracle database behind a firewall
Updated outdated web browsers
May 6
May 16
May 26
Jun 6
Your Score
Peer average



Top competitors

Your security score: C 83 ↗ 3

Competitor average B 86

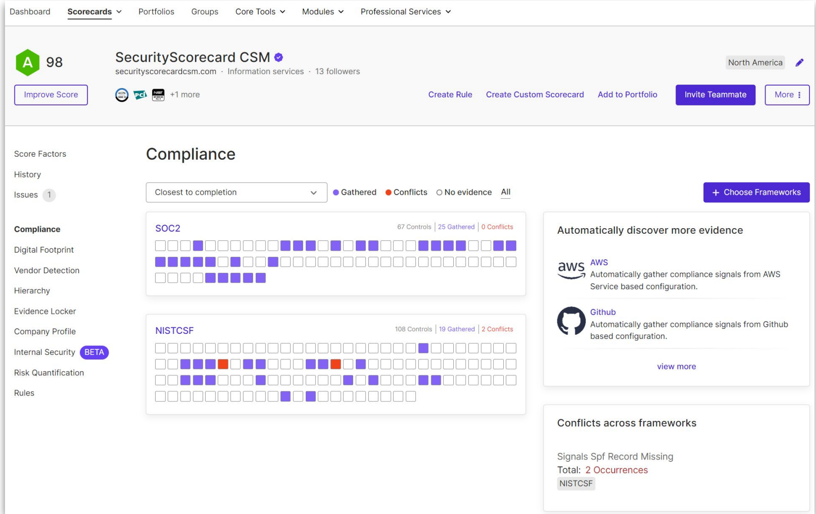
Technology average A 98

Compliance Readiness Assessment

Centralize evidence collection for faster, more effective audits

Automatically gather evidence that indicates adherence to or violation of compliance frameworks

How this helps you: Gain a quick understanding of compliance readiness and prioritize where to focus



A 98

SecurityScorecard CSM

securityscorecardcsm.com · Information services · 13 followers

North America

Compliance

SOC2 — 67 Controls | 25 Gathered | 0 Conflicts

NISTCSF — 108 Controls | 19 Gathered | 2 Conflicts

Automatically discover more evidence

AWS — Automatically gather compliance signals from AWS Service based configuration.

Github — Automatically gather compliance signals from Github based configuration.

Conflicts across frameworks

Signals Spf Record Missing
Total: 2 Occurrences
NISTCSF

Other Use Cases this Enables:

- **Compliance:** Continuously monitor compliance and reduce compliance drift ahead of audits
- **Third-Party Risk Management:** Implement onboarding framework for low-tier vendors that don't require questionnaires
- **Cyber Insurance:** Evaluate insureds against underwriting or insurance renewal guidelines
- **Regulatory Oversight:** Independently monitor regulated entities and their adherence to regulatory requirements

LEARN MORE

Asset Categories

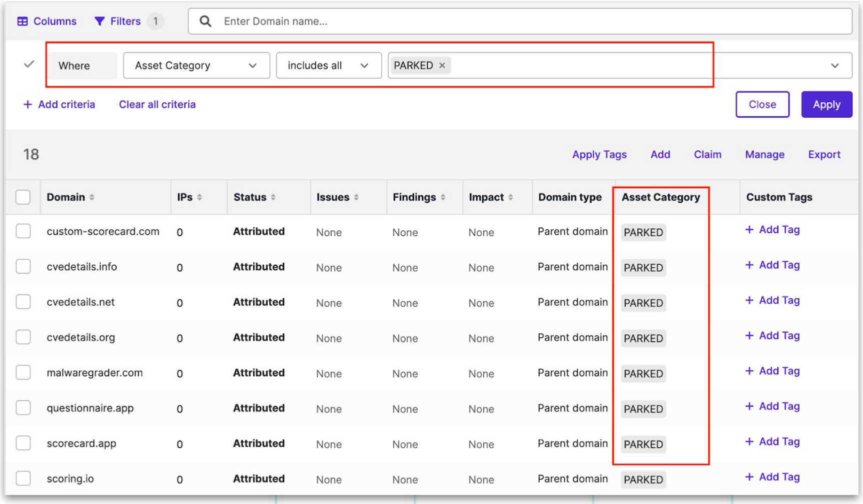
Enable more segmented monitoring and risk mitigation

Label assets for easy assignment of ownership for IPs and Domains.

How this helps you: Auto-assigned and user-contributed categories for assets, making it easier to determine ownership of assets within teams. These categories provide a more accurate picture of an organization's attack surface and Top Level Score.

Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Infosec managers can leverage ‘asset category’ to get visibility on exposure and assign assets to their respective teams for effective monitoring and risk mitigation.



Where | Asset Category | includes all | PARKED ×

18

□	Domain	IPs	Status	Issues	Findings	Impact	Domain type	Asset Category	Custom Tags
□	custom-scorecard.com	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	cvedetails.info	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	cvedetails.net	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	cvedetails.org	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	malwaregrader.com	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	questionnaire.app	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	scorecard.app	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag
□	scoring.io	0	Attributed	None	None	None	Parent domain	PARKED	+ Add Tag

LEARN MORE

Custom Scorecard Filters

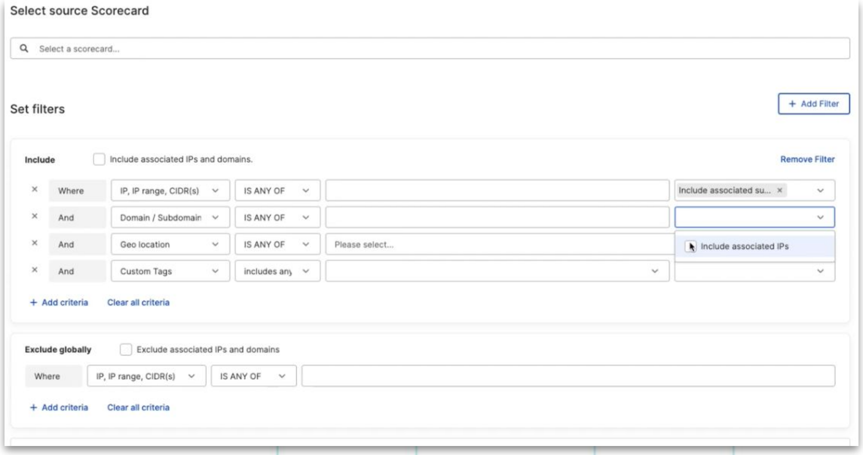
More tagging and filtering criteria for quickly building Custom Scorecards.

Better geolocation and subdomain filtering for segmented Scorecards

How this helps you: Expedite the allocation of assets and easily select associated IPs, domains and subdomains for selected assets, and geo-location based on options made available to them in these filters.

Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Build custom scorecards for your organization to have a more accurate view of your organization and prioritize remediation based on geolocation, subdomains, and other filtering options.



Select source Scorecard

Select a scorecard...

Set filters

Include □ Include associated IPs and domains.

Where IP, IP range, CIDR(s) IS ANY OF — Include associated su...
And Domain / Subdomain IS ANY OF — □ Include associated IPs
And Geo location IS ANY OF Please select...
And Custom Tags includes any

Exclude globally □ Exclude associated IPs and domains

Where IP, IP range, CIDR(s) IS ANY OF

LEARN MORE

Subsidiary Scorecard Issue View

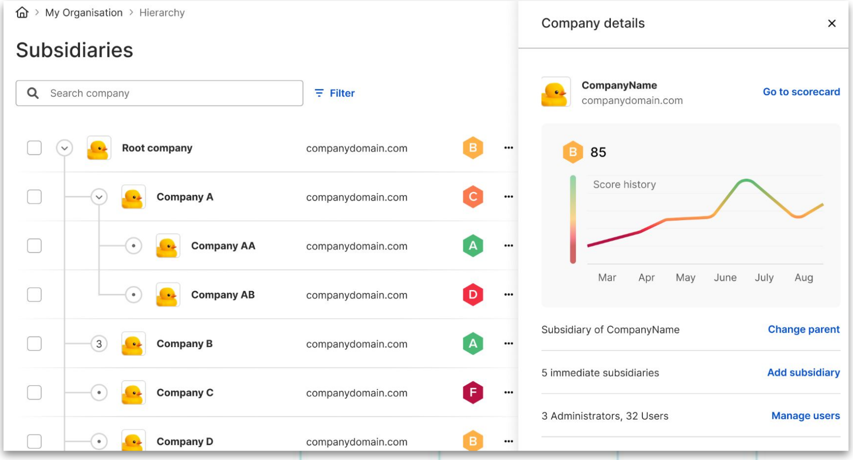
Continuously monitor the security posture of your organization and subsidiaries.

Access complete issue evidence for your subsidiaries

How this helps you: Improve the overall security posture of an entity faster and understand common risks to quickly prioritize subsidiaries that require additional resources or attention to reduce cyber risk.

Other Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Faster remediation and hence risk mitigation for overall organizational posture.
- **Executive Level Reporting:** Accurately report on and analyze the security posture and efforts of certain business units within the entire entity



My Organisation > Hierarchy

Subsidiaries

Search company

Filter

□	Root company	companydomain.com	B
□	Company A	companydomain.com	C
□	Company AA	companydomain.com	A
□	Company AB	companydomain.com	D
□	3 Company B	companydomain.com	A
□	Company C	companydomain.com	F
□	Company D	companydomain.com	B

Company details ×

CompanyName
companydomain.com
Go to scorecard

B 85

Score history

Subsidiary of CompanyName — Change parent

5 immediate subsidiaries — Add subsidiary

3 Administrators, 32 Users — Manage users

LEARN MORE

Threat Intelligence

- BreachDetails
- Visual Search in Attack Surface Intelligence
- Table view in Attack Surface Intelligence
- CVEDetails.com

BreachDetails

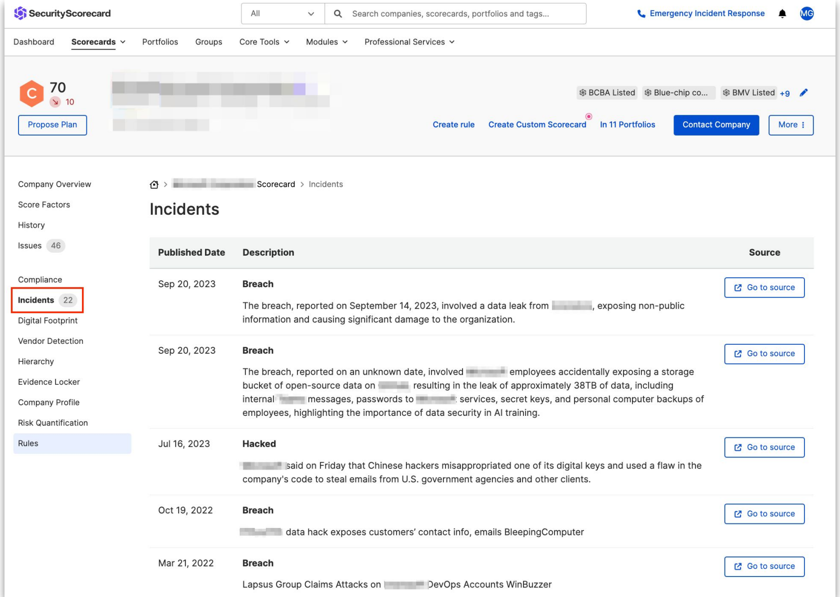
Respond with confidence when a breach is detected in your business ecosystem

Accurately identify breaches, reduce false positives, improve timeliness of breach notifications, and increase geographic coverage.

How this helps you: Using an in-house method for collecting and analyzing breach data provides greater control over breach notices and on-demand addition of breach detection sources providing you with even more detail for a breach.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Continuously monitor your entire third-party ecosystem for any detected breaches and be prepared to comply with regulatory guidelines.
- **Enterprise-Cyber RIsk Management:** Effectively report and respond to breaches impacting your own organization with timely and accurate Breach Notices and Incidents.
- **Cyber Insurance:** Validate application responses regarding past claims and identify breaches that could be covered under claims made policies



Incidents

Published Date	Description	Source
Sep 20, 2023	**Breach** The breach, reported on September 14, 2023, involved a data leak from [redacted], exposing non-public information and causing significant damage to the organization.	Go to source
Sep 20, 2023	**Breach** The breach, reported on an unknown date, involved [redacted] employees accidentally exposing a storage bucket of open-source data on [redacted] resulting in the leak of approximately 38TB of data, including internal [redacted] messages, passwords to [redacted] services, secret keys, and personal computer backups of employees, highlighting the importance of data security in AI training.	Go to source
Jul 16, 2023	**Hacked** [redacted] said on Friday that Chinese hackers misappropriated one of its digital keys and used a flaw in the company's code to steal emails from U.S. government agencies and other clients.	Go to source
Oct 19, 2022	**Breach** [redacted] data hack exposes customers' contact info, emails BleepingComputer	Go to source
Mar 21, 2022	**Breach** Lapsus Group Claims Attacks on [redacted] DevOps Accounts WinBuzzer	Go to source

LEARN MORE

Visual Search in Attack Surface Intelligence

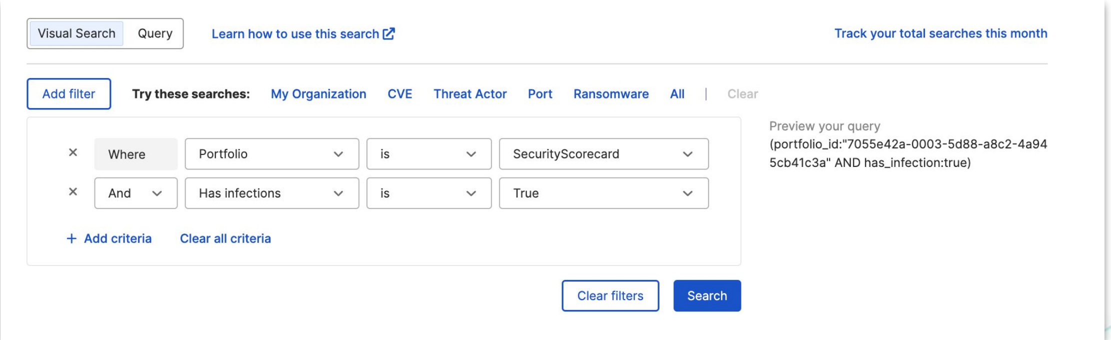
Surfacing threat intelligence fast and intuitively.

Enabling users without query syntax knowledge to quickly and efficiently conduct searches to gain the answers they need to drive decisions.

How this helps you: **Save time** with an effortless view of threat results with the ability to search, sort, and see more details without multiple clicks.

Other Use Cases this Enables:

- **Third-Party Risk Management**
- **Enterprise-Cyber RIsk Management**
- **M&A Due Diligence**
- **Cyber Insurance**



Visual Search | Query

Learn how to use this search

Track your total searches this month

Add filter

Try these searches: My Organization CVE Threat Actor Port Ransomware All | Clear

× Where Portfolio is SecurityScorecard

× And Has infections is True

+ Add criteria Clear all criteria

Preview your query
(portfolio_id:"7055e42a-0003-5d88-a8c2-4a94 5cb41c3a" AND has_infection:true)

Clear filters Search

Table View in Attack Surface Intelligence

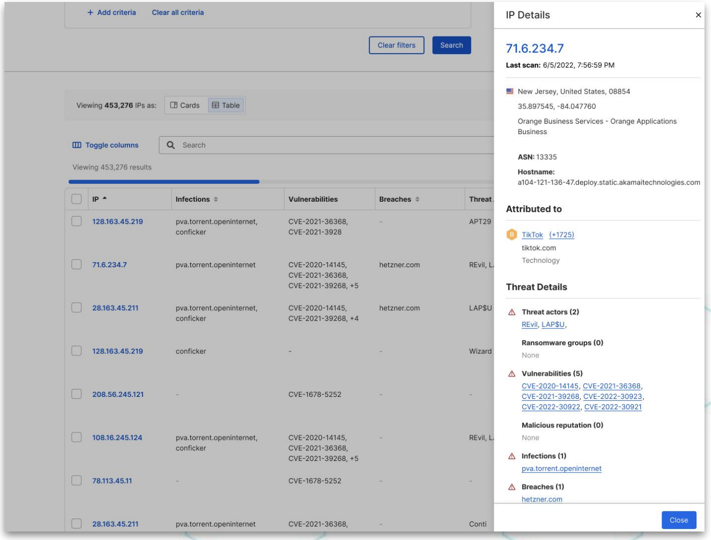
Gain a consolidated and searchable view of threat intelligence search results .

Effectively and efficiently find what you are looking for without leaving the results page.

How this helps you: **Save time** with an effortless view of threat results with the ability to search, sort, and see more details without multiple clicks.

Other Use Cases this Enables:

- Third-Party Risk Management
- Enterprise-Cyber RIsk Management
- M&A Due Diligence
- Cyber Insurance



Viewing **453,276** IPs as:

Viewing 453,276 results

	IP	Infections	Vulnerabilities	Breaches	Threat
□	128.163.45.219	pva.torrent.openinternet, conficker	CVE-2021-36368, CVE-2021-3928	-	APT29
□	71.6.234.7	pva.torrent.openinternet	CVE-2020-14145, CVE-2021-36368, CVE-2021-39268, +5	hetzner.com	REvil, L
□	28.163.45.211	pva.torrent.openinternet, conficker	CVE-2020-14145, CVE-2021-39268, +4	hetzner.com	LAP$U
□	128.163.45.219	conficker	-	-	Wizard
□	208.56.245.121	-	CVE-1678-5252	-	-
□	108.16.245.124	pva.torrent.openinternet, conficker	CVE-2020-14145, CVE-2021-36368, CVE-2021-39268, +5	-	REvil, L
□	78.113.45.11	-	CVE-1678-5252	-	-
□	28.163.45.211	pva.torrent.openinternet	CVE-2021-36368,	-	Conti

IP Details ×

71.6.234.7

Last scan: 6/5/2022, 7:56:59 PM

New Jersey, United States, 08854

35.897545, -84.047760

Orange Business Services - Orange Applications Business

ASN: 13335

Hostname: a104-121-136-47.deploy.static.akamaitechnologies.com

Attributed to

B TikTok (+1725)
tiktok.com
Technology

Threat Details

⚠ **Threat actors (2)**
REvil, LAP$U,

Ransomware groups (0)
None

⚠ **Vulnerabilities (5)**
CVE-2020-14145, CVE-2021-36368, CVE-2021-39268, CVE-2022-30923, CVE-2022-30922, CVE-2022-30921

Malicious reputation (0)
None

⚠ **Infections (1)**
pva.torrent.openinternet

⚠ **Breaches (1)**
hetzner.com

CVEDetails.com *Beta*

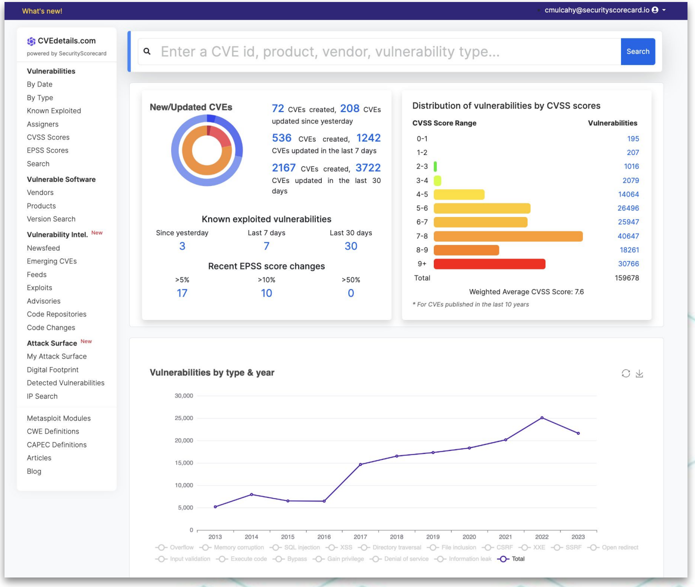
Harness vulnerability intelligence to understand the impact to your attack surface.

Gain a comprehensive understanding of details associated with all published and upcoming CVEs to drive remediation decisions.

How this helps you: **Make faster decisions** with insight into the severity of a CVE and any known exploits to determine the impact to the business.

Other Use Cases this Enables:

- **Enterprise-Cyber RIsk Management**
- **Vulnerability Management**



New/Updated CVEs

72 CVEs created, 208 CVEs updated since yesterday

536 CVEs created, 1242 CVEs updated in the last 7 days

2167 CVEs created, 3722 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
3	7	30

Recent EPSS score changes

>5%	>10%	>50%
17	10	0

Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	195
1-2	207
2-3	1016
3-4	2079
4-5	14064
5-6	26496
6-7	25947
7-8	40647
8-9	18261
9+	30766
Total	159678

Weighted Average CVSS Score: 7.6

** For CVEs published in the last 10 years*

Vulnerabilities by type & year

LEARN MORE

Professional Services

- Managed Cyber Risk Services *Soft launch*
- Zero-Day-as-a-Service *Soft launch*
- Request Services in Platform

Managed Cyber Risk Services *Soft Launch*

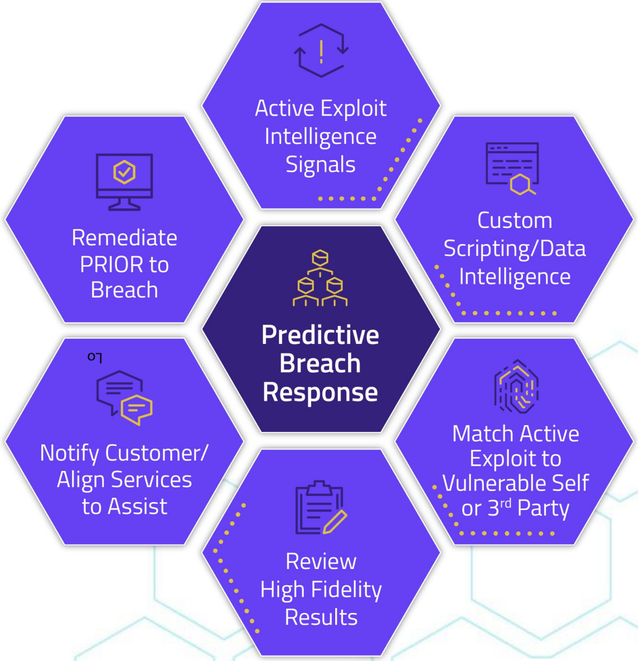
Operationalize your third-party cyber risk program to stop attacks before they happen

Augment your existing cyber risk program alongside cybersecurity professionals to proactively identify the likelihood of a cyber incident in your vendor ecosystem.

How this helps you: Partner with cyber experts to assess, monitor, and mitigate blindspots across your supply chain to reduce cyber risk and increase efficiencies across your third party risk program.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Using the powerful risk signals and threat insights from the SecurityScorecard platform, proactively analyze and mitigate cyber risk associated with your vendor landscape.



Active Exploit Intelligence Signals
Custom Scripting/Data Intelligence
Match Active Exploit to Vulnerable Self or 3rd Party
Review High Fidelity Results
Notify Customer/ Align Services to Assist
Remediate PRIOR to Breach
Predictive Breach Response

LEARN MORE

Zero-Day-as-a-Service *Soft Launch*

Early warning and detection service for new and emerging zero-days across your vendor ecosystem

Comprehensive report detailing newly-identified zero-days, third-parties potentially susceptible, and actionable steps to track and combat the zero-day.

How this helps you: **Safeguards your organization** against emerging security threats across your third party vendor ecosystem.

Other Use Cases this Enables:

- **Third-Party Risk Management:** Using the powerful risk signals and threat insights from the SecurityScorecard platform, proactively analyze and mitigate cyber risk associated with your vendor landscape. Available as part of the Managed Cyber Risk Services offering or as an individual offering.

LEARN MORE

Request Services in Platform

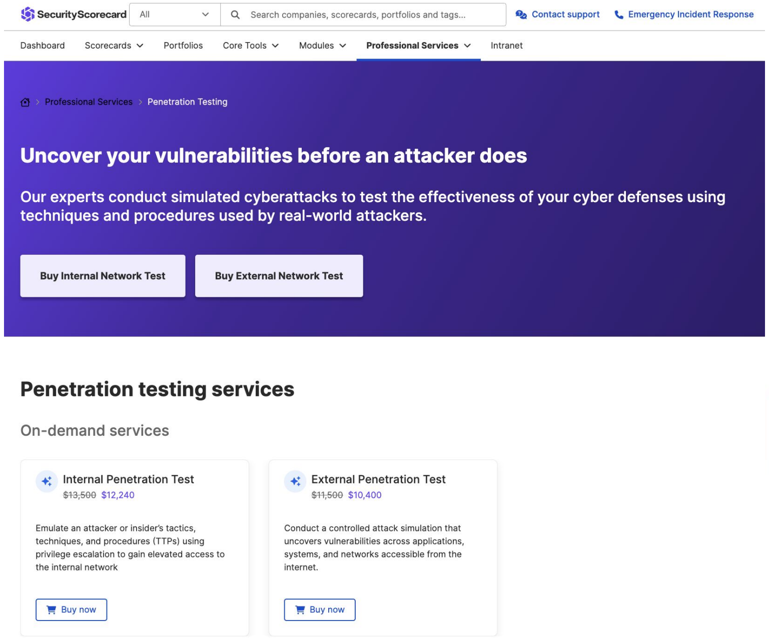
Purchase or schedule a consultation for Professional Services within the platform

Tabletop Exercises, Penetration Testing, and Incident Response support are available to be purchased or to schedule a time with our team on-demand.

How this helps you: Saves time and streamlines gaining access to SecurityScorecard Professional Services to help you strengthen your cybersecurity defenses.

Other Use Cases this Enables:

- **Enterprise-Cyber RIsk Management:** If you're under attack or simply looking to proactively strengthen your controls, our Services team is here to help! Quickly gain access to the team on-demand from the platform.


SecurityScorecard
All
Search companies, scorecards, portfolios and tags...
Contact support
Emergency Incident Response
Dashboard
Scorecards
Portfolios
Core Tools
Modules
Professional Services
Intranet
Professional Services > Penetration Testing
Buy Internal Network Test
Buy External Network Test
Buy now
Buy now

Uncover your vulnerabilities before an attacker does

Our experts conduct simulated cyberattacks to test the effectiveness of your cyber defenses using techniques and procedures used by real-world attackers.

Penetration testing services

On-demand services

Internal Penetration Test ~~$13,500~~ $12,240

Emulate an attacker or insider's tactics, techniques, and procedures (TTPs) using privilege escalation to gain elevated access to the internal network

External Penetration Test ~~$11,500~~ $10,400

Conduct a controlled attack simulation that uncovers vulnerabilities across applications, systems, and networks accessible from the internet.

LEARN MORE

Marketplace

- ProcessUnity
- Jira On-Demand Ticket Creation
- S&P Risk Indicator
- Cybersecurity Risk Insights
- Salesforce Scorecard IMporter
- Threat Quotient
- Netskole CCI Integration

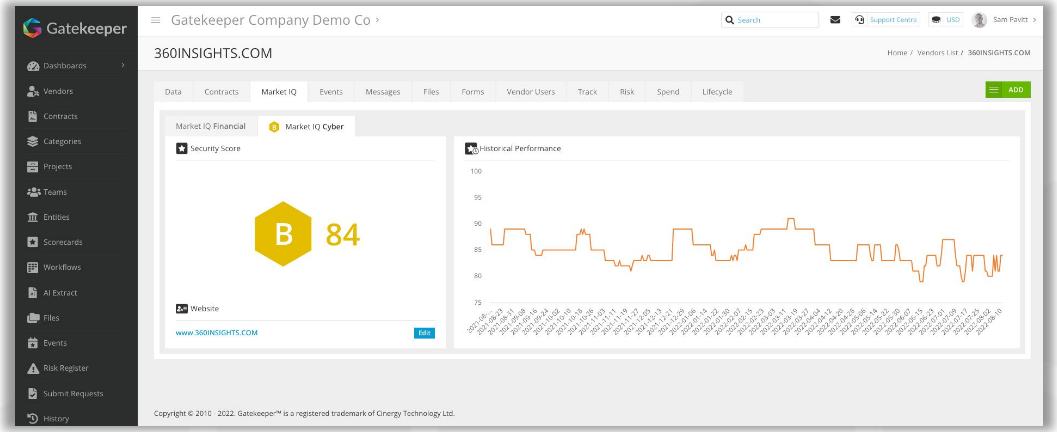
Gatekeeper

Deliver total visibility and awareness of security risks through the lifecycle of engagement with your third-parties

How this helps you: View top-level SecurityScorecard grades without leaving the Gatekeeper MarketIQ module

Use Cases this Enables:

- **Vendor Risk Management**: Monitor cyber risk from your third-parties and work with them to manage issues that arise



360INSIGHTS.COM

Website

www.360INSIGHTS.COM

Copyright © 2010 - 2022. Gatekeeper™ is a registered trademark of Cinergy Technology Ltd.

LEARN MORE

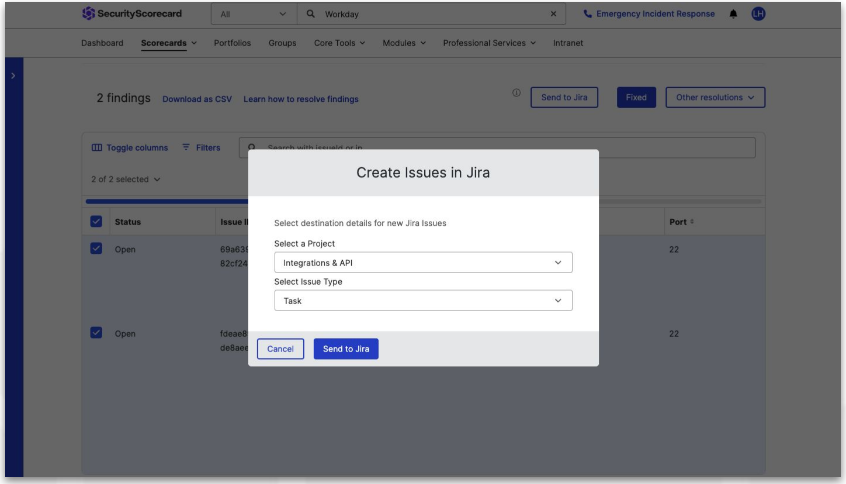
Jira On-Demand Ticket Creation

Automatically create actionable and detailed Jira tickets for individual Issue Findings from SecurityScorecard.

How this helps you: Triage individual issues in SecurityScorecard based on severity and score impact.

Use Cases this Enables:

- **Enterprise Cyber Risk Management:** Automatically create actionable and detailed Jira tickets for individual Issue Findings selected from SecurityScorecard.



2 findings

Create Issues in Jira

Select destination details for new Jira Issues

Select a Project: Integrations & API

Select Issue Type: Task

☑	Status	Issue I	Port
☑	Open	69a639 82cf24	22
☑	Open	fdeae8 de8aee	22

LEARN MORE

S&P Supplier Risk Indicator

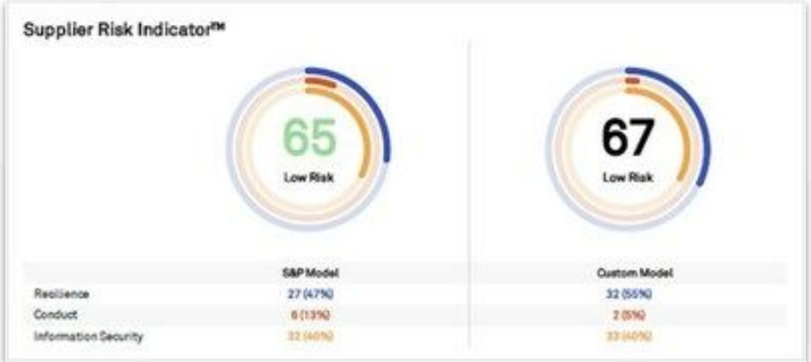
Evaluate any organization's supply chain risk.

S&P Global
Market Intelligence

How this helps you: Evaluate supplier's with a single score based on key risk factors including cyber, financial, and ESG. Receive trusted data from two of the industry's leading Ratings companies.

Use Cases this Enables:

- **Supply Chain Risk Management:** Monitor for and quantify supply chain risk with a single Supplier Risk Indicator (SRI) score**.** Drill down into the factors comprising the score to prioritize individual issues that could put your organization at risk.



Supplier Risk Indicator™

	S&P Model	Custom Model
Resilience	27 (47%)	32 (55%)
Conduct	6 (13%)	2 (5%)
Information Security	32 (40%)	33 (40%)

LEARN MORE

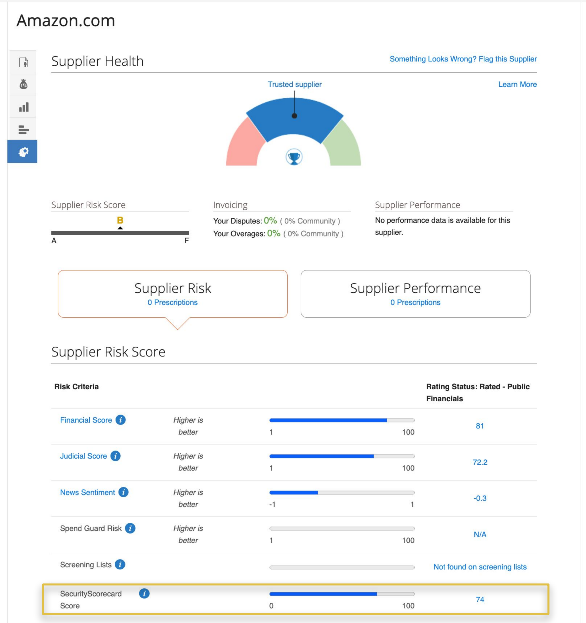
Cybersecurity Risk Insights App for Coupa

Understand how cyber risk impacts your Supplier’s overall health in Coupa.

How this helps you: Continuously monitor and understand a supplier’s overall cyber security posture across the entire procurement and supplier lifecycle to make more informed business decisions.

Use Cases this Enables:

- **Vendor Risk Management:** Use SecurityScorecard’s trusted cyber scores to evaluate suppliers during due diligence, onboarding, payment, and on an ongoing basis.
- **Procurement:** Automate approval workflows based on acceptable cybersecurity ratings. Automatically flag high-risk suppliers.



Amazon.com

Supplier Health

Something Looks Wrong? Flag this Supplier

Trusted supplier

Learn More

Supplier Risk Score

B

A F

Invoicing

Your Disputes: 0% (0% Community)

Your Overages: 0% (0% Community)

Supplier Performance

No performance data is available for this supplier.

Supplier Risk
0 Prescriptions

Supplier Performance
0 Prescriptions

Supplier Risk Score

Risk Criteria			Rating Status: Rated - Public Financials
Financial Score	*Higher is better*	1 100	81
Judicial Score	*Higher is better*	1 100	72.2
News Sentiment	*Higher is better*	-1 1	-0.3
Spend Guard Risk	*Higher is better*	1 100	N/A
Screening Lists			Not found on screening lists
SecurityScorecard Score		0 100	74

LEARN MORE

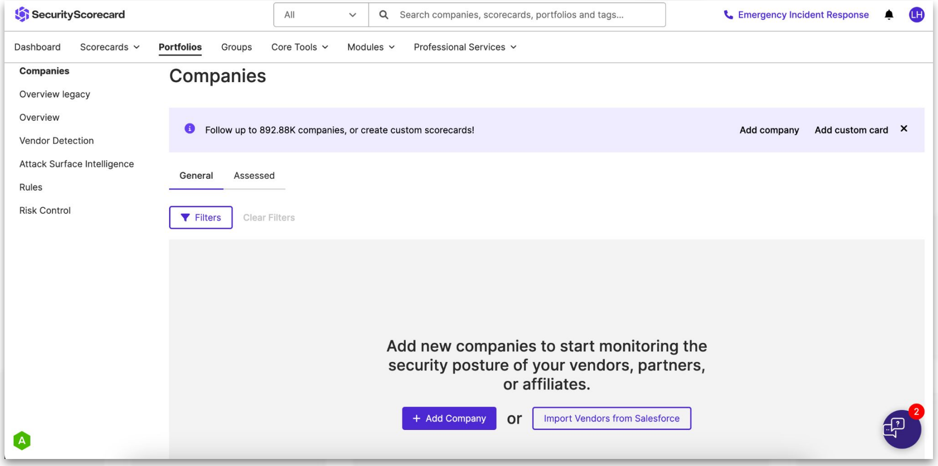
Salesforce Scorecard Importer

Bulk import vendor accounts from Salesforce to automatically create Scorecards.

How this helps you: Monitor Scorecards for your Salesforce vendor accounts with one-click using the Salesforce Scorecard Importer.

Use Cases this Enables:

- **Vendor Risk Management:** Bulk import vendor details to fast from salesforce to fast-track SecurityScorecard onboarding.
- **Cyber Insurance:** Import client details from Salesforce to hit the ground running collaborating in SecurityScorecard



Companies

Follow up to 892.88K companies, or create custom scorecards!

Add new companies to start monitoring the security posture of your vendors, partners, or affiliates.

Add Company or Import Vendors from Salesforce

LEARN MORE

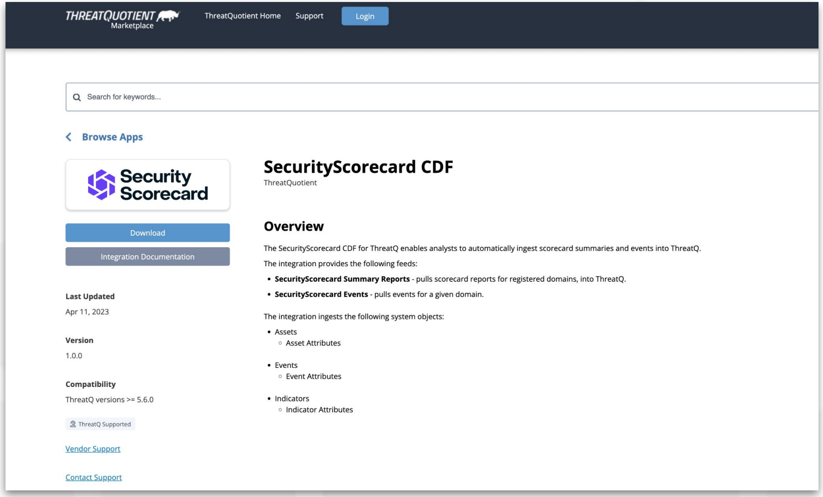
ThreatQuotient Ratings Integration

Automate continuous monitoring of your cybersecurity posture and that of your third-parties.

How this helps you: Accelerate threat detection and response with important data on your security posture.

Use Cases this Enables:

- **Third-Party Risk Management:** Automatically monitor for vulnerable third-parties in your ecosystem by ingesting scorecard reports for registered domains into ThreatQ.
- **Enterprise Cyber Risk Management:** Import your organization's Scorecard data on 10 key risk factors into ThreatQ.
- **Security Ops:** Prioritize investigation and remediation based on events identified by SecurityScorecard



SecurityScorecard CDF
ThreatQuotient

Overview

The SecurityScorecard CDF for ThreatQ enables analysts to automatically ingest scorecard summaries and events into ThreatQ.

The integration provides the following feeds:

- **SecurityScorecard Summary Reports** - pulls scorecard reports for registered domains, into ThreatQ.
- **SecurityScorecard Events** - pulls events for a given domain.

The integration ingests the following system objects:

- Assets
  - Asset Attributes
- Events
  - Event Attributes
- Indicators
  - Indicator Attributes

Last Updated
Apr 11, 2023

Version
1.0.0

Compatibility
ThreatQ versions >= 5.6.0

ThreatQ Supported

Vendor Support

Contact Support

LEARN MORE

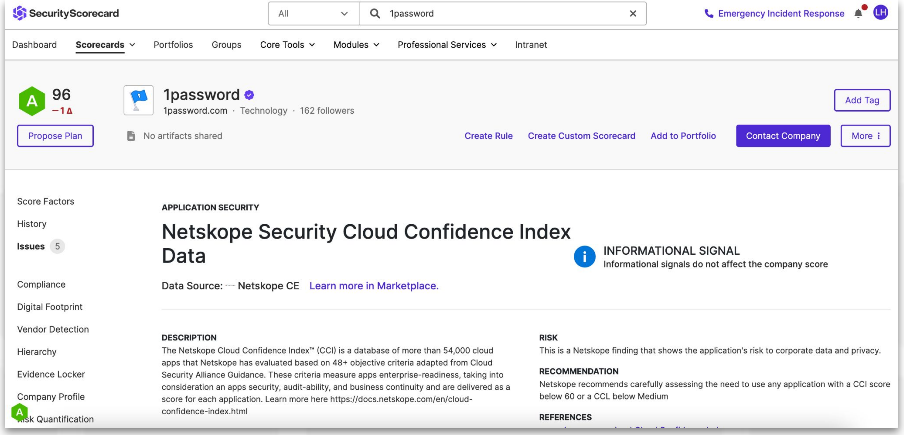
Netskope CE Integration

Confidently make policy decisions based on accurate and comprehensive security risk data for your SaaS applications.

How this helps you: Understand the risk of applications being used by employees and how your ecosystem could be affected.

Use Cases this Enables:

- **Third-Party Risk Management:** Enhanced vendor risk management with out-of-the box enablement of timely and actionable information on vendors' cybersecurity posture.
- **Enterprise Cyber Risk Management:** Get important risk information and IoCs to help security teams focus on the most critical threats in real-time.



APPLICATION SECURITY

Netskope Security Cloud Confidence Index Data

INFORMATIONAL SIGNAL
Informational signals do not affect the company score

Data Source: Netskope CE Learn more in Marketplace.

DESCRIPTION
The Netskope Cloud Confidence Index™ (CCI) is a database of more than 54,000 cloud apps that Netskope has evaluated based on 48+ objective criteria adapted from Cloud Security Alliance Guidance. These criteria measure apps enterprise-readiness, taking into consideration an apps security, audit-ability, and business continuity and are delivered as a score for each application. Learn more here https://docs.netskope.com/en/cloud-confidence-index.html

RISK
This is a Netskope finding that shows the application's risk to corporate data and privacy.

RECOMMENDATION
Netskope recommends carefully assessing the need to use any application with a CCI score below 60 or a CCL below Medium

REFERENCES

LEARN MORE

Platform

- Data Residency Compliance
- Audit Log
- Global Navigation

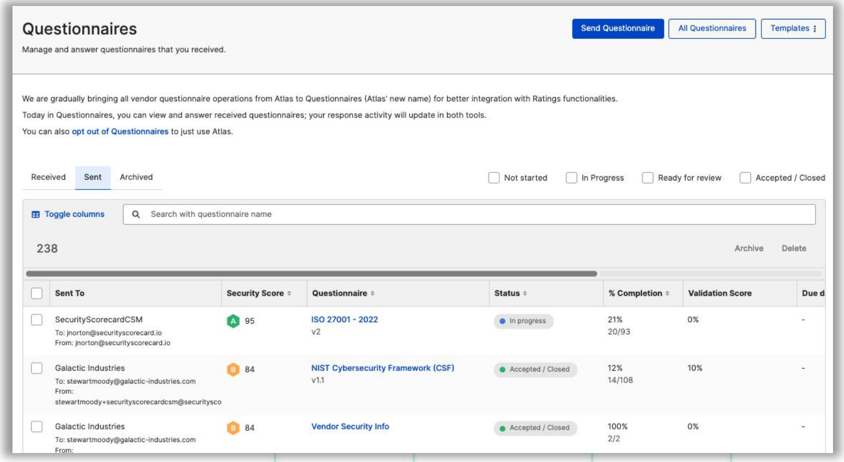
Data Residency Compliance

Collaborate with your global vendors in one platform.

Confidently send and receive questionnaires with your partners in Europe and APAC.

How this helps you: Data residency requirements define which types of sensitive data need to be stored or processed within a specific geographic location in order to meet local data privacy laws.

Sensitive data provided by customers in Europe or the Asia Pacific region in Questionnaires, Evidence Locker, and other parts of our platform now resides locally.



Questionnaires

Manage and answer questionnaires that you received.

We are gradually bringing all vendor questionnaire operations from Atlas to Questionnaires (Atlas' new name) for better integration with Ratings functionalities.

Today in Questionnaires, you can view and answer received questionnaires; your response activity will update in both tools.

You can also opt out of Questionnaires to just use Atlas.

Received | Sent | Archived

□ Not started □ In Progress □ Ready for review □ Accepted / Closed

Toggle columns | Search with questionnaire name

238 | Archive | Delete

□	Sent To	Security Score	Questionnaire	Status	% Completion	Validation Score	Due d
□	SecurityScorecardCSM To: jnorton@securityscorecard.io From: jnorton@securityscorecard.io	A 95	ISO 27001 - 2022 v2	● In progress	21% 20/93	0%	-
□	Galactic Industries To: stewartmoody@galactic-industries.com From: stewartmoody+securityscorecardcsm@securitysco	B 84	NIST Cybersecurity Framework (CSF) v1.1	● Accepted / Closed	12% 14/108	10%	-
□	Galactic Industries To: stewartmoody@galactic-industries.com From:	B 84	Vendor Security Info	● Accepted / Closed	100% 2/2	0%	-

Audit Log

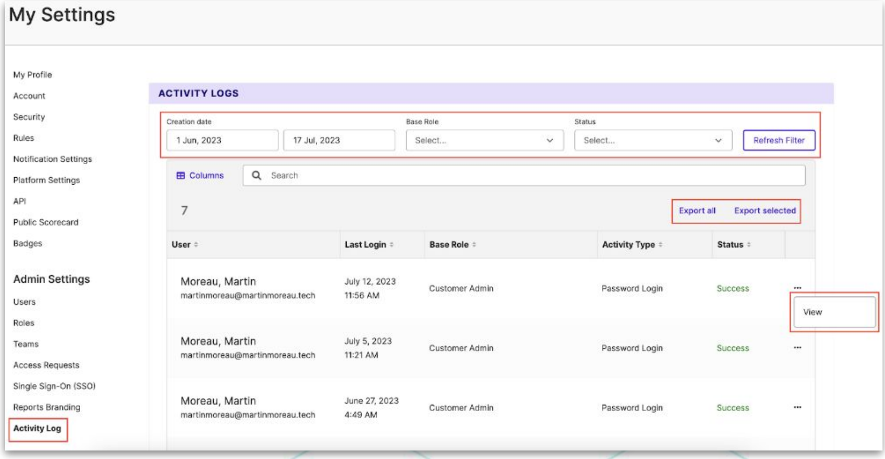
Easily track activities and actions that are taking place on the platform.

Improve internal controls and data security by regularly monitoring user audit logs.

How this helps you: Easily track who is accessing your data, what data is being accessed, and where it is being accessed from to improve internal controls, data security, and meet compliance and regulatory requirements

Other Use Cases this Enables:

- **Enterprise-Cyber RIsk Management:** Enhance your continuous monitoring efforts with a live Audit Log to track which teammates and which activities have been taken within the platform
- **Compliance:** Improve internal controls and meet regulatory requirements with continuous tracking of platform activity



Creation date: 1 Jun, 2023 – 17 Jul, 2023
Base Role: Select...
Status: Select...

7

User	Last Login	Base Role	Activity Type	Status
Moreau, Martin martinmoreau@martinmoreau.tech	July 12, 2023 11:56 AM	Customer Admin	Password Login	Success
Moreau, Martin martinmoreau@martinmoreau.tech	July 5, 2023 11:21 AM	Customer Admin	Password Login	Success
Moreau, Martin martinmoreau@martinmoreau.tech	June 27, 2023 4:49 AM	Customer Admin	Password Login	Success

LEARN MORE

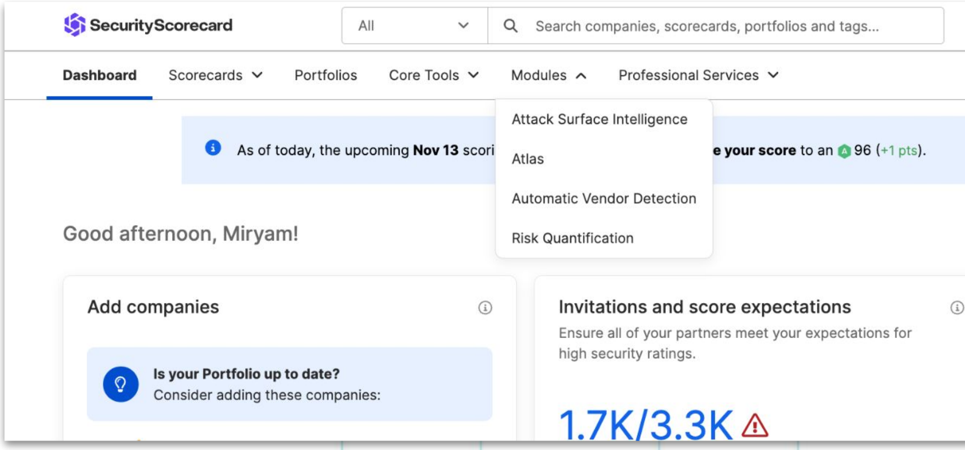
Global Navigation

Simplify your workflows in SecurityScorecard with a smarter menu.

Harness the full power of the SecurityScorecard platform with an even easier to navigate navigation bar.

How this helps you: We’ve enhanced our navigation menu within the SecurityScorecard Platform, enabling you to accomplish what you need, faster.

Find what you need more easily with all Scorecard tools – including Scorecards, Portfolios, Core Tools, and Services — condensed into a simpler interface.



As of today, the upcoming **Nov 13** scori

e your score to an 96 (+1 pts).

Good afternoon, Miryam!

Add companies

Is your Portfolio up to date?
Consider adding these companies:

Invitations and score expectations

Ensure all of your partners meet your expectations for high security ratings.

1.7K/3.3K ⚠

Additional Resources

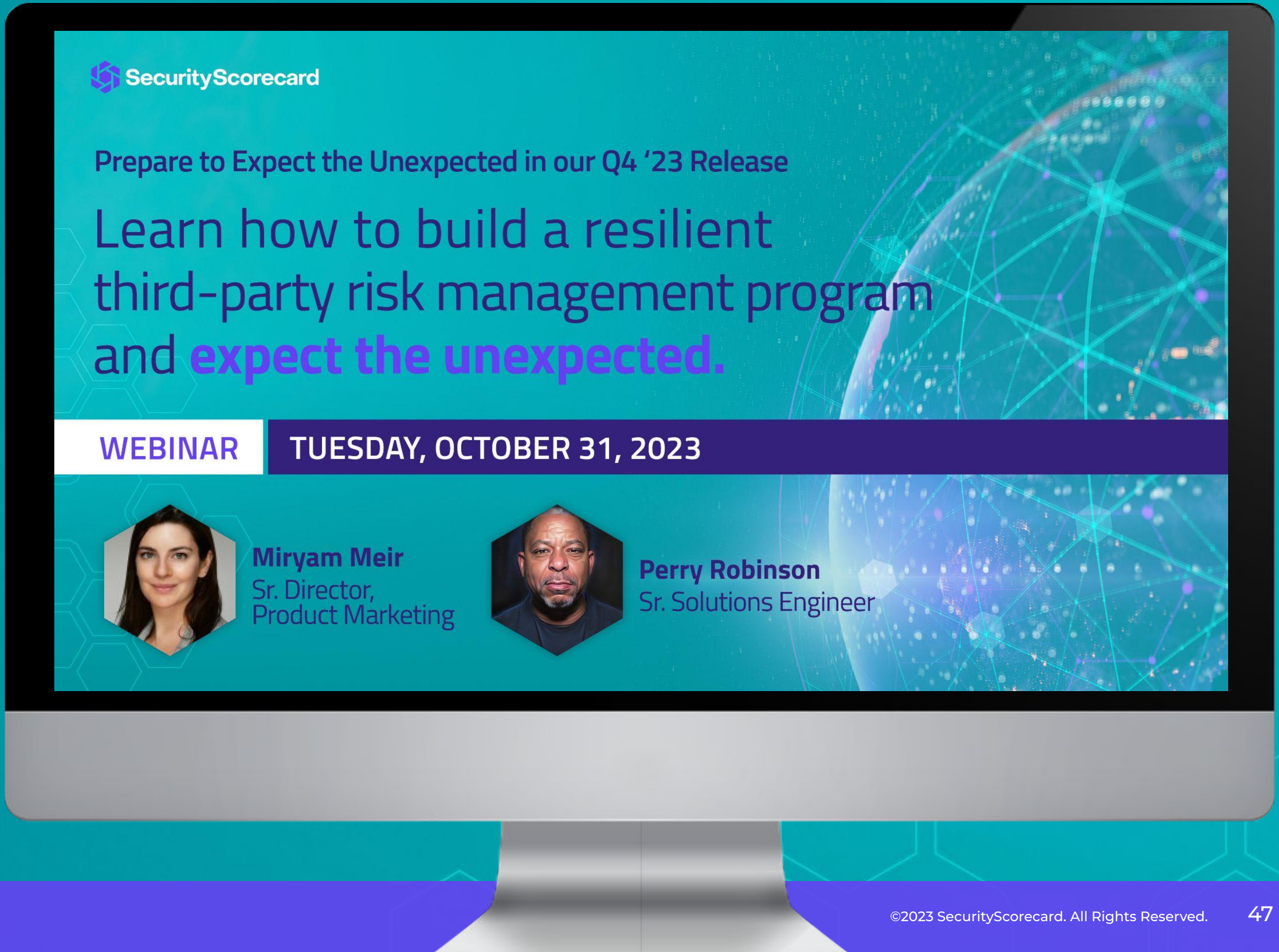
EXPECT the UNEXPECTED

Live Webinar

October 31st, 2022
2pm EST

Join us and learn how you can prepare to expect the unexpected.

REGISTER HERE



SecurityScorecard

Prepare to Expect the Unexpected in our Q4 '23 Release

Learn how to build a resilient third-party risk management program and **expect the unexpected.**

WEBINAR | TUESDAY, OCTOBER 31, 2023

Miryam Meir
Sr. Director,
Product Marketing

Perry Robinson
Sr. Solutions Engineer

Q4 ‘23 Release Notes on our Help Center

Visit our Help Center to learn more about the Q4 ‘23 Release, see our release notes, and learn more about the SecurityScorecard Platform!

https://support.securityscorecard.com/hc/en-us/articles/19207337800603

Learn more with our resources linked here!

Learn about:

- [Ebook] Expand your Vendor Intelligence to Identify Active Threats
- [Video] Building a Resilient Security Program with Moriah Hara, vCISO and Advisor
- [Video] What does it mean to Expect the Unexpected in third-party risk?
- [Whitepaper] DORA and Cyber Risk: A New Framework for Third-Party Risk in the European Union
- And more!

Thank You

EXPECT the UNEXPECTED