WHITEPAPER | USE CASE

EXPAND YOUR VENDOR INTELLIGENCE TO IDENTIFY ACTIVE THREATS

Manage your third- and fourth-party attack surface

SecurityScorecard

Table of Contents

PAGE

How to Manage Your Third- and Fourth-Party Attack Surface

Research by **Ponemon Institute** reports that **59%** of survey respondents have confirmed that their organization has experienced a data breach caused by one of their third parties, with 54% of the incidents occurring in the past 12 months. What is more alarming is that only 34% of organizations are confident their suppliers would notify them of a breach that could put their business at risk. As the global attack surface continues to expand, it's more important than ever to tighten and mature Third- Party Risk Management (TPRM) programs, also referred to as Vendor Risk Management. Staying ahead of weaponized vulnerabilities and threat actors targeting your vendors' assets decreases the chances of a cyber disruption to your organization.

KEY TAKEAWAYS

1. Learn how to mature your third-party risk management program by incorporating threat intelligence to uncover true risk and threats across your vendor ecosystem.

2. Understand the difference between cybersecurity ratings, which identifies potential risk, and threat intelligence, which surfaces active threats that put your vendor and your business at harm, and how the two complement each other.

3. Evaluate how a large enterprise customer uses SecurityScorecard's Attack Surface Intelligence to proactively pinpoint risks, alert the vendor and provide the incident response team with context and actionable next steps.

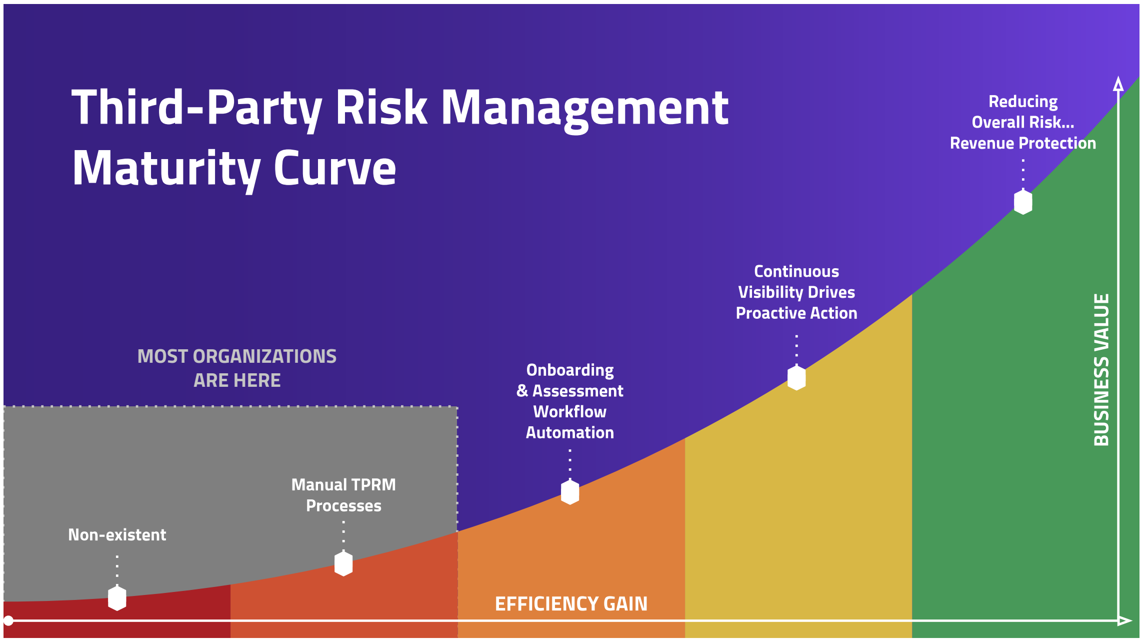
What is Third-Party Risk Management?

In addition to the evolving nature of cyber threats, technology stacks are expanding and the use of third-party vendors is growing at a high rate, introducing more risk into the environment. It is crucial for cybersecurity teams to know the level of risk to the organization from each of these business relationships.

Third-Party Risk Management (TPRM) is the process of monitoring yourthird-, fourth-, and even fifth-party relationships to ensure that they do not create unfavorable business outcomes, disrupt day-to-day operations, or expose your organization to a security risk. This is typically done through a third-party Risk Management program, including processes, procedures, and technology to help organizations assess, monitor, and manage risk exposure that stems from these relationships. Should there be a third-party risk event, TPRM programs also include comprehensive plans for risk mitigation to reduce the impact of legal liabilities and reputational damage.

How Mature is Your Organization's Third-Party Risk Management Program?

No organization's TPRM program is the same; however, most are at a level where they are moderately managing vendor risk. Let's take a look at the different levels of the TPRM maturity curve below and steps you can take to uplevel your program to mitigate third-party risk.



Third-Party Risk Management Maturity Curve

Determine Your Third-Party Risk Management Program's Maturity

QUIZ
Part 1

01

Does your organization have fully built-out and updated TPRM policies and procedures?

YES or NO

02

Does your TPRM program have a dedicated person to manage vendors?

YES or NO

03

Are vendor questionnaires sent out and tracked through a platform, not spreadsheets?

YES or NO

If you answered yes to a majority of the questions, skip to the next quiz. If you answered no to a majority of the questions, read below to understand the next steps to mature your program.

Next Steps:
Based on your answers, your organization's maturity level is in the early stages with mostly **manual processes**. Recommended next steps are:

- Identify business goals and objectives of managing third-party vendors to create a more formal TPRM program.
- Develop or reevaluate policies and procedures based on **best practices.**
- Choose a process or **platform** for sending and receiving responses to questionnaires.

Understand how and what to report to business leaders to show value and maintain the forward the momentum of the TPRM program.

QUIZ
Part 2

01

Does your organization tier your vendors by criticality to the business?

YES or NO

02

Does your organization continuously monitor vendor risk through a **cybersecurity ratings** solution that takes an outside-in view of multiple security controls?

YES or NO

03

Are vendor questionnaires tailored based on the cyber risk rating or recent security events that impact your third-party vendor?

YES or NO

04

Are you able to clearly articulate vendor risk to the board on a consistent basis?

YES or NO

05

Are cyber risk ratings used to make business decisions in regard to mergers and acquisitions, procurement, and contractual language in contracts?

YES or NO

If you answered yes to a majority of the questions, skip to the next quiz. If you answered no to a majority of the questions, read below to understand the next steps to mature your program.

Next Steps:
Based on your answers, your organization's maturity level is moving in the right direction with the development of **onboarding and assessment workflow automation.** Recommended next steps are:

- Begin to develop and tier vendors based on impact to your business
- Work with your cybersecurity ratings provider to **operationalize the platform with your business goals**
- Automate tedious vendor risk management duties to reduce the amount of time spent evaluating vendors and completing assessments
- Socialize your TPRM program with your vendors and customers to lay the foundation of trust and due-diligence in working together

QUIZ
Part 3

01

Does your organization evaluate risk posed by your fourth- and fifth-party vendors?

YES or NO

02

Does your organization automatically report cyber risk findings through easy-to-understand visualizations of the data to help the board and business leaders see solid ROI and understand TPRM efforts?

YES or NO

03

Are you able to measure the financial impact of a potential attack through a third-party vendor?

YES or NO

If you answered yes to a majority of the questions skip to the next quiz. If you answered no to a majority of the questions, read below to understand the next steps to mature your program.

Next Steps:
Based on your answers, your organization's TPRM program is close to delivering **continuous visibility to drive proactive action.** Recommended next steps are:

- Continuously and easily provide key metrics to the board and key stakeholders
- Measure the financial **impact** of a potential attack on your vendors to help quantify cyber risk
- Automate the detection of **all vendors in your digital ecosystem** and create workflows to identify potential issues
- Further mature your TPRM risk program through **advisory services** that focus on elevating your TPRM program beyond assessment completion and evaluation

QUIZ
Part 4

01

Does your TPRM program have the capability to easily digest and know how to use threat intelligence to understand, identify, and alert vendors of their threats and vulnerabilities that put your organization at risk?

YES or NO

02

Does your organization have a process to validate the vendors' security posture with a deeper view into their attack surface?

YES or NO

03

Are you able to provide deep vendor intelligence insights to the incident response and vulnerability management teams to help them understand how to prioritize remediation?

YES or NO

04

Is your TPRM program advocated by the leadership team, building a risk-aware culture company-wide?

YES or NO

If you answered yes to a majority of the questions, congratulations! You are a leader among your TPRM peers. Check out how **SecurityScorecard's** expanded vendor intelligence helps find the unknown unknowns in your vendors' attack surface.

If you answered no to a majority of the questions, read below to understand the next steps to mature your program.

Next Steps:
Based on your answers, your organization's TPRM program is ready to build a deeper foundation to **reduce overall risk and protect revenue.** Recommended next steps are:

- Identify how to add threat intelligence insights to your TPRM workflow. SecurityScorecard's **Attack Surface Intelligence** solution allows program owners to discern who in their vendor portfolio has active threats.
- Develop and set up workflows for proactive vendor notification or provide incident response teams with contextual information to take action.
- Prove the ROI of incorporating threat intelligence into your TPRM program to business leaders through sharing trending data.

No matter where your organization is in the process of managing vendor risk, you can't let your guard down or you could be the next victim of a cyber attack. **Reach out to experts to help you today.**

GET STARTED

How Intelligence Builds a Stronger and Proactive Offense

A cyber attack through one of your third-party vendors could be prevented by using intelligence to track and alert you of your vendors' critical vulnerabilities and active threats that they may not be able to see themselves. Incorporating intelligence as part of your Third-Party Risk Management program helps you answer the following questions:

01

Have any of my third- or fourth-party vendors been part of a recent ransomware attack?

02

Which of my critical vendors in my portfolio have active threats and what is the severity of these threats to my business?

03

What vulnerabilities in my vendors' attack surface are at risk of being weaponized?

04

How do I provide deeper insights and context for my incident response team to investigate an at-risk vendor?

When threat intelligence is surfaced in an easily digestible fashion—for instance, when viewing your vendor portfolios—you catch your vendors' vulnerabilities in minutes and before they're exploited. Expanded vendor intelligence enables you to analyze your vendor-induced risk by exposing how your vendor's vulnerabilities in minutes and collaborate with them to remediate before these vulnerabilities are exploited.

Not only can you identify threats, but you can ingest the intelligence data that is arranged contextually to alert your vendor to take action with a clear path to remediate and reduce the risk to your expanding attack surface.

Understand and Identify Risks in Your Vendors' Attack Surface with SecurityScorecard's Intelligence

SecurityScorecard's Attack Surface Intelligence allows everyone to be a threat researcher with the most contextualized global threat intelligence for you to drive actionable decisions to defend against attacks. SecurityScorecard provides a fully comprehensive solution to managing vendor risk including its cybersecurity ratings, vendor questionnaire engine, workflow capabilities through integrations and APIs, and more. SecurityScorecard Ratings help organizations view attributed cyber risk, providing a look into a vendor's security posture to give businesses a way to measure the probability of risk. Threat intelligence provided through SecurityScorecard's Attack Surface Intelligence module offers a unique capability to display real threats that are active in a 360-degree view by vendor portfolio or magnified at the individual vendor level. Malicious threats shown in your vendors' environments mean that the door is open for your organization to experience an attack.

Let's take a look at how SecurityScorecard's **Attack Surface Intelligence** helps TPRM teams advance their program and show proven ROI of how they've saved the organization time and money, and stopped potential disruption early.

USE CASE

How Attack Surface Intelligence Helped Oceano Industries Proactively Assess Vendor Risk

While Attack Surface Intelligence fits a variety of organization profiles in terms of size, maturity, and TPRM methodology, we will share a real-life example of one of SecurityScorecard's customers. For privacy purposes, the name of the customer has been altered.

Oceano Industries is a large manufacturer. Their customer base includes cruise lines, shipping companies, and even the U.S. Government. With this variety of clientele they are heavily regulated and required to comply with multiple frameworks, such as CMMC, PCI, NIST, and others. Oceano is also affiliated with an industry-based, information sharing and analysis center (ISAC).

Given the complexity of their operations, Oceano has more than 800 vendors in their SecurityScorecard Portfolios. The sheer volume of third-party risk has driven

EXPANDED CAPABILITIES

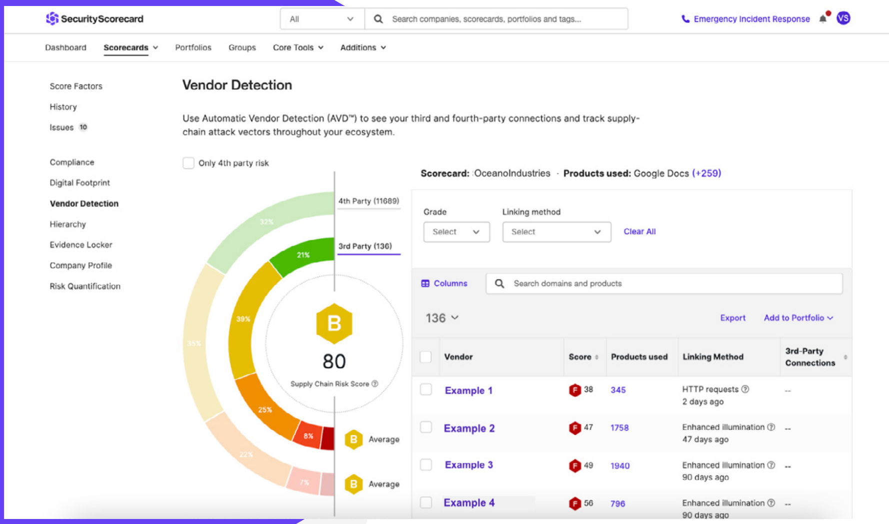
Oceano's parent TPRM team typically monitors vendors and vets potential vendors at an administrative level, focusing more on questionnaire assessments. Upon learning about significant security events, such as significant score drops or breaches, they engage their incident response team to contact affected vendors to investigate these events, provide remediation recommendations, set remediation expectations, and track progress. SecurityScorecard's Platform and Services suite supports this TPRM model in a number of ways

Oceano to invest in a mature TPRM program with a well-staffed team and even an incident management “sub-team”.

Prioritizing Threats with Existing Vendors

Oceano’s TPRM team is tasked with monitoring their 900-plus vendors and identifying risks on an ongoing basis.

At an administrative level, this means sending each vendor an annual, quarterly, or even monthly review-assessment, depending on the vendor’s criticality to Oceano’s operations and their level of system permissions or exposure to sensitive information. Sending questionnaires from SecurityScorecard, the TPRM team inquires about any changes affecting the vendor’s security posture, such as deployment of new cyber-defense products, renewed compliance with key frameworks, and breaches.



Vendor Detection

Use Automatic Vendor Detection (AVD™) to see your third and fourth-party connections and track supply-chain attack vectors throughout your ecosystem.

Scorecard: OceanoIndustries · **Products used:** Google Docs (+259)

Vendor	Score	Products used	Linking Method	3rd-Party Connections
Example 1	F 38	345	HTTP requests 2 days ago	--
Example 2	F 47	1758	Enhanced illumination 47 days ago	--
Example 3	F 49	1940	Enhanced illumination 90 days ago	--
Example 4	F 56	796	Enhanced illumination 90 days ago	--

At a tactical level, the TPRM team uses SecurityScorecard’s **Rule Builder** to generate automatic alerts on any significant changes to vendor Scorecards, such as significant score drops or breaches. This ensures that they never miss a change or potential critical vulnerability that could affect one of their vendors. Additionally, they use **Automatic Vendor Detection** to identify their vendors’ third- and fourth-party ecosystems for low scores, the products their vendors use, and other items of concern.

Zeroing in on Actionable Threats with Attack Surface Intelligence

This broader coverage keeps Oceano apprised of their vendors’ cyber-health on a continuing basis. With Attack Surface Intelligence, the TPRM team can quickly scan their portfolios for threats that demand immediate attention.

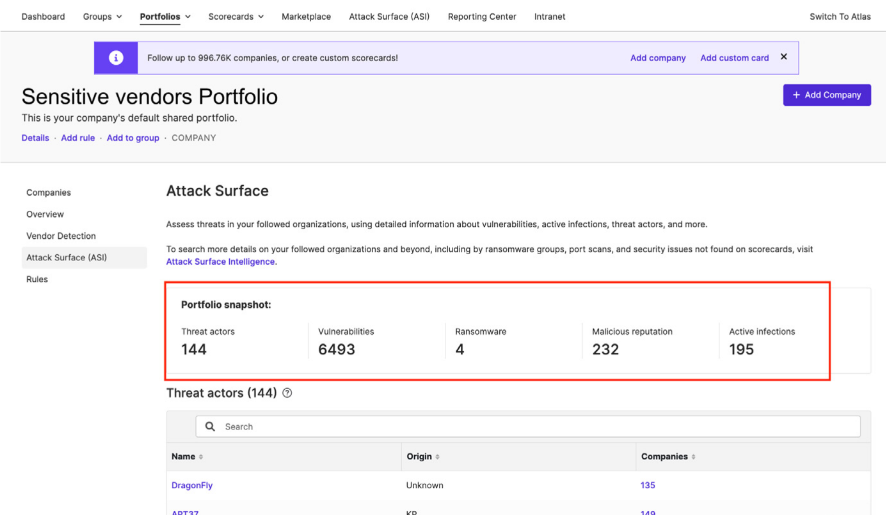
Clicking the Attack Surface Intelligence tab of any portfolio, the team immediately sees tallies of actionable threats, such as:

- Detected **ransomware events**

- **Threat actors** known to have weaponized vulnerabilities found on vendors' assets

- Vendor IPs with **malicious reputations**, which indicate that they may have been breached and controlled by threat actors to launch attacks on other internet targets

- Detected active **malware infections**



Follow up to 996.76K companies, or create custom scorecards!

Sensitive vendors Portfolio

This is your company's default shared portfolio.

Attack Surface

Assess threats in your followed organizations, using detailed information about vulnerabilities, active infections, threat actors, and more.

To search more details on your followed organizations and beyond, including by ransomware groups, port scans, and security issues not found on scorecards, visit Attack Surface Intelligence.

Portfolio snapshot:

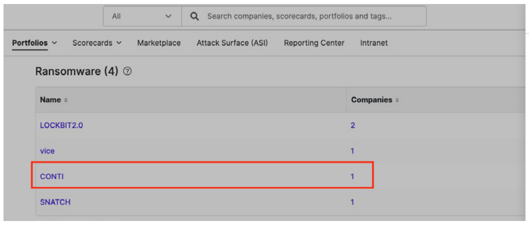
Threat actors	Vulnerabilities	Ransomware	Malicious reputation	Active infections
144	6493	4	232	195

Threat actors (144)

Name	Origin	Companies
DragonFly	Unknown	135
APT37	KP	149

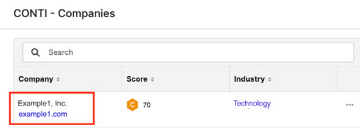
Scrolling down the Attack Surface Intelligence landing page, they can drill into these actionable threats to determine which vendors are implicated and gain more critical details and context to pass on to their incident response team.

Noting four ransomware events, they scroll to the *Ransomware* section of the page and see which of their vendors are affected.



Ransomware (4)

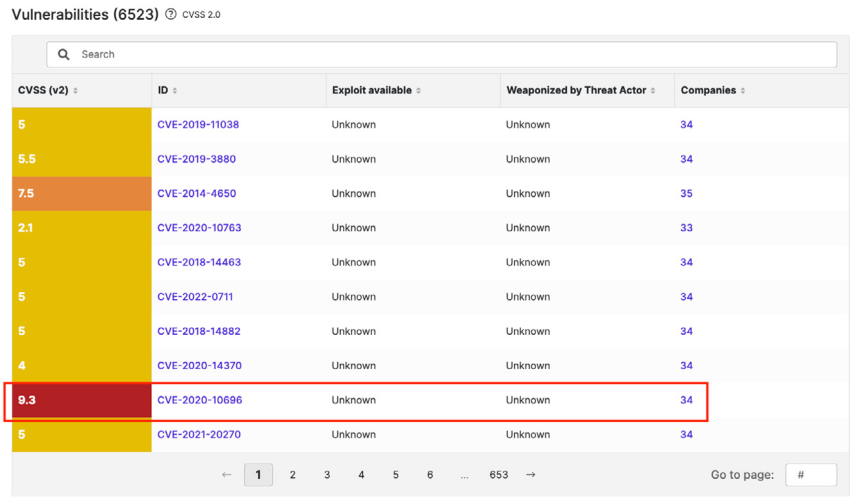
Name	Companies
LOCKBIT2.0	2
vice	1
CONTI	1
SNATCH	1



CONTI - Companies

Company	Score	Industry
Example1, Inc. example1.com	C 70	Technology

Sorting common vulnerabilities and exposures (CVEs) by severity, Oceano brings the highest-severity CVEs to the surface and clicks the number of companies affected by these vulnerabilities...



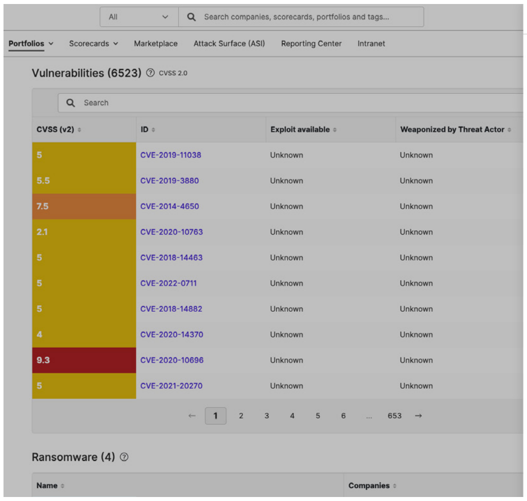
Vulnerabilities (6523) ⓘ CVSS 2.0

🔍 Search

CVSS (v2)	ID	Exploit available	Weaponized by Threat Actor	Companies
5	CVE-2019-11038	Unknown	Unknown	34
5.5	CVE-2019-3880	Unknown	Unknown	34
7.5	CVE-2014-4650	Unknown	Unknown	35
2.1	CVE-2020-10763	Unknown	Unknown	33
5	CVE-2018-14463	Unknown	Unknown	34
5	CVE-2022-0711	Unknown	Unknown	34
5	CVE-2018-14882	Unknown	Unknown	34
4	CVE-2020-14370	Unknown	Unknown	34
9.3	CVE-2020-10696	Unknown	Unknown	34
5	CVE-2021-20270	Unknown	Unknown	34

← 1 2 3 4 5 6 ... 653 → Go to page: #

...and then notes the lowest-scoring companies as requiring the most urgent attention.



Vulnerabilities (6523) ⓘ CVSS 2.0

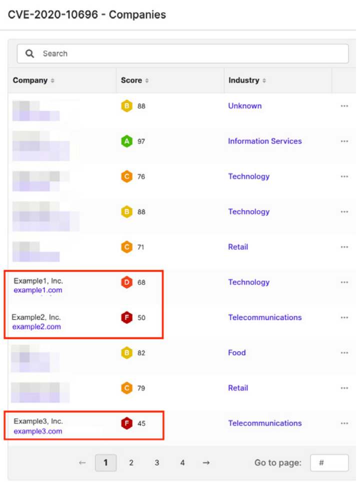
🔍 Search

CVSS (v2)	ID	Exploit available	Weaponized by Threat Actor
5	CVE-2019-11038	Unknown	Unknown
5.5	CVE-2019-3880	Unknown	Unknown
7.5	CVE-2014-4650	Unknown	Unknown
2.1	CVE-2020-10763	Unknown	Unknown
5	CVE-2018-14463	Unknown	Unknown
5	CVE-2022-0711	Unknown	Unknown
5	CVE-2018-14882	Unknown	Unknown
4	CVE-2020-14370	Unknown	Unknown
9.3	CVE-2020-10696	Unknown	Unknown
5	CVE-2021-20270	Unknown	Unknown

← 1 2 3 4 5 6 ... 653 →

Ransomware (4) ⓘ

Name	Companies



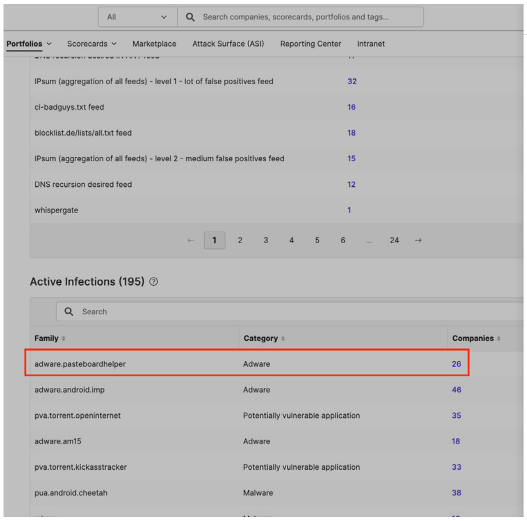
CVE-2020-10696 - Companies

🔍 Search

Company	Score	Industry	
[redacted]	B 88	Unknown	···
[redacted]	A 97	Information Services	···
[redacted]	C 76	Technology	···
[redacted]	B 88	Technology	···
[redacted]	C 71	Retail	···
Example1, Inc. example1.com	D 68	Technology	···
Example2, Inc. example2.com	F 50	Telecommunications	···
[redacted]	B 82	Food	···
[redacted]	C 79	Retail	···
Example3, Inc. example3.com	F 45	Telecommunications	···

← 1 2 3 4 → Go to page: #

Oceano's TPRM team does the same with active infections...



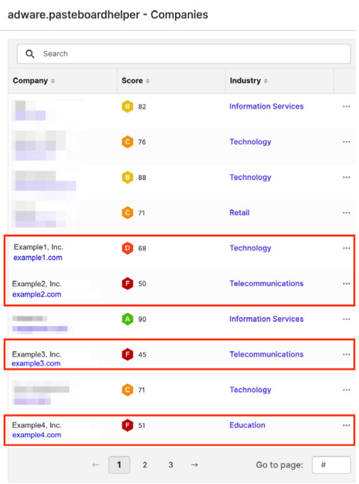
IPsum (aggregation of all feeds) - level 1 - lot of false positives feed	32
ci-badguys.txt feed	16
blocklist.de/lists/all.txt feed	18
IPsum (aggregation of all feeds) - level 2 - medium false positives feed	15
DNS recursion desired feed	12
whispergate	1

← 1 2 3 4 5 6 ... 24 →

Active Infections (195) ⓘ

🔍 Search

Family	Category	Companies
adware.pasteboardhelper	Adware	26
adware.android.imp	Adware	46
pva.torrent.openinternet	Potentially vulnerable application	35
adware.am15	Adware	18
pva.torrent.kickasstracker	Potentially vulnerable application	33
pua.android.cheetah	Malware	38



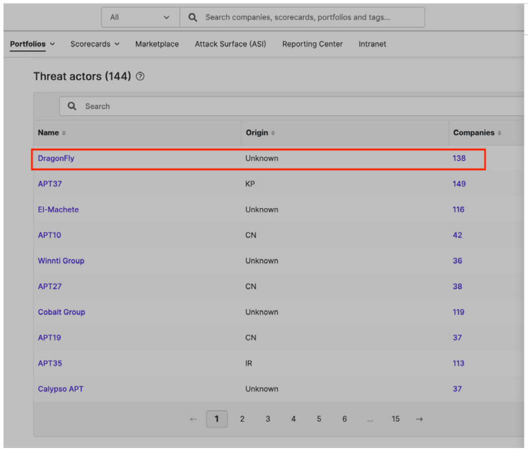
adware.pasteboardhelper - Companies

🔍 Search

Company	Score	Industry	
[redacted]	B 82	Information Services	···
[redacted]	C 76	Technology	···
[redacted]	B 88	Technology	···
[redacted]	C 71	Retail	···
Example1, Inc. example1.com	D 68	Technology	···
Example2, Inc. example2.com	F 50	Telecommunications	···
[redacted]	A 90	Information Services	···
Example3, Inc. example3.com	F 45	Telecommunications	···
[redacted]	C 71	Technology	···
Example4, Inc. example4.com	F 51	Education	···

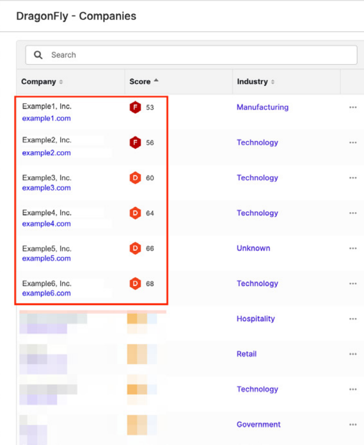
← 1 2 3 → Go to page: #

...threat actor connections,...



Threat actors (144)

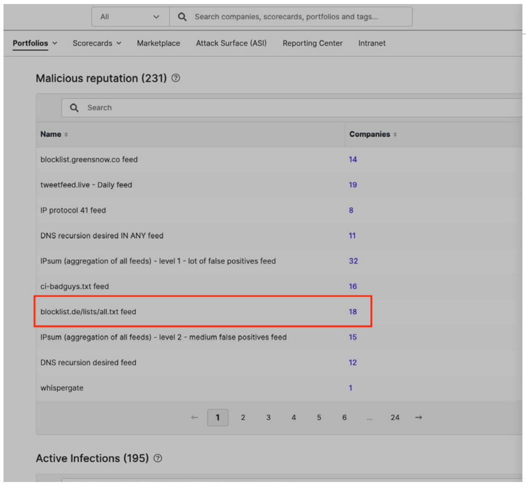
Name	Origin	Companies
DragonFly	Unknown	138
APT37	KP	149
El-Machete	Unknown	116
APT10	CN	42
Winnti Group	Unknown	36
APT27	CN	38
Cobalt Group	Unknown	119
APT19	CN	37
APT35	IR	113
Calypso APT	Unknown	37



DragonFly - Companies

Company	Score	Industry
Example1, Inc. example1.com	F 53	Manufacturing
Example2, Inc. example2.com	F 56	Technology
Example3, Inc. example3.com	D 60	Technology
Example4, Inc. example4.com	D 64	Technology
Example5, Inc. example5.com	D 66	Unknown
Example6, Inc. example6.com	D 68	Technology
[redacted]	[redacted]	Hospitality
[redacted]	[redacted]	Retail
[redacted]	[redacted]	Technology
[redacted]	[redacted]	Government

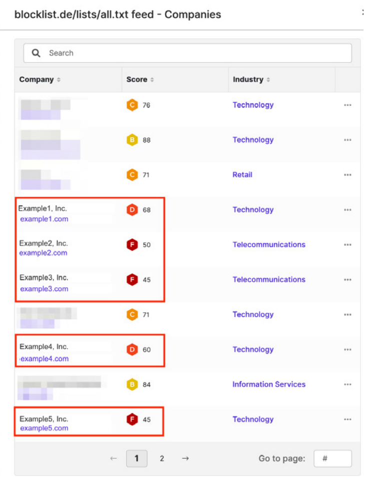
...and malicious reputation posts.



Malicious reputation (231)

Name	Companies
blocklist.greensnow.co feed	14
tweetfeed.live - Daily feed	19
IP protocol 41 feed	8
DNS recursion desired IN ANY feed	11
IPsum (aggregation of all feeds) - level 1 - lot of false positives feed	32
ci-badguys.txt feed	16
blocklist.de/lists/all.txt feed	18
IPsum (aggregation of all feeds) - level 2 - medium false positives feed	15
DNS recursion desired feed	12
whispergate	1

Active Infections (195)



blocklist.de/lists/all.txt feed - Companies

Company	Score	Industry
[redacted]	C 76	Technology
[redacted]	B 88	Technology
[redacted]	C 71	Retail
Example1, Inc. example1.com	D 68	Technology
Example2, Inc. example2.com	F 50	Telecommunications
Example3, Inc. example3.com	F 45	Telecommunications
[redacted]	C 71	Technology
Example4, Inc. example4.com	D 60	Technology
[redacted]	B 84	Information Services
Example5, Inc. example5.com	F 45	Technology

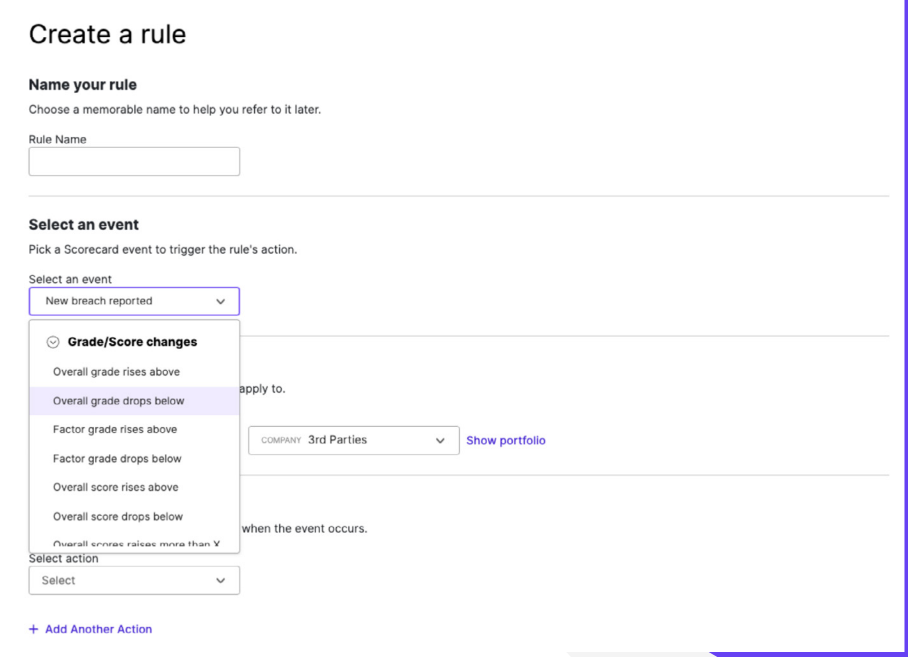
Create Automated Rules for Vendor Event Notifications

Using the rule builder, the TPRM team is able to automatically add or remove a vendor from a portfolio, create a report, send a vendor an alert, or send a questionnaire.

Rules are triggered by various changes in a vendor scorecard including:

- Change in score
- High severity issue
- CVE detected
- Breach detected

Producing a list of at-risk companies helps Oceano's incident response team engage the vendors without much effort on their part.



Create a rule

Name your rule

Choose a memorable name to help you refer to it later.

Rule Name

Select an event

Pick a Scorecard event to trigger the rule's action.

Select an event: New breach reported

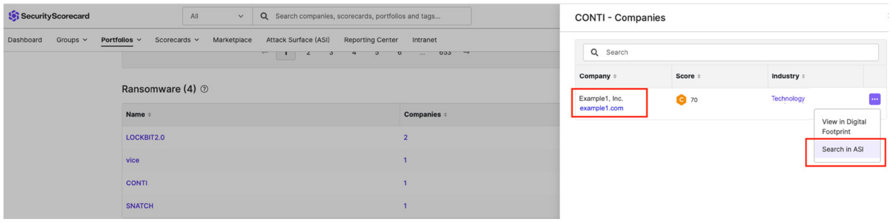
Supporting Vendor Outreach

Oceano's incident response team reviews the TPRM team's list and uses Attack Surface Intelligence throughout its outreach operations.

For each vendor, the incident response team queries Attack Surface Intelligence for key, threat-related details. Running a vendor query from the portfolio is as simple as selecting an Attack Surface Intelligence search link for a given vendor in any of the threat-related views where they appear:

- Threat actors
- Vulnerabilities
- Active infections
- Malicious reputation
- Ransomware (as in the following screenshot)

The queries bring up details about each IP address attributed to the vendor, such as all detected vulnerabilities and threat-related data points. The details also include geographic location and comprehensive data about processes running on open ports.



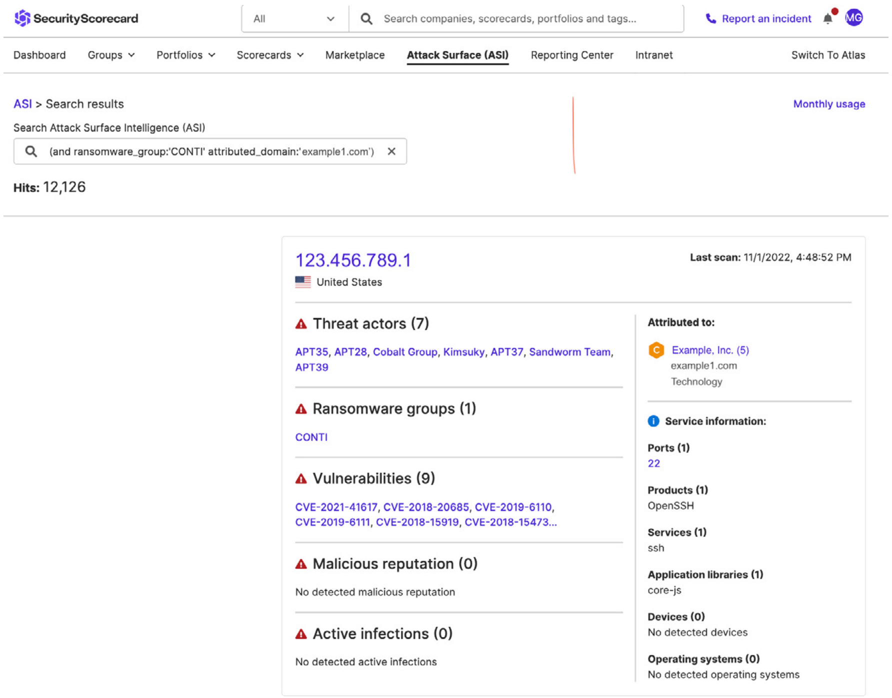
Ransomware (4)

Name	Companies
LOCKBIT2.0	2
vice	1
CONTI	1
SNATCH	1

CONTI - Companies

Company	Score	Industry
Example1, Inc. example1.com	C 70	Technology

Using this intelligence, Oceano's incident response team can put together a deeply contextual understanding of the risks these vendors carry.



ASI > Search results

Search Attack Surface Intelligence (ASI)

(and ransomware_group:'CONTI' attributed_domain:'example1.com')

Hits: 12,126

123.456.789.1

United States

Last scan: 11/1/2022, 4:48:52 PM

Threat actors (7)

APT35, APT28, Cobalt Group, Kimsuky, APT37, Sandworm Team, APT39

Ransomware groups (1)

CONTI

Vulnerabilities (9)

CVE-2021-41617, CVE-2018-20685, CVE-2019-6110, CVE-2019-6111, CVE-2018-15919, CVE-2018-15473...

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Attributed to:

C Example, Inc. (5)
example1.com
Technology

Service information:

Ports (1)
22

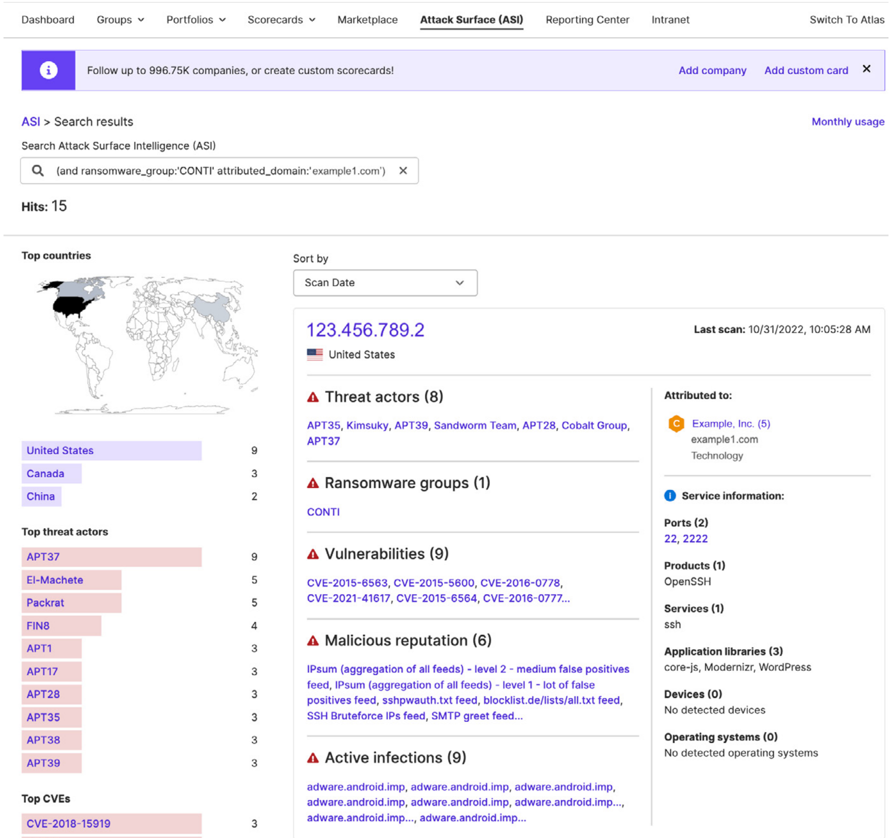
Products (1)
OpenSSH

Services (1)
ssh

Application libraries (1)
core-js

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems



Dashboard · Groups · Portfolios · Scorecards · Marketplace · **Attack Surface (ASI)** · Reporting Center · Intranet · Switch To Atlas

Follow up to 996.75K companies, or create custom scorecards! Add company · Add custom card ✕

ASI > Search results

Monthly usage

Search Attack Surface Intelligence (ASI)

(and ransomware_group:'CONTI' attributed_domain:'example1.com') ✕

Hits: 15

Top countries

Top countries	
United States	9
Canada	3
China	2

Top threat actors

Top threat actors	
APT37	9
El-Machete	5
Packrat	5
FIN8	4
APT1	3
APT17	3
APT28	3
APT35	3
APT38	3
APT39	3

Top CVEs

Top CVEs	
CVE-2018-15919	3

Sort by: Scan Date

123.456.789.2

United States

Last scan: 10/31/2022, 10:05:28 AM

Threat actors (8)

APT35, Kimsuky, APT39, Sandworm Team, APT28, Cobalt Group, APT37

Ransomware groups (1)

CONTI

Vulnerabilities (9)

CVE-2015-6563, CVE-2015-5600, CVE-2016-0778, CVE-2021-41617, CVE-2015-6564, CVE-2016-0777...

Malicious reputation (6)

IPsum (aggregation of all feeds) - level 2 - medium false positives feed, IPsum (aggregation of all feeds) - level 1 - lot of false positives feed, sshpwauth.txt feed, blocklist.de/lists/all.txt feed, SSH Bruteforce IPs feed, SMTP greet feed...

Active infections (9)

adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp..., adware.android.imp..., adware.android.imp...

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (2)
22, 2222

Products (1)
OpenSSH

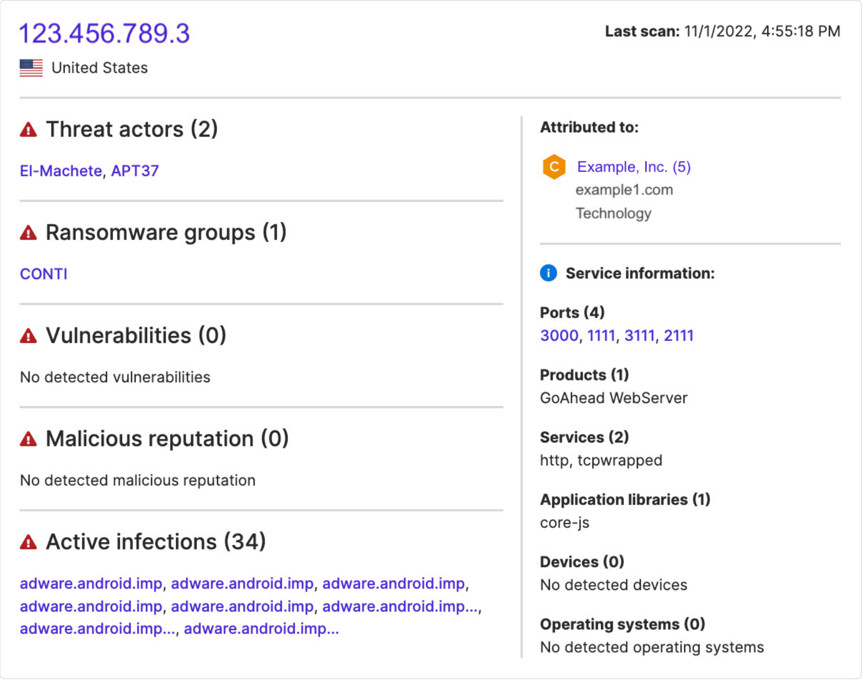
Services (1)
ssh

Application libraries (3)
core-js, Modernizr, WordPress

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

When they reach out to vendors about these issues, they use their Attack Surface Intelligence findings to answer any vendor disputes about the raised issues and to help the vendors in their own remediation efforts.



123.456.789.3

United States

Last scan: 11/1/2022, 4:55:18 PM

Threat actors (2)

El-Machete, APT37

Ransomware groups (1)

CONTI

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (34)

adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp, adware.android.imp..., adware.android.imp..., adware.android.imp...

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (4)
3000, 1111, 3111, 2111

Products (1)
GoAhead WebServer

Services (2)
http, tcpwrapped

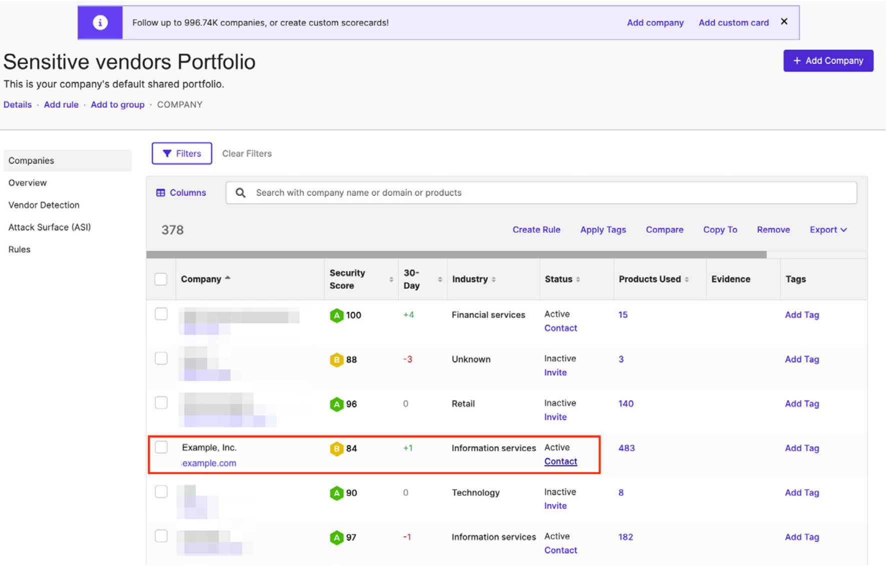
Application libraries (1)
core-js

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

Reaching Out to Vendors Right From the Ratings Platform

When they're ready to engage with vendors to address concerning issues, Oceano's team contacts them directly from the Portfolio...



Follow up to 996.74K companies, or create custom scorecards! Add company Add custom card ✕

Sensitive vendors Portfolio

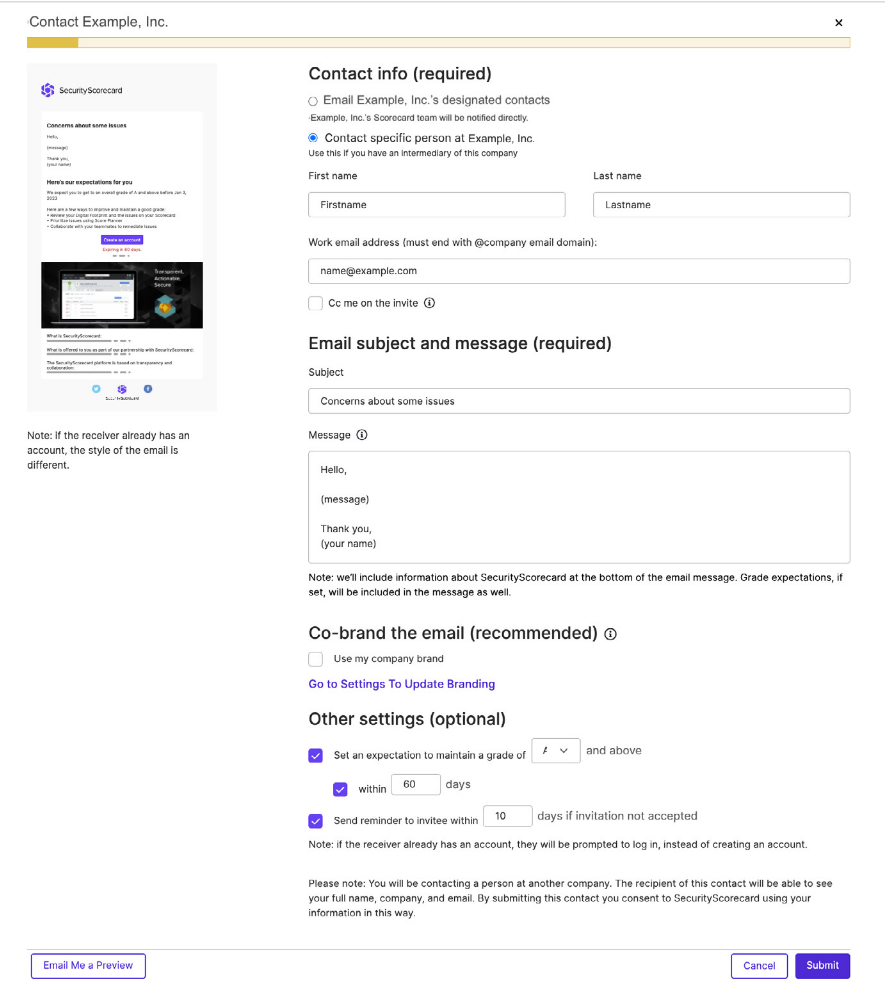
This is your company's default shared portfolio.

Details · Add rule · Add to group · COMPANY
Companies
Overview
Vendor Detection
Attack Surface (ASI)
Rules
Filters
Clear Filters
Columns
Search with company name or domain or products

378

□	Company	Security Score	30-Day	Industry	Status	Products Used	Evidence	Tags
□	[redacted]	A 100	+4	Financial services	Active Contact	15		Add Tag
□	[redacted]	B 88	-3	Unknown	Inactive Invite	3		Add Tag
□	[redacted]	A 96	0	Retail	Inactive Invite	140		Add Tag
□	Example, Inc. example.com	B 84	+1	Information services	Active Contact	483		Add Tag
□	[redacted]	A 90	0	Technology	Inactive Invite	8		Add Tag
□	[redacted]	A 97	-1	Information services	Active Contact	182		Add Tag

...and sends them a personalized message with the option to set expectations for score improvement within a certain timeframe.



Contact Example, Inc. ✕

Concerns about some issues

Hello,

(message)

Thank you,
(your name)

Here's our expectations for you

We expect you to get to an overall grade of A and above before Jan 3, 2023

Here are a few ways to improve and maintain a good grade:
- Review your Digital Footprint and the issues on your Scorecard
- Prioritize issues using Score Planner
- Collaborate with your teammates to remediate issues

Expiring in 60 days.

What is SecurityScorecard:

What is offered to you as part of our partnership with SecurityScorecard:

The SecurityScorecard platform is based on transparency and collaboration:

Note: if the receiver already has an account, the style of the email is different.

Contact info (required)

○ Email Example, Inc.'s designated contacts
Example, Inc.'s Scorecard team will be notified directly.

● Contact specific person at Example, Inc.
Use this if you have an intermediary of this company

First name	Last name
Firstname	Lastname

Work email address (must end with @company email domain): name@example.com

□ Cc me on the invite ⓘ

Email subject and message (required)

Subject: Concerns about some issues

Message ⓘ

Hello,

(message)

Thank you,
(your name)

Note: we'll include information about SecurityScorecard at the bottom of the email message. Grade expectations, if set, will be included in the message as well.

Co-brand the email (recommended) ⓘ

□ Use my company brand

Go to Settings To Update Branding

Other settings (optional)

☑ Set an expectation to maintain a grade of A and above

☑ within 60 days

☑ Send reminder to invitee within 10 days if invitation not accepted

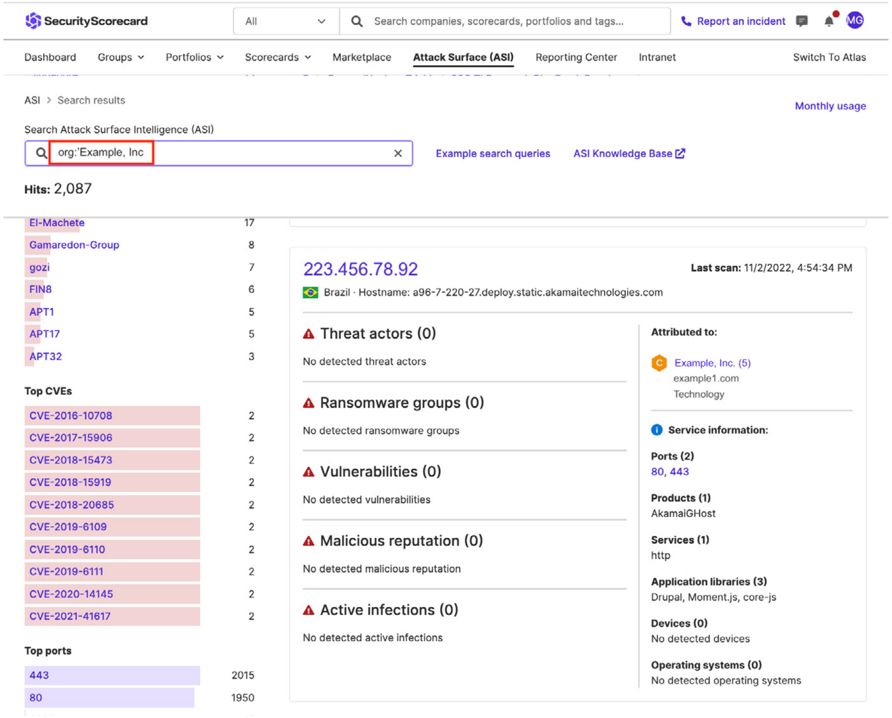
Note: if the receiver already has an account, they will be prompted to log in, instead of creating an account.

Please note: You will be contacting a person at another company. The recipient of this contact will be able to see your full name, company, and email. By submitting this contact you consent to SecurityScorecard using your information in this way.

Assessing Risk with Potential Vendors

By running queries through Attack Surface Intelligence, Oceano's TPRM team can vet potential vendors for risk at different levels of depth and breadth. Queries return detailed threat-relevant information about every internet-facing asset a vendor has deployed.

They can simply query on an organization's name to get a comprehensive view.



SecurityScorecard | All | Search companies, scorecards, portfolios and tags... | Report an incident

Dashboard | Groups | Portfolios | Scorecards | Marketplace | Attack Surface (ASI) | Reporting Center | Intranet | Switch To Atlas

ASI > Search results

Monthly usage

Search Attack Surface Intelligence (ASI)

org:'Example, Inc

Example search queries | ASI Knowledge Base

Hits: 2,087

El-Machete	17
Gamaredon-Group	8
gozi	7
FIN8	6
APT1	5
APT17	5
APT32	3

Top CVEs

CVE-2016-10708	2
CVE-2017-15906	2
CVE-2018-15473	2
CVE-2018-15919	2
CVE-2018-20685	2
CVE-2019-6109	2
CVE-2019-6110	2
CVE-2019-6111	2
CVE-2020-14145	2
CVE-2021-41617	2

Top ports

443	2015
80	1950

223.456.78.92

Last scan: 11/2/2022, 4:54:34 PM

Brazil · Hostname: a96-7-220-27.deploy.static.akamaitechnologies.com

Threat actors (0)

No detected threat actors

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (2)
80, 443

Products (1)
AkamaiGHost

Services (1)
http

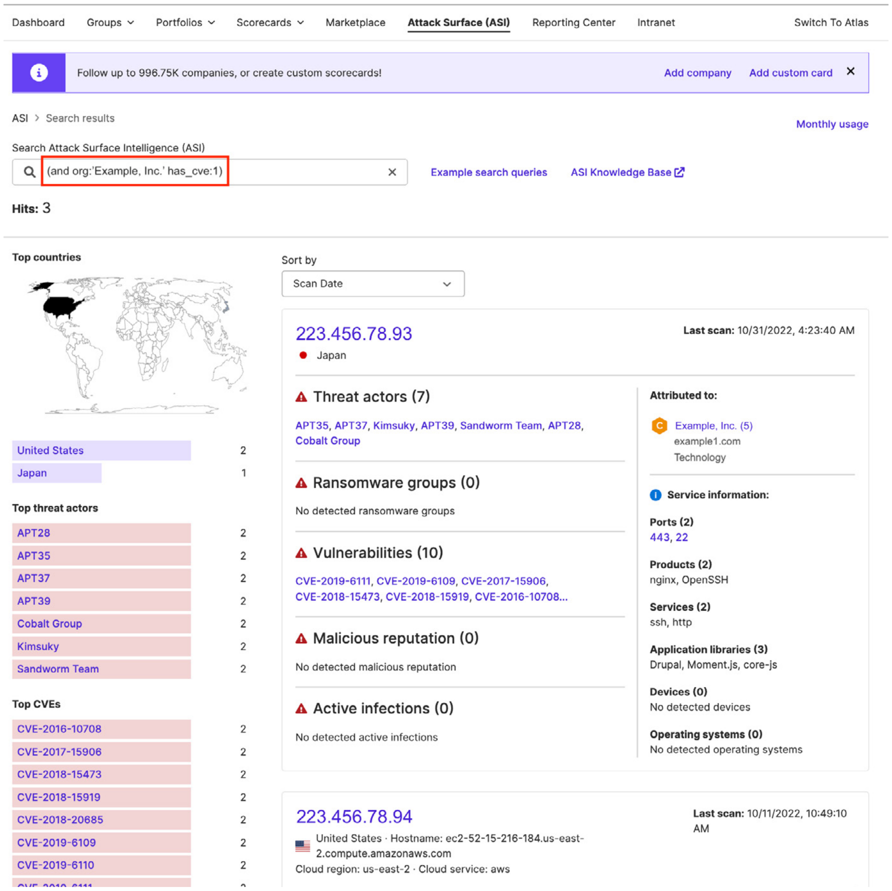
Application libraries (3)
Drupal, Moment.js, core-js

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

They can narrow the query to only IPs that have vulnerabilities...

...or ransomware events.



Dashboard | Groups | Portfolios | Scorecards | Marketplace | Attack Surface (ASI) | Reporting Center | Intranet | Switch To Atlas

Follow up to 996.75K companies, or create custom scorecards! | Add company | Add custom card

ASI > Search results

Monthly usage

Search Attack Surface Intelligence (ASI)

(and org:'Example, Inc.' has_cve:1)

Example search queries | ASI Knowledge Base

Hits: 3

Top countries

United States	2
Japan	1

Top threat actors

APT28	2
APT35	2
APT37	2
APT39	2
Cobalt Group	2
Kimsuky	2
Sandworm Team	2

Top CVEs

CVE-2016-10708	2
CVE-2017-15906	2
CVE-2018-15473	2
CVE-2018-15919	2
CVE-2018-20685	2
CVE-2019-6109	2
CVE-2019-6110	2

Sort by: Scan Date

223.456.78.93

Last scan: 10/31/2022, 4:23:40 AM

Japan

Threat actors (7)

APT35, APT37, Kimsuky, APT39, Sandworm Team, APT28, Cobalt Group

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (10)

CVE-2019-6111, CVE-2019-6109, CVE-2017-15906, CVE-2018-15473, CVE-2018-15919, CVE-2016-10708...

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (2)
443, 22

Products (2)
nginx, OpenSSH

Services (2)
ssh, http

Application libraries (3)
Drupal, Moment.js, core-js

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

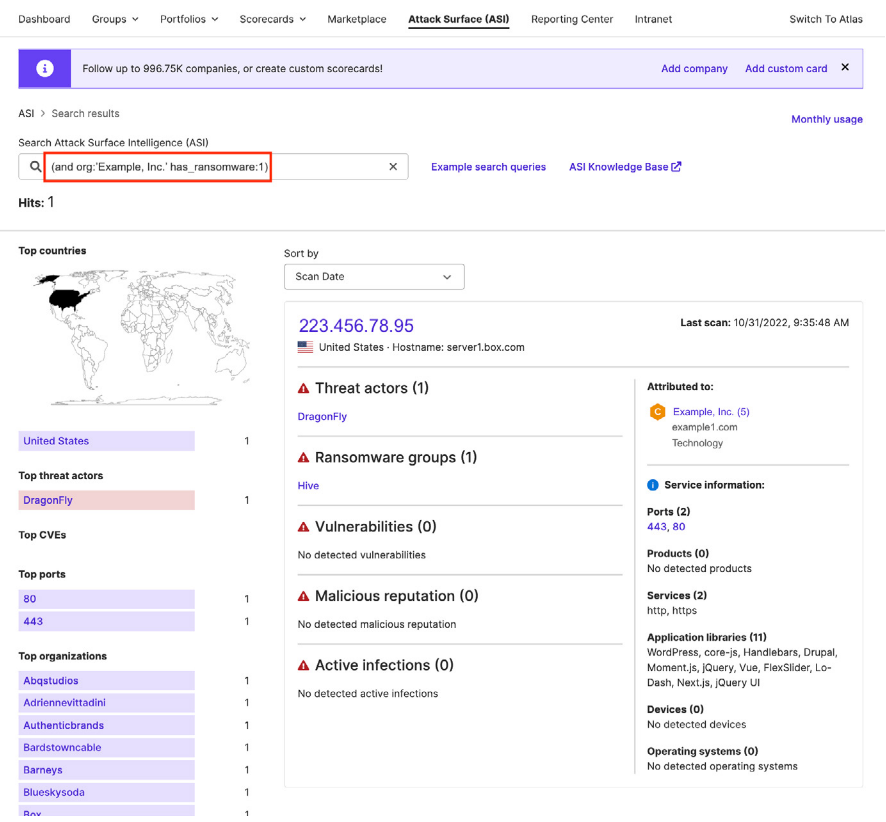
223.456.78.94

Last scan: 10/11/2022, 10:49:10 AM

United States · Hostname: ec2-52-15-216-184.us-east-2.compute.amazonaws.com
Cloud region: us-east-2 · Cloud service: aws

And they can combine data facets to refine results, for example, finding IPs with CVEs and threat actor connections.

This level of detail is especially relevant for prospective vendors who would have higher network permissions or access to sensitive data, such as a database host provider.



Follow up to 996.75K companies, or create custom scorecards!

ASI > Search results

Search Attack Surface Intelligence (ASI)

(and org:'Example, Inc.' has_ransomware:1)

Hits: 1

Top countries

United States	1

Top threat actors

DragonFly	1

Top CVEs

Top ports

80	1
443	1

Top organizations

Abqstudios	1
Adriennevittadini	1
Authenticbrands	1
Bardstowncable	1
Barneys	1
Blueskysoda	1
Box	1

Sort by

Scan Date

223.456.78.95

Last scan: 10/31/2022, 9:35:48 AM

United States · Hostname: server1.box.com

Threat actors (1)

DragonFly

Ransomware groups (1)

Hive

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (2)
443, 80

Products (0)
No detected products

Services (2)
http, https

Application libraries (11)
WordPress, core-js, Handlebars, Drupal, Moment.js, jQuery, Vue, FlexSlider, Lo-Dash, Next.js, jQuery UI

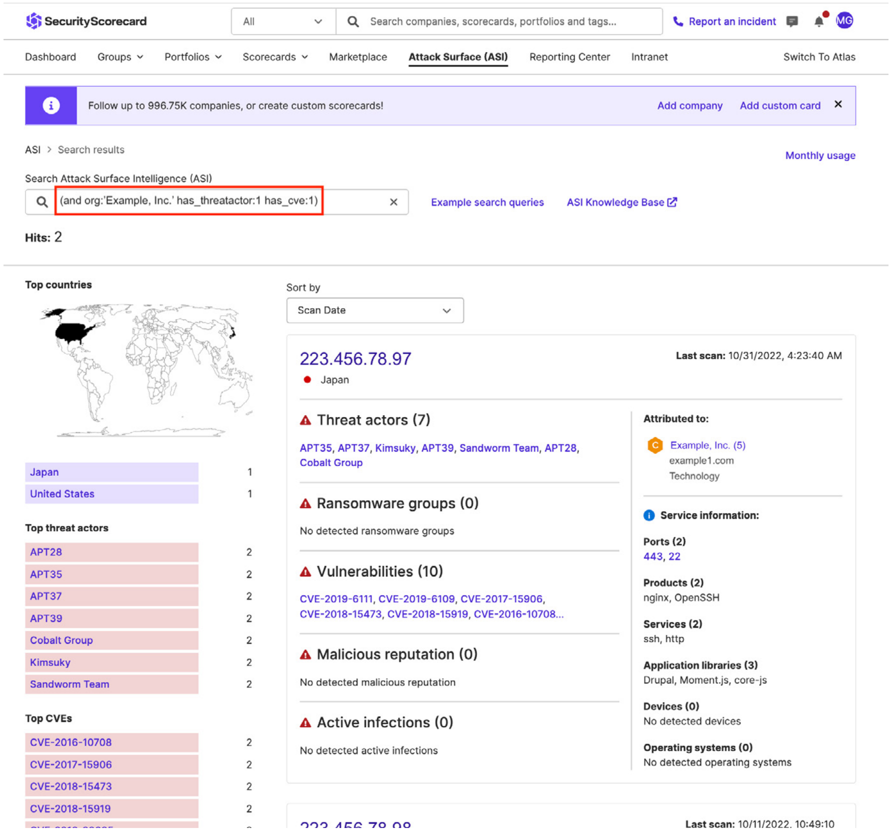
Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

Assessing Risk of Mergers and Acquisitions (M&A) Targets

Attack Surface Intelligence queries provide Oceano a discreet way to study prospects for mergers and acquisitions. Oceano can avoid adding these organizations to portfolios that might be visible across the organization, preventing unwanted attention early on in the M&A process.

Leverage Attack Surface Intelligence as part of your due diligence process for M&A and start collaborating internally on the level or risk to accept or address.



Follow up to 996.75K companies, or create custom scorecards!

ASI > Search results

Search Attack Surface Intelligence (ASI)

(and org:'Example, Inc.' has_threatactor:1 has_cve:1)

Hits: 2

Top countries

Japan	1
United States	1

Top threat actors

APT28	2
APT35	2
APT37	2
APT39	2
Cobalt Group	2
Kimsuky	2
Sandworm Team	2

Top CVEs

CVE-2016-10708	2
CVE-2017-15906	2
CVE-2018-15473	2
CVE-2018-15919	2

Sort by

Scan Date

223.456.78.97

Last scan: 10/31/2022, 4:23:40 AM

● Japan

Threat actors (7)

APT35, APT37, Kimsuky, APT39, Sandworm Team, APT28, Cobalt Group

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (10)

CVE-2019-6111, CVE-2019-6109, CVE-2017-15906, CVE-2018-15473, CVE-2018-15919, CVE-2016-10708...

Malicious reputation (0)

No detected malicious reputation

Active infections (0)

No detected active infections

Attributed to:

Example, Inc. (5)
example1.com
Technology

Service information:

Ports (2)
443, 22

Products (2)
nginx, OpenSSH

Services (2)
ssh, http

Application libraries (3)
Drupal, Moment.js, core-js

Devices (0)
No detected devices

Operating systems (0)
No detected operating systems

223.456.78.98

Last scan: 10/11/2022, 10:49:10

Conclusion

With threat intelligence incorporated into your TPRM program, finding the unknown unknowns in your vendor's attack surface is a whole lot easier. **Schedule a demo of Attack Surface Intelligence** or **reach out** to our Cyber Risk Intelligence team to learn how our threat hunting experts can support your efforts and help you gain cyber clarity on your vendors' attack surface.

How SecurityScorecard Can Help You Find and Resolve Security Risks

DRIVE CONFIDENT DECISION MAKING

SecurityScorecard is proud to support over 50,000 organizations with a platform to integrate, leverage, and present security data for security teams, non-technical audiences, and the board to understand and act upon. SecurityScorecard's platform expands its offerings beyond traditional security ratings capabilities so that organizations can gain needed insights to help mitigate these new risks.

SecurityScorecard Products

Security Ratings

Consistent and data-driven cybersecurity scores enable our customers to understand the vulnerabilities in their own environment as well as their third and fourth parties. A standard A-F grading scale streamlines cyber risk communication and empowers risk mitigation across the entire vendor ecosystem.

Cyber Risk Quantification

Put cyber risk into monetary values so that all investments are justifiable and aligned with broader business goals.

Security Data

Power your existing business workflows with the industry's most trusted security data about your organization and business ecosystem.

Attack Surface Intelligence

Most threat hunters find it challenging to stay up to date on current threats as threat adversaries become more sophisticated and the global attack surface continuously evolves. Attack Surface Intelligencel aids threat hunters in collecting thorough and essential data on the global attack surface for faster, more effective risk mitigation and threat prioritization.

Reporting Center

Contextualize and communicate cyber risk into business problems with a flexible reporting dashboard that tailors to your business needs.

Automatic Vendor Detection

Security and third-party risk management teams are struggling to keep up with the growing ecosystems of third- and fourth-party vendors supporting their business. Automatic Vendor Detection instantly gives you a view of your entire business ecosystem, enabling you to visualize and take active steps to mitigate risk.

Marketplace

Security, IT, and VRM teams deploy an average of 47 different cybersecurity technologies and solutions, and many don't integrate with each other. The SecurityScorecard Marketplace helps you maximize and integrate investments in your security stack with out-of-the-box integrations with leading technology organizations, and the ability to build your own custom solutions with our Rule Builder and SecurityScorecard's APIs.

Integrate SecurityScorecard data into your tech stack to drive integrated workflows, mitigate risk faster, and augment security data through our ecosystem of 90+ integrations, apps, and digital risk intelligence data.

Assessments

Save time and gain a 360-degree view of your vendors with the only customizable questionnaire to automatically validate responses against

Evidence Locker

Vendor Risk Managers spend countless hours, even days, chasing down answers and validating questionnaires. With SecurityScorecard, organizations can openly exchange security artifacts to simplify the vendor risk assessment process. Save time by managing compliance artifacts, track artifact history, and monitor the compliance initiatives in a single view.

SecurityScorecard Academy

Uplevel internal stakeholders with certifications and knowledge to augment your security program, with courses ranging from cyber insurance, board reporting, third-party risk management, and more. We give your team the products to fill knowledge gaps and gain the skills they need to take control of your organization's cybersecurity.

Cyber Resilience Services

Proactive Security

Defend your organization with a range of services that battle test your security controls to eliminate risk, including penetration testing, red team exercises, and tabletop exercises.

Digital Forensics and Incident Response

Respond confidently and mitigate business interruptions from a cyber attack by partnering with industry-leading experts in digital forensics and incident response services–24x7.

Third-Party Risk Program Development

Transform your Third Party Risk program to improve efficiencies, bolster security posture, and ultimately reduce vendor risk.

Cyber Risk Intelligence

Get customized deep threat intelligence about emerging threats that are attacking or targeting your organization, third-party vendors, and executives from SecurityScorecard's threat intelligence team. We partner with security teams to identify the cyber threats that require immediate attention by sorting through the volumes of information and identifying where and how to prioritize security resources.

LEARN MORE

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings 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 50,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating.

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

SecurityScorecard.com
info@securityscorecard.com

Tower 49
12 E 49th St
New York, NY 10017

United States: (800) 682-1701
International: +1(646) 809-2166

SecurityScorecard