



# Cybersecurity Monitoring: A Best Practice - SecurityScorecard

October 12, 2022

Devin Lynch, Senior Policy & Government Affairs Director  
Dr. Robert Ames, Staff Threat Researcher

# Agenda

**Trends in Ransomware for State and Local Governments**

**New Ransomware Findings Enabled by SSC Tools**

**Ransomware Findings and Cyber Risk Intelligence-as-a-Service**

**NACo-SecurityScorecard Partnership**

# **Threat Intelligence Focus: Ransomware Threats to Counties**

# Trends in Ransomware for SLTT Governments

- Despite speculation that business email compromise (BEC) will supplant ransomware as the major cyber threat to state and local governments, ransomware has tremendous disruptive potential.
- The by-now familiar initial access vectors (phishing, RDP compromise and reuse of breached credentials) remain threats.
- Third-party breaches resulting from ransomware also affect local institutions.
  - The attacks against Illuminate Education and Battelle for Kids both exposed local school districts' data.
- Our platform enables cybersecurity monitoring that can help mitigate these risks for both themselves and their vendors.
  - We detect and report exposed RDP ports, email security misconfigurations that can enable phishing, and breached credentials.
- Our tools have also enabled researchers to develop new hypotheses regarding ransomware TTPs in the course of recent investigations.

# Threat Analysis

## New Ransomware Findings Enabled by SecurityScorecard Tools

- SecurityScorecard researchers have identified what may be novel methods by which ransomware groups have accessed victim systems by using our different tools and datasets in concert with one another.
  - When investigating a summer attack against a school district by the Vice Society ransomware group, we:
    - First, identified the district's most at-risk IP addresses consulting the district's **digital footprint** and **network security** findings in our **ratings platform**;
    - Then leveraged our **exclusive access to network flow (netflow)** data to collect a sample of traffic to those high-risk IPs from the months leading up to the attack;
    - Finally, used our **Attack Surface Intelligence (ASI)** tool to analyze that traffic.
      - ASI identified additional exposed ports at the school district IPs that our platform does not normally report
      - ASI's **malicious reputation data** linked many of the IP addresses communicating with the school district to attacks specifically targeting the exposed ports ASI identified.
  - Public reporting has not previously linked this particular tactic to Vice Society, but in investigations into more recent attacks, including another claimed by Vice Society, we have seen a similar pattern of traffic to exposed ports of victim IP addresses.
  - ASI may therefore have aided in the identification of a new Vice Society TTP.

# Threat Analysis

## New Ransomware Findings Enabled by SecurityScorecard Tools

- SecurityScorecard's netflow tool detected considerable traffic that may indicate that a series of possible SSH brute force attacks against the school district took place in June and July.
- 3,571 of 8,281 flows used port 22 (the usual port for SSH traffic).
  - We normally see a much higher proportion of traffic using ports 443 and 80 in our netflow data.
- The dates with the five heaviest concentrations of traffic using port 22 were June 5, June 7, June 19, June 10, and July 1.
- ASI indicated that port 22 was open and running vulnerable SSH software at the school district IP addresses that experienced this traffic.

# Threat Analysis

## New Ransomware Findings Enabled by ASI

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, threat data.

72.52.219.150

22 ssh

Aug 01 2022 - ssh OpenSSH 5.3

SCAN:

banner  
SSH-2.0-OpenSSH\_5.3

ssh2-enum-algs

key\_algor(these): (4)  
diffie-hellman-group-exchange-sha256  
diffie-hellman-group-exchange-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group1-sha1  
server\_host\_key\_algor(these): (2)  
ssh-rsa  
ssh-dss

encryption\_algor(these): (13)  
aes128-ctr  
aes192-ctr  
aes256-ctr  
arcfour128  
arcfour256  
rc4-128  
rc4-256

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, threat data.

20719119742

NO THREAT ACTOR CONNECTIONS DETECTED 0 results

Unrecognized campaigns 2 results

CVSS	CVE ID	Campaign techniques
5	CVE-2018-15473	Metasploit exploits with CVE assigned feed
4.3	CVE-2016-6210	Metasploit exploits with CVE assigned feed

NO MALICIOUS REPUTATION 0 results

NO ACTIVE INFECTIONS 0 results

Open Ports 2 results

22 ssh

Jul 26 2022 - ssh Unknown ssh

161 snmp

Aug 02 2022 - snmp Unknown snmp

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, threat data.

20719119741

Unrecognized campaigns 2 results

CVSS	CVE ID	Campaign techniques
5	CVE-2018-15473	Metasploit exploits with CVE assigned feed
4.3	CVE-2016-6210	Metasploit exploits with CVE assigned feed

NO MALICIOUS REPUTATION 0 results

NO ACTIVE INFECTIONS 0 results

Open Ports 3 results

22 ssh

Jul 25 2022 - ssh Unknown ssh

161 snmp

Jul 31 2022 - snmp Unknown snmp

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, threat data.

20719119742

NO THREAT ACTOR CONNECTIONS DETECTED 0 results

Unrecognized campaigns 2 results

CVSS	CVE ID	Campaign techniques
5	CVE-2018-15473	Metasploit exploits with CVE assigned feed
4.3	CVE-2016-6210	Metasploit exploits with CVE assigned feed

NO MALICIOUS REPUTATION 0 results

NO ACTIVE INFECTIONS 0 results

Open Ports 3 results

22 ssh

Jul 24 2022 - ssh Unknown ssh

161 snmp

Jul 24 2022 - snmp Unknown snmp

# Threat Analysis

## New Ransomware Findings Enabled by SecurityScorecard Tools

- Both other vendors and ASI linked most IP addresses involved in the traffic over port 22 to SSH brute force attacks.
- The timing of these possible attacks in June and July may suggest that Vice Society attempted brute force attacks on the school district's SSH services at an earlier stage in its operations, prior to encrypting the district's systems in early August.
- Researchers have not previously linked Vice Society to SSH brute force attempts; this traffic may therefore represent a novel dimension of Vice Society's activity.

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, the

159.65.240.232

Malicious Reputation 9 results

Date	Description
May 31 2022	IPsum (aggregation of all feeds) - level 1 - lot of false positives feed
May 31 2022	IPsum (aggregation of all feeds) - level 4 - very low false positives feed
May 31 2022	SSH Bruteforce IPs feed
May 31 2022	IPsum (aggregation of all feeds) - level 3 - low false positives feed
May 31 2022	sshpwauth.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 5 - ultra false positives feed
May 31 2022	blocklist.greensnow.co feed
May 31 2022	blocklist.de/lists/all.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 2 - medium false positives feed

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, the

198.211.113.126

Malicious Reputation 7 results

Date	Description
May 31 2022	IPsum (aggregation of all feeds) - level 1 - lot of false positives feed
May 31 2022	blocklist.de/lists/all.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 2 - medium false positives feed
May 31 2022	blocklist.greensnow.co feed
May 31 2022	IPsum (aggregation of all feeds) - level 3 - low false positives feed
May 31 2022	sshpwauth.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 4 - very low false positives feed

Attack Surface Intelligence  
Powered by SecurityScorecard

This experience will be sunset on August 18, 2022

Search domains, IPs, CIDR blocks, CVEs, or malware hashes to analyze current, global, the

164.90.194.36

Malicious Reputation 9 results

Date	Description
May 31 2022	IPsum (aggregation of all feeds) - level 2 - medium false positives feed
May 31 2022	sshpwauth.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 1 - lot of false positives feed
May 31 2022	blocklist.greensnow.co feed
May 31 2022	blocklist.de/lists/all.txt feed
May 31 2022	ci-badguys.txt feed
May 31 2022	IPsum (aggregation of all feeds) - level 4 - very low false positives feed
May 31 2022	SSH Bruteforce IPs feed
May 31 2022	IPsum (aggregation of all feeds) - level 3 - low false positives feed

# Case Study - County Ransomware Findings

- A recent investigation into **a ransomware attack against a county government** revealed overlaps in TTPs with other recent attacks
  - In these recent investigations used ASI and netflow data to find evidence resembling that observed in the previous school district ransomware case, in which threat actors may have targeted exposed SSH services.
  - Netflow data indicated suspicious traffic to and from four particular county IP addresses, which, among other things, received notable amounts of traffic to port 22 prior to that attack..
  - ASI revealed these IP addresses to have port 22 open and running vulnerable SSH software.

[IP address] Last scan: 8/25/2022, 10:04:58 AM

United States Hostname: smtp. ....gov

---

**▲ Threat actors (7)**  
APT37, APT39, Sandworm Team, APT28, APT35, Kimsuky, Cobalt Group

---

**▲ Ransomware groups (0)**  
No detected ransomware groups

---

**▲ Vulnerabilities (10)**  
CVE-2017-15906, CVE-2019-6109, CVE-2018-20685, CVE-2019-6111, CVE-2021-41617, CVE-2018-15919...

---

**Attributed to:**  
C S. ....gov  
Legal

---

**Service information:**  
**Ports (3)**  
22, 443, 161

---

**Products (3)**  
Unknown https, OpenSSH, Unknown snmp

[IP address] Last scan: 8/27/2022, 4:46:56 AM

United States

---

**▲ Threat actors (7)**  
Kimsuky, APT35, APT37, APT39, Cobalt Group, APT28, Sandworm Team

---

**▲ Ransomware groups (0)**  
No detected ransomware groups

---

**▲ Vulnerabilities (10)**  
CVE-2016-10708, CVE-2018-15919, CVE-2017-15906, CVE-2019-6111, CVE-2018-15473, CVE-2019-6110...

---

**Attributed to:**  
C S. ....gov  
Legal

---

**Service information:**  
**Ports (3)**  
443, 22, 161

---

**Products (3)**  
Unknown snmp, OpenSSH, Unknown https

# Case Study - County Ransomware Findings

- ASI's malicious reputation data links many of the IP addresses communicating with the vulnerable county government assets to malicious activity, including attacks against SSH services.

<p><b>165.22.45.117</b> United States</p> <p><b>▲ Threat actors (14)</b> Gamaredon Group, The Shadow Brokers, APT35, APT39, APT28, Lazarus Group, IronHusky, TA505, Cobalt Group, Kimsuky, Sandworm Team, Equation Group, APT37, UNC2452</p> <p><b>▲ Ransomware groups (0)</b> No detected ransomware groups</p> <p><b>▲ Vulnerabilities (48)</b> CVE-2018-1301, CVE-2018-1312, CVE-2017-7679, CVE-2020-1927, CVE-2018-1302, CVE-2018-1333...</p> <p><b>▲ Malicious reputation (3)</b> IPsum (aggregation of all feeds) - level 1 - lot of false positives feed, blocklist.de/lists/all.txt feed, sshpwaath.txt feed</p>	<p><b>178.62.223.53</b> Netherlands</p> <p><b>▲ Threat actors (14)</b> APT35, APT39, Sandworm Team, Cobalt Group, APT28, APT37, Gamaredon Group, TA505, Equation Group, The Shadow Brokers, Kimsuky, IronHusky, UNC2452, Lazarus Group</p> <p><b>▲ Ransomware groups (0)</b> No detected ransomware groups</p> <p><b>▲ Vulnerabilities (53)</b> CVE-2019-10092, CVE-2018-1302, CVE-2019-17567, CVE-2019-0196, CVE-2018-17199, CVE-2022-26377...</p> <p><b>▲ Malicious reputation (7)</b> sshpwaath.txt feed, SSH Bruteforce IPs feed, blocklist.de/lists/all.txt feed, CyberCure - IP Feed feed, blocklist.greensnow.co feed, IPsum (aggregation of all feeds) - level 2 - medium false</p>	<p><b>161.35.154.124</b> Netherlands</p> <p><b>▲ Threat actors (0)</b> No detected threat actors</p> <p><b>▲ Ransomware groups (0)</b> No detected ransomware groups</p> <p><b>▲ Vulnerabilities (7)</b> CVE-2021-41617, CVE-2021-36368, CVE-2020-12062, CVE-2016-20012, CVE-2020-14145, CVE-2021-28041...</p> <p><b>▲ Malicious reputation (8)</b> sshpwaath.txt feed, IPsum (aggregation of all feeds) - level 1 - lot of false positives feed, blockrules of rules.emergingthreats.net feed, CyberCure - IP Feed feed, IPsum (aggregation of all feeds) - level 4 - very low false positives feed, blocklist.de/lists/all.txt</p>	<p><b>64.225.31.219</b> United States - Hostname: enel-digital.cl</p> <p><b>▲ Threat actors (8)</b> Equation Group, UNC2452, Lazarus Group, TA505, IronHusky, APT28, The Shadow Brokers, Gamaredon Group</p> <p><b>▲ Ransomware groups (0)</b> No detected ransomware groups</p> <p><b>▲ Vulnerabilities (7)</b> CVE-2016-20012, CVE-2020-12062, CVE-2021-28041, CVE-2020-14145, CVE-2021-41617, CVE-2021-36368...</p> <p><b>▲ Malicious reputation (7)</b> sshpwaath.txt feed, blocklist.greensnow.co feed, IPsum (aggregation of all feeds) - level 2 - medium false positives feed, blocklist.de/lists/all.txt feed, IPsum (aggregation of all feeds) - level 3 - low false positives feed, IPsum (aggregation of all feeds) -</p>
--	---	--	---

# Case Study - County Ransomware Findings

- Beyond internal tools, researchers consulted public resources to identify other data related to the attack.
- VirusTotal revealed files containing victim domains and linked to the Cryxos trojan.
  - Cryxos facilitates tech support scams, some involving the distribution of remote access software
    - Netflow data may reflect the distribution of such software.
  - This access could have led to subsequent compromises culminating in ransomware deployment.
    - We previously observed a collection of Cryxos-linked files containing another ransomware victim's domains; this may suggest that attackers employed similar TTPs in both incidents.

22 security vendors and no sandboxes flagged this file as malicious

70.93 KB Size 2022-05-14 13:16:54 UTC 4 months ago

Community Score: ?

DETECTION DETAILS COMMUNITY

Security Vendors' Analysis

Ad-Aware	JS:Trojan.Cryxos.6645	AhnLab-V3	Trojan.HTML.Chilvs.I1283
ALYac	JS:Trojan.Cryxos.6645	Avast	JS:Trojan.Cryxos.D19F5
Avast	Script.SMH-gen [Trj]	AVG	Script.SMH-gen [Trj]
Avira (no cloud)	HTML:Exploit.Gen2	BitDefender	JS:Trojan.Cryxos.6645
Cyren	Malicious (score: 99)	Cyren	JS:Agent.ADOEkorasto
Emisoft	JS:Trojan.Cryxos.6645 (B)	eScan	JS:Trojan.Cryxos.6645
ESET-NOD32	JS:Kryptik.BP1r	Fortinet	JS:Kryptik.BP1r
GData	JS:Trojan.Cryxos.6645	Ikarus	Trojan.JS.Crypt
MAX	Malware (ai Score=44)	NANO-AntiVirus	Trojan.Script.Agent.jortix
QuickHeal	JS:Trojan.Cryxos.43357	Rising	Trojan.KryptikUSH1.C7DF (CLASSIC)
Singler Engine Zero	Malware (Generic-Script.Save.msi1)	Trellix (FireEye)	JS:Trojan.Cryxos.6645

1 security vendor and no sandboxes flagged this file as malicious

35.09 KB Size 2022-07-11 13:42:12 UTC 2 months ago

Community Score: ?

DETECTION DETAILS COMMUNITY

Security Vendors' Analysis

MaxSecure	Trojan.VIR32.cryxos.5913	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Avast	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Blau Pro	Undetected	ClamAV	Undetected
Comodo	Undetected	Cyren	Undetected
Cyren	Undetected	DfWeb	Undetected
Emisoft	Undetected	eScan	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
Fortinet	Undetected	GData	Undetected



# **NACo - SecurityScorecard Partnership [and Pilot]**

# SecurityScorecard - NACo Pilot

## (March-May 2022)

In March, NACo and SecurityScorecard initiated a pilot program with 35 counties to evaluate the use-case and efficacy of SSC's security ratings platform for county governments.

Pilot Participants received:

- Specific training on the platform and use cases.
- 7 free slots for vendor risk management.
- Weekly Office Hours with SecurityScorecard to surface and answer questions and troubleshoot solutions.

Pilots also participated in a security survey



# SecurityScorecard - NACo Pilot

(March-May 2022)

## County Observations

Able to see what the world can publicly see (including hacking community  
Graphs and reports are easier for leadership to understand

Participants

- found the interface to be intuitive and easy to navigate

- found issues that their teams needed to address

- Uncovered linkages that affected the county score (i.e. fire, water, airport infrastructure) and able to correct

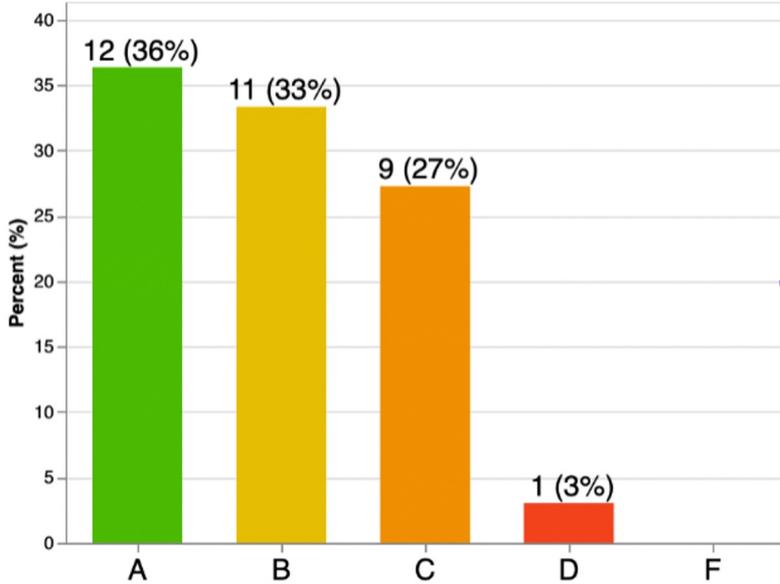
Uncovered some subdomain issues that needed cleared up (i.e. subdomain of a state domain)

The platform helped improve collaboration within the county

Participants appreciated seeing what the cyber insurers are seeing!

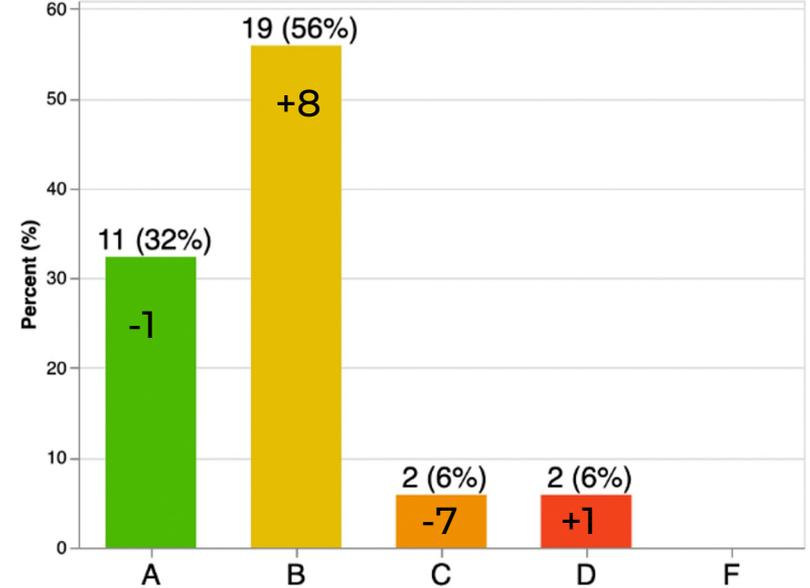
# Pilot Participants' Total Scores' Distribution

Total Scores' Distribution



March 27, 2022

Total Scores' Distribution



May 31, 2022

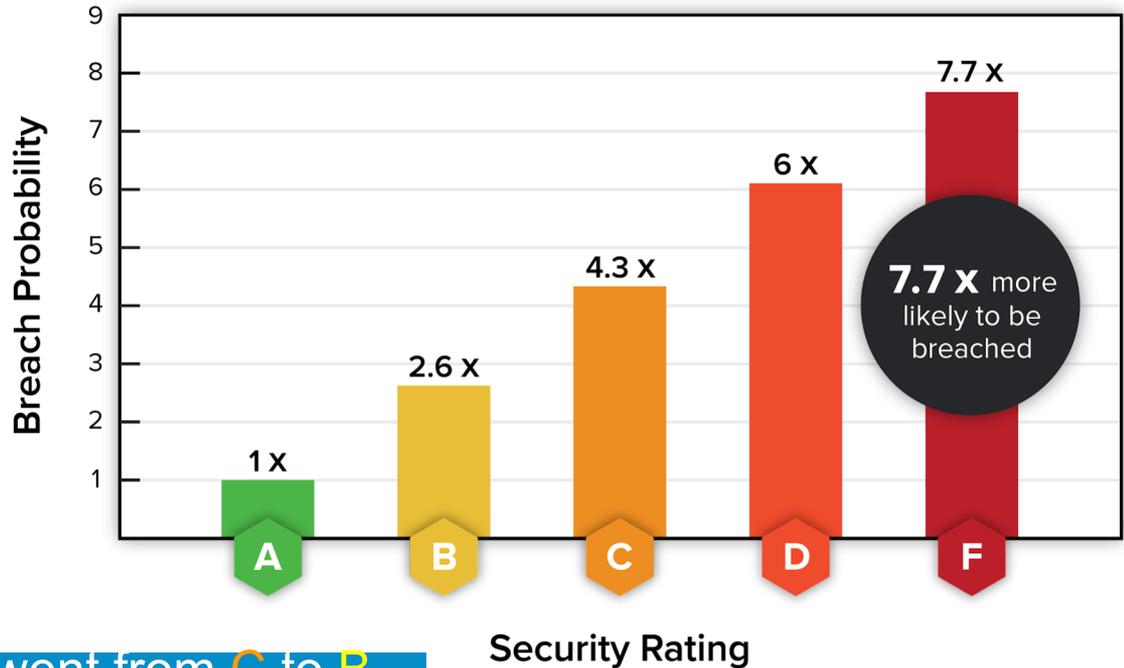
Overall scores of pilot participants improved over our 2-month pilot.

# Companies with a Better Security Rating are More Resilient.

## Independent analysis of our Security Ratings:

<b>Evaluation Period</b>	3 Years
<b>No. Data Breaches</b>	2,228
<b>No. Organizations</b>	99,076

Organizations with an F have **7.7x higher likelihood** of breach compared to organizations with a grade of A.



The 8 pilot participants who went from C to B reduced their risk of cyber breach by 140%.

# County Feedback



*Bob Kennedy, CIO*



**INFORMATION TECHNOLOGY**



**Lehigh County**  
Pennsylvania



**Thank you.**

Email the SSC team - [naco@securityscorecard.io](mailto:naco@securityscorecard.io)

Sign up for your FREE account - <https://securityscorecard.com/naco-cel>

## ATTACK SURFACE INTELLIGENCE (ASI)

## IDENTIFY THREATS FASTER WITH A UNIFIED VIEW OF YOUR ATTACK SURFACE

### VISUALIZING ATTACK SURFACE RISK CAN BE COMPLEX

According to ESG, nearly a third of all companies only actively monitor 75-85% of their known internet facing assets. Not only that, but more than 43% of companies report that it takes 80 hours to discover assets; due to lack of resources, this time-intensive process means that security teams can only engage in periodic monitoring, and **aren't able to keep up with the ever-changing attack surface.**

As a result, their lack of up-to-date information to make intelligent decisions leaves their organizations extremely **vulnerable to supply chain attacks.**

### INTELLIGENTLY UNCOVER BLINDSPOTS AND SHRINK YOUR ATTACK SURFACE

**SecurityScorecard's Attack Surface Intelligence (ASI)** is the first scorecard ratings platform to provide a **unified and complete view of risk** across your entire attack surface, including third-party vendors and unknown assets. Risk decisions and vulnerability prioritization has never been more clear when armed with a **layered approach, including contextual insights, cyber-attack attribution, and threat intelligence.**

Understand what a hacker sees across your attack surface with billions of up-to-date points data from SecurityScorecard's rich data lake of 12M+ digital footprints, available in the GUI or API. Pinpoint threats and Investigate the source by **domain, IP, IP range, CVE, CDIR, and Malware Hashes.**

### SECURITYSCORECARD SOLVES THESE ATTACK SURFACE INTELLIGENCE CHALLENGES

**01.**

**Where are our attack vectors and potential exposures?**

**02.**

**Can I automatically search by Domain associated to an IP or be notified of an IP in a Domain?**

**03.**

**How do I continuously monitor my entire attack surface, including vendors?**

**04.**

**How do I understand the breadth of my attack surface and my third parties?**

**05.**

**Can I reduce the number of tools I use and reduce license costs?**

**06.**

**Is it possible to get forensic threats to help with security strategy?**

### BENEFITS THAT MATTER THE MOST

In a single console, **ASI combines threat intelligence, IP scanning, domain attribution, vendor risk management, and CVE/malware trackers** to give your organization more depth to data, along with powerful cyber analytics capabilities.



**IDENTIFY AND RESPOND TO THREATS FASTER**



**SCALE YOUR TEAM AND UNITE KEY STAKEHOLDERS**



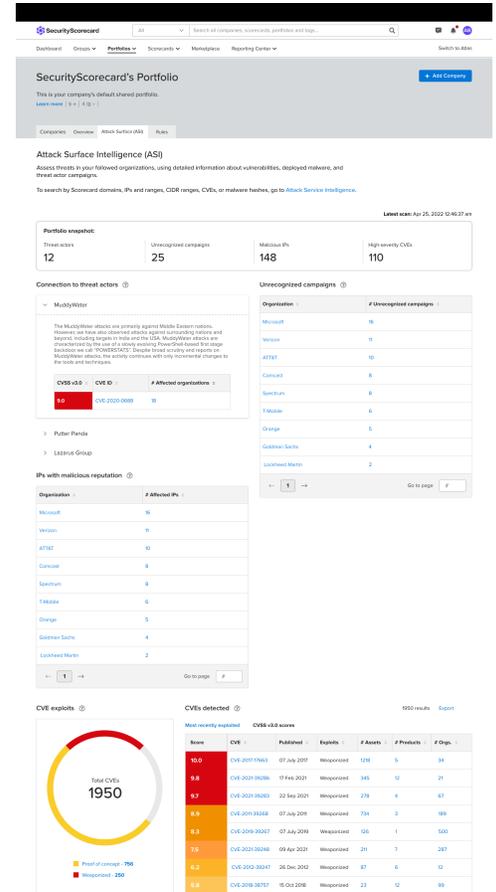
**SAVE TIME WITH CLEAR VULNERABILITY PRIORITIZATION**



**REDUCE FINANCIAL IMPACT FROM THREATS WITH POWERFUL INSIGHTS**

# KEY FEATURES

- 01. CONTINUOUS MONITORING AND SMART ALERTS**  
Early detection, attribution, and notifications to monitor security posture and third-party vendors.
- 02. SEARCHABLE DATABASE**  
Easily search historical and current data by domain, IP, IP range, CIDR, CVEs, and malware hashes right at your fingertips.
- 03. THREAT FORENSICS MADE EASY**  
Understand when an attack starts, identify who owns and controls the assets, and share threat information internally and externally to prevent further breaches.
- 04. DIGESTIBLE THREAT INTELLIGENCE REPORTING**  
Make informed decisions faster with actionable reporting that maps your attack surface, and identifies weaknesses, patterns, and trends to determine the full breadth of potential threats.
- 05. INTEGRATION FOR GREATER VISIBILITY**  
Create automated workflows and connect threat intelligence data with your SIEM, ticketing system, and vulnerability management tools.



## One Powerful Platform for Different Stakeholders

### MONITOR THREATS AND VULNERABILITIES

Threat hunters  
Cyber threat researchers  
Data Data scientist  
Managed security service providers  
IT operations analysts  
Digital forensics

### UNDERSTAND CYBER RISK WITHOUT TECHNICAL KNOWLEDGE

Compliance  
Procurement  
Accountants  
Lawyers  
Chief Risk Officers



### SECURITYSCORECARD'S PROMISE

We empower our customers with the ability to easily quantify cyber risk, deeply understand and reduce risk within your ecosystem, and explore deeper cyber analytics today and in the future.

### TAKE CONTROL OF ATTACK SURFACE

**Talk to a SecurityScorecard representative today** to learn how Attack Surface Intelligence enables you to scale higher.



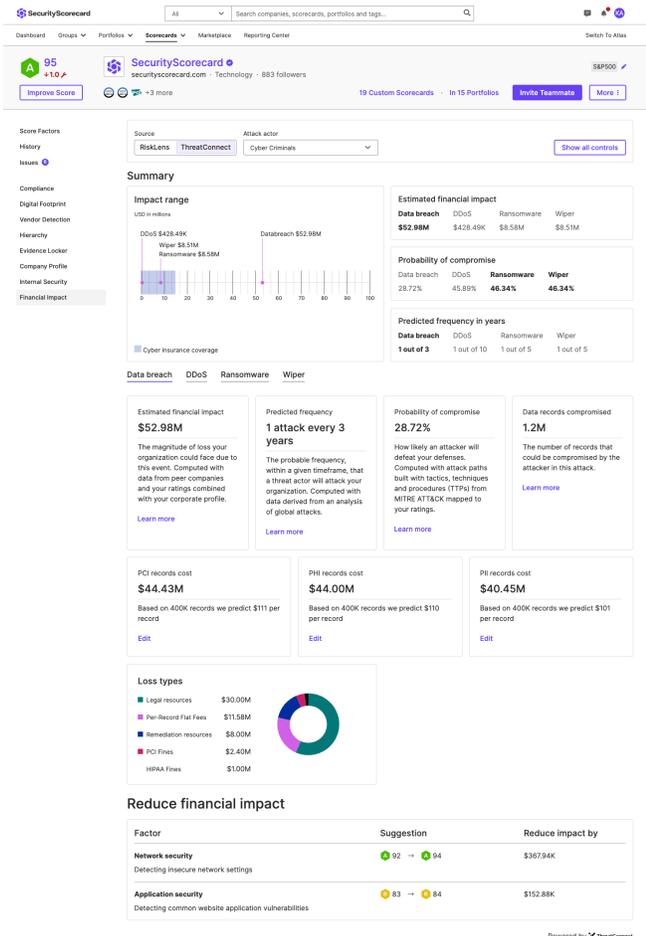
# HOW TO

# OPTIMIZE CYBER RISK MANAGEMENT INVESTMENTS

## INCREASE THE RETURN ON INVESTMENT OF YOUR SECURITY PROGRAM

Executives struggle to connect security budgets to business outcomes, hindering a CISO's ability to justify their cybersecurity budgets and often leading to a tension for budget allocation. Simply allocating a percentage of the company's total budget doesn't guarantee strong security performance.

SecurityScorecard's risk quantification capabilities translates cyber risk into monetary values, assisting you in a cost-benefit analysis of different cyber investment options.



### 01. LOWER YOUR CYBER RISK

Reduce the impact of cyber incidents by prioritizing security investments towards the most likely or damaging loss scenarios.

### 02. STRENGTHEN THE BALANCE SHEET

Direct capital towards the security enhancements that are most closely aligned with business goals and financial performance.

### 03. IMPROVE COMMUNICATION AND COLLABORATION

Simplify the way cyber risk is discussed with your peers by defining it in an universally understood metric.

## QUANTIFY CYBER RISK AT SCALE



**12 MILLION+**

COMPANIES CONTINUOUSLY RATED



**54 BILLION+**

SECURITY ISSUES DISCOVERED WEEKLY



**2**

RISK QUANTIFICATION FRAMEWORKS SUPPORTED

# SECURITYSCORECARD ENABLES YOU TO

## 01. IDENTIFY THE BIGGEST THREATS

Confirm whether ransomware, data breaches, denial of service or some other attack mode is your main concern.

## 02. DETERMINE THE DRIVERS OF LOSS

Understand how much capital is lost to expenses like remediation costs and legal fees when an incident occurs.

## 03. ESTIMATE THE LIKELIHOOD OF INCIDENTS

Gain insight into the probability of incidents happening in a given year and their rate of success.

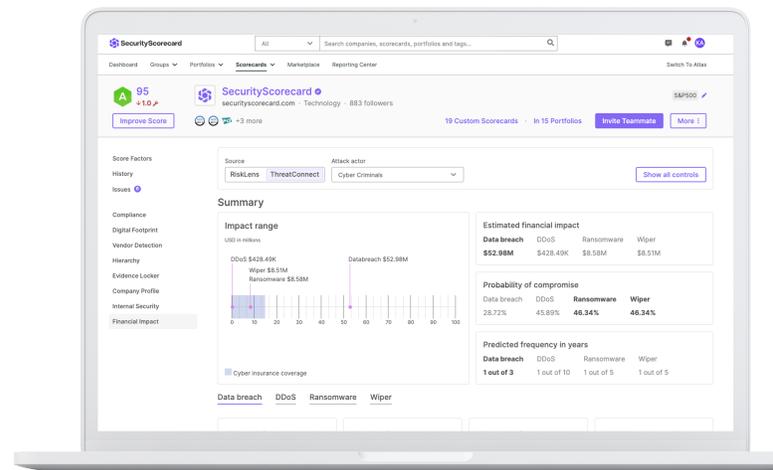
## 04. MEASURE THE IMPACT OF INVESTMENTS

Quantify the reduction in expected losses if issues like open ports, outdated websites, or weak endpoints are resolved.

## CONTEXT, SCALE, AND RELEVANCE

Our unique combination of security ratings and risk quantification frameworks enables data-driven decisions with the speed and accuracy needed to face the ever evolving cyber threats.

SecurityScorecards allow you to implement a repeatable and trustworthy model for quantifying cyber risk instead of relying on labor intensive assessments that take weeks to complete and are based on outdated snapshots of the business.



## STOP ARBITRARILY THROWING MONEY AT THE PROBLEM

Talk to a **SecurityScorecard representative today** to learn how to optimize your cyber risk management investment decisions

## CONTACT US TO LEARN MORE

[Request a demo today.](#)