

Third-Party Cyber Risk: From Obligation to Opportunity



SecurityScorecard: Recognized Leader

Company

Leading, global cybersecurity firm with a global presence. Over 100k companies use our platform to monitor 3M+ organizations daily.

Technology

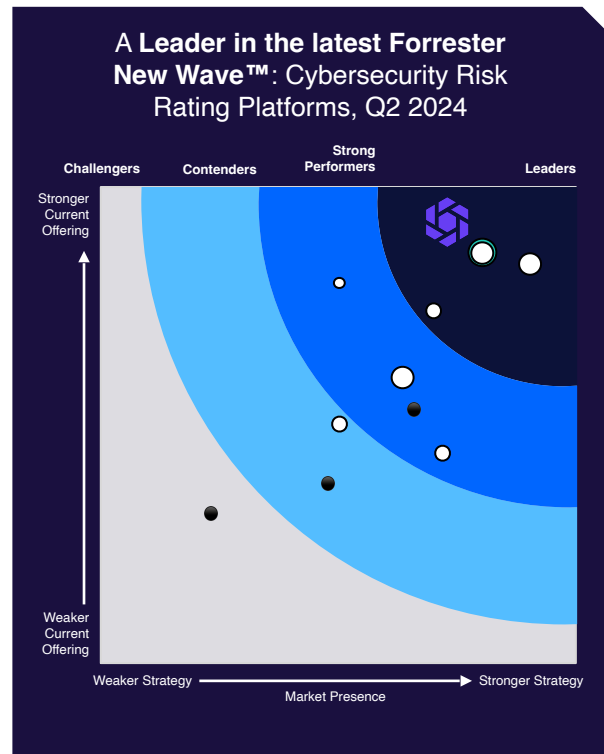
Global intelligence data collection at scale by STRIKE engine: over 1B+ security events per second. Ratings efficacy vetted by Marsh McLennan.

Platform

Enterprise solutions: Outside-in Ratings;; EASM; CRQ; Supply Chain Detection and Response.

Gartner®

Gartner Market Guide for
Third-Party Risk
Management
Solutions, 2022



Source: Gartner, Forrester.



Supply chain risks are fast growing concerns

Your Dependencies

Partners

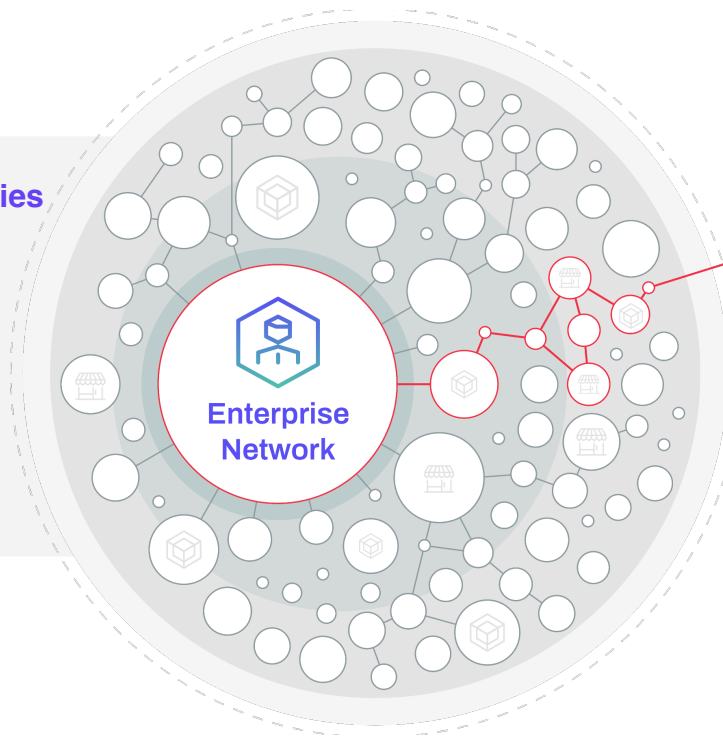
Trusted connections for direct info exchanges

Suppliers

Critical for business operations

Vendors

Implied shared trust



Supply Chain Risks



Threat actors
May impersonate vendors



Hacktivity
Focused on disruption



Opportunistic Actors
"Drive-by" scanning for unpatched issues

68%

Increase in supply chain breaches year over year

Source: 2024 Verizon Data Brief Investigation Report

41%

Of material cyber attacks originated from a third party

Source: World Economic Forum, Global Cybersecurity Outlook 2024

40%

Higher costs compared to first-party breaches

Source: Gartner, 4 Third-Party Risk Principles That CISOs Must Adopt

Compliance pressures are increasing

Failure to manage risks can result in fines, reputational damage, and operational disruptions

Common compliance gaps



Informal cyber risk strategy and governance



Inability to assess and continuously monitor of suppliers



No visibility of third-party suppliers and concentration risks



Rapid reporting of material cybersecurity incidents

89%

of GRC professionals expect an audit finding related to third-party risk management

Source: Hyperproof, 2025 IT Risk and Compliance Benchmark Report





Global Breaches Keep Getting Larger and More Costly

CYBERSCOOP

Topics ▾ Special Reports Events Podcasts Videos

CYBERCRIME

As many as 165 companies 'potentially exposed' in Snowflake-related attacks, Mandiant says

The impact of the operation targeting customers of the cloud storage giant continues to grow.

Microsoft | Support Microsoft 365 Office Products ▾ Devices ▾ More ▾

National Public Data breach: What you need to know



Parents & Students Support Search Login

Products ▾ Customers ▾ Your Needs ▾ Support a Role ▾ Global Regions ▾ PowerSchool AI ▾ Resources ▾ Company ▾

PowerSchool Cybersecurity Incident

This site will be updated periodically as PowerSchool learns more information and takes additional steps in response to a recent security incident.

May 7, 2025

PowerSchool is aware that a threat actor has reached out to multiple school district customers in an attempt to extort them using data from the previously reported December 2024 incident. We do not believe this is a new incident, as samples of data match the data previously stolen in December. We have reported this matter to law enforcement both in the United States and in Canada, notified all PowerSchool SIS customers of the development, and are working closely with our customers to support them. We sincerely regret these developments – it pains us that our customers are being threatened and re-victimized by bad actors.

Any organization facing a ransomware or data extortion attack has a very difficult and considered decision to make during a cyber incident of this nature. In the days following our discovery of the December 2024 incident, we made the decision to pay a ransom because we believed it to be in the best interest of our customers and the students and communities we serve. It was a difficult decision, and one which our leadership team did not make lightly. But we thought it was the best option for preventing the data from being made public, and we felt it was our duty to take that action. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to us.

Change Healthcare's Breach Costs Could Reach \$2.5 Billion

Costs Have Already Hit \$2 Billion, Parent Company UnitedHealth Group Reports

Mathew J. Schwartz (@euroinfosec) · July 17, 2024

Share Tweet in Share Credit Eligible Get Permission





What do these breaches have in common?

CYBERSCOOP

Topics ▾ Special Reports Events Podcasts Videos

CYBERCRIME

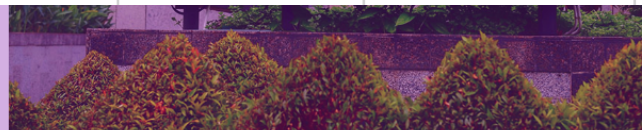
As many as 165 companies 'potentially exposed' in Snowflake-related attacks. Mandiant says

Microsoft | Support Microsoft 365 Office Products ▾ Devices ▾ More ▾

National Public Data breach:

| Breach | Industry | 1st/3rd Party | SOC2:Type2 | Due Dilligence Completed |
|----------------------|-------------------------|---------------|------------|--------------------------|
| Snowflake | IT Software | 3rd | Yes | Yes |
| Change Healthcare | Healthcare | 3rd | Yes | Yes |
| PowerSchool | Public Sector /Software | 3rd | Yes | Yes |
| National Public Data | FinTech | 3rd | Yes | Yes |

nature, in the days following our discovery of the December 2024 incident, we made the decision to pay a ransom because we believed it to be in the best interest of our customers and the students and communities we serve. It was a difficult decision, and one which our leadership team did not make lightly. But we thought it was the best option for preventing the data from being made public, and we felt it was our duty to take that action. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to us.





Compliance can provide a false sense of security



Millions of customer records accessed with single stolen credential



Common security certifications and controls were in place



Actual risks included 50x more leaked credentials and 390 critical/high CVEs



Challenges in operationalizing supply chain security



No standard or clear response process when a supplier is involved in a breach



Vulnerabilities arise, and **vendors are overwhelmed with volume of requests**



Vendor risk managers struggle to **turn noisy data into actions** and workflows



Security analysts are bogged down with **check the box compliance**

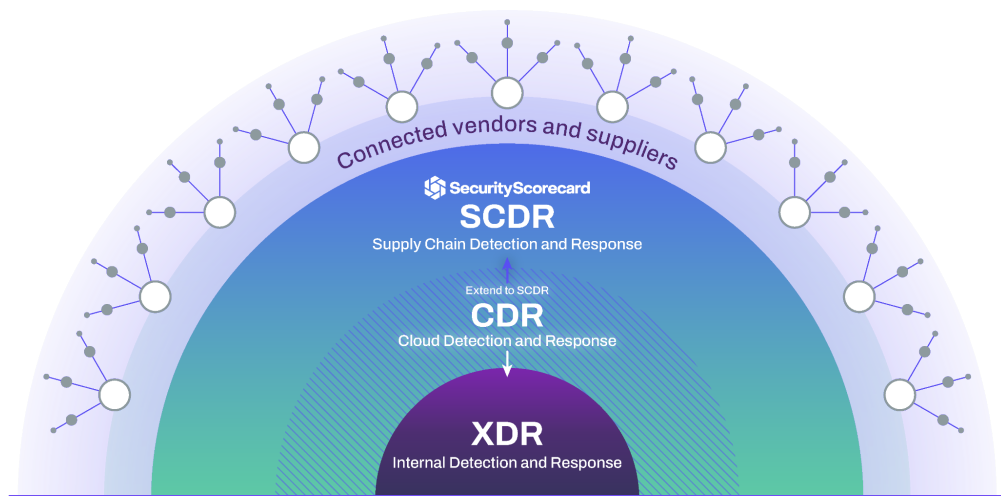


TPRM and SOC teams are not aligned



Introducing Supply Chain Detection and Response

Extends XDR and CDR principles to operationalize supply chain cybersecurity



Supplier Visibility

Holistic and contextual view of **configuration risk**, **shadow IT** and **attack surface vulnerabilities**

Incident Response

Prioritize activation of **supply chain risk insights** through **SOC automation capabilities**

Supplier Remediation

Asset management capabilities and **issue resolution workflows** enable effective remediation

Operationalizing supply chain security with MAX

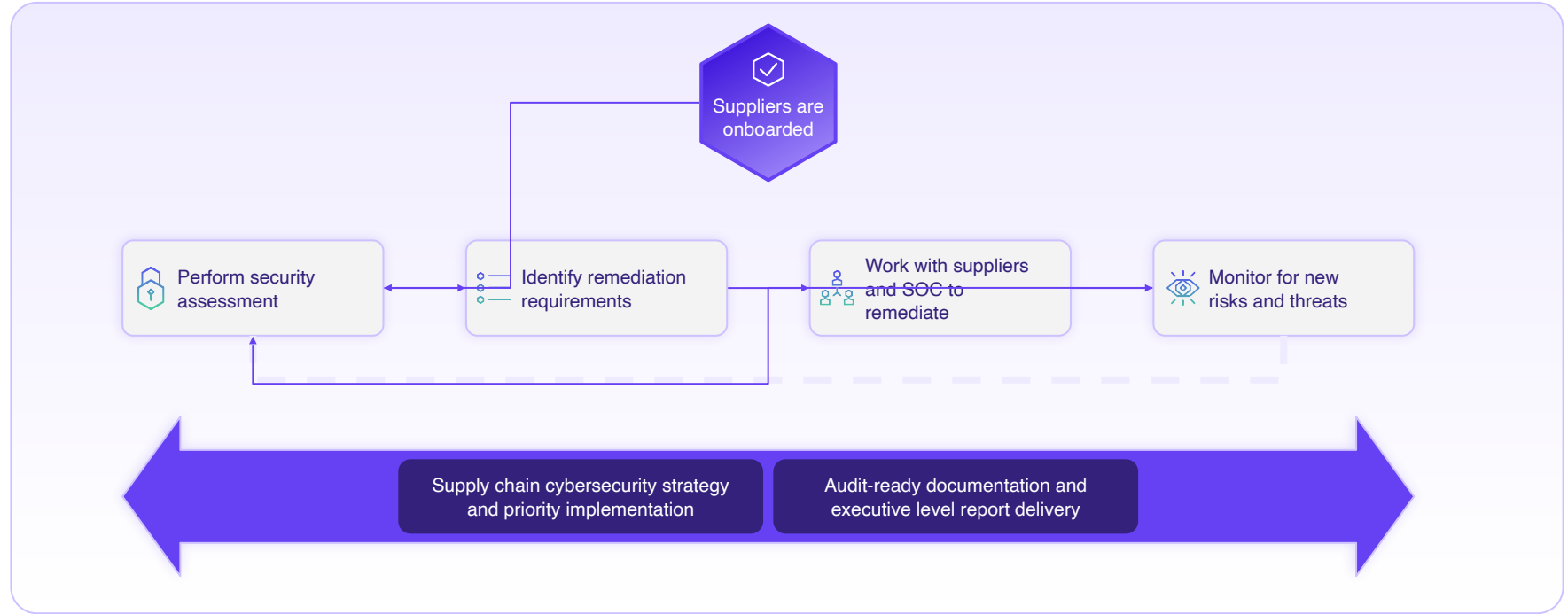
SecurityScorecard MAX aligns your TPRM and SOC on risk mitigation and incident response





Supply Chain Detection and Response at work

Proactive preventive measures and post-incident response capabilities



Your supplier's security problems are your problems



**Threat actor behavior
has shifted**

68%

Increase in supply chain
breaches

**Regulators demand
high maturity levels**

89%

Expect audit findings related
to TPRM

**Multiple priorities
stretch resources**

37%

Lack budget to meet vendor
assessment requirements



Anatomy of a 3rd Party Breach



IMAGE: UNSPLASH

James Reddick

February 22nd, 2024

Cybercrime

News



Get more insights with the
Recorded Future
Intelligence Cloud.

[Learn more.](#)

Prescriptions nationwide impacted by cyber incident at Change Healthcare

Pharmacies across the country are running into issues filling prescriptions due to a cyber incident affecting a multibillion-dollar healthcare conglomerate involved in processing half of all medical claims in the U.S.

Nashville-based Change Healthcare **first announced disruptions** to certain applications early on Wednesday, before saying in the afternoon that the company was “experiencing a network interruption related to a cyber security issue.”

On Thursday, it issued another update, saying: “Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact.”

In 2022, Change Healthcare completed a \$7.8 billion merger with the healthcare services provider Optum, a subsidiary of UnitedHealth Group.

In its notice about the incident, the company said the issues are “specific” to Change Healthcare and do not affect “other systems across UnitedHealth Group.”

Pharmacies took to social media on Wednesday and Thursday to warn customers of issues processing prescriptions. Lone Star Pharmacy in Santa Fe, Texas, **wrote on Facebook** that they were “currently unable to process any prescriptions on insurance due to a software issue.”



How did this happen???

Ransomware gang starts leaking alleged stolen Change Healthcare data



The RansomHub extortion gang has begun leaking what they claim is corporate and patient data stolen from United Health subsidiary Change Healthcare in what has been a long and convoluted extortion process for the company.

In February, Change Healthcare suffered a cyberattack that caused massive disruption to the US healthcare system, preventing pharmacies and doctors from billing or sending claims to insurance companies.

The attack was ultimately linked to the BlackCat/ALPHV ransomware operation, who later said they stole 6 TB of data during the attack.

After facing increased pressure from law enforcement, the BlackCat gang shut down their operation. This occurred amid claims they were pulling an exit scam by stealing a \$22 million Change Healthcare ransom payment from the affiliate who conducted the attack.



How did this happen? BREADCRUMBS!





Current Day: After “The Boom”

Dashboard Scorecards ▾ Portfolios Core Tools ▾ Modules ▾ Professional Services ▾

Companies

▼ Filters Clear Filters

Toggle columns

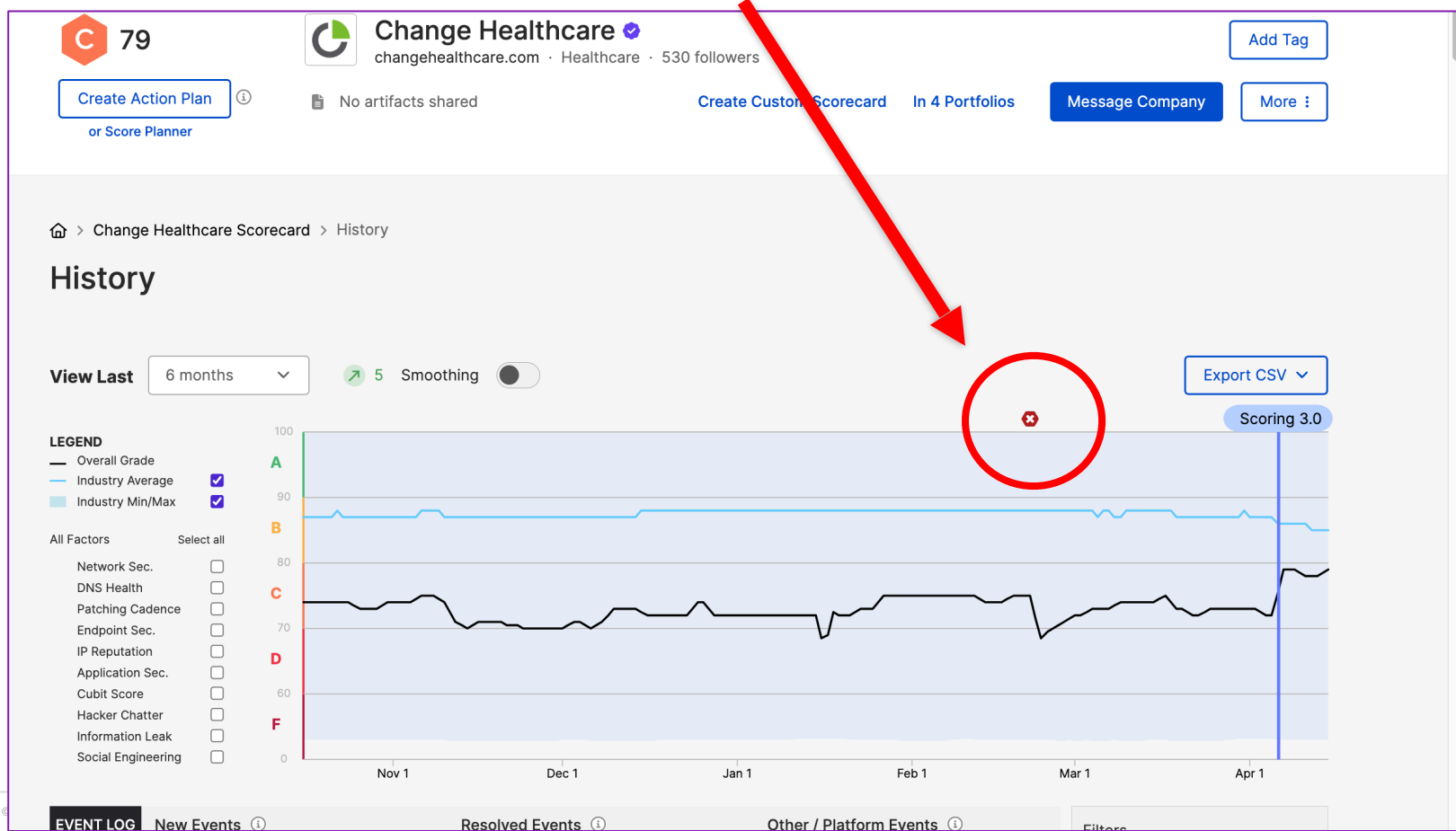
Q Search with company name or domain or products

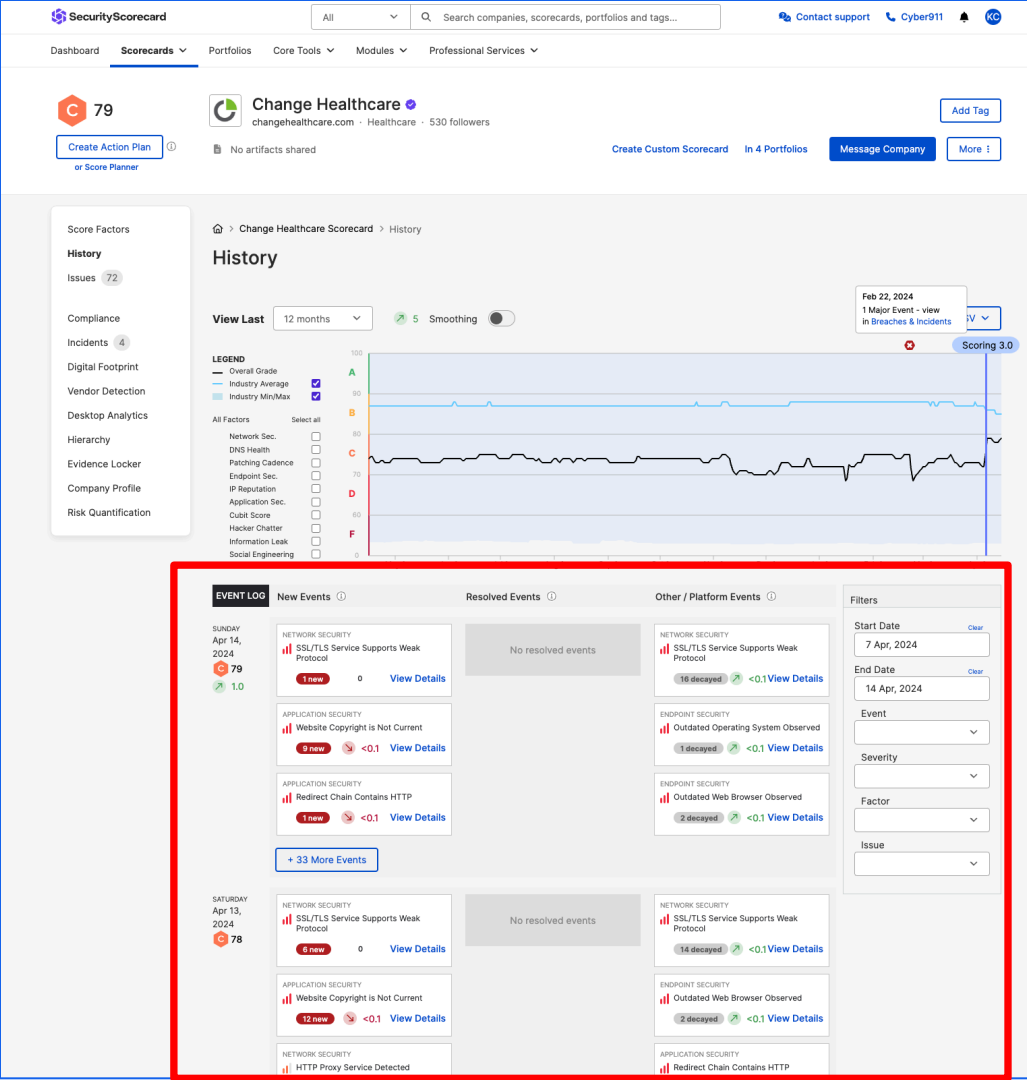
716 Assign Business Impact ▾ Apply Tags Compare Copy To Remove Export ▾

| <input type="checkbox"/> | Company ▾ | Security Score ▾ | 30-Day ▾ | Industry ▾ | Business Impact ▾ | Status ▾ | Date Added ▾ | Evidence | Public Tags | Products Used |
|--------------------------|---|------------------|----------|----------------------|-------------------|-------------------------------------|--------------|----------------------------------|-------------|---------------|
| <input type="checkbox"/> | Change Healthcare changehealthcare.com | C 79 | 0 | Healthcare | | Inactive Contact | Apr 15, 2024 | Request evidence | | 1388 |
| <input type="checkbox"/> | Mc1global mc1global.com | B 82 | 7 | Technology | | Active Contact | Mar 21, 2022 | Request evidence | | N/A |
| <input type="checkbox"/> | Press Ganey pressganey.com | B 84 | 2 | Healthcare | | Active Contact | Mar 21, 2022 | Request evidence | | 447 |
| <input type="checkbox"/> | Questionmark questionmark.com | B 85 | 1 | Information Services | | Inactive Contact | Mar 21, 2022 | Request evidence | | 72 |
| <input type="checkbox"/> | Kontek kontek.se | D 68 | 1 | Pharmaceutical | | Inactive Invite | Mar 21, 2022 | Request evidence | | 10 |

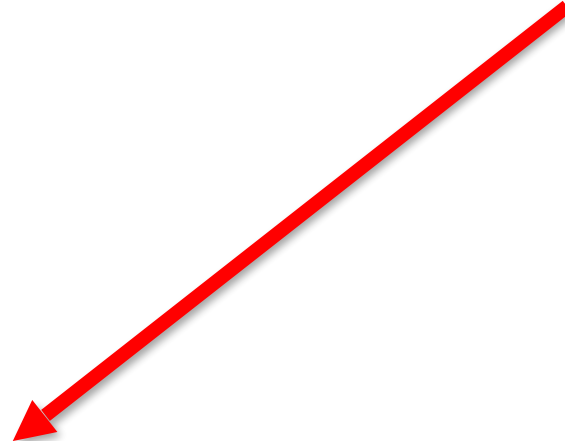


The Boom (Breach Disclosure)

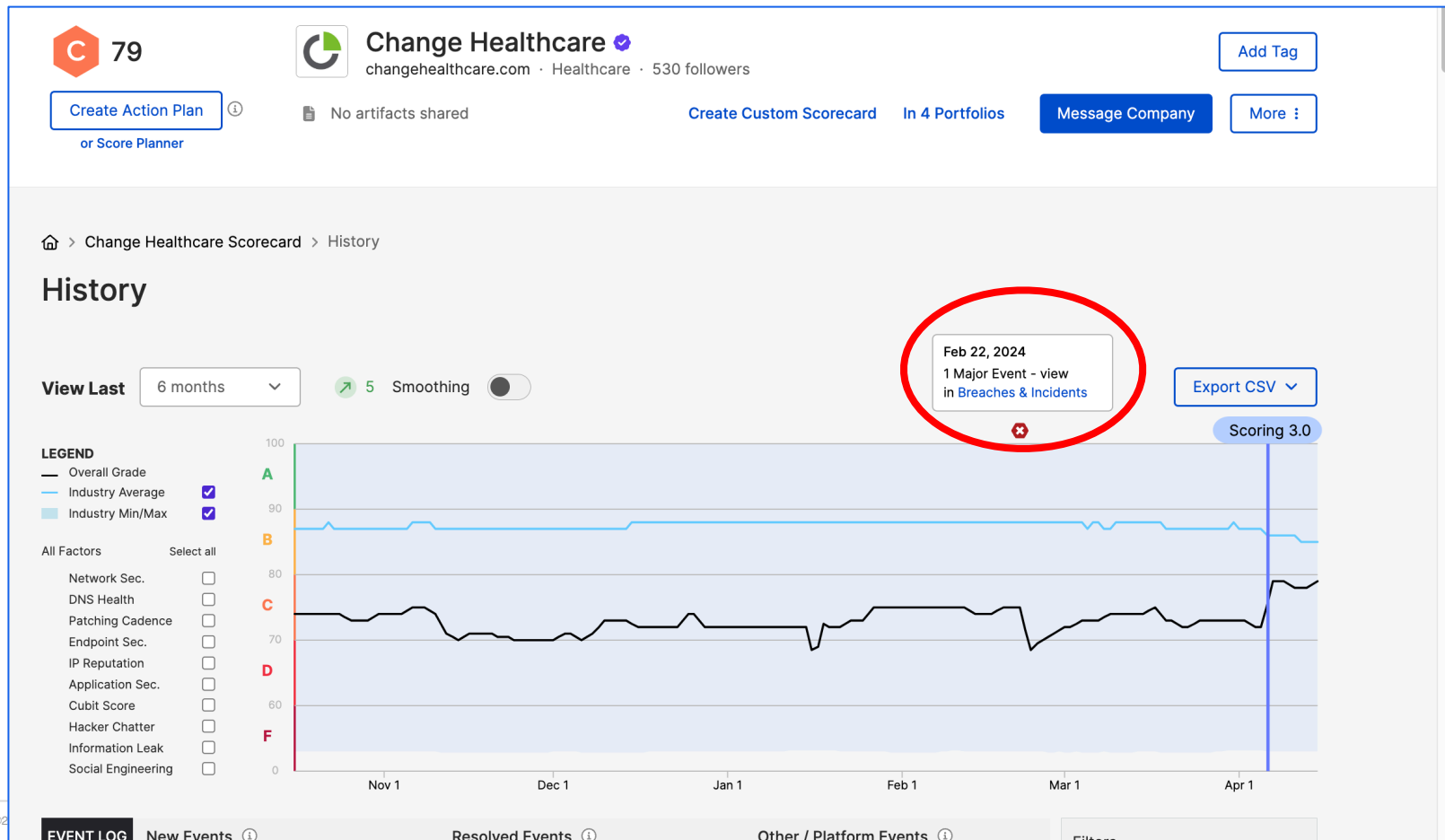


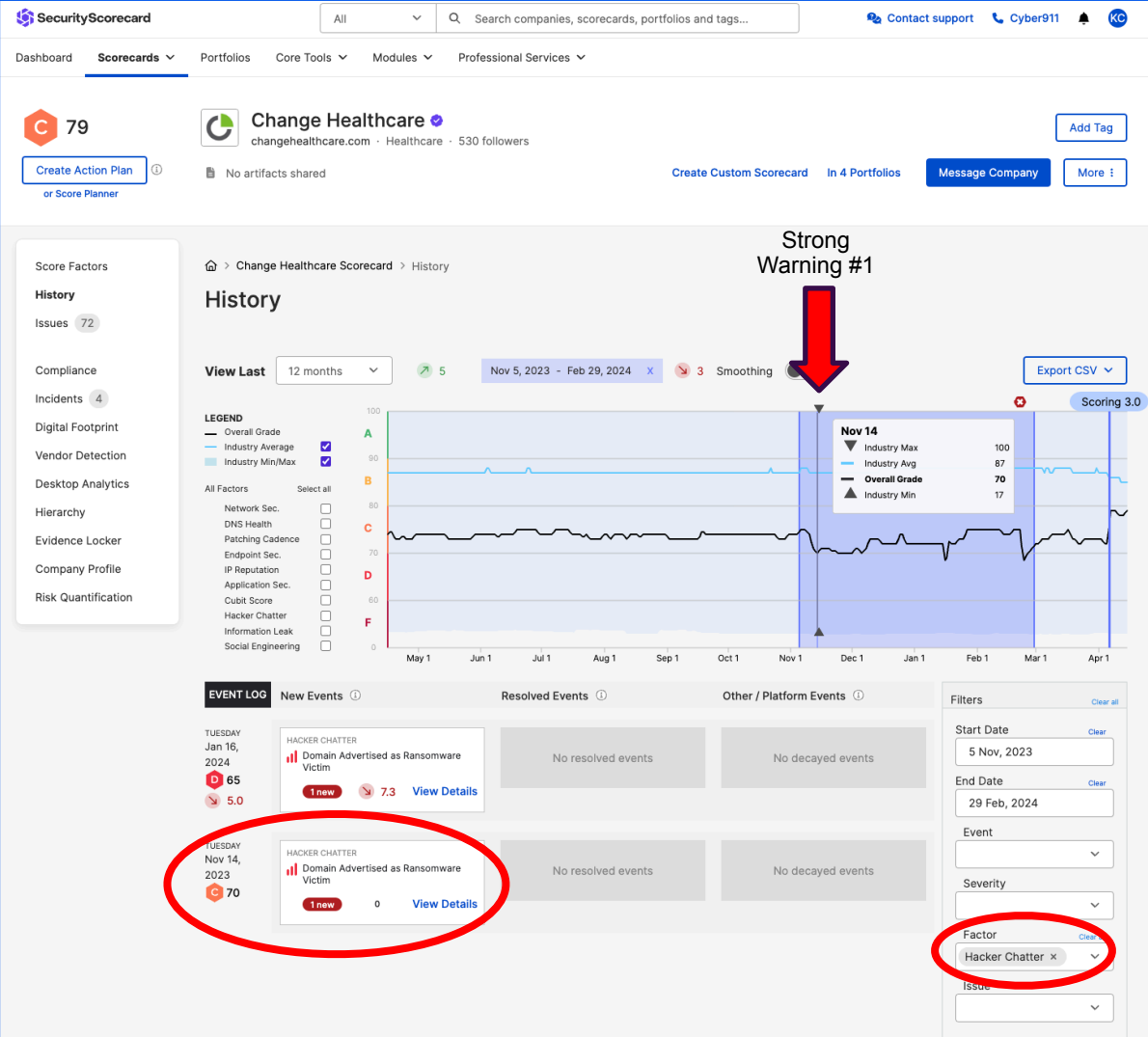


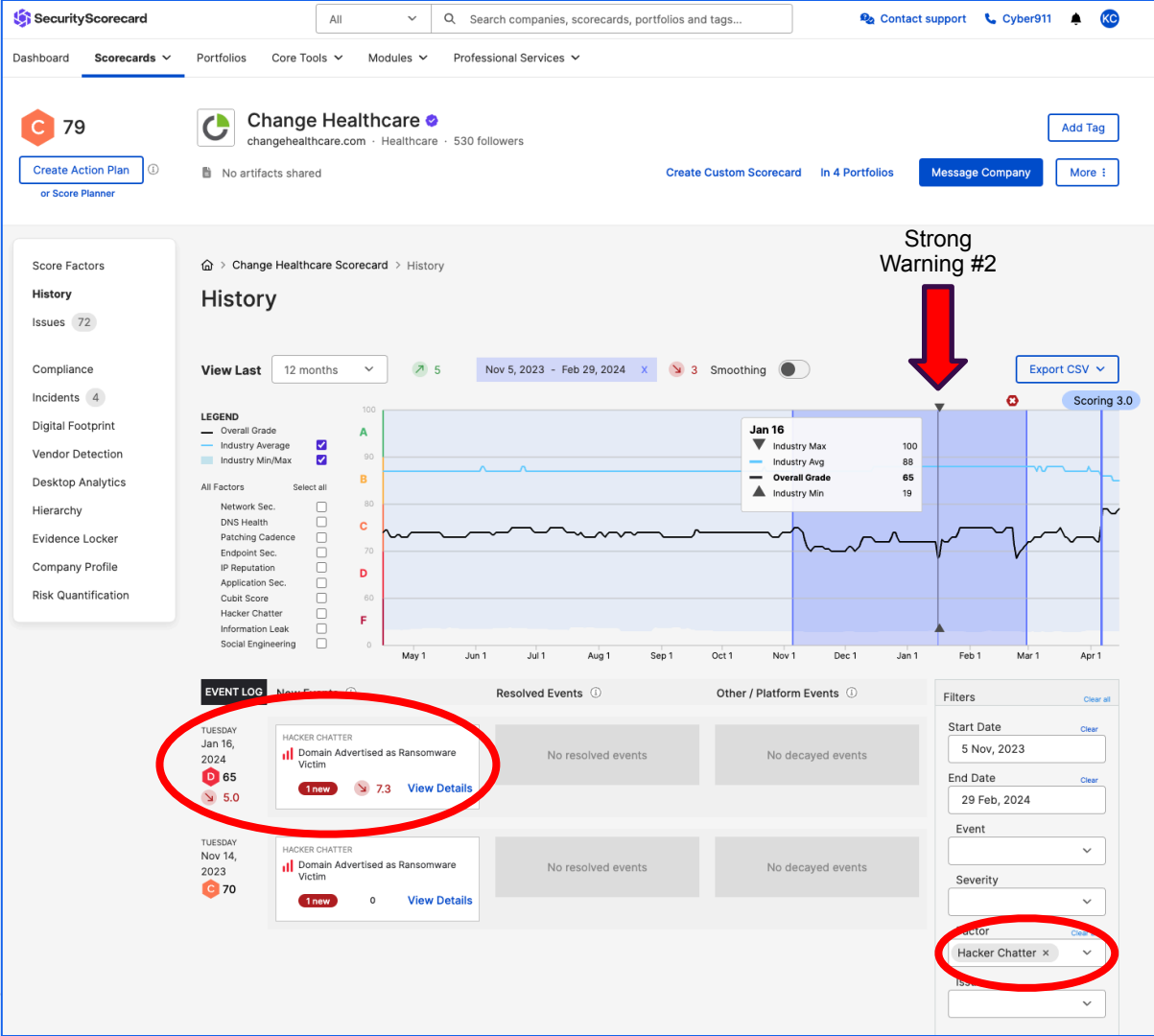
Cybersecurity Findings Activity Log



Could this breach have been predicted?







C 79

Create Action Plan or Score Planner

Change Healthcare changehealthcare.com · Healthcare · 530 followers

Add Tag

No artifacts shared

Create Custom Scorecard In 4 Portfolios Message Company More

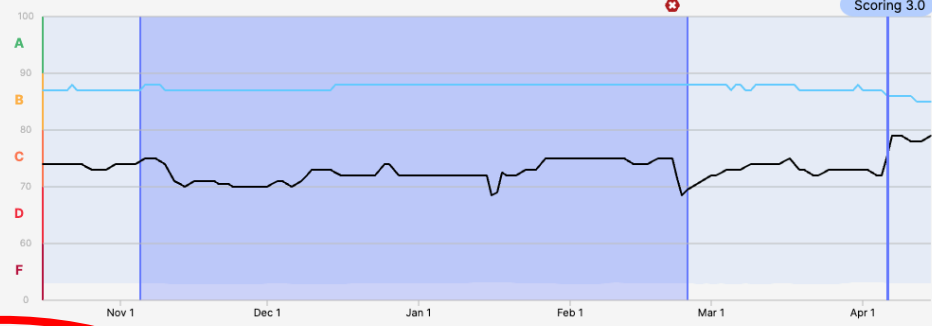
- Score Factors
- History**
- Issues 72
- Compliance
- Incidents 4
- Digital Footprint
- Vendor Detection
- Desktop Analytics
- Hierarchy
- Evidence Locker
- Company Profile
- Risk Quantification

Change Healthcare Scorecard History

History

View Last 6 months 5 Nov 5, 2023 - Feb 25, 2024 5 Smoothing Export CSV

- LEGEND**
- Overall Grade
 - Industry Average
 - Industry Min/Max
- All Factors Select all
- Network Sec.
 - DNS Health
 - Patching Cadence
 - Endpoint Sec.
 - IP Reputation
 - Application Sec.
 - Cubit Score
 - Hacker Chatter
 - Information Leak
 - Social Engineering



EVENT LOG New Events 1

FRIDAY Feb 23, 2024 68

BREACH

Records N/A Go to Breaches

Resolved Events 1 Other / Platform Events 1

No resolved events No decayed events

Filters Clear all

Start Date Clear 5 Nov, 2023

End Date Clear 25 Feb, 2024

Event Clear all Breach x

Severity

SecurityScorecard

All

Search companies, scorecards, portfolios and tags...

Contact supportCyber911

DashboardScorecardsPortfoliosCore ToolsModulesProfessional Services

C79

Create Action Plan

or Score Planner

Change Healthcare

changehealthcare.com · Healthcare · 530 followers

Add Tag

No artifacts shared

Create Custom ScorecardIn 4 PortfoliosMessage CompanyMore

Score Factors

History

Issues72

Compliance

Incidents4

Digital Footprint

Vendor Detection

Desktop Analytics

Hierarchy

Evidence Locker

Company Profile

Risk Quantification

Open issues

Hacker Chatter

Domain Advertised as Ransomware Victim

Hacker Chatter

High severity

Domain Advertised as Ransomware Victim

This issue maps to

MITRE

DESCRIPTION

A ransomware leak site is an online platform established by ransomware operators to publicly disclose sensitive information stolen from their victims. After infiltrating an organization's network and encrypting its data, ransomware attackers often demand payment in exchange for decrypting the files. If the victim fails to comply with their demands, the attackers may upload portions of the stolen data onto these leak sites as a form of leverage. These sites typically feature a searchable database of compromised information, allowing visitors to browse through the stolen files. They're also used to pressure victims into paying the ransom by threatening further data releases.

RISK

Your organization being listed on a ransomware leak site carries serious consequences. Beyond the immediate impact of having sensitive data exposed to the public, there are broader implications. It could severely damage your organization's reputation, leading to loss of trust among customers, partners, and stakeholders. Leaked proprietary information could give competitors an edge, affecting your market position. Legal ramifications may follow, including regulatory fines for data breaches and potential lawsuits from affected parties. Financially, the costs of incident response, data recovery, and potential ransom payment can be substantial. Overall, being listed on a ransomware leak site poses a multifaceted threat that can have lasting repercussions for your organization.

RECOMMENDATION

Implement robust cybersecurity measures, including firewalls, antivirus software, and intrusion detection systems.

Regularly update software and systems to patch known vulnerabilities.

Conduct thorough employee training on cybersecurity best practices, including phishing awareness and password management.

SecurityScorecard

All

Search companies, scorecards, portfolios and tags...

Contact supportCyber911

DashboardScorecardsPortfoliosCore ToolsModulesProfessional Services

There are 2 findings you can investigate right now. Resolving findings can affect your rating.

Resolve FindingsLearn More

COMPARISON TO SIMILAR COMPANIES

4% have this issue, just like this company

96% do not have this issue

1 finding on average

2 findings for this company

2 findings

To send issues to Jira, [install integration](#)

Fixed

Other resolutions

Download as CSV

Learn how to resolve findings

Toggle columns1 hiddenFilters

Search with issued or domain

2

| | Status | Domain | Victim Site | Ransomware Name | Last Observed |
|--------------------------|--------|--|-------------|-----------------|-------------------|
| <input type="checkbox"/> | Open | uhcsr.com + Add Tag | uhcsr.com | clOp | 2024-04-13T12:00Z |
| <input type="checkbox"/> | Open | mcna.net + Add Tag | mcna.net | lockbit3.0 | 2024-02-17T12:00Z |



What can MAX/SCDR tell us about the attack path?



What can MAX/SCDR tell us about the attack path?



SecurityScorecard All [Contact support](#) [Cyber911](#)

Dashboard **Scorecards** Portfolios Core Tools Modules Professional Services

Monitoring hacker sites for chatter about your company 2 findings

Information Leak

Potentially confidential company information which may have been inadvertently leaked 8.3K findings

A 100

| HIGH SEVERITY | MEDIUM SEVERITY | LOW SEVERITY |
|---|--|------------------------------------|
| No high risk issues to detect for this factor | Cleartext password exposed 0 | Attempted Information Leak 0 |
| | Credentials at Risk 0 | Credentials at Risk (Historical) 0 |
| | Email exposed 0 | Employer exposed 0 |
| | Exploit Attempt Detected 0 | IP address exposed 0 |
| | Password hint exposed 0 | |
| | Security question and answer exposed 0 | |
| | Social Security number exposed 0 | |

POSITIVE SIGNALS

No positive risk issues to detect for this factor

INFORMATIONAL 8.3K findings

- API key exposed 0
- Age exposed 0
- Birthday exposed 0
- Credentials at Risk For Up to Two Years 743**
- Credentials at Risk for Up to 120 days 7.5K**
- Hardcoded password exposed 0

No artifacts shared

Create Custom Scorecard In 4 Portfolios

Message Company

More



Open issues Information Leak Credentials at Risk for Up to 120 days

Information Leak Informational signal

Credentials at Risk for Up to 120 days

This issue maps to

MITRE

DESCRIPTION

Our sensors observed user names and passwords associated with accounts in this domain in the logs of infostealer malware. Infostealers harvest credentials and other data from compromised devices.

RISK

We discovered credentials for accounts associated with employee addresses that were stolen up to 120 days ago. Threat actors could sell these credentials or use them to access assets in this domain.

RECOMMENDATION

Ensure employees are not using the affected credentials for any corporate or third-party logins. Ensure that all passwords have been changed since the indication of breach. In the case of corporate passwords, check logs for repeated failed login attempts or repeated password reset attempts from suspicious IP addresses. See additional recommendations in the MITRE ATT&CK Mitigations site.

Threat level

Set by our security team

Breach risk

Data-driven likelihood

Overall score in portfolio

Impact of all 500 items

| SecurityScorecard | | | | | |
|--------------------------|------------|--|----------------|-----------------|-----------------------|
| All | | Search companies, scorecards, portfolios and tags... | | | |
| Dashboard | Scorecards | Portfolios | Core Tools | Modules | Professional Services |
| 500 | | | | | |
| | Status | Domain | User Name | Leaked Password | Infection Date |
| <input type="checkbox"/> | Open | www.myuhc.com + Add Tag | kybo20 | ****THY7 | April 06, 2024 |
| <input type="checkbox"/> | Open | identity.onehealthcareid.com + Add Tag | saniam123 | ****2023 | March 15, 2024 |
| <input type="checkbox"/> | Open | www.healthsafe-id.com + Add Tag | lojeda787 | *****@888 | March 12, 2024 |
| <input type="checkbox"/> | Open | accounts.myuhc.com + Add Tag | rgroody320119 | *****wn48 | April 12, 2024 |
| <input type="checkbox"/> | Open | healthsafeid.optumfinancial.com + Add Tag | kybo20 | *****4t*k | April 06, 2024 |
| <input type="checkbox"/> | Open | login.optumbank.com + Add Tag | willie1234 | *****za1l | April 12, 2024 |
| <input type="checkbox"/> | Open | accounts.werally.com + Add Tag | fracturedheart | *****ve87 | December 18, 2023 |
| <input type="checkbox"/> | Open | identity.onehealthcareid.com + Add Tag | kchoffice | ****2021 | March 15, 2024 |
| <input type="checkbox"/> | Open | identity.onehealthcareid.com + Add Tag | mmehmood420 | *****2023 | March 15, 2024 |
| <input type="checkbox"/> | Open | www.uhone.com + Add Tag | chioma27 | ****le16 | April 14, 2024 |
| <input type="checkbox"/> | Open | accounts.myuhc.com + Add Tag | lafesler | *****ts1 | April 11, 2024 |
| <input type="checkbox"/> | Open | www.healthsafe-id.com | fiamap1991 | *****g1* | April 14, 2024 |

No artifacts shared

Create Custom Scorecard In 4 Portfolios

Message Company

More

Add Tag



Open issues Information Leak Credentials at Risk for Up to 120 days

Information Leak Informational signal

Credentials at Risk for Up to 120 days

This issue maps to

MITRE

What do these scores mean? Find out

DESCRIPTION

Our sensors observed user names and passwords associated with accounts in this domain in the logs of infostealer malware. Infostealers harvest credentials and other data from compromised devices.

Threat level

Set by our security experts



Info

RISK

We discovered credentials for accounts associated with **en** **days** ago. Threat actors could sell these credentials or use

RECOMMENDATION

Ensure employees are not using the affected credentials for all passwords have been changed since the indication of b logs for repeated failed login attempts or repeated password See additional recommendations in the MITRE ATT&CK Mit

W14 x fx hxxps://identity.onehealthcareid.com/app/index.html

| | P | Q | R | S | W | AB |
|----|------------------------------|-------------------|-----------------|----------------|--|-------------------|
| | Domain | User Name | Leaked Password | Infection Date | url | Last Observed |
| 1 | www.healthsafe-id.com | jaxx0044 | *****45## | 7-Sep-23 | hxxps://www.healthsafe-id.com/register/createaccount | 2023-12-17T00:00Z |
| 2 | healthid.optum.com | natarajan2020 | *****2020 | 16-Sep-23 | hxxps://healthid.optum.com/tb/app/index.html | 2023-12-24T00:00Z |
| 3 | www.myuhc.com | jianhao198-i | *****s123 | 17-Sep-23 | hxxps://www.myuhc.com/member/prewelcome.do | 2023-12-24T00:00Z |
| 4 | app.uhcdoctorchat.com | unknown | *****122? | 30-Sep-23 | hxxps://app.uhcdoctorchat.com/patients/invitation/accept | 2024-01-03T00:00Z |
| 5 | rba-ose.myuhc.com | unknown | ****r | 30-Sep-23 | hxxps://rba-ose.myuhc.com/aa-web/evaluate;sessionId=253ed0ff0b632c57 | 2024-01-03T00:00Z |
| 6 | www.myuhc.com | danonjody420 | *****w420 | 30-Sep-23 | hxxps://www.myuhc.com/member/prewelcome.do | 2024-01-03T00:00Z |
| 7 | provider.umr.com | j.william18 | *****@786 | 14-Oct-23 | hxxps://provider.umr.com/tpa-ap-web/ | 2023-12-24T00:00Z |
| 8 | www.healthsafe-id.com | unknown | *****ns55 | 14-Oct-23 | hxxps://www.healthsafe-id.com/rt/login/myuhc/en | 2023-12-19T00:00Z |
| 9 | www.encoderpro.com | transcure1 | *****2021 | 14-Oct-23 | hxxps://www.encoderpro.com/epro/ | 2023-12-24T00:00Z |
| 10 | identity.onehealthcareid.com | benantbss | *****2022 | 14-Oct-23 | hxxps://identity.onehealthcareid.com/app/index.html | 2023-12-24T00:00Z |
| 11 | healthid.optum.com | p201604 | *****@258 | 14-Oct-23 | hxxps://healthid.optum.com/tb/app/index.html | 2023-12-24T00:00Z |
| 12 | identity.onehealthcareid.com | p201605 | *****7869 | 14-Oct-23 | hxxps://identity.onehealthcareid.com/app/index.html | 2023-12-24T00:00Z |
| 13 | identity.onehealthcareid.com | mehrunfhcadmin134 | *****2116 | 14-Oct-23 | hxxps://identity.onehealthcareid.com/app/index.html | 2023-12-24T00:00Z |
| 14 | identity.onehealthcareid.com | unknown | *****,143 | 26-Oct-23 | hxxps://identity.onehealthcareid.com/app/index.html | 2024-01-03T00:00Z |
| 15 | member-all savers.optum.com | npp123456 | *****2345 | 26-Oct-23 | hxxps://member-all savers.optum.com/tpa-ap-web/ | 2024-01-03T00:00Z |
| 16 | provider.umr.com | j.william18 | *****@786 | 29-Oct-23 | hxxps://provider.umr.com/tpa-ap-web/ | 2024-01-03T00:00Z |
| 17 | identity.onehealthcareid.com | aulislam | *****2478 | 29-Oct-23 | hxxps://identity.onehealthcareid.com/app/index.html | 2024-01-03T00:00Z |
| 18 | healthid.optum.com | kmailm32 | *****p002 | 20-Oct-23 | hxxps://healthid.optum.com/tb/kmailm32login.inf | 2024-01-13T00:00Z |



Real World Consequences of Cyber Incidents

SecurityScorecard | All | Search companies, scorecards, portfolios and tags... | Contact support | Cyber911 | KC

Dashboard | Scorecards | Portfolios | Core Tools | Modules | Professional Services

79 | **Change Healthcare** | changehealthcare.com · Healthcare · 530 followers

Create Action Plan or Score Planner | No artifacts shared | Create Custom Scorecard | In 4 Portfolios | Message Company | More

Score Factors | History | Issues 72 | Compliance | Incidents 4 | Digital Footprint | Vendor Detection | Desktop Analytics | Hierarchy | Evidence Locker | Company Profile | Risk Quantification

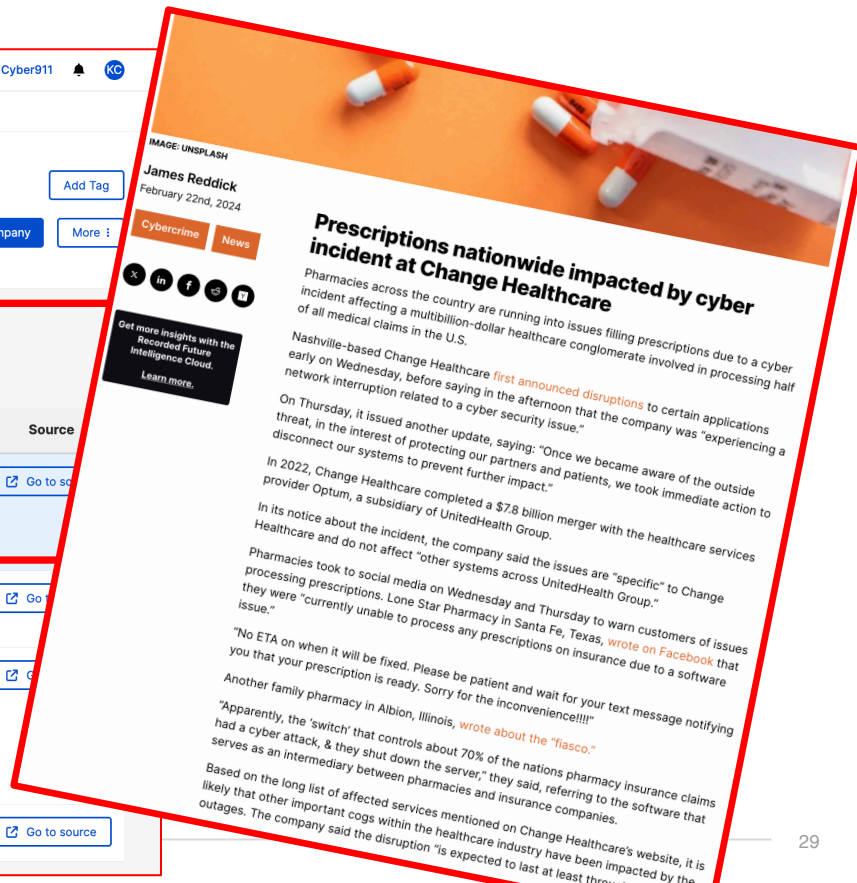
Change Healthcare Scorecard > Incidents

Incidents

| Published Date | Description | Source |
|----------------|---|------------------------------|
| Feb 22, 2024 | Breach A cyber incident affecting Change Healthcare, a healthcare conglomerate, has caused disruptions to prescription processing, with the breach reported on an unspecified date and impacting the company's network and systems. | Go to source |
| Jul 7, 2022 | Paper/Films Change Healthcare Data Security hack as reported to the U.S. Department of Health and Human Services | Go to source |
| Mar 1, 2013 | Breach An employee of the covered entity's business associate (BA) lost a portable thumb drive containing the electronic protected health information (ePHI) of over 6,000 individuals. The ePHI included demographic information, Medicaid identification numbers, and prescription information. The covered entity (CE), Utah Department of Health, provided hack notification to HHS, affected individuals, and the... | Go to source |

Show more

<https://therecord.media/prescriptions-nationwide-impacted-by-change-healthcare-incident>





The MAX/SCDR value



Comprehensive cyber risk visibility

Unified view of security risks, including partners and suppliers



Improved compliance

Aligns with NIST, GDPR, CMMC, and more



Enhanced threat response

Advanced tools for faster detection and mitigation



Expert risk and security guidance

Access to tailored insights from cybersecurity consultants



Measurable results

Track security improvements and justify investments



Fortune 500 scales supply chain resilience

From 50 to **2600 vendors** under management. **Zero business-impacting events.**

Challenge

Reactive and fragmented TPRM program paralyzed by overwhelming supply chain risk

Solution

Drive risk reduction actions throughout all aspects of vendor lifecycle

Next Steps

Accelerate implementation of supply chain security insights and standards for global org

3X

Reduction in high risk vendors

97%

Remediation rate for zero-day incidents

73%

Actively engaged vendors

***“SecurityScorecard MAX** provides us the opportunity to bolster our third-party cybersecurity posture quickly and efficiently through proactive, real-time risk monitoring and remediation.”*

- Director of Technology Risk Management



Desired outcomes

Supply chain resilience

- Gain full visibility into nth-party suppliers and concentration risks
- Reduce the number of supply chain incidents
- Decrease time to respond to supply chain breaches

Regulatory compliance

- Communicate cyber risk strategy and governance
- Standardize vendor security assessments and continuous monitoring
- Meet regulatory requirements and mitigate compliance violation risk

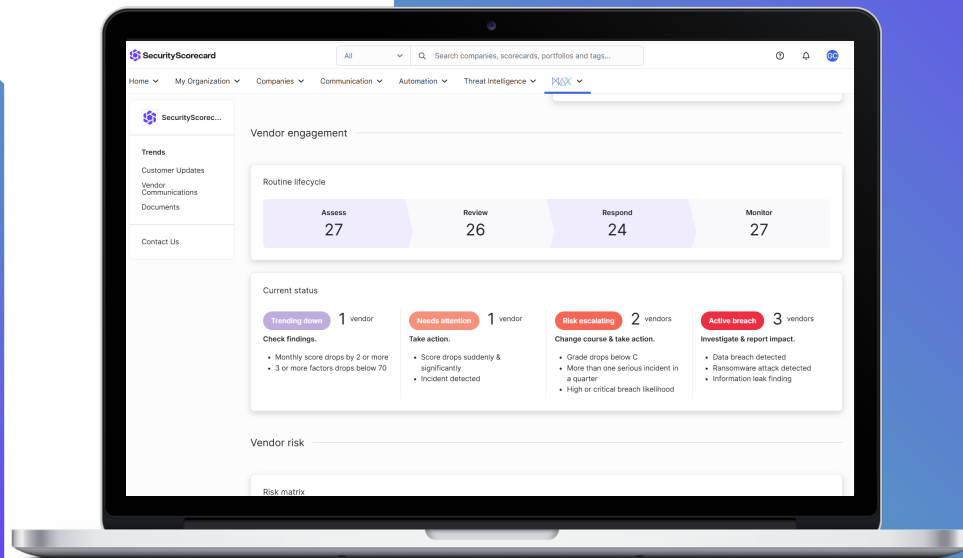
Board assurance

- Secure assets that drive revenue and profitability
- Reduce supply chain cybersecurity costs
- Protect the organization's brand and reputation

Supply Chain Cyber Risk: Your Detailed Analysis

10 vendor investigation reports
evaluating their cybersecurity health
Cyber risk rating of Low, Medium, High, or Critical

3 comprehensive vendor/entity
cybersecurity assessments
Detailed report based on up to 6 months of cyber
hygiene history and digital behaviors



Brian Hanlon brian.hanlon@securityscorecard.io
Major Account Director, Public Sector



Thank you

Brian Hanlon brian.hanlon@securityscorecard.io
Major Account Director, Public Sector