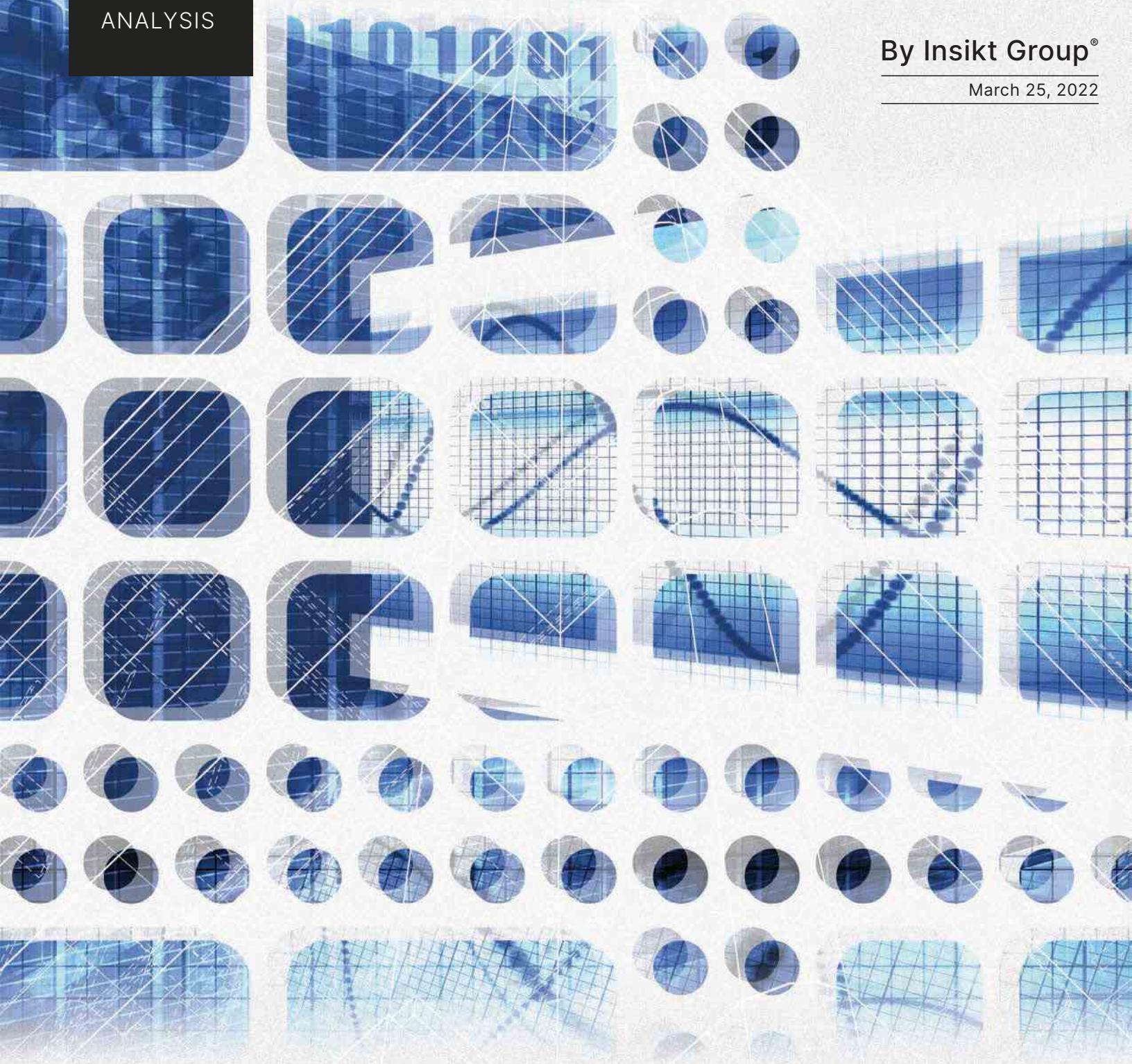
CYBER
THREAT
ANALYSIS

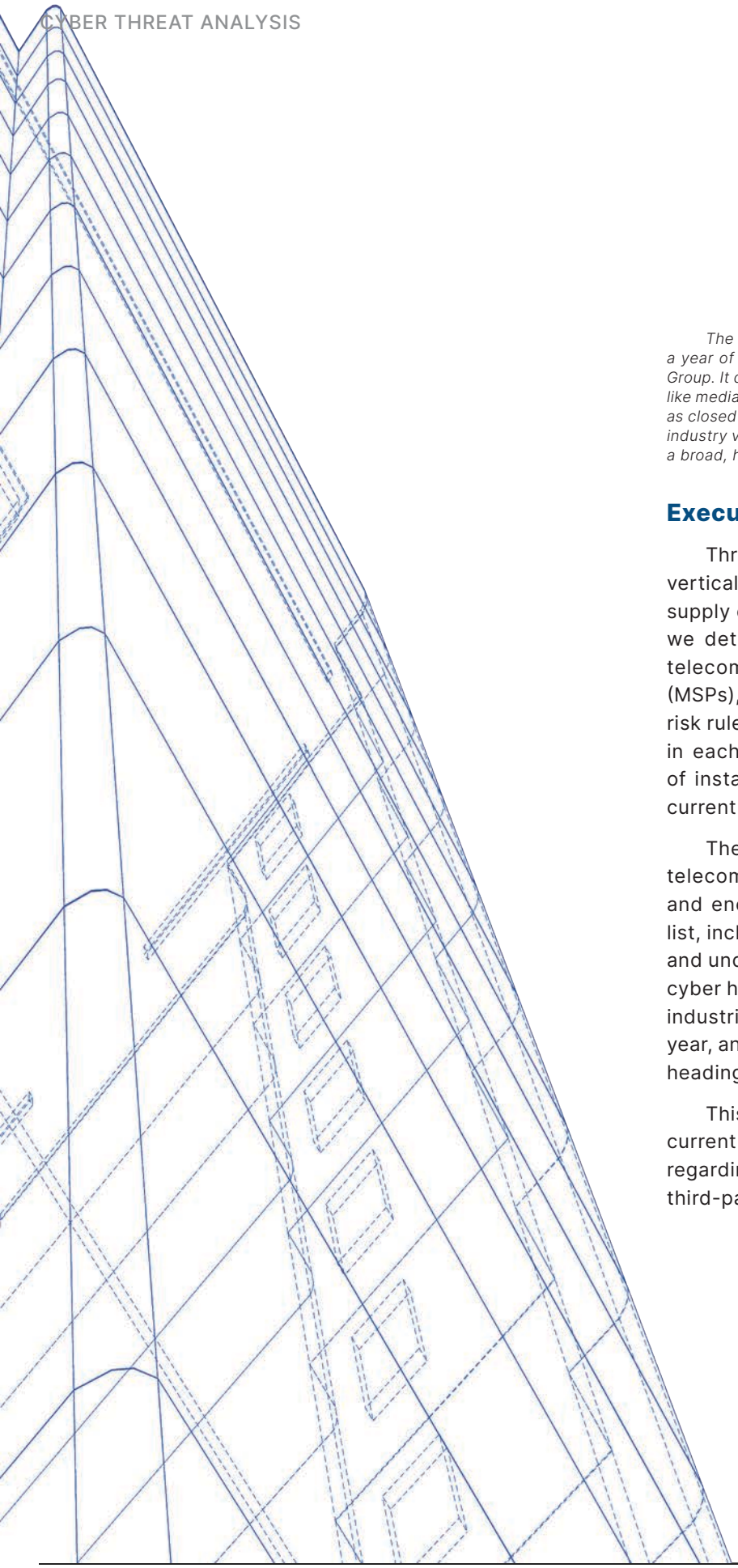
Recorded Future®

By Insikt Group®

March 25, 2022



2021 Third-Party Intelligence Threat Landscape



The annual threat report surveys the threat landscape of 2021, summarizing a year of intelligence produced by Recorded Future's threat research team, Insikt Group. It draws from data on the Recorded Future® Platform, including open sources like media outlets and publicly available research from other security groups, as well as closed sources on the criminal underground, to analyze global risk trends across industry verticals throughout 2021. This report will be of interest to anyone seeking a broad, holistic view of the third-party risk landscape in 2021.

Executive Summary

Throughout 2021, third-party relationships across all industry verticals were put to the test by major data compromises and supply chain attacks. Using Recorded Future Platform risk data, we determined comprehensive risk profiles for 5 industries: telecommunications, healthcare, managed service providers (MSPs), finance, and energy. The trends in the average number of risk rules triggered by the top 25 most referenced organizations in each respective industry vertical and the average number of instances a risk rule was triggered help us understand the current third-party risk landscape in each respective industry.

The industry that triggered the most risk rules in 2021 was telecommunications, followed by healthcare, MSPs, finance, and energy. We considered several factors when making this list, including data breach activity, IP/domain security, dark web and underground forum chatter, leaked credentials, and general cyber hygiene. Doing so gives us a clear understanding of which industries maintained a strong security posture throughout the year, and which are struggling to safeguard against novel threats heading into 2022.

This report is designed to help organizations understand the current risk trends across industries and make informed choices regarding the security health of an industry prior to entering a third-party relationship or acquisition in 2022.

Table of Contents

Industry Risk Trends

In an effort to evaluate the state of third-party intelligence in 2021, we used Platform data to identify the most commonly triggered high- and medium-severity risk rules across 5 major industries, including: finance, healthcare, managed service providers (MSPs), telecommunications, and energy. These industries were chosen for this report based on what we have observed as historical, high-trending threat activity over the past 1 to 5 years. From these industries, we analyzed the 25 most referenced organizations in the Recorded Future Platform for each industry and the number of risk rules triggered by each organization. Selecting these organizations based on reference count is an effective way of understanding the risk rules that were associated with the most prominent threats throughout the year; however, there are likely other data sets to consider for deeper analysis in the future, such as each organization's market share relative to the level of risk associated.

While risk rules triggered, both by quantity and volume, helps us understand the threats associated with each industry, we have also considered the effects of each industry's risk levels on other industries. For example, MSPs did not trigger the most risk rules overall; however, MSPs have greater third-party integration than other industries. Therefore, an attack on an MSP would represent a greater risk to third parties than an attack on a healthcare provider, which is more likely to harm customers and patients rather than industry partners.

From this data, we determined that the industry with the highest likelihood of a compromise affecting third-party partners is MSPs, due to the high volume of integrations between MSPs and third parties, as well as the likelihood that a compromise of an MSP could result in exploitation of other downstream partners. Despite major attacks against Shell, Colonial Pipeline, and Saudi Aramco, Recorded Future risk data indicates that the energy industry triggered the fewest risk rules in 2021, with only 20 high- and medium-severity risk rules triggered and an average of 8 triggered instances per risk rule. The energy sector is also the least likely to be affected by major third-party compromises considering how limited energy sector integration is with partner industries. For a full breakdown of the top 5 risk rules triggered by industry, as well as the high-severity risk rules triggered by industry, refer to Appendices A and B.

Managed Service Providers (MSPs): Increased Public Scrutiny Leads to Improved Security

Considering how 2020 ended and how 2021 began for MSPs, the industry showed signs of improvement throughout the year. In spite of a tumultuous first half of 2021, culminating with the Kaseya supply chain attack in early July, MSPs produced the lowest average instances per risk rule triggered among observed industries with 8. No risk rules triggered by the MSPs analyzed in this report were triggered by more than 17 organizations. The average instances per risk rule across the other 4 industries' top 5 risk rules triggered was 21.7, while MSPs only produced an average of 13.8 across their top 5 triggered risk rules. This likely indicates that, even taking into consideration the large-scale attacks that occurred within the industry throughout 2021, MSPs were not targeted as frequently as other observed industries.

The industry also triggered the second-fewest risk rules overall, with just 20 rules among the top 25 organizations analyzed; further, 71% of references to cyber events related to the MSP industry occurred in the first half of 2021. Credential and email exposure was also lowest among observed industries, though as previously mentioned, this does not necessarily indicate that threat actors have no credentials to leak. One possibility is that they are biding their time following a successful first half.

Where MSPs still struggle in relation to other industries is with a relatively high number of technologies deployed that are associated with high-risk vulnerabilities or unsupported versions. This explains the nature of the biggest MSP compromises in 2021: both the Accellion compromise and the Kaseya attack were the result of successful exploitation of zero-day vulnerabilities residing in technologies deployed either by the company itself (Kaseya) or consumers deploying a compromised technology (Accellion FTA).

It appears MSPs have turned things around following a catastrophic first half of the year. However, organizations seeking to establish a third-party relationship with an MSP in 2022 should still proceed with caution, as the scope of the data is limited. Relationships with MSPs should come under deep scrutiny due to the nature of the data-sharing relationships MSPs have with their customers. As observed following last year's SolarWinds attack and the Accellion compromise this year, a successful attack on an MSP can lead to follow-on attacks potentially targeting thousands of downstream customers.

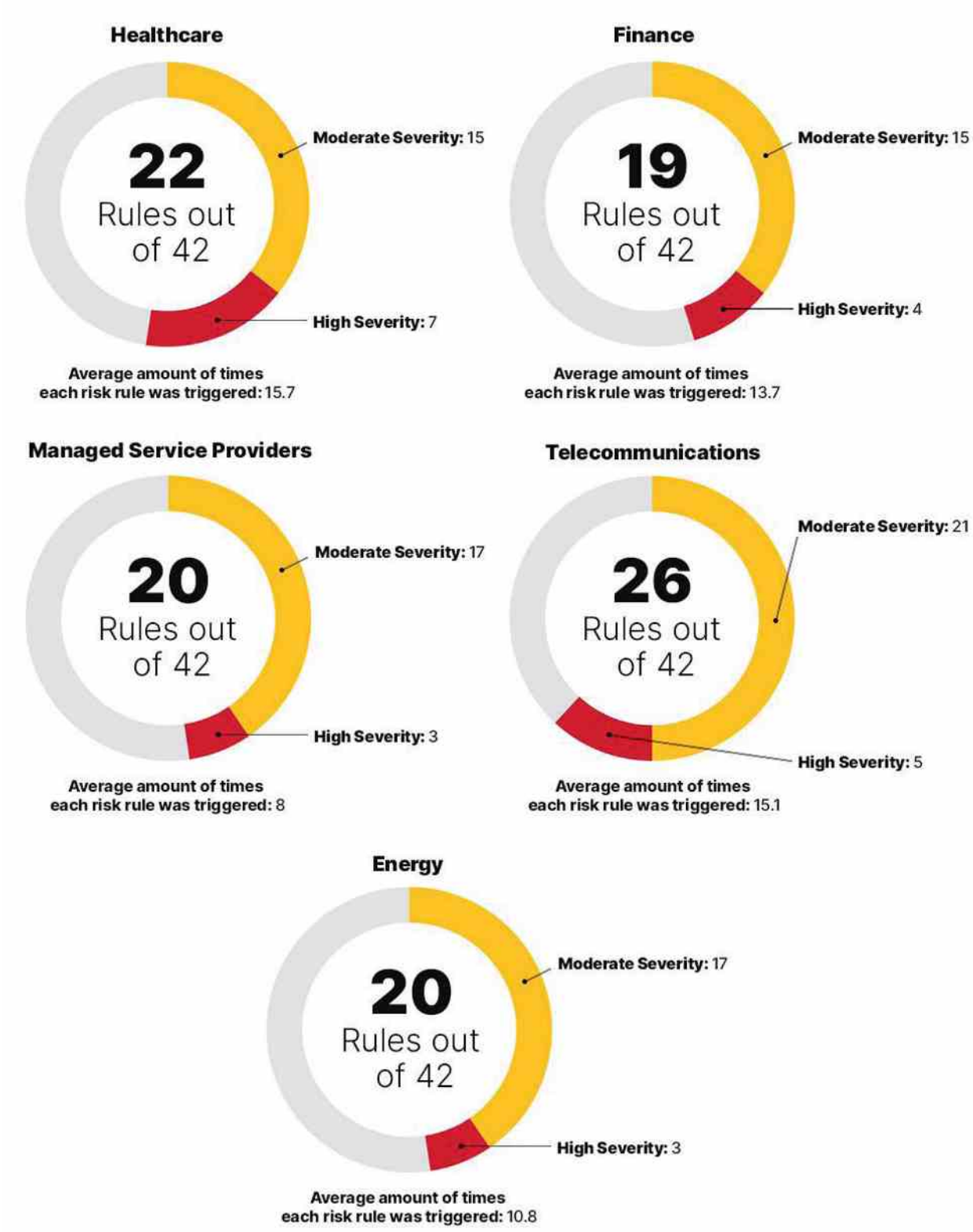


Figure 1: Recorded Future Platform risk rules triggered by industry (Source: Recorded Future)

Platform data suggests that the industry has made a concerted effort to shore up its defenses in the face of growing media scrutiny and, as a result, many MSPs have improved their public image heading into the new year. Overall, the industry's risk profile indicates that MSPs have come a long way since this time last year.

Telecommunications: Threat Actors Swoon Over Industry-wide Weaknesses

According to Recorded Future Platform data, the telecommunications industry represents the greatest level of risk to third-party partners in terms of cyber compromise or disruption in 2021, due to several factors. First, out of the 5 observed industries, the top 25 telecommunications companies triggered the most risk rules, with 26 out of 42. It can be inferred that a greater number of risk rules triggered is indicative of a wider attack surface industry-wide. Compared to other observed industries in this report, the industry triggered the largest number of high-severity risk rules by a very wide margin. At the time of writing, telecommunications companies have triggered 40 high-severity risk rules, with the next closest industry being MSPs with 10. This is an indication that not only is telecommunications industry risk heightened by the volume of risk rules triggered, but the severity of an attack is likely to be greater than in other industries.

High-profile attacks on the industry throughout 2021 likely attracted further interest from threat actors. Since December 30, 2020, telecommunications giant T-Mobile has been the victim of 4 cyberattacks (1, 2, 3, 4), resulting in the exposure and theft of personally identifiable information (PII) from millions of T-Mobile customers. US Cellular ended 2021 as it began, with threat actors accessing customer PII in January and December 2021. SingTel, Singapore's largest mobile carrier, announced that it had fallen victim to the Accellion FTA compromise in February, potentially exposing the PII data of a large percentage of its customer base. In essence, the data indicates that security gaps in the telecommunications industry are substantial and bountiful, and threat actors are flocking to the industry for easy wins.

For companies who have third-party partnerships with telecommunications providers, now is the time to review these relationships and take action as necessary. With respect to overall cyber activity, 2021 was a terrible year for the industry. Taking this into account along with the current state of the industry's risk profile, we are skeptical that the situation will improve heading into 2022. Furthermore, the likelihood of a major attack is greater than the other observed industries, due to the comparatively large number of high-severity risk rules triggered. Like MSPs in 2021, perhaps the telecommunications industry would benefit from greater public scrutiny in 2022 as added motivation to reduce its risk level. The industry is responsible for far too much PII and operational data, both in terms of sensitivity and quantity, for it to afford to have another year like 2021.

Healthcare: Too Many Security Gaps for Such Sensitive Data

Healthcare, another industry with too much at stake to be this high up the list, represents the third-greatest risk of compromise to third-party partners in 2021. With 22 risk rules triggered, it may not have the breadth of attack opportunities that the telecommunications industry has, but it does boast the highest rate of instances per risk rule triggered, with an average of 15.7 instances of companies triggering a risk rule, compared to telecommunications, which produced 15.1 instances across 26 rules. Working in the healthcare industry's favor is the fact that, relative to the telecommunications industry, the majority of risk rules triggered are of medium severity: healthcare is tied for third in our list of triggered high-severity risk rules, with 7.

The issues arise for the healthcare industry in the volume of organizations deploying websites with unsupported technology versions and associated with technologies with high-risk vulnerabilities. Of the 5 industries in this report, it is the only industry in which all 25 companies analyzed triggered risk rules for "Company Website Using Technology Version With High-Risk Vulnerability" and "Company Website Using Unsupported Technology Version". This is cause for concern: operating technologies with known, high-severity CVEs increases the risk of data exfiltration, unauthorized access to sensitive information systems, website exploitation, or attack. Also, unsupported software no longer receives product support or updates. Existing or newly discovered vulnerabilities will never receive an official patch. Compared to other industries, the healthcare sector prioritizes patient privacy over general system security due to the strict standards and hefty penalties imposed on healthcare organizations by HIPAA. This likely results in hospitals and patient care facilities overlooking systems in their network that do not explicitly handle patient data. The issue is further complicated by the lack of cybersecurity professionals in the healthcare sector capable of recognizing vulnerabilities within their networks.

Lackluster public-facing security controls and the ongoing COVID-19 pandemic made the healthcare industry a prime target for ransomware operators and threat actors seeking to exploit zero-day vulnerabilities in global healthcare networks in 2021. In February, the South Korean government announced that Pfizer was likely the target of a data exfiltration attack by North Korean organizational threat actors, resulting in the theft of valuable COVID-19 vaccine and treatment data. In May, Health Service Executive, the publicly funded healthcare system in the Republic of Ireland, took its IT systems offline in response to a ransomware attack that a Health Service Executive (HSE) spokesperson described as "significant". The attack and the resulting shutdown affected many different services, including COVID-19 testing and hospital appointments, with some hospitals having to cancel all but the most urgent outpatient appointments. Just a month later, San Diego-based Scripps Health fell prey to a ransomware attack that resulted in the exfiltration of nearly 150,000 patients' PHI data. The theme throughout these events was the exploitation of zero-day vulnerabilities in public-facing systems, a trend reflected by Recorded Future Platform data.

Organizations considering a third-party partnership with a healthcare or health insurance provider in 2022 are strongly advised to carry out thorough security audits of website technologies deployed before agreeing to do business. Healthcare organizations are responsible for safeguarding some of our most sensitive information, and due to the lack of effective security controls, hospitals prioritizing patient data privacy over general system security, and a growing deficit in qualified cybersecurity professionals in the industry, these organizations are finding it more and more difficult to cope with this burden as threat activity increases. Based on the industry's current risk profile, combined with the success experienced by threat actors targeting the industry in 2021, we are likely to continue to see more of the same in 2022. Healthcare organizations must come to terms with the vital role they play in our lives and act accordingly to safeguard patient data if they hope to buck this downward trend.

Finance: Still a Valuable Target in the Eyes of Threat Actors, Despite a Strong Security Posture

Recorded Future Platform data shows that, of the observed industries in this report, the finance industry triggered the fewest risk rules with 19, yet trigger instances were high, with an average of 13.7 instances per risk rule triggered. Coupled with the second-highest rates of dark web and high-tier underground forum references, it seems that while finance industry security controls appear to be strong, it does not appear to be stopping threat actors from targeting financial institutions. This is likely because the earnings potential of a successful attack on a financial institution is greater than other industries, thanks to the value of the data they store. However, Platform data likely also includes discussions around committing fraud against financial customers or exploiting fintech infrastructure to move and launder money, which represent less significant threats to financial organizations and more to their customers. According to Recorded Future data, the financial industry was the industry most associated with cyber threat activity of the observed industries in 2021.

Another cause for concern for the financial industry is the high volume of credential and email address exposure industry-wide, although this is not necessarily an indication that observed leaked credentials are associated with recent cyber events. For example, it has been documented that threat actors will sit on stolen data for months, sometimes years, before sharing publicly, depending on their motive.

Several high-profile customer data breaches affected the financial industry in 2021 and threatened to tarnish the reputations of security teams across the sector. In May, French insurance firm AXA was struck by Avaddon Ransomware, resulting in the exposure of customer PII data across Southeast Asia. The Accellion compromise in July resulted in the exposure and theft of personal information of some Morgan Stanley customers. Just a few weeks after Morgan Stanley was hit, BRI Life, the insurance arm of Indonesia's Bank Rakyat Indonesia (BRI), reported that unknown threat actors published the firm's data. The incident involved a collection of 460,000 documents compiled from the user data of over 2 million BRI Life clients that were allegedly advertised in the underground forum Raid Forums by an unnamed threat actor.

We will continue to observe trends in the finance industry in 2022 with optimistic forecasts, considering the industry's current risk profile, as well as what appear to be strong security controls. Vendors seeking to do business with financial institutions in the new year would be wise to research past data breaches and dark web activity for credential leaks that threaten both internal and customer-facing systems. Based on the broad effects of supply chain compromises such as Accellion, as well as the disclosure of prominent vulnerabilities like Log4Shell, we anticipate some activity from 2021 to spill into 2022 while finance organizations continue to shore up their defenses. However, as a result of strong overall security controls industry-wide, coupled with new regulatory bodies like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act forcing financial institutions to implement cybersecurity controls that prioritize consumer rights and data privacy, we anticipate a continued downward trend in successful threat activity targeting the industry.

Energy: Major Attacks Aside, The Overall Industry Risk Profile Inspires Hope for 2022

According to Recorded Future risk data, the energy sector triggered the fewest risk rules in 2021 out of the pre-selected industries based on a number of factors. This shows the industry's willingness to bounce back after major attacks throughout the year targeting Shell, Colonial Pipeline, and Saudi Aramco. First, of the observed industries analyzed in this report, the energy industry produced the second fewest triggered risk rules with 20, as well as the second-lowest average instances per risk rule with 10.75. Both these are strong indicators of healthy security industry-wide. While these are not the lowest numbers observed in this report, the energy sector triggered the least attention on high-tier and dark web forum sources. Where the other observed industries triggered "High Volume of Attention on High-Tier Forums" an average of 20.5 times and "High Volume of Attention on Dark Web Markets" an average of 22 times, the energy sector produced 10 and 5 instances for each rule, respectively.

This suggests that threat actors are beginning to understand the difficulty, the potential consequences, and the futility of targeting the energy sector, considering the lack of monetizable data for which energy organizations are responsible. It is possible that the geopolitical backlash as a result of the Colonial Pipeline attack in May caused threat actors to reconsider before targeting energy companies again.

Overall, Recorded Future Platform risk data indicates a strong security posture for the energy sector. Because energy companies rely less on public-facing platforms like other industries in this report, it should not come as a surprise to see fewer risk rules triggered. However, the data suggests that the energy sector does struggle to maintain healthy general cyber hygiene. Compared to other observed industries throughout this report, the energy sector produced the most triggered domain security risk rules. The current risk profile snapshot for the industry produces the most instances of "Domain With Insecure SSL Protocol" and "Domain With Self-Signed SSL/TLS Certificate" risk rules.

While the energy sector was the subject of some major news headlines in 2021, Recorded Future data indicates that the industry is well poised to handle potential challenges in 2022. Beneath the high-profile attacks, the industry's attack surface remains small relative to other industries. This likely means we may continue to see the occasional large-scale attack succeed, but the volume of attacks across the industry should remain low. The industry has to be cautious of ransomware attacks carrying over from the previous year, though it appears threat actors may be more cautious following the Colonial Pipeline event. Organizations looking to do business with energy partners in 2022 would benefit from reviewing prospective organizations' cyber hygiene and emphasizing domain security to ensure a strong, public-facing security apparatus.

Appendix A: Top 5 Risk Rules Triggered by Industry

MSPs

Top 5 Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Domain With Ineffective HSTS Configuration	Hygiene	Company domain with ineffective HSTS max-age configuration.	Current	17
Company Website Using Technology Version With High-Risk Vulnerability	Other	Company websites are running products affected by high-risk CVEs. Different patching methods and software fixes should be taken into account when reviewing this information.	All Time	15
High Volume of Attention on Dark Web Markets	Dark Web	Dark Web Market users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	15
High Volume of Attention on High-Tier Forums	Dark Web	Dark Web High-Tier Forum users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	12
Domain With Insecure SSL Protocol	Hygiene	Company domain using SSL 2.0 or SSL 3.0 protocols.	Current	10

Telecommunications

Top 5 Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Company Website Using Technology Version With High-Risk Vulnerability	Other	Company websites are running products affected by high-risk CVEs. Different patching methods and software fixes should be taken into account when reviewing this information.	All Time	25
Company Website Using Unsupported Technology Version	Technology	Company website is running a software version that is no longer supported by the manufacturer. (See Unsupported Technology Versions)	All Time	25
Domain With Ineffective HSTS Configuration	Hygiene	Company domain with ineffective HSTS max-age configuration.	Current	24
Domain With Overly Permissive SPF Record	Hygiene	Company domain has a loose policy statement.	Current	23
High Volume of Attention on High-Tier Forums	Dark Web	Dark Web High-Tier Forum users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	22

Healthcare

Top 5 Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Company Website Using Technology Version With High-Risk Vulnerability	Other	Company websites are running products affected by high-risk CVEs. Different patching methods and software fixes should be taken into account when reviewing this information.	All Time	25
Company Website Using Unsupported Technology Version	Technology	Company website is running a software version that is no longer supported by the manufacturer. (See Unsupported Technology Versions)	All Time	25
Domain With Ineffective HSTS Configuration	Hygiene	Company domain with ineffective HSTS max-age configuration.	Current	24
Domain With Overly Permissive SPF Record	Hygiene	Company domain has a loose policy statement.	Current	23
High Volume of Attention on High-Tier Forums	Dark Web	Dark Web High-Tier Forum users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	22

Finance

Top 5 Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
High Volume of Attention on High-Tier Forums	Dark Web	Dark Web High-Tier Forum users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	23
High Volume of Attention on Dark Web Markets	Dark Web	Dark Web Market users have extensively talked about your company, sold accounts to your platform, or discussed using your platform for suspicious activities.	All Time	23
Domain With Ineffective HSTS Configuration	Hygiene	Company domain with ineffective HSTS max-age configuration.	Current	22
Recent Typosquat Similarity to Company Domain - DNS Sandwich	Domain	A high volume of typosquats were detected as DNS Sandwich typosquats (e.g. excitingoffer.recordedfuture.com.suspicious.site.com)	Last 90 Days	21
Company Website Using Technology Version With High-Risk Vulnerability	Other	Company websites are running products affected by high-risk CVEs. Different patching methods and software fixes may should be taken into account when reviewing this information.	All Time	19

Energy

Top 5 Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Domain With Ineffective HSTS Configuration	Hygiene	Company domain with ineffective HSTS max-age configuration.	Current	20
Company Website Using Unsupported Technology Version	Technology	Company website is running a software version that is no longer supported by the manufacturer.	All Time	20
Domain With Insecure SSL Protocol	Hygiene	Company domain using SSL 2.0 or SSL 3.0 protocols.	Current	17
Domain With Self-Signed SSL/TLS Certificate	Hygiene	Company domain where subject and issuer names are the same.	Current	16
Company Website Using Technology Version With High-Risk Vulnerability	Other	Company websites are running products affected by high-risk CVEs. Different patching methods and software fixes may should be taken into account when reviewing this information.	All Time	15

Appendix B: High Risk Rules Triggered by Industry

MSPs

High Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Recent High-Impact Abuse of Company Infrastructure	IP Address	Hosting Command & Control server or URL, Hosting Phishing site or URL, or Hosting Malware download site or URL.	Last 56 Days	6
Recent Single-Document Credential Exposure	Leaked Credentials	Company email addresses with passwords were seen on a single source in the last 90 days for the first time (newly observed by Recorded Future).	Last 90 Days	3
Domain with Unrestricted SPF Record	Hygiene	Company domain has an unrestricted policy statement (+all).	Current	1

Telecommunications

High Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Recent Single-Document Credential Exposure	Leaked Credentials	Company email addresses with passwords were seen on a single source in the last 90 days for the first time (newly observed by Recorded Future).	Last 90 Days	14
Recent High-Impact Abuse of Company Infrastructure	IP Address	Hosting Command & Control server or URL, Hosting Phishing site or URL, or Hosting Malware download site or URL.	Last 56 Days	10
Hosts Recently Communicating With C&C Server	IP Address	An IP address belonging to the company has been observed recently communicating to a known malware command and control server on uncommon ports.	Last 30 Days	9
Domain with Unrestricted SPF Record	Hygiene	Company domain has an unrestricted policy statement (+all).	Current	4
Recent Validated Cyber Attack	Breach or Incident Reporting	Insikt Group assessed/validated a significant cyber event affecting this company in the last 90 days.	Last 90 Days	3

Healthcare

High Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Recent Security Breach Disclosure	Breach or Incident Reporting	Company reported a data breach in the last 90 days.	Last 90 days	1
Domain with Unrestricted SPF Record	Hygiene	Company domain has an unrestricted policy statement (+all).	Current	2
Likely IT Policy Violation	IP Address	Hosting a TOR network node.	Current	1
Recent High-Impact Abuse of Company Infrastructure	IP Address	Hosting Command & Control server or URL, Hosting Phishing site or URL, or Hosting Malware download site or URL.	Last 56 Days	2
Recent Single-Document Credential Exposure	Leaked Credentials	Company email addresses with passwords were seen on a single source in the last 90 days for the first time (newly observed by Recorded Future).	Last 90 Days	1
Cyber Exploit Signal: Critical	Other	Current Cyber Exploit Reporting trend analytic is at Critical level.	Current	1
Domain With DKIM Record With Weak Encryption	Hygiene	Company domain with a DKIM record that has an encryption strength less than 1024 bits.	Current	1

Finance

High Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Recent Single-Document Credential Exposure	Leaked Credentials	Company email addresses with passwords were seen on a single source in the last 90 days for the first time (newly observed by Recorded Future).	Last 90 Days	5
Recent High-Impact Abuse of Company Infrastructure	IP Address	Hosting Command & Control server or URL, Hosting Phishing site or URL, or Hosting Malware download site or URL.	Last 56 Days	2
Domain with Unrestricted SPF Record	Hygiene	Company domain has an unrestricted policy statement (+all).	Current	1
Cyber Exploit Signal: Critical	Other	Current Cyber Exploit Reporting trend analytic is at Critical level.	Current	1

Energy

High Risk Rules Triggered				
Rule Name	**Category**	**Description**	**Time Frame**	**# of Affected Organizations**
Recent Validated Cyber Attack	Breach or Incident Reporting	Insikt Group assessed/validated a significant cyber event affecting this company in the last 90 days.	Last 90 Days	3
Recent Single-Document Credential Exposure	Leaked Credentials	Company email addresses with passwords were seen on a single source in the last 90 days for the first time (newly observed by Recorded Future).	Last 90 Days	1
Domain with Unrestricted SPF Record	Hygiene	Company domain has an unrestricted policy statement.	Current	1

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About the Author

Andrew McIntyre

Threat Intelligence Analyst, Insikt Group®

Andrew McIntyre has been a cyber threat intelligence analyst with Recorded Future's Insikt Group since 2021. His research covers a range of topics including third-party intelligence, geopolitical trends, and threats to military veterans organizations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.