ARCTIC WOLF

ARCTIC WOLF

SECURITY OPERATIONS

2024 REPORT

TABLE OF CONTENTS

FOREWORD

While it's largely become a cliché in cybersecurity circles to talk about the evolving threat landscape, the reality is that such language is entirely justified. All manner of threat actors — from nation-state agencies, to ransomware groups, to hacktivists, to individuals — continually discover and refine their tactics, techniques and procedures (TTPs). These advancements push the leading edge of cyber attacks, putting pressure on defenders to keep up.

At the same time, IT environments are continually changing, with relatively recent examples including adoption of software-as-a-service (SaaS), remote work, and the increasing role of identity and access management (IAM). Each of these changes introduce new risks for organizations and new challenges for cyber defenders; collectively, they represent a massive transformation in a very short time.

Yet, the more things change, the more they stay the same. Organizations still have endpoints: laptops, workstations, servers, Internet of Things (IoT) devices, and more — and still run operating systems and software clients. And, of course, they still have people, with all of their associated strengths and weaknesses.

Attackers still employ tried-and-true approaches like social engineering and enjoy considerable success exploiting vulnerabilities for which patches were issued years ago. Some months, we see **500% more phishing activity than others**, as attackers work around the clock to best leverage the distraction of their targets **(45% of alerts were generated outside of weekday working hours,** with an additional **20% generated on weekends)**. Even more, wide-scale IT outages and global instability compound challenges for security teams, and even the most prepared organizations have experienced the inescapability of Murphy's Law.

So while cyber defenders go to great lengths to stay up to date, they can't lose sight of the past. Viewed through this lens, cyber defense is a challenge that grows larger by the day.

Arctic Wolf is in the unique position of providing security operations to thousands of organizations of all sizes and in practically all industries around the world, and we consider it both a privilege and a responsibility to share insights gleaned from more than **253 trillion observations** over 12 months across this diverse install base. Using the right combination of people, process, and technology, we sift through those hundreds of trillions of data points to distill **a single alert for every 100 million observations**, freeing our customers' security teams to focus only on critical issues without interrupting operations.

The dominant theme of this report is that organizations with 24x7 security operations are much better able to defend themselves against modern attacks. While the threat landscape may be daunting, there is hope for those who can effectively operationalize their investments in cybersecurity.

In this report, we'll cover:

- Which global events influenced a spike in activity from threat actors
- The industries most at risk for cyber incidents
- The top 10 threats or indicators of compromise (IOCs) leading to alerts
- Technology and processes that provide the best defense against sophisticated attacks
- Hopeful indicators of progress against ransomware attacks, **with only 2% of Arctic Wolf customers experiencing the impacts of a ransomware event vs. an industry average of 45%**

Drawing upon our own experiences, this report presents a mix of aggregate observations, security trends, and examples that illustrate the evolving threat landscape, while also providing guidance to help organizations and other cyber defenders benefit from the same insights we leverage to protect our customers every day.

After reading this report, you'll not only come away with a more comprehensive view of the threats against your own organization, but — crucially — with some actionable ideas on how to reduce your own cyber risk.

Mark Manglicmot,
Senior Vice President, Security Services

KEY TAKEAWAYS

The following information comes from the Arctic Wolf® Platform and our customers' experiences, highlighting the key security findings for 2024 that we discuss in this report. Below are our top takeaways.

45%

45% OF ALERTS ARE GENERATED AFTER HOURS AND 20% TAKE PLACE OVER THE WEEKENDS.

Threats don't take time off. We found that 45% of incidents are alerted outside of traditional working hours. Furthermore, 20% of alerts were found to occur on the weekend, highlighting the need for 24x7 security operations.

ONE ALERT OCCURS FOR EVERY 100 MILLION PIECES OF OBSERVATIONAL DATA.

Identifying a threat is finding a needle in a telemetry haystack. In order to detect a threat, it is crucial to maintain a high level of visibility into all aspects of an environment, but without the proper processes in place to reduce access noise, this amount of telemetry data can become overwhelming and detrimental.

THE MOST EXPLOITED APPLICATIONS ARE ONES USED FOR CORE BUSINESS FUNCTIONS.

Compiling the top five applications attackers most often attempted to exploit in the past 12 months resulted in a list composed of critical business tools such as Microsoft Outlook, Windows 10, and Cisco IOS. This shows that organizations must be prepared for an inherent baseline level of risk in any modern network.

IDENTITY AND ACCESS MANAGEMENT (IAM) TELEMETRY IS THE MOST COMMON SOURCE OF EARLY DETECTION.

IAM telemetry made up seven of the top 10 indicators of compromise that lead to security investigations. That's because unauthorized or suspicious usage of credentials is an early indicator of a threat actor. Unfortunately, IAM telemetry is plentiful and can be burdensome, which requires a strong process to eliminate noise.

26%

26% OF ALERTS ISSUED WERE THREATS TARGETING MANUFACTURERS.

At the beginning of 2024, Arctic Wolf® Labs warned that nation-state actors would attempt to target manufacturers to obtain intellectual property (IP) and trade secrets. Reviewing alerts issued for this report revealed that over a quarter were related to threats targeting organizations focused on manufacturing, fulfilling that prediction.

KEY TAKEAWAYS, CONTINUED.

+500%

A 500% INCREASE IN PHISHING ACTIVITY WAS OBSERVED IN ONE MONTH.

Phishing is one of the most effective ways for an attacker to obtain sensitive information, with widespread phishing campaigns attempting to leverage world events, including political news and natural disasters, to increase the likelihood of their success. We observed one such surge in April 2023 with a 500% increase in phishing attempts. Interestingly, this spike coincided with high-stakes news events such as a state grand jury formally issuing criminal charges against former U.S. President Donald Trump, as well as President Biden officially announcing his reelection campaign, in addition to a series of devastating tornadoes ripping through the central U.S. In April 2024, we also saw a 150% increase in phishing attempts which corresponded with other political announcements and occurrences, including controversial state Supreme Court rulings in Arizona, ongoing Russia-Ukraine and Israel-Hamas conflicts, and damaging extreme weather events in the southern and central U.S.

+2000

WE OBSERVED OVER 2,000 INSTANCES OF WIN32.ZBOT TROJAN OCCURRING WEEKLY.

Obtaining user credentials is often a primary goal for threat actors since it greatly increases the likelihood of a successful attack. That is why attackers will leverage commodity malware like trojans as a method to steal this data. Throughout the year, a steady stream of weekly detections related to the popular Win32.Zbot trojan occurred in amounts ranging from 100 instances to campaigns of over 2,000 weekly detections occurring for multiple weeks.

THE GLOBALPROTECT ZERO-DAY EXPLOIT LED TO 171 INVESTIGATIONS AND ZERO CASES OF IDENTIFIED RANSOMWARE OR DATA EXFILTRATION.

When the CVE-2024-3400 zero-day appeared as a 10.0 CVSS vulnerability, Arctic Wolf executed the mega event strategic high-touch runbook, finding more than 1,800 customers utilizing Palo Alto firewalls. Initial detections showed multiple waves of attacks — including 13 in a single day. The results included 171 security investigations, the development of new intelligence, implementation of new threat detections, and zero cases of identified ransomware execution or data exfiltration.

PREVENTING IMPACTS OF RANSOMWARE IS ATTAINABLE WITH SECURITY OPERATIONS.

May 2023 through April 2024 saw 56,000 potential ransomware-related indicators of compromise observed, yet less than 2% of Arctic Wolf customers experienced any impact from ransomware events in this 12-month period – **drastically below the industry average of 45%** reported in the 2024 Arctic Wolf Trends Report (published May 2024).

SPECIAL MENTION: AN UPDATE ON REAL-WORLD OUTAGES

On July 19, 2024, our industry faced an unprecedented IT outage of over 8.5 million devices — the largest in history. Although this event occurred after the data collection period for this report, we believe it's crucial to highlight how our security operations team navigated this crisis and supported our customers so you too can learn from the experience.

At approximately 12 a.m., our Security Operations Center (SOC) proactively detected a loss of telemetry from CrowdStrike customers. We immediately alerted the affected customers, even before the full scope of the global event was understood. Thanks to the broad integration of data sources within our platform, we were able to intensify alerting for the telemetry sources that remained online. This was a critical step, as adversaries quickly sought to exploit the chaos and disruptions caused by the outage.

> **Our top priority was helping our customers restore their operations and ensure they were not compromised while recovery was in progress. Our security team worked hand-in-hand with customers, providing technical support and instructional videos on how to remediate the issue. We kept them informed with proactive updates from Microsoft and CrowdStrike as they became available.**

Our unique Concierge Delivery Model was built precisely for moments like these. While such massive outages are rare, they share characteristics with all-too-common security incidents. Security is a collaborative effort, and the best outcomes occur when customers have direct access to experts who understand their environment, business, and team. The last thing you want during a major incident is to find yourself speaking to someone for the first time, trying to explain both who you are and what is happening. In many cases, support from the impacted vendor is hard to access or delayed, leaving customers scrambling for immediate assistance.

This recent IT event is just another reminder of the importance of preparation. To be ready for such incidents, it's essential to ensure you have the right people, processes, and technology in place to:

- Continuously monitor your environment, even if a key technology or telemetry source goes offline
- Collaborate with a diverse set of vendors to avoid over-reliance on a single platform
- Develop a plan with your security partners for when things go wrong
- Adopt a security operations approach to minimize your overall risk

Although we sympathize with all of those who were affected by this outage, it is also important to acknowledge the important lessons learned. While no vendor is immune to the potential for outages, whether they originate from attackers or internal misconfigurations, this situation highlights the critical need to eliminate single points of security failure.

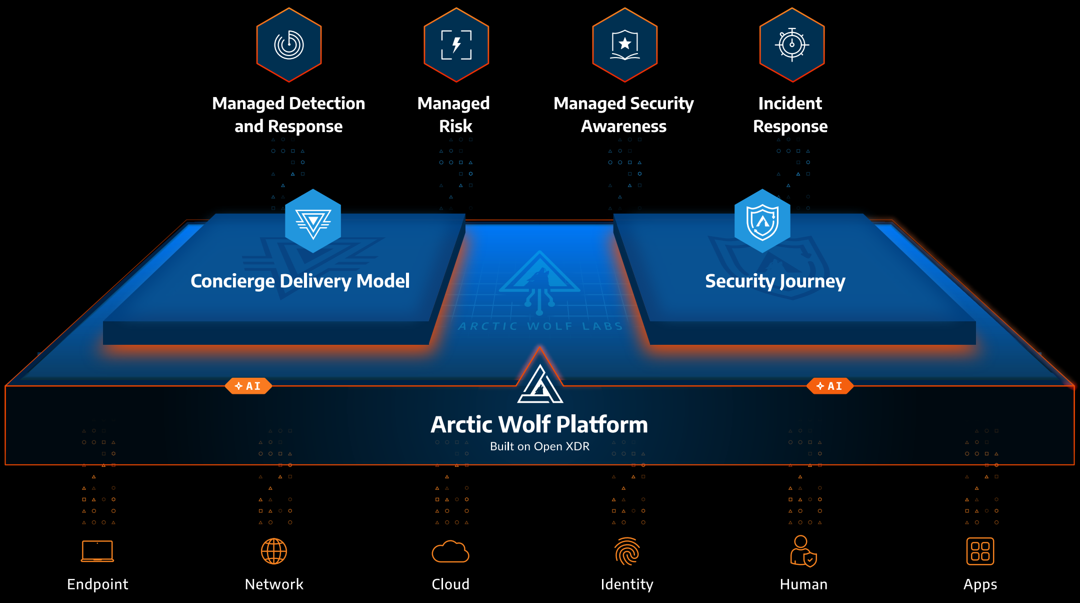
> **Instead, effective security operations gained from skilled security engineers paired with the power of an open-XDR platform can ensure your ability to detect and respond to even the greatest threats in unprecedented times of crisis.**

DATA SOURCES

While we also cite past Arctic Wolf publications and third-party sources, the majority of the facts, figures, and statistics in this report are based upon 253 trillion analyzed observations made from May 1, 2023, through April 30, 2024, across our global customer base of more than 6,500 organizations.

These observations are augmented by ~57,000 Security Posture In-Depth Reviews (SPiDRs) — a combination of Arctic Wolf-led security assessments, configuration reviews, and best practice knowledge transfers that help customers improve their security posture.

Powering this scale is the Arctic Wolf® Security Operations Cloud — a purpose-built, vendor-neutral platform that ingests, enriches, and analyzes our customers' security data and enables our teams to rapidly and effectively find signal in an otherwise overwhelming volume of noise.



Feeding this platform is more than a petabyte of data per day originating from:

~4.3 MILLION	~33,000	~22,000	~5,600
Agents active within customer environments	Network sensors	Cloud sensors	Scanners

ARCTIC WOLF LABS

Making behind-the-scenes contributions to this report is Arctic Wolf Labs, which brings together elite multidiscipline security professionals to deliver cutting-edge threat intelligence and security research, develop advanced threat detection models, and drive continuous improvements in speed, scale, and efficacy.

MANAGING CYBER RISK IN TODAY'S THREAT ENVIRONMENT

KEY TAKEAWAYS:

A security operations (SecOps) approach that aligns with the NIST Cybersecurity Framework 2.0 is a proven way to assess, mitigate, and transfer cyber risk.

Around-the-clock monitoring is a modern-day necessity — 40-45% of incidents we encounter are identified outside of traditional working hours, with 16-20% occurring on the weekend.

SecOps teams should aim to simultaneously achieve a low false-negative rate and a high true-positive rate, but doing so is a tremendous challenge due to the sheer volume of security telemetry.

The Role of Security Operations

To address today's cybersecurity challenges, we believe organizations should take measures to assess, mitigate, and transfer their cyber risk.

A proven enabler of this ongoing journey is SecOps, which refers to the people, processes, and technology that all work together as a central hub to create and manage a security architecture for an organization.

Whether delivered by an internal team, an external service provider, or a hybrid combination of both, benefits of a SecOps-oriented model include:

- Faster responses to threats and incidents, as measured by mean time to detect (MTTD) and similar metrics
- The stopping of potential threats before they become breaches
- More effective and efficient identity and access management
- Continually improved security posture
- A more unified approach to security

Rather than reinventing the wheel, many security operations teams choose to follow a framework to help guide their responsibilities — with one of the most common being the **NIST Cybersecurity Framework (CSF) 2.0**. Under this version of the CSF, a new function, Govern, has been added alongside the existing five of Identify, Protect, Detect, Respond, and Recover.

Although many aspects of the Govern function existed within prior versions of the CSF, Govern's elevation to a key function in CSF 2.0 reframes cybersecurity in terms of a broad risk agenda. Diving a bit more deeply, the Govern aspect aims to help organizations incorporate cybersecurity into broader risk management programs by presenting "outcomes" or desired states to inform what an organization may do to achieve and prioritize the other five functions.

While humans are the heart of security operations — and will continue to be, even as technology advances — tools play a major role as well. Common tools include (but are not limited to):

- Vulnerability management software
- Security information event management (SIEM)

- Endpoint and network detection and response (EDR and NDR) platforms
- Identity and access management (IAM) systems
- Cloud security posture management (CSPM) and cloud monitoring utilities
- Newer additions such as attack surface management (ASM) and continuous threat exposure management (CTEM)

However, as many organizations have discovered, deploying security solutions requires considerable expertise to configure tools, aggregate the telemetry they provide, and analyze the enormous volumes of data they produce to determine when intervention or other responses are warranted.

Finding Signals within Noise

A prerequisite for identifying and responding to real threats without burdening organizations with false alarms is for a security operations center (SOC) to achieve both:

- A low **false-negative rate**, to ensure that few threat signals go unnoticed
- A high **true-positive rate**, to avoid contributing to alert fatigue with false alarms

In addition to finding enough personnel to staff the operation (the most common SOC size is between 11 and 25 staff members), this is another area where in-house approaches to SecOps can run into major challenges. Even today's smaller organizations have IT environments that span endpoints, networks, and both public and private clouds, to say nothing of **a long list of SaaS applications**, hardware devices, Internet of Things (IoT) devices, and/or operational technology (OT).

Simply gaining the necessary breadth and depth of visibility into this expansive and dynamic attack surface is a major hurdle; leveraging the telemetry acquired is another — as the sheer volume can quickly overwhelm a security team.

To illustrate, let's explore the Arctic Wolf observation funnel (depicted in Figure 1).

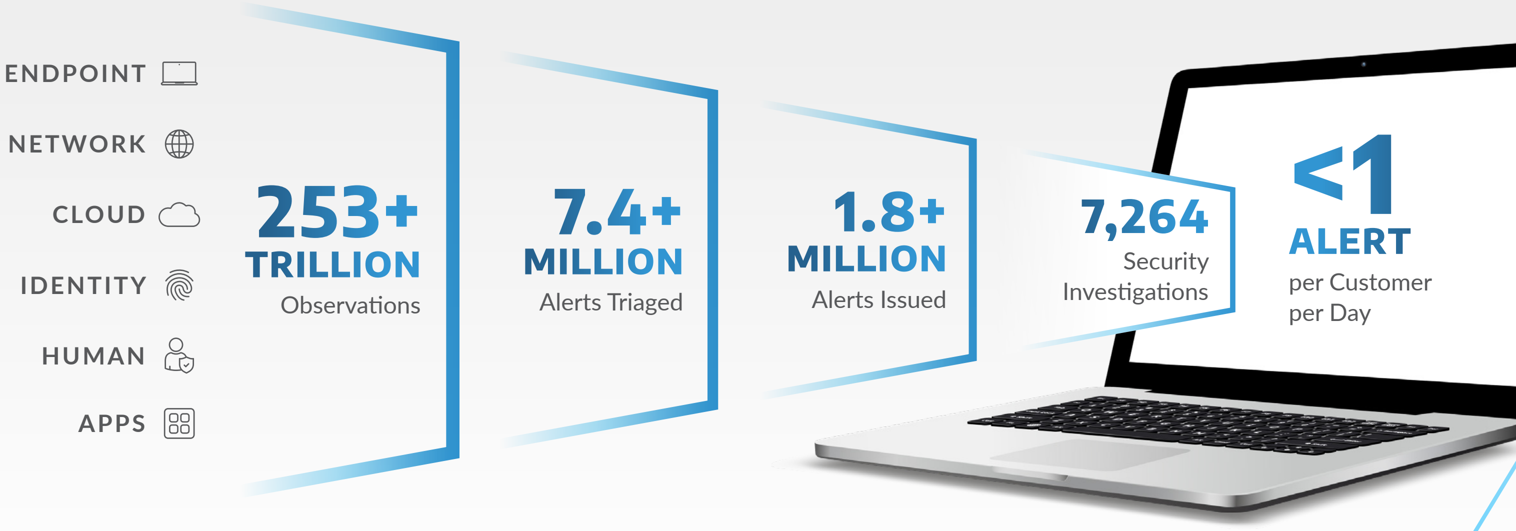

ENDPOINT
NETWORK
CLOUD
IDENTITY
HUMAN
APPS
253+ TRILLION Observations
7.4+ MILLION Alerts Triaged
1.8+ MILLION Alerts Issued
7,264 Security Investigations
<1 ALERT per Customer per Day

Figure 1 - Most organizations receive thousands of alerts per day from dozens of disparate security tools, forcing fatigued IT and security professionals to alter alert thresholds or turn off entire classes of alert — in contrast, the Arctic Wolf Platform is optimized so that customers only spend time on true threats.

To best understand the data that fuels this report, and the corresponding findings presented throughout, it is important that we provide appropriate context around the Arctic Wolf Platform as it collects, enriches, and optimizes events to deliver the security outcomes covered within these pages.

Working with tools each customer already has, and deploying additional agents and sensors as needed to provide sufficient coverage, all available telemetry is ingested into the Arctic Wolf Platform. This **raw observation data** consists of every observational data point of potential value within a customer's environment. The Arctic Wolf Platform processes all of this combined data, which on average, exceeds 5.3 trillion observations* each week across the Arctic Wolf customer base.

Next, the data is parsed, enriched, and analyzed using a mix of AI and behavioral analysis — all applied on a per-customer basis in the context of environment-specific baselines that are continually refined over time. This process raises the signal-to-noise ratio, resulting in **analyzed observations** that are comparatively free of duplicate signals, benign activity, and other superfluous data.

At the next stage, we further amplify the signal within those analyzed observations by combining them with additional context, primarily in the form of security-relevant data points, to create **events**. For example, a network connection from an unknown IP address may be combined with the geolocation of the IP, the time of the connection, the destination, and available user context to comprise an event.

These events are then further analyzed, with our technology stack identifying those which could indicate activity that requires further investigation.

At this point, Arctic Wolf Security Engineers apply their experience and expertise, aided by real-time threat intelligence, to triage the available evidence within the pertinent customer's business context — ultimately determining whether an event is of sufficient interest to alert the customer.

Security outcomes we deliver to our customers through this process include:

- The Arctic Wolf Platform reduces data by 99.999999% before an alert is issued
- We maintain a true positive rate of 99.9%, helping customers make informed decisions while eliminating alert fatigue
- On average, a typical customer receives one alert per day from Arctic Wolf
- When appropriate, Arctic Wolf will respond by containing and mitigating an active threat

> **Or, to put it another way, our Security Engineers issue one alert for every 100 million pieces of observational data that come into the platform — and only one out of every 1,000 alerts issued is later discovered to be a false positive.**

Upon receiving an alert, the customer can work with their Concierge Security® Team (CST) to make informed decisions and take the appropriate steps to achieve their security objectives.

52 WEEKS — BY THE NUMBERS

This report is largely built upon one year of SecOps data, spanning:

- 253 trillion raw observations (averaging over 5.3 trillion per week as of April 2024)
- 7.4 million alerts triaged
- 1.8 million alerts issued
- 7,264 security investigations
- 320 instances of confirmed malicious activity

*as of April 2024

SCHRÖDINGER'S ALERT: PENETRATION TESTING

Arctic Wolf routinely encounters a situation in which an alert is simultaneously both a true and false positive:

- True, because a real threat action was detected
- False, because of the perpetrator's identity and intentions

A penetration test, also known as pen test, is an authorized and simulated cyber attack performed on an IT system (or systems) to evaluate existing security controls.

Pen testing tries to replicate real-world attacks cybercriminals use. This means that a pen test goes much further than other assessments and exercises meant to identify risk, and may include permission to:

- Access or escalate accounts or permissions through unauthorized means
- Install simulated malicious code
- Modify system configurations
- Demonstrate the ability to exfiltrate data or disrupt business operations

During the research period of this report, Arctic Wolf identified over 1,100 pen tests within customer environments, led by these five industries:

01 Banking

02 Financial

03 Manufacturing

04 Healthcare

05 Legal

Arctic Wolf believes offensive security validation, or penetration testing, can be effective tools for assessing your security operations effectiveness. To get the most out of these services, however, each organization must ensure they are partnering with the right vendor who can help them achieve their goals.

Arctic Wolf works with our customers to help them identify what goals they hope to accomplish with a pen test and partners with them to help achieve those outcomes.

Around-the-Clock Monitoring Is a Necessity

Stopping today's threat actors requires around-the-clock monitoring of your entire environment, as cybercriminals regularly launch attacks outside of regular working hours to decrease risk of detection, increase dwell time, and take advantage of a reduced response capacity.

Our direct observations underscore this reality:

- 40-45% of alerts generated are identified in the "after-hours" period from 8 p.m. to 8 a.m.
- 16-20% of alerts generated in the weekend period between 8 p.m. Friday and 8 a.m. Monday

Timestamp of Alerts Generated: Count by Hour of Day

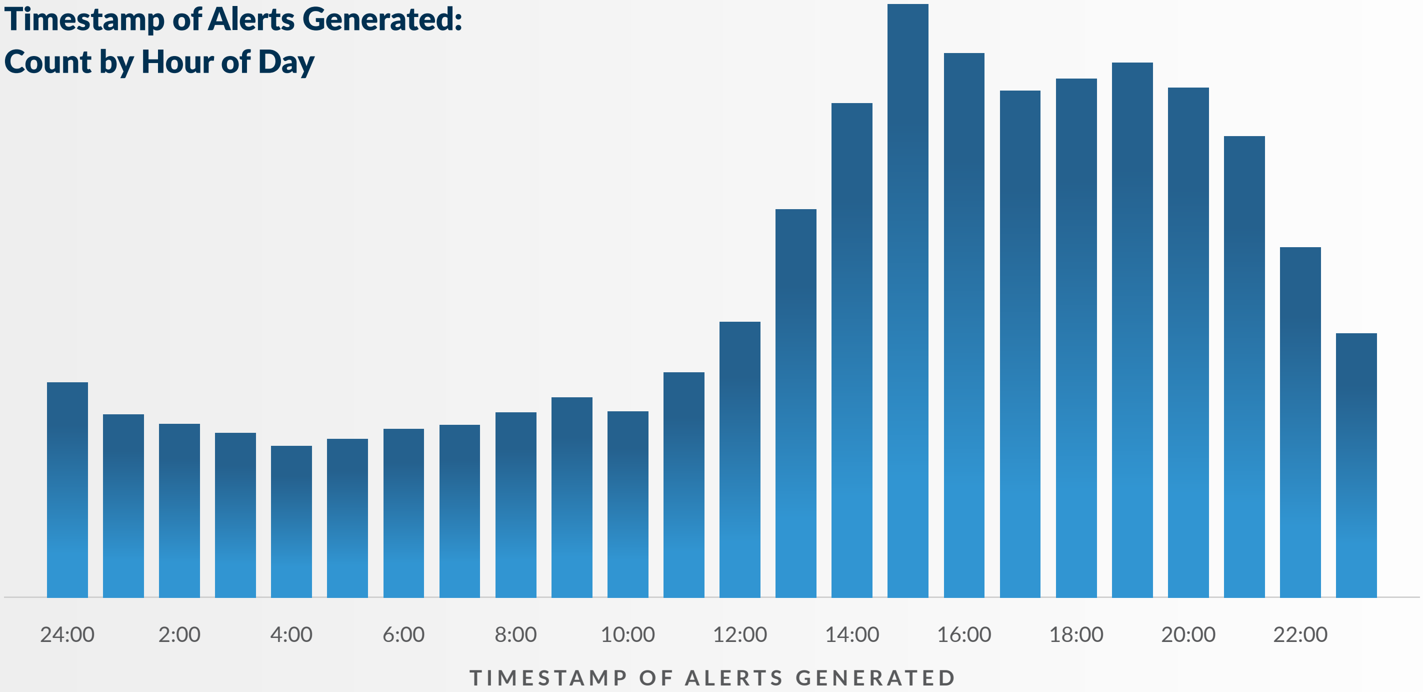


Figure 2 –Although alert generation certainly has an ebb and flow, it tends to lag the traditional workday — with the majority of alerts created from mid-afternoon through late evening.

Timestamp of Alerts Generated: Count by Day of Week

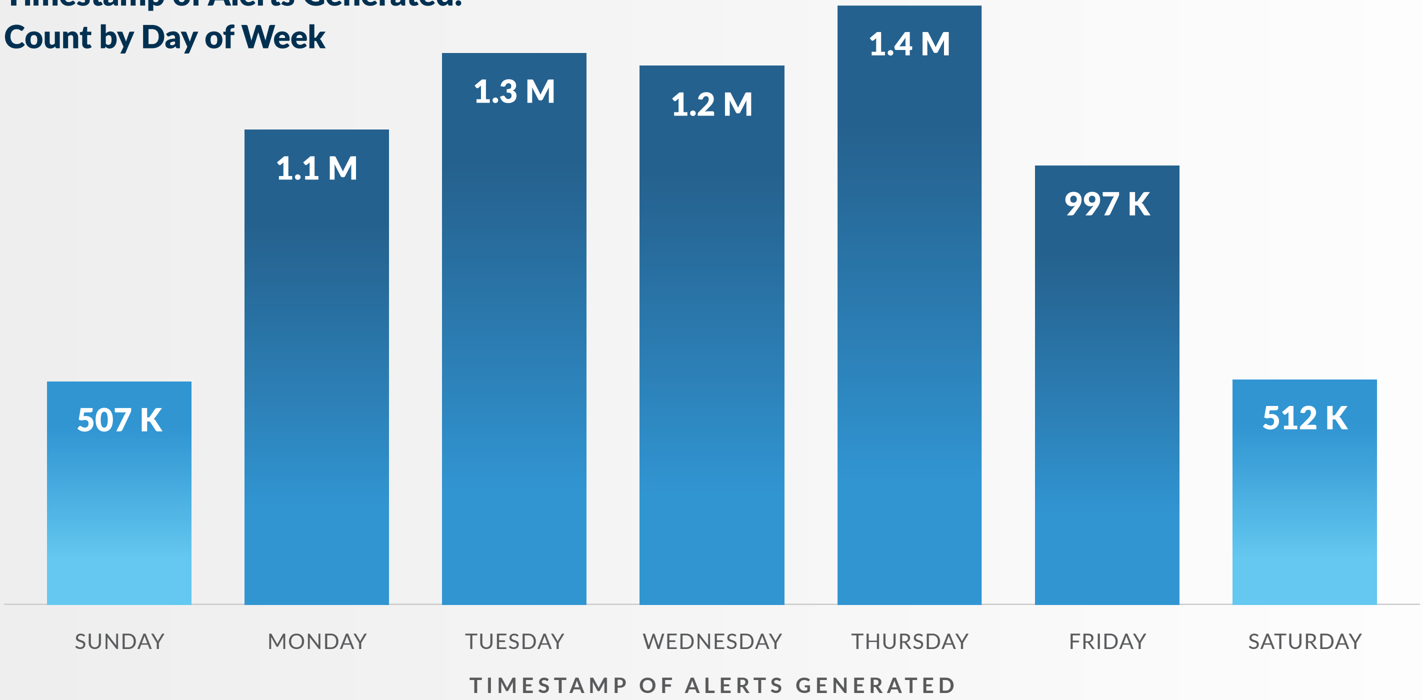


Figure 3 – Likewise, although weekdays exhibit higher alert generation, weekends still have a baseline level of activity.

MEGA EVENT SPOTLIGHT

When discussing threats, it's important to understand that, although any threat can have devastating impact on an environment, that doesn't mean all threat events are equal in size, scale, and potential for harm.

Some threat events are discovered as they quickly evolve into widespread attacks, which is why Arctic Wolf has recently begun using the term **"mega event"** to describe any critical threat event that may impact a significant portion of our customer base. Examples of such events include:

> SolarWinds breach and supply chain compromise
>
> Log4j remote code execution (RCE) vulnerability
>
> Spring4Shell RCE vulnerability
>
> Microsoft Exchange ProxyShell and ProxyLogon vulnerabilities

During a mega event, Arctic Wolf executes a strategic runbook designed to minimize the impact on our customer base.

This runbook combines active investigation and response with a high-touch approach that provides updates and actionable intelligence to our customers.

During the period covered by this report, one event stood out above all others. During this event, we:

- Executed a 96-hour response timeline
- Issued three security bulletins
- Contacted 1,800 customers
- Conducted 171 security investigations
- Developed five new threat detections to identify vulnerability exploitation
- Thwarted 13 active attacks against a single customer **in a single day**

And, most important of all, zero cases of ransomware or data exfiltration were identified.

Zero-Day Mega Event: Active Exploitation of PAN-OS Firewalls (CVE-2024-3400)

On April 12, 2024, Palo Alto Networks (PAN) published **a security advisory** detailing an actively exploited vulnerability (CVE-2024-3400) affecting the GlobalProtect feature of several versions of the PAN-OS firewall. This vulnerability was severe enough to receive the maximum Common Vulnerability Scoring System (CVSS) score of 10.0, which is a relative rarity.

CVE-2024-3400 allows an unauthenticated remote threat actor to execute arbitrary code with root privileges on the firewall. Or, put another way, the vulnerability allows an attacker to not only bypass the firewall's defenses, but also to leverage the firewall itself as a beachhead for a larger intrusion.

This vulnerability was identified as a zero-day by **Volexity**, which observed the threat actor UTA0218 installing a custom Python backdoor named UPSTYLE on firewall devices. Following the initial breach, UTA0218 downloaded additional tools from remote servers controlled by the compromised devices to gain deeper access into victims' internal networks. Subsequent lateral movements within these networks allowed the extraction of credentials and sensitive files.

REMOTE CONNECTIVITY TOOLS ARE TOP TARGETS

Notably, this is not the first time threat actors have targeted GlobalProtect. A similar vulnerability (CVE-2019-1579) was exploited in 2019.

Given the widespread adoption of remote work, tools that enable remote access to corporate networks are — and will remain — enticing targets for threat actors.

On April 14, 2024, Palo Alto Networks **released hotfixes** to address the vulnerability. By this time, a wider array of threat actors had already automated attack workflows and launched attack campaigns to exploit vulnerable devices.

When the vulnerability information was announced, Arctic Wolf began implementing our mega event runbook. Security engineers immediately contacted the more than 1,800 customers with a Palo Alto firewall appliance to inform them of the situation, update them on their risk status, and guide them through next steps. Patch guidance was issued and discussed with affected customers, and those who were at risk were continually monitored.

The mega event declaration was quickly validated, as we immediately observed exploit attempts. Fortunately, thanks to the joint efforts of the Arctic Wolf Security Teams and our customers, zero cases of lateral movement or ransomware deployment were detected.

MEGA EVENT HIGHLIGHTS

Issued **3 security bulletins**

Contacted **1,800 customers**

Conducted **171 security investigations**

Developed **5 new threat detections** to identify vulnerability exploitation

Thwarted **13 active attacks** in a single day

Executed a **96-hour response timeline**

OBSERVATIONS FROM SECURITY OPERATIONS DATA

We now turn our attention to insights that can be gleaned from Arctic Wolf's security operations data, highlighting key takeaways and noteworthy observations throughout.

The High-Level View

KEY TAKEAWAYS:

Compliance activities should be regarded as proactive investments in risk management, rather than as burdensome overhead. Our observations show that organizations in highly regulated industries (banking, legal, and healthcare) have the strongest security postures.

Fulfilling a prediction made by Arctic Wolf Labs, manufacturers are under attack — the manufacturing sector accounts for 26% of alerts associated with our 10 most-represented industries, well ahead of healthcare (16%) and education (14%).

An effective vulnerability remediation program remains one of the most straightforward and efficient ways to protect your organization, most attacks using software exploits target core business applications that have fallen behind on patching.

Highly Regulated Industries Have the Strongest Security Postures

For IT and security teams, staying ahead of the latest cyber threats and attack vectors is an ongoing endurance test.

To help customers understand their security posture at all times — and to measure their security journey progress — Arctic Wolf calculates a rolling security score aligning with the NIST Cybersecurity Framework. We consider a range of environmental factors when calculating this score, including:

Coverage: How much visibility does the organization have into their environment (NIST - Identify)

Risk: Calculated level of risk based on internal and external vulnerabilities (NIST - Protect)

Detections: Calculated volume and criticality of alerting within the environment (NIST - Detect)

Responsiveness: The time to respond to alerts and threats (NIST - Respond)

Security Reviews: Output, determination, and response to security reviews (NIST - Govern)

For the period covered by this report, our observations show considerable variation across the 10 industries with the largest representation in our customer base (Figure 4).

Arctic Wolf Security Score by Industry

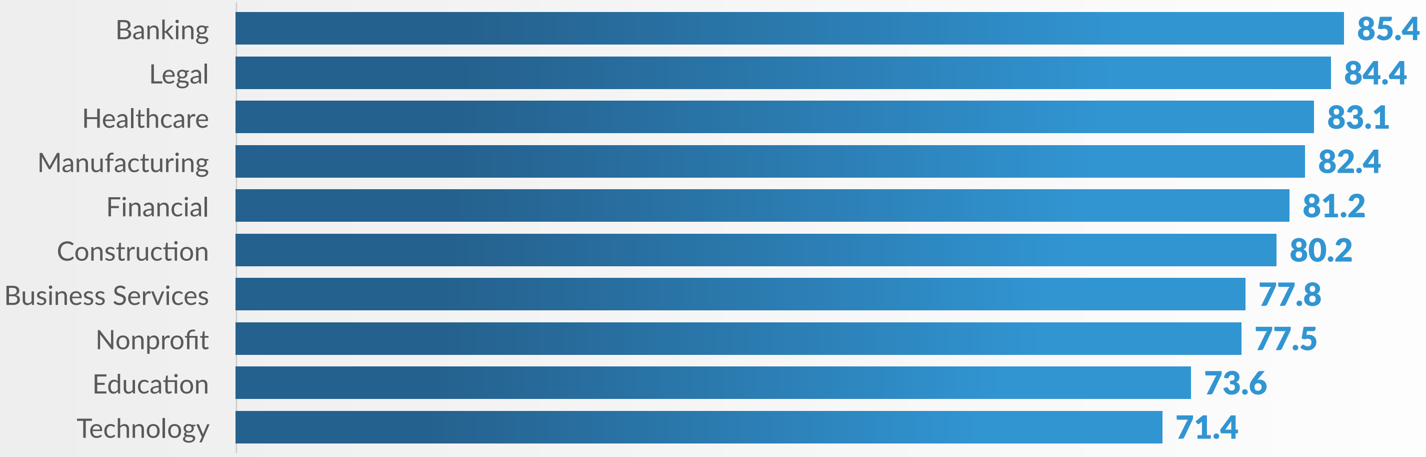


Figure 4 – Out of the 10 industries with the most representation within the Arctic Wolf customer base, three heavily regulated ones — banking, legal, and healthcare — have the highest average security scores.

Topping the list are three highly regulated industries — banking (an average organization score of 85.4 out of 100), legal (84.4), and healthcare (83.1).

When we consider that these verticals are regulated or guided by professional rules and responsibilities, and must adhere to an array of compliance requirements, their strong security postures are both unsurprising and reassuring.

The three industries with the lowest security scores are technology (71.4), education (73.6), and nonprofit (77.5).

While the reasons behind these comparatively lower scores are plentiful and may vary by organization, some conclusions may be drawn based upon factors driving their industries.

> **"The technology industry's focus on velocity and growth often contributes to their general attitude of seeing regulation as secondary, while educational institutions are usually known to have complex architectures clashing with restrictive budgets that may limit their ability to build and maintain a strong security posture,"**
> – Dan Schiappa, Chief Product & Services Officer

THE 5 MOST COMMON RISKS

Arctic Wolf's **Managed Risk** solution helps customers identify risks within their environments and develop strategic plans to effectively address and correct these issues.

In the environments we examined, the five most common risks we observed are:

01 TCP Timestamps Information Disclosure

02 ICMP Timestamp Reply Information Disclosure

03 SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

04 Content Security Policy (CSP) Header Not Set

05 Strict-Transport-Security Header Not Set

Manufacturers Are Under Attack

In the Arctic Wolf Labs 2024 Predictions Report, we foresaw that "Industrial espionage and intellectual property theft campaigns will be aggressively pursued via China's cyber operations," and we noted that manufacturers would likely be favorite targets as the Chinese government aggressively pushes industrial modernization initiatives.

Our observations indicate that this prediction was right on the mark, as manufacturing organizations account for 26% of all alerts associated with our 10 most-represented industries (Figure 5) — 2.6x the expected volume if threats were evenly distributed.

Healthcare and education placed second (16%) and third (14%) on the list, respectively. While at first glance these industries may seem to have little in common, in truth they have a few things in common:

- Both industries hold vast troves of personal information, including payment details
- Both industries have little tolerance for downtime
- Many organizations in both industries have robust research functions, making them rich sources of cutting-edge intellectual property

Ticket Volume by Industry (Share of Tickets)

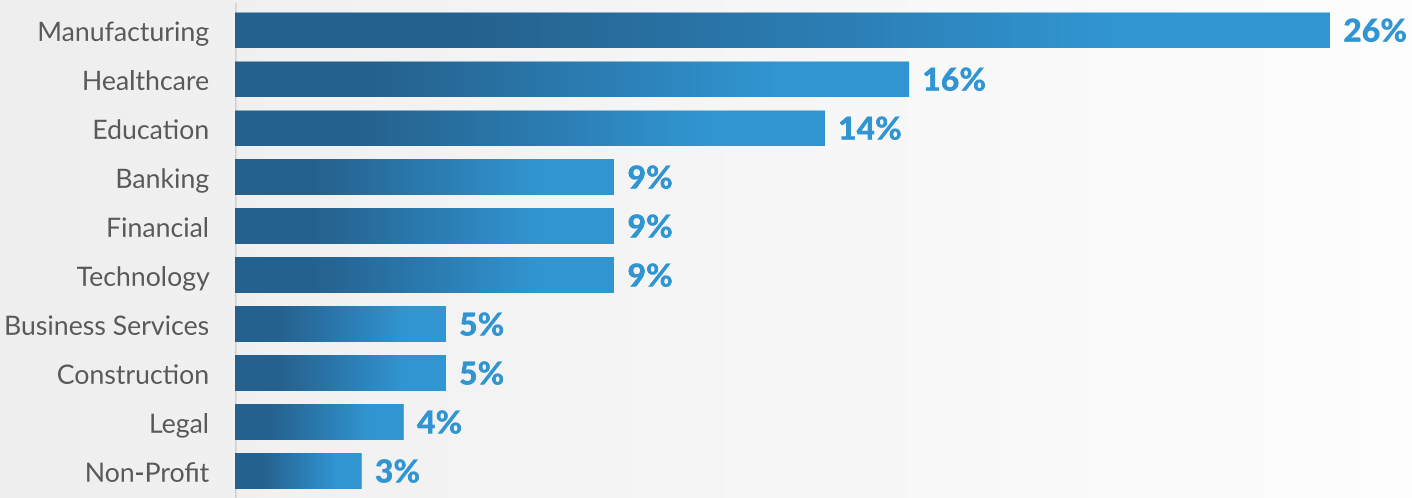


Figure 5 – Valuable intellectual property and a need for high uptime make manufacturers prime targets for industrial espionage and disruptive attacks.

Attackers Target Core Business Applications

Detecting and responding to malicious activity are essential for minimizing or, ideally, outright preventing disruption — but stopping an attack is only part of the job. Understanding the root causes of incidents is just as important, as doing so allows us both to help individual customers progress on their security journey and to apply lessons learned across our entire customer base in a "rising tide" manner.

Our observations from May 2023 through April 2024 indicate that the software applications most commonly leveraged for exploitation by attackers were:

01 Windows 10 OS (Unpatched or missing critical patches)

02 MS Outlook (2016 and 2013)

03 Cisco IOS XE WebUI

04 Office 365 (2016 Click-to-Run)

05 Apache ActiveMQ

06 JetBrains TeamCity

THIS LIST PROVIDES TWO IMPORTANT TAKEAWAYS.

01

First, these aren't obscure applications or examples of shadow IT, but are instead core business applications that are ubiquitous in today's organizations. This fact suggests that a certain amount of baseline risk is absolutely unavoidable, whether it comes from an industry-agnostic office suite or from an industry-specific application.

02

Now, having acknowledged the reality of baseline risk, we can add the second takeaway — maintaining a risk management program that can identify vulnerabilities and help formulate a plan **to keep your software up to date remains an effective way to reduce risk by safeguarding against known vulnerabilities.**

ROOT CAUSE VS INITIAL ACCESS POINT

Whereas the **initial access point** describes the device or attack surface that is first compromised, **root cause analysis** focuses on the methods used by threat actors to obtain initial access to the victim's systems.

WHAT ABOUT ZERO-DAY THREATS?

It's worth repeating a point made in the **Arctic Wolf Labs 2024 Threat Report**: the vast majority of exploitations take advantage of vulnerabilities for which patches are available — many of them for months or even years.

In fact, our observations indicate that exploitation of known and patched vulnerabilities outnumber exploitation of zero-day vulnerabilities by ~7.5 times.

So while zero days are a nightmare, the attention they receive threatens to overshadow the larger — and more readily manageable — risk of unpatched systems.

PROTECTING YOUR ORGANIZATION WITH VULNERABILITY REMEDIATION

Vulnerability remediation is the act of removing a vulnerability through patching or another process. By focusing on remediation, organizations can greatly reduce their cyber risk and prevent threat actors from exploiting vulnerabilities as an attack vector.

There are four main questions an organization needs to ask itself as it sets out to conduct vulnerability remediation:

01 Which vulnerabilities should I remediate first?

02 How can I efficiently remediate those vulnerabilities?

03 How do I prioritize vulnerabilities based on my resources and business risk tolerance?

04 How do I set realistic deadlines for my vulnerability remediation plan?

Of course, those questions are easier to ask than to answer, and for many organizations that lack resources, time, or budget, vulnerability remediation can seem like an endless mountain to climb.

Compounding the challenge, it's difficult to determine which vulnerability to remediate first if you don't have a clear understanding of your overall attack surface. Plus, efficient remediation is all but impossible without contextualization of your entire environment. Unfortunately, that contextualization — including your risk policies, asset context, and service level objectives (SLOs) — is not easy to achieve when you have limited resources and an overwhelmed IT team. Not to mention the time and resources needed to **conduct security scans** and do the actual remediating.

That's why remediation should just be one part of **a full vulnerability management program**, which prioritizes continuous vulnerability remediation and assessment, with other components of the program complementing and assisting overall remediation and mitigation.

IDENTITY IS AN EMERGING BATTLEGROUND

KEY TAKEAWAYS:

Identity and access management controls play an increasing role in a strong security posture — identity signals represent seven of the top 10 threats or IOCs leading to alerts.

To complicate or evade detection, threat actors continue to employ infostealers to acquire active credentials or session cookies. At times, we observed more than 2,000 weekly instances of the Win32.Zbot infostealer Trojan across our customer base.

Whether a threat actor is subtly leveraging known credentials or using password spraying to brute-force your login box or API, identity controls — especially enforcing MFA usage — contribute to detecting and blocking attacks.

Identity Telemetry Is Vital — But Making Sense of the Signals Requires Expertise

During the period covered by this report, identity telemetry dominates the list of the top 10 threats or IOCs leading to alerts (Figure 6).

Generally, this list is consistent across the full range of industry verticals represented within our customer base, which demonstrates that different attacks make use of the same 'building blocks.' The one notable exception is the banking industry, for which "Anomalous Firewall Change" occupied the top spot, with "Restricted Country Login" in second place.

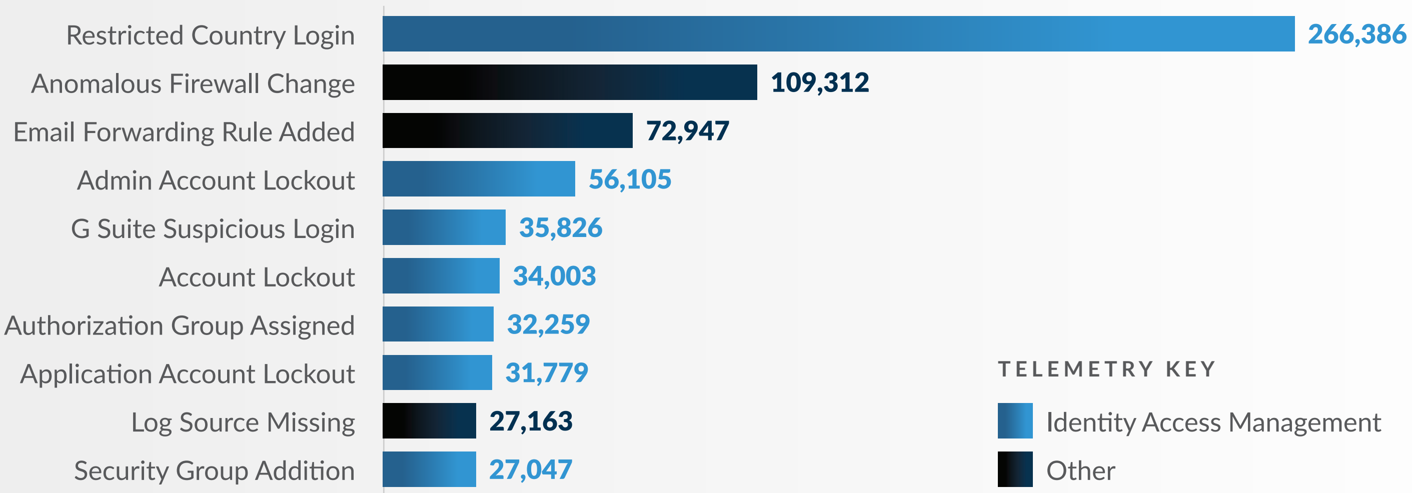


Figure 6 – Identity telemetry dominates this top 10 list, illustrating IAM's importance in detecting modern threats.

The prevalence of identity telemetry in this top 10 list underscores the crucial role of IAM in a strong security posture and as an enabler of zero trust initiatives, but — as we touch on below — also hints at a growing challenge.

A GROWING IDENTITY CHALLENGE

Increasingly, telemetry from IAM systems is regarded as incredibly valuable for detecting an intrusion.

However, recognizing malicious activity among the high volume of innocuous everyday activity is a tremendous challenge — especially if one examines IAM data in isolation. And the challenge is only growing, as organizations adopt even more SaaS applications and implement finer-grained access controls. **It takes careful, organization-specific tuning and correlation with other sources to fully leverage IAM activity.**

Learn more about how identity systems can help to secure your organization in:

→ **The Importance of Identity and Access Management**

→ **Understanding Identity Threat Detection and Response**

Leading the way by a sizeable margin is an attempted login from a restricted country. Despite the availability of VPNs and proxy techniques that can disguise a threat actor's location, unexpected login attempts from unusual or outright restricted locations remain a common indicator of malicious activity — after all, in a workforce context there's likely no legitimate reason for a login attempt to originate from an IP/AS range belonging to a country where an organization doesn't have a presence.

In addition, we can see a handful of entries corresponding to other authentication activities, including account lockouts (e.g., due to too many failed login attempts, which can be a sign of a brute-force attack) and suspicious logins (e.g., from an unusual location or at an unusual time of day).

Also falling under the IAM umbrella are two configuration changes relating to permissions: Authorization Group Assigned and Security Group Addition. Privilege escalation is a common intermediate step during intrusions, as threat actors look to move about environments to perform reconnaissance, access high-value data, and compromise administrative systems — and adding compromised accounts to privileged groups is one way to achieve this goal.

Occupying the second and third places in Figure 6 are two other configuration alterations that can indicate malicious intent: firewall changes and the addition of email forwarding rules. The former essentially unlocks a vital perimeter defense while the latter can be a sign of a business email compromise (BEC) attack or data exfiltration.

Finally, today's attackers recognize how valuable logs are both for detecting an in-progress attack and for performing root cause analysis. Accordingly, intruders often attempt to disable and delete logs that might reveal their presence and tactics, techniques and procedures (TTPs) — which is why the unexpected disappearance of a log source (i.e., Log Source Missing) warrants investigation.

Before we move on, it's worth making one last point about Figure 6: it doesn't include any malware signatures, software exploits, or other entries that are 100% indicative of malicious activity. The reason for this is that, although such clear IOCs do exist, they're vastly outnumbered by activities that could be malicious but, mathematically speaking, probably aren't. Additionally, today's threat actors frequently try to "live off the land" by abusing existing tools and utilities. Viewed in isolation, it's difficult or even impossible to distinguish a specific use of a particular admin tool as being malicious versus benign; rather, it's only through higher-level correlation with other observations that a pattern of behavior and intent starts to take shape.

So, in the numbers game of threat detection (recall the section explaining the data pipeline), for every login that corresponds to a real threat there may be many that look suspicious or fail, but are ultimately innocuous; at the same time, genuinely malicious login activity may also outnumber clear-cut threats — like the use of a software exploit — by orders of magnitude.

All of this speaks to how challenging it is to find that precious signal within a cacophony of noise; to enable security teams to act on real threats without encumbering them with false positives.

Infostealers and Account Takeovers (ATOs)

SaaS apps, remote connectivity tools, cloud infrastructure — basically, anything with an account — are all high-value targets due to the information and access they provide threat actors. So long as organizations continue to put faith in passwords, and so long as users continue to exhibit poor password hygiene, attackers will have a relatively low-resistance way to execute account takeovers (ATOs).

For instance, threat actors have a number of ways to get credentials or otherwise hijack an account:

- Sourcing them from the dark web, whether buying credentials for specific targets or acquiring massive collections
- Brute-forcing login boxes (or APIs) by 'spraying' combinations of usernames — which are trivial to construct for each target organization — and lists of common passwords
- Employing social engineering techniques like phishing to trick a user into providing their login information
- Using infostealers to acquire credentials or active session cookies from compromised devices and environments

The rise of infostealers, in particular, is a concerning, ongoing, and pervasive trend.

As just one example, from May 2023 through April 2024, we observed extensive usage of the Win32.Zbot Trojan, with weekly detections ranging from ~100 instances to over 2,000 across our customer base.

While any account takeover has the potential to cause problems, one type deserves special attention: email account takeover (EAT), a subset of business email compromise.

The FBI's most recent Internet Crime Report puts BEC-related losses at $2.7 billion USD in 2022 (80 times that of ransomware). Moreover, while not all BEC scams lead to a data breach, according to IBM's **Cost of a Data Breach Report 2024** those that do cost an average of $4.88 million USD.

But EAT attacks represent an even greater, albeit relatively less common, risk than other forms of BEC, because they can be very difficult for victims to detect.

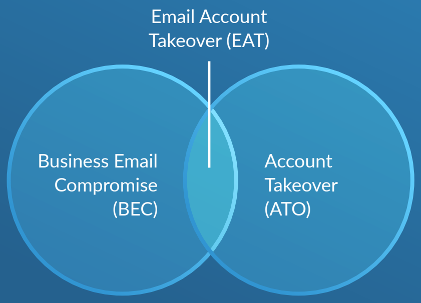
VPN APPLIANCES UNDER ATTACK

In March 2024, we issued a security bulletin **(Password Spraying Activity Targeting Various VPN Appliances, Firewalls, and Other Public Web-Based Applications)** that corresponded to a 200% increase in observed ATO activity.

BUSINESS EMAIL COMPROMISE (BEC)

Business email compromise is a type of email-borne phishing fraud in which a threat actor attempts to trick members of an organization into transferring funds, sensitive data, or something else of value.

While the term originally referred to attacks in which a threat actor hijacked a legitimate email account (i.e., an EAT), it has evolved to now include incidents in which a threat actor spoofs a trusted account — for instance, by using a domain that, at a glance, looks like an organization known to the target (e.g., goog1e.com).



Even though only a small minority of BEC incidents lead to an insurance claim and only the most severe typically lead to a full IR engagement, BEC attacks still make up roughly 30% of the total cases investigated by Arctic Wolf® Incident Response over the past few years.

For example, in January 2024, **the U.S. Attorney's Office, District of Maryland unsealed an eight-count federal grand jury indictment** against a Nigerian national accused of using a BEC attack to defraud two charitable organizations out of $7.5 million USD. In this incident, the alleged perpetrator obtained credentials for two charitable organizations and executed an EAT against the email accounts of people within both charities.

Over three months, the attacker used these accounts to request and approve financial transactions, while employing inbox filtering rules (reminiscent of Email Forwarding Rule Added in Figure 6) to hide the relevant email exchanges.

DEFENDING AGAINST ATOS

While we recommend closely working with your IAM and application providers to strengthen your defenses against ATOs and — more generally — to enforce strong credential controls, here are five best practices:

01 Implement and enforce multi-factor authentication (MFA)

02 Block authentication attempts from hosting-based traffic; this may be extended to include proxy services, which criminals also use to hide their origins

03 Set automated blocking on authentication attempts to hinder password-spraying activities

04 Configure syslog to forward your organization's VPN and firewall logs to your security operations provider

05 Implement geolocation-based blocking (e.g., restricted countries, impossible travel scenarios)

DESPITE A VOLATILE ECOSYSTEM, RANSOMWARE REMAINS A MAJOR THREAT

KEY TAKEAWAYS:

An effective SecOps function dramatically reduces the risk posed by ransomware — despite near-constant attacks leading to 158 instances of attempted ransomware, less than 2% of our customers were impacted (well below the industry average of 45%).

The unexpected use of legitimate tools can be strong indicators of an attack or ongoing intrusion — we observed surges in Cobalt Strike and sqlmap corresponding to specific threats (e.g., the PaperCut Print Management Server RCE vulnerability) and baseline ransomware activity.

Cybercriminals continue to use social engineering because it works. Even after receiving notice of an upcoming phishing simulation, 15% of organizations had at least one user fall for a lure (the most successful was an email with the subject "Updated Vacation Policies 2024").

SecOps Strengthens Resilience to Ransomware

In the past 18 months, the ransomware landscape has shifted dramatically due to the combination of law enforcement takedowns and the resulting erosion of trust between groups and affiliates.

Nevertheless, attacks continue — from May 2023 through April 2024, Arctic Wolf Security Engineers responded to 158 instances of attempted ransomware.

Despite the constant threat, we found that **indicators of ransomware activity were detected in fewer than 2% of our MDR customer base,** which stands in stark contrast to the 45% of organizations overall that reported suffering a ransomware attack when surveyed for **Arctic Wolf's The State of Cybersecurity: 2024 Trends Report**.

One reason for the extreme difference is that, per the survey behind that trends report, 67% of ransomware victims weren't employing a method of network threat detection. So, while network-based detections aren't a universal cure-all, the absence of such defenses certainly correlates with a higher likelihood of suffering a full-blown ransomware incident.

Monitoring Ransomware Precursors

Ransomware doesn't simply appear out of nothing, in isolation — rather, it is deployed and detonated following a chain of malicious actions that generally include, but aren't limited to:

- Gaining initial access to an environment
- Establishing persistence
- Performing reconnaissance
- Exfiltrating data

Detecting these precursors as quickly as possible is an effective way to disrupt or break the attack chain, so Arctic Wolf analysts carefully monitor for activity known to have close historical ties to ransomware.

For example, in April 2023 we observed a 425% increase in botnet activity, the majority of which was associated with Cobalt Strike command-and-control (C2) traffic.

Underscoring the widespread abuse of Cobalt Strike by attackers (see sidebar on next page), some of this increased activity was associated with the **PaperCut Print Management Server RCE vulnerability** (CVE-2023-27350), while the remainder is consistent with ongoing ransomware campaigns active during this period.

RANSOMWARE RISKS DEMAND EXTRA DILIGENCE

Given the widespread concern about ransomware and its potential to impose devastating disruptions and costs, we place added emphasis on analyzing and investigating potential ransomware activity. This begins with the elimination of noise and false-positive alerts.

For example, of the almost 56,000 potential ransomware incidents we were alerted to in the year covered by this report, only 14% of those resulted in an alert being issued to our customers, thereby saving customers both time and unnecessary stress.

If we look at it from a different angle, this means our analysts accurately reviewed and determined that 86% of initial ransomware alerts were either false or benign positives and should not be escalated to a customer. An important fact when we consider that alert fatigue is one of the primary contributors to delays in critical response time.

Similarly, **during November 2023, we spotted a 125% increase in indicators of SQL injection activity — and, in particular, the use of sqlmap** (see sidebar) in a series of customer environments.

> **"An SQL injection is an attack technique that inserts unauthorized structured query language (SQL) code into a web application database. Web applications use SQL to communicate with their databases, and often allow a user to input information, such as login credentials. When inputs are not sufficiently filtered, or a vulnerability exists within the application, attackers can use SQL injections to gain access to the database and perform actions such as retrieval or manipulation of the data, spoofing user identity, and executing remote commands,"** – explains Lisa Tetrault, Vice President, Security Operations

Organizations Remain Susceptible to Social Engineering

From May 2023 through April 2024, Arctic Wolf® Managed Security Awareness ran phishing simulation exercises to help approximately 2,000 customers educate and evaluate their workforce. In a statistic that should raise alarm bells for security leaders everywhere, **15% of customer environments had at least one user — which is all that it takes — fall for a simulated phishing lure**, with many environments having multiple users do so.

To place this figure in an even more sobering context, most of these organizations notified their workforce before the simulated phishing campaigns.

What does this have to do with ransomware?

For a threat actor launching a multiphase attack, it can be easier and more efficient to use social engineering — especially email or SMS phishing — to manipulate a user into running a loader that fetches a ransomware payload than it is to employ sophisticated techniques to bypass defenses.

TOOL ABUSE: COBALT STRIKE AND SQLMAP

Attackers are resourceful and often favor the path of least resistance. Consequently, they regularly abuse legitimate tools during their attacks.

For example, Cobalt Strike is a security tool used by penetration testers and security researchers to assess the security of networks and systems.

However, for several reasons — including its power and versatility, its ability to remotely control and monitor intrusions, its reporting capabilities, and its C2 framework — it is also widely abused by threat actors.

Similarly, sqlmap —an open-source penetration testing tool — is often abused by attackers, typically to perform SQL injections.

Any unexpected observation of Cobalt Strike or sqlmap should be investigated with urgency.

RAISING AWARENESS AND RESILIENCE

Organizational security improves when the workforce as a whole is aware of cyber threats and reinforces positive everyday habits.

From May 2023 through April 2024, Arctic Wolf Managed Security Awareness delivered 526,578 awareness education sessions to customers, who later completed 198,331 quizzes — with an average score of 85%. This figure shows that end users are able to retain what they have learned and practically apply it.

Like many cyber threats, phishing exhibits both a constant steady state of activity but also campaign-related surges.

For example, **in April 2023 we observed a nearly 500% increase in phishing attempts**. Interestingly, this spike coincided with high-stakes news events such as a state grand jury formally issuing criminal charges against former U.S. President Donald Trump, as well as President Biden officially announcing his reelection campaign, in addition to a series of devastating tornadoes ripping through the central U.S.

Similarly — but likely coincidentally — April 2024 saw a 150% increase. This surge corresponded to similar events including controversial Supreme Court rulings in Arizona, ongoing Russia-Ukraine and Israel-Hamas conflicts, and damaging extreme weather events in the southern and central U.S.

Threat actors can be counted on to continue to use polarizing events and geopolitical instability to distract and exploit end users. Building resilience against phishing (and all forms of social engineering) requires ongoing training to help your entire workforce — including contractors and other third parties with access to your systems — recognize the sometimes-subtle signs that indicate a potential threat.

SPEARS AND NETS

Spear phishing is a precisely targeted form of social engineering typically aimed at specific individuals (e.g., executives, administrators, people in financial roles).

The lures are carefully crafted, and frequently leverage personal details and other information gathered through open-source intelligence (OSINT) techniques and prior breaches.

However, most phishing campaigns cast a wider net, using generalized lures that apply to a larger share of the workforce. For example, in the phishing simulation exercises mentioned in the body of this report, **the most successful lure was an email with the subject "Updated Vacation Policies 2024"** — a subject of interest to all recipients!

BUILDING RESILIENCE AGAINST SOCIAL ENGINEERING

It only takes a single user to be tricked into helping a threat actor for an entire organization to suffer a breach — making robust security awareness training an essential element of an overall cybersecurity strategy.

Look for training that includes:

- Up-to-date content, relevant to your organization's industry
- Empowering language that treats users as a key element of the organization's cybersecurity strategy, rather than a weak link
- Phishing simulations to track progress and test skills
- Microlearning for better retention and understanding
- Education that builds an organization-wide culture of security

Ideally, the leadership team will set an example by taking cybersecurity seriously, embodying best practices, and avoiding the type of time-sensitive, high-pressure tactics that scammers employ.

CONCLUSION

Effective security operations is your best defense against today's financially motivated attacks and government-backed espionage.

At Arctic Wolf, we've long recognized that the cybersecurity industry has an effectiveness problem: despite a growing list of technologies and vendors, and record spending on solutions, organizations worldwide continue to suffer disruptive and damaging cyber attacks.

Clearly, a lack of available tools isn't the problem. Instead, organizations aren't getting the most out of the tools they already have — and that suggests the underlying issue is one of operations.

Our research highlights key elements required for an organization to implement a world-class SecOps capability, in pursuit of reducing cyber risk:

FOCUS ON OPEN PLATFORMS AND BEST FIT

Recent vendor-related widescale IT outages and historic breaches highlight the need for companies to transition away from the single-vendor approach that many have previously taken. When an organization chooses to build their security operations stack entirely under the banner of a single vendor, they introduce a single point of failure into their environment.

Instead, the best security operations outcomes are achieved through working from an open platform that allows security tools to be chosen based on organizational best-fit and best-in-class designation within a product category. This not only allows organizations to tailor their security tech stack to their needs, but also offers redundancy in the event one vendor suffers an outage or must be removed from the stack.

FIND THE CORRECT BALANCE OF PEOPLE, PROCESSES, AND TECHNOLOGY

Detecting and responding to the next generation of threats requires the right mix of human expertise, defined processes, and cutting-edge technology — having any of these elements out of balance results in a failure to deliver necessary outcomes.

For example, focusing on implementation of technology alone without the human expertise to use this technology is like buying a hammer without anyone to swing it. Investing in both technology and people — but lacking defined processes on how, when, and why the technology should be used — can result in an operational breakdown.

Leaders should strive to ensure this balance is one that is always maintained, and should be skeptical of vendor claims that a new product or technology meaningfully reduces the need for people or processes.

BECOME AND REMAIN OUTCOME DRIVEN

No two organizations are the same, therefore no two security operations programs should be the same.

Organizations may benefit from following a framework, such as NIST CSF 2.0, when building their programs, but it is important to focus on the outcomes you are trying to achieve and the necessary customizations that are required to be successful.

Rather than solely focusing on responding to alerts, effective security operations outcomes are achieved by those organizations who implement a plan of continuous improvement and truly govern cybersecurity as the business-critical program it is.

BE PREPARED TO ADAPT

Technology is rapidly evolving and becoming further integrated into everyday operational tasks. For security operations to remain effective, it must be designed to quickly scale to match an organization's needs.

Historically we have seen where the inability to scale has had detrimental results. For example, the adoption of cloud technology introduced new vulnerabilities many organizations were not prepared to address — contributing to increases in successful breaches.

In what could be a similar concern, recent advances in generative AI and large language models (LLMs) may now threaten those organizations who are still not prepared to expand the scope of their security operations to new areas of weakness.

A security operations program should be designed for open-ended growth rather than simply meeting current needs.

ARCTIC WOLF CUSTOMERS RELY ON US TO SECURE THEIR ORGANIZATION AGAINST THREATS – AND MAKE SECURITY WORK.

Organizations that embrace security operations are more secure, more resilient, and better able to adapt to the ever-evolving threat landscape — but the reality is that very few organizations have the resources to build such capabilities in house.

We help level the playing field against attackers, ensuring that every organization of every size has the expertise and foundational cybersecurity needed to defend itself.

If you aren't getting the outcomes you're looking for from the solutions you have today, or if you are looking for ongoing expertise to put your existing investments to work, Arctic Wolf is a trusted security operations partner that builds customers' confidence in their security posture, readiness, and long-term resilience.

→ **For more information about Arctic Wolf, visit arcticwolf.com.**

GLOSSARY

Arctic Wolf Labs

Arctic Wolf Labs brings together elite security researchers, data scientists, and security development engineers to help end cyber risk for organizations around the globe by leveraging trillions of security events the Arctic Wolf Security Operations Cloud ingests, parses, enriches, and analyzes each week.

Arctic Wolf Platform

The Arctic Wolf Platform, built on an open XDR architecture, leverages universal ingestion to eliminate “rip and replace” culture, remove the need to choose which data sources are important or not, and enriches, analyzes, and surfaces anomalies, threats, and incidents using data science and artificial intelligence to augment our human analyst teams.

CVE

The Common Vulnerabilities and Exposures system provides a reference method for publicly known information-security vulnerabilities and exposures.

Mega Event

A critical threat event that may impact a significant portion of our customer base. Examples of such events include:

- SolarWinds breach and supply chain compromise
- Log4j remote code execution (RCE) vulnerability
- Spring4Shell RCE vulnerability
- Microsoft Exchange ProxyShell and ProxyLogon vulnerabilities

Observations

Data points of potential value within a customer’s environment.

Scanner

A scanner or security scanner is a tool that is used to analyze your environment (i.e., attack surfaces) for vulnerabilities and threats.

Security Bulletin

An Arctic Wolf Security Bulletin is issued when there is a significant threat identified in the threat landscape, such as a critical vulnerability, an active threat campaign, or other high-profile threats that we believe warrant the security community’s attention.

Security Posture In-Depth Review (SPIDRs)

Security Posture In-Depth Reviews (SPIDRs) — a combination of Arctic Wolf-led security assessments, configuration reviews, and best practice knowledge transfers that help customers improve their security posture.

Alert Triaged, Alert Issued

The Arctic Wolf Platform ingests, analyzes, and enriches trillions security observations each and every week. The Platform leverages that enriched data to generate alerts for our Triage Security Engineers to analyze. Through this analysis (i.e., triage) process, hundreds of thousands of those alerts are eliminated, while only a small sub-set of alerts are then issued to end-customers for actioning.