Smarttech
YOUR 24/7 SECURITY PARTNER

GLOBAL CYBERSECURITY — PERSPECTIVES AND TRENDS FOR 2024

Table of Contents

Smarttech
YOUR 24/7 SECURITY PARTNER

Foreword

"As we are parting ways with the turbulence of 2023, we anticipate an exhilarating journey ahead, where innovation breakthroughs are set to shape our future. The last twelve months have seen profound changes in technological and geopolitical arenas leading to a reshaping of the threat landscape, shifting cybersecurity methodologies and giving rise to regulatory reforms. As we step into the realm of 2024, the intersection of innovative technologies and the ever-expanding digital landscape presents both opportunities and challenges for cybersecurity.

***Attack Surface** – the industry term poised to take center stage in 2024. As the threat landscape evolves at an alarming pace, the attack surface does so simultaneously. Organizations are turning their attention towards the unseen, the 'dark side of the moon'. Their exposure as it pertains to the internal and external attack surface will be a crucial topic on Board agendas globally. Security priorities are changing. Organizations will seek to consolidate their vendors and simplify their security operations by making smart investments - not only in their technology stack but also in their partnerships. CIOs and CISOs will turn to their security partners for support, with increased expectations for enhanced quality and proactive measures in cybersecurity collaboration. The ongoing democratization of AI will significantly reduce the barriers for threat actors, enabling even those lacking experience and skills to target and compromise organizations at a large scale. This will lead to an escalation in both the quantity and sophistication of cyber threats. The pulse of 2024 will resonate with major global events, particularly elections. Geopolitical tensions will continue to fuel cyber espionage and attacks on critical infrastructure and in turn, we expect nations to ramp up cybersecurity laws and regulations.*
These complexities are reshaping the role of the CISO, intensifying the pressures they face. Senior security leaders will turn their attention to the effectiveness of their SecOps, risk management, and existing security architecture projects. Their role will make the difference between success and failure for many organizations.

The world is evolving. Technology is evolving. Our attack surface is bigger than it has ever been. It is time to change the way we address threats, recognizing that cybersecurity is not a purely technological matter, but a business challenge that requires active commitment from executives to increase organizational resilience."

Raluca Saceanu
CEO, Smarttech247

THE EVOLVING THREAT LANDSCAPE

Smarttech
YOUR 24/7 SECURITY PARTNER

If there's anything 2023 has shown us, it's that cyber attacks have continued to grow, both in quantity and in sophistication. Our Threat Intelligence Centers reported a 50% increase in cyberattacks in 2023 compared to the previous year. Unfortunately, the research shows us that many organizations under-report cyberattacks, which could skew the perception of the true scale of the threat. Looking at the vulnerability landscape, the total number of CVE vulnerabilities reported so far in 2023 is 26124, a 5% increase from 2022 (total number of CVE reported vulnerabilities in 2022: 25082). External malicious actors continue to account for the majority of data breaches (83%).

Financial motives are still the driving force behind over 94% of actual breaches. Ransomware and the growing role of AI are particularly concerning as threat actors increase the volume and size of attacks through automation and the sophistication of attacks with AI. We see this increase in the sophistication of social engineering content and increasingly deceptive phishing emails. Use of Stolen Credential (>40%) and Phishing (>20%) continue to feature strongly as action categories in actual data breaches

94% of actual breaches are driven by financial motives

83% of Data Breach Attacks involve external malicious actors

50% increase in cyber attacks in 2023 compared to 2022

The cyber threat landscape of 2023 was characterized by an expanded target scope, a relentless focus on disruption and novel ways to compromise systems. Here are some recurring themes observed over the past 12 months :

- Escalating geopolitical tensions have amplified the overall risk landscape, placing state-sponsored cyber attacks at the forefront of global concerns.
- The surge in Distributed Denial of Service (DDoS) attacks mirrors the intensification of geopolitical conflicts.
- The increasing sophistication of the underground market for cyber tools and services particularly ransomware-as-a-service was evident in 2023. Entities like Alphv and LockBit exemplify the speed and expertise with which cyber adversaries operate, catalyzing widespread business disruptions on a global scale.
- Artificial Intelligence (AI) has augmented the arsenal of cybercriminals and expanded the attack surface.
- More and more organizations have struggled to employ proper network segmentation, allowing threats to propagate unchecked across infrastructures.
- Supply chain security risks continue to present a growing threat, enabling attackers to weaponize environments with alarming efficacy.
- The audacity of cyber attackers reaches new heights, as evidenced by instances where breaches are brazenly reported to regulatory bodies such as the SEC. This boldness underscores the evolving tactics of adversaries for financial gain.
- Unmanaged devices persist as a critical vulnerability, serving as a gateway for 80-90% of ransomware attacks.

Notable Vulnerabilities, Attacks and Breaches

Citrix Bleed

Citrix Bleed, marked by its critical nature and prolonged exploitation, has become the talk of the cybersecurity landscape in 2023, dominating discussions and raising widespread concerns about the vulnerabilities that organizations face in the digital age.

Citrix Bleed has not only been actively exploited in the wild since at least October 23, but its severity is underscored by the involvement of ransomware groups such as LockBit 3.0 and Medusa. These groups leverage the vulnerability as part of attacks against organizations, adopting a strategy of double extortion, where they encrypt files and steal sensitive information to threaten victims into paying a ransom. The downstream impact of this vulnerability extends across various industries, including finance, government organizations, technology, professional services, legal, freight, and defense.

Despite Citrix releasing patches to address Citrix Bleed, the potential for stolen session tokens to persist poses an ongoing threat. Affected organizations are urged to assume compromise, conduct an incident response investigation, and take additional measures outlined by Citrix to remove active or persistent sessions. The timeline of events, including the zero-day exploitation discovered by Mandiant and subsequent in-the-wild attacks, paints a concerning picture of the widespread exploitation and the urgency for organizations to address this critical vulnerability promptly.

MOVEit

In May 2023, the ransomware group Clop exploited a zero-day vulnerability in Progress Software's MOVEit Transfer tool, triggering a far-reaching cyber assault affecting government bodies, public institutions, and businesses globally. Despite swift patches released by Progress, the aftermath proved severe, with data breaches striking prominent entities like New York City's public school system and a UK-based HR solutions company, impacting esteemed clients such as British Airways and BBC.

This breach impacted over 2,600 organizations worldwide and compromised the data of more than 77 million individuals, predominantly within the United States. The repercussions extended to distressing revelations, including the theft of sensitive information encompassing newborns and expecting patients in Ontario, affecting approximately 3.4 million people from 2010 to 2023. Legal repercussions followed, with class action lawsuits filed against companies like IBM, Prudential Financial, and Progress Software, while regulatory changes, such as the SEC's mandate for swift cybersecurity incident disclosures by public companies, underscored the far-reaching consequences of these high-profile cyber attacks. Other victim organizations included Avast, Welltok, SIEMENS, UCLA, Allegiant Air, Jackson Financial among others.

Royal Mail

The LockBit ransomware group claimed responsibility for the cyberattack on Royal Mail, causing significant disruption to the UK's leading mail delivery service, which temporarily suspended international shipping services. Initially, LockBitSupport, the group's public representative, denied involvement, attributing the attack to other threat actors using their leaked LockBit 3.0 ransomware builder. However, they later confirmed their affiliation's role in deploying ransomware on Royal Mail's systems through a forum post. The attackers demand a ransom and threaten to leak stolen data, scheduled for publication on February 9.

Royal Mail detected the attack on January 10 and engaged external forensic experts for investigation. While the company acknowledged service disruptions for international shipping, it referred to the incident as a "cyber incident" and is collaborating with UK security agencies, including the National Crime Agency and the UK National Cyber Security Centre (NCSC). Despite potential implications of a data breach due to LockBit's data theft practices, Royal Mail has yet to explicitly label the incident as a ransomware attack. This event compounds the company's IT challenges following a previous November 2022 outage, occurring amid ongoing negotiations and planned strikes with the Communication Workers Union, further impacting its mail services.

Notable Vulnerabilities, Attacks and Breaches

Chat GPT

ChatGPT, known for its groundbreaking AI capabilities, entered public discussions for its revolutionary technology. However, in late March, the company encountered a setback as it disclosed a data breach. OpenAI officials, the parent company of ChatGPT, revealed that in the hours leading up to ChatGPT's temporary shutdown on Monday, certain users had the potential to view another active user's first and last name, email address, payment address, and only the last four digits of a credit card number along with the credit card expiration date. It is emphasized that complete credit card numbers were never exposed.

Star Blizzard

In December, a combined advisory from cyber security authorities in five-eyes states reviled details of a global spear phishing campaign. This was linked to the Russian FSB (Federal Security Service). The Star Blizzard threat actor has targeted academia, defence, governmental organisations and NGO's since 2019, and have concentrated on the US, UK and other NATO states. Star Blizzard uses open-source resources to conduct reconnaissance, creates email accounts and social media profiles to impersonate contacts of their targets, and use conference invites as a lure.

The spear-phishing emails mostly targeted personal emails, rather than business accounts, to by-pass security controls. Once trust has been established, the threat actor shares a link that will prompt the target to share email credentials. Once Star Blizzard has access to a targets email account, it accesses the information, and they have also used the compromised accounts for follow on targeting. It is assessed as likely that Star Blizard's activities are part of Russia's information strategy in the information-psychological cyberspace.

The UK Electoral Commission

The UK Electoral Commission faced a severe data breach exposing personal information of around 40 million individuals, a revelation made public on August 8th, 2023, despite the incident being detected in October 2022. The breach compromised various personal data types, including names, email addresses, home addresses, contact numbers, and content from web forms and emails. Additionally, personal images sent to the Commission and Electoral Register entries were compromised, containing details like voting age attainment dates. Initially termed a 'complex cyber-attack,' investigations revealed lapses in cybersecurity practices. A whistleblower disclosed that the Commission failed a Cyber Essentials audit around the time of the breach. Moreover, security researchers found an unpatched Microsoft Exchange Server, susceptible to the ProxyNotShell attack when the breach occurred.

Sellafield Breach

In December 2023, it was announced that Sellafield suffered a breach. Nuclear power plants and their operators have been the target of offensive cyber operations in the US in 2023, Ukraine in 2022, India in 2019 Germany in 2016, and Iran in 2010. The reported failure to meet standards by a nuclear power operator is concerning. While agencies like the NCSC in the UK and Ireland are trying their best to support critical national infrastructure, it is imperative that they are resourced adequately to match the current threat landscape. The Guardian has reported a possible link to Russian and Chinese threat actors, and the cyber domain cannot be viewed in isolation, so real-world events will drive the motivations for grey zone aggression. In the medium term, hopefully, initiatives like the Cybersecurity Tech Accord will solidify norms around the use of cyberspace, but in the short term – organizations need to prioritize their cyber defence.

T-Mobile

In May, T-Mobile experienced its second data breach of 2023, wherein a hack exposed the personal information, including PINs, full names, and phone numbers, of more than 800 customers. This incident marks the ninth data breach for the company since 2018 and the second for the year. In January 2023, T-Mobile detected unauthorized access to their systems in the previous November, resulting in the theft of personal data, such as names, emails, and birthdays, from over 37 million customers. Once the breach was identified, T-Mobile swiftly located and contained the source within a day.

T-Mobile anticipates facing substantial costs associated with this data breach, in addition to the $350 million settlement agreed upon in relation to a data breach in August 2021. The company not only suffered significant financial losses due to security vulnerabilities but also eroded customer trust through repeated compromises of personal information.

Yanfeng

The cyberattack on the China-based supplier had an instant cascading impact on the automotive manufacturing supply chain in North America, leading to disruptions at multiple US factories, including those operated by the worldwide automaker Stellantis. The Yanfeng website was unavailable for more than a week and customer service lines were also out of service for several days. Manufacturing sites of Chrysler, Dodge, Jeep, and others at North American factories continue to be on hold as a result of the Yanfeng hack (at the time of writing). The Qilin ransom group has asserted responsibility for the November 13th ransomware attack.

Notable Vulnerabilities, Attacks and Breaches

MGM Resorts

MGM Resorts International, a major player in the global gambling industry, faced a significant cyberattack that disrupted its operations. In response to the breach, the company decided to temporarily shut down its systems to contain potential damage. This incident occurred in the past and is expected to have a substantial financial impact, with MGM projecting a $100 million hit to its third-quarter results. Additionally, the company foresees incurring a one-time cost of less than $10 million related to the aftermath of the cyberattack during the quarter ending on September 30.

Customers who experienced the disruption shared images on social media, showcasing slot machines displaying error messages and noticeable queues at MGM's hotels in Las Vegas. The cyberattack was claimed by a hacking group named AlphV, and reports suggested their collaboration with another entity called Scattered Spider. The alleged objective of this breach was to infiltrate MGM's systems, steal data, and employ it for extortion purposes.

JCI Hack

In September, Johnson Controls International experienced a cyberattack that is still under investigation, raising concerns about potential downstream impacts on its customers. Originally founded in Milwaukee and now headquartered in Ireland, the company, which engages extensively with U.S. federal agencies and the defense industrial base sector, disclosed the incident on September 27 in a filing with the Securities and Exchange Commission. The attack, believed to be ransomware, disrupted internal IT infrastructure and applications, with the Department of Homeland Security (DHS) investigating whether sensitive physical security information, including agency building floor plans, was compromised.

Johnson Controls manufactures industrial control systems, physical security alarm systems, and facility-related technology. Despite the ongoing investigation, the company has not shared new details about the incident and has referred back to its SEC filing. DHS officials, assessing potential impacts, clarified that it was not a breach of any DHS network or system. The Cybersecurity and Infrastructure Security Agency is closely coordinating with Johnson Controls to understand the incident's impacts and provide necessary assistance. The attack highlights concerns about government contractors' security standards, with experts emphasizing the need for accountability and enforcement of minimum cybersecurity standards across the Department of Defense's global supply chain. The threat actor behind the attack, identified as Dark Angels, is known for creating ransomware variants and has targeted organizations in various sectors, including healthcare, government, finance, and education.

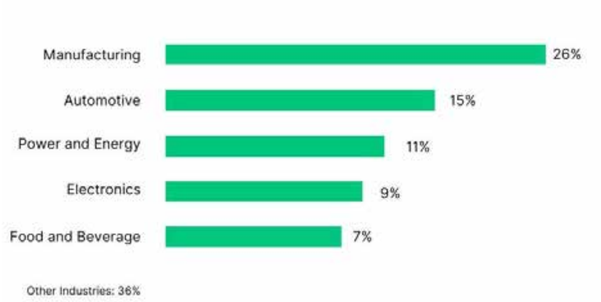


Figure 1: Top 5 attacked industries in 2023, Smarttech247 Threat Intel Research

Mail Chimp

MailChimp encountered another breach as hackers exploited an internal support tool, accessing data from 133 customers. Discovered on January 11th, the attack involved manipulating employees through social engineering to obtain credentials. MailChimp swiftly suspended impacted accounts, notifying customers within 24 hours.

Though no credit card or password details were compromised, accessed data included names, URLs, addresses, and emails. While assurance was given by WooCommerce regarding data misuse, such information is often used in phishing attacks or for malware installation. This incident isn't MailChimp's first; previous breaches in August and April 2022 impacted several accounts, leading to concerns about data protection for MailChimp's customers.

Notable Vulnerabilities, Attacks and Breaches

Caesars Scattered Spider attack

Caesars Entertainment, a prominent U.S. casino chain known for its extensive loyalty program, faced a severe breach where a database containing customer loyalty information was stolen. Initially observed on September 7th, Caesars promptly reported the incident to the US Securities and Exchange Commission through a form 8-K. Fortunately, the company confirmed no evidence of compromised member passwords, PINs, bank account details, or payment card information.

However, it was revealed that Caesars made a ransom payment of approximately $15 million to prevent the leaked data's publication, despite the attackers initially demanding $30 million. Bloomberg later identified the culprit as the Scattered Spider cybercrime group, also recognized as Roasted 0ktapus or UNC3944. Caesars disclosed that the breach occurred due to social engineering targeting an outsourced vendor. Despite the ransom payment, the company cannot assure the safety of its loyalty customers' data, prompting proactive measures like scanning darknet sites and promising customer alerts if their information surfaces. Additionally, Caesars offers complimentary giveaways and free services to customers, aiming to enhance data protection moving forward.

Microsoft Storm-0558

Microsoft disclosed an incident involving the Chinese hacking group, Storm-0558, which gained access to a Microsoft account (MSA) consumer key. This enabled the forging of tokens, granting unauthorized access to Outlook.com (OWA) accounts across approximately 25 organizations. This sophisticated attack, likely state-sponsored, aimed at espionage.

Reportedly, a customer flagged unusual access to Exchange Online on June 16th, alerting Microsoft to the issue. The attackers manipulated the MSA consumer key to forge Azure AD tokens. As a precautionary measure, Microsoft invalidated all active MSA keys. Although several US Government Departments were impacted, neither Microsoft nor the US Government released specific details regarding the extent of the breach or the duration before discovery.

23andMe Data Leak

In early October 2023, 23andMe faced a data leak impacting potentially millions of customers. Hackers accessed legitimate accounts through credential stuffing attacks, collecting data using the platform's 'DNA Relatives' search feature. The leaked information, available for sale online at $1 to $10 per account, includes personal details but does not seem to involve raw DNA data. This incident, while not massive in scale, highlights the risks posed to DNA databases, signaling a concerning trend for companies storing sensitive genetic information.

AT&T

In March, AT&T disclosed a substantial third-party data breach impacting around 9 million customer records. The exposed data included customers' first names, wireless account numbers, phone numbers, email addresses, wireless plan names, due amounts, monthly payments, charges, and usage minutes. However, AT&T clarified that no credit card information, Social Security numbers, account passwords, or highly sensitive personal data were compromised.

Identified as a supply chain attack involving dated device upgrade eligibility data, the breach occurred in January through an unidentified third-party vendor. Although no highly sensitive financial details were exposed, the revealed information could make victims susceptible to targeted phishing attempts. AT&T customers are advised to bolster password security and stay vigilant against unsolicited emails or suspicious account activities.

BlackBasta Ransomware Rampage

The Black Basta ransomware group has escalated attacks in 2023, targeting organizations across Europe and English-speaking countries. Using double extortion tactics, they encrypt data and demand ransom; if refused, they publish data on the dark web. ABB, a Swiss automation giant, was hit in May 2023, disrupting operations and projects. In June 2023, US-based companies faced attacks employing QakBot, impacting various sectors like healthcare, finance, and retail.

NOTABLE TRENDS & DEVELOPMENTS FROM 2023

Smarttech
YOUR 24/7 SECURITY PARTNER

2023 Trends

MITRE ATT&CK TTPs & Vulnerabilities Trends

MITRE ATT&CK® is a global knowledge base of adversary tactics and techniques based on real-world observations.

The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

We are seeing a continuous evolution of the framework and with the release of v14 the framework statistics are a s follows:

- Enterprise: 201 Techniques, 424 Sub-Techniques, 141 Groups, 648 Pieces of Software, 23 Campaigns, 43 Mitigations, and 109 Data Sources
- Mobile: 72 Techniques, 42 Sub-Techniques, 8 Groups, 108 Pieces of Software, 1 Campaign, 12 Mitigations, and 15 Data Sources
- ICS: 81 Techniques, 13 Groups, 21 Pieces of Software, 52 Mitigations, 3 Campaigns, 14 Assets, and 34 Data Sources

New TTPs added in 2023:

- Acquire Access
- Acquire Infrastructure: Malvertising
- Cloud Administration Command
- Command and Scripting Interpreter: Cloud API
- Device Driver Discovery
- Exfiltration Over Web Service: Exfiltration to Text Storage Sites
- Impair Defenses: Spoof Security Alerting
- Masquerading: Masquerade File Type
- Modify Authentication Process: Network Provider DLL
- Obfuscated Files or Information: Command Obfuscation
- Obfuscated Files or Information: Fileless Storage
- Remote Services: Cloud Services
- Unsecured Credentials: Chat Messages
- Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access
- Account Manipulation: Additional Container Cluster Roles
- Content Injection
- Credentials from Password Stores: Cloud Secrets Management Stores
- Exfiltration Over Web Service: Exfiltration Over Webhook
- Financial Theft
- Hide Artifacts: Ignore Process Interrupts
- Impair Defenses: Disable or Modify Linux Audit System
- Impersonation
- Log Enumeration
- Masquerading: Break Process Trees
- Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations
- Obfuscated Files or Information: LNK Icon Smuggling
- Phishing: Spearphishing Voice
- Phishing for Information: Spearphishing Voice
- Power Settings
- Remote Services: Direct Cloud VM Connections
- System Network Configuration Discovery: Wi-Fi Discovery

> **“ Once threat actors infiltrate, it can lead to a comprehensive compromise of the entire environment, particularly in Active Directory setups.**

Looking at the Top 10 TTPs from attacks in the wild:

- "T1047 Windows Management Instrumentation"
- "T1059 Command and Scripting Interpreter"
- "T1053 Scheduled Task/Job"
- "T1562 Impair Defenses"
- "T1021 Remote Services"
- "T1003 OS Credential Dumping"
- "T1543 Create or Modify System Process"
- "T1574 Hijack Execution Flow"
- "T1548 Abuse Elevation Control Mechanism"
- "T1055 Process Injection"

Over the years, our definitive observation has been that, invariably, once threat actors infiltrate, it can lead to a comprehensive compromise of the entire environment, particularly in Active Directory setups.

The primary and foremost concern revolves around the question of "How did they gain access?" Although Phishing (T1566) continues to be the most frequently employed technique for initial access (approximately 70%), a closer examination of the Top TTPs for Initial Access reveals several noteworthy alternative techniques.

• **External Remote Services (T1133):** Identified as the predominant method for initiating access, this technique involves attackers exploiting remote services such as VPN gateways or firewalls to infiltrate networks.

• **Exploit Public-Facing Application (T1190):** Following closely as the second most prevalent initial access technique, attackers leverage vulnerabilities in applications accessible from the internet to gain entry.

• **Valid Accounts (T1078):** In 70% of cases, the misuse of valid accounts was coupled with the exploitation of external remote services. This approach is noteworthy as valid accounts are frequently necessary for initial access through a remote service. Additionally, in the first six months of 2023, compromised credentials, categorized under this method, constituted 50% of the root causes of attacks, surpassing vulnerability exploitation, which accounted for 23%.

2023 Trends

Phishing

The evolution of phishing tactics, particularly the adoption of "Adversary-in-the-Middle" (AiTM) techniques, marks a significant advancement in the methods employed by cyber attackers. Here's a breakdown of this evolution and its implications:

- **Traditional Phishing to AiTM Phishing:** Traditional phishing often involved basic tactics like deceptive emails leading users to fraudulent websites. However, with AiTM phishing, attackers position themselves in the communication flow between the user and the legitimate service. This approach is more sophisticated and harder to detect.
- **Use of Tools like Evilginx, Modlishka, and Browser-in-the-Browser Attacks:**

  Evilginx and Modlishka: These are examples of AiTM phishing tools. They work by creating a proxy layer between the user and the legitimate website, capturing credentials and session cookies, including those used for two-factor authentication (2FA).

  Browser-in-the-Browser (BitB) Attacks: This technique involves creating a fake browser window within the legitimate browser, tricking users into entering their credentials on a fraudulent site that appears legitimate.

- **Bypassing Two-Factor Authentication (2FA):** AiTM techniques can bypass 2FA methods like Time-based One-Time Passwords (TOTP). Since the attacker intercepts the entire session, they can capture and use the 2FA tokens in real-time.
- **The Need for FIDO MFA:** The Fast Identity Online (FIDO) protocol for Multi-Factor Authentication (MFA) is more secure against AiTM attacks. FIDO uses cryptographic login credentials that are not reusable, reducing the effectiveness of AiTM phishing.
- **Use of "Legitimate" Tools and Techniques:** Attackers are increasingly using tools and techniques that appear legitimate to bypass detection systems. For example, incorporating a Captcha on a phishing site can thwart automated systems from detecting the fraudulent nature of the site. This makes it harder for security tools to differentiate between legitimate and malicious websites.

2023 Trends

Traitorware

"Traitorware" refers to a form of cyber threat where legitimate, trusted software or hardware is manipulated or exploited to perform malicious activities.

Because these tools are legitimate and trusted within the environment, they often bypass standard security measures like antivirus software and firewalls, making detection more challenging.

Examples and Techniques:

- **Living Off the Land (LOL) bins:** Attackers use built-in system tools (like PowerShell, Windows Management Instrumentation, or system utilities) to carry out attacks, hence avoiding the need to install external malware.
- **Compromising Remote Management Software:** Software used for legitimate remote management and monitoring can be hijacked to gain unauthorized access and control over systems.
- **Manipulating Security Software:** Even security software like SIEM and antivirus agents can be manipulated for malicious purposes.
- **Whitelisting:** In the Kaseya VSA supply chain attack, certain paths had to be whitelisted. Attackers can exploit such whitelisted paths to avoid detection.

Projects like https://lolbas-project.github.io/ expose full potentiation of functions which can be proven (and abused) by legitimate tools that can be found on most computers.

The use of traitorware highlights the need for a more nuanced approach to cybersecurity, where the integrity and behavior of internal tools and systems are continuously monitored and assessed, not just external threats.

...the not-so sophisticated techniques are still important

Beyond the allure of novel techniques, a careful examination of our own experiences and the global threat landscape reveals that age-old security issues continue to wield a substantial threat. Take the notorious MOVEit incident, for instance, where the vulnerability at play was an "SQL Injection" - a type of issue for which effective remediation measures are well-established. Despite the strides made through properly implemented secure software development lifecycles, it's disconcerting to encounter such issues persisting in a widely-used platform in the year 2023.

We are seeing a continuous evolution of the framework and with the release of v14 the framework statistics are as follows:

- **Absence of mandatory SMB Signing**
- **Utilization of weak, reused, or default vendor passwords**
- **Employing highly privileged accounts for routine tasks**
- **Insufficient implementation of Network Level Authentication (NLA) in RDP**
- **Default SNMP Community Names**

StealerLogs

A notable surge in cybersecurity issues originates from Stealer Logs, representing threat actors' response to organizations transitioning to cloud services, adopting BYOD policies, and implementing multifactor authentication (MFA). Stealer logs not only harvest credentials but also authentication tokens from infected computers, enabling threat actors to access organizational resources—a heightened form of initial access for credentials.

Within most environments, these assets are intricately interconnected, either directly or indirectly. Threat actors can exploit compromised credentials from a third-party leaked website to gain access to the victim's Active Directory. Through lateral movement and privilege escalation, they can obtain the "keys to the kingdom."

The risk associated with a SaaS application hosted on a cloud service extends beyond the vendor; it also pertains to the organization using it. If a service is granted excessive information or privileges within the environment, a compromise of the SaaS platform can have severe repercussions on the organization.

2023 Trends

A Dark(web) View

Relevant Statistics:

- **117** Dark Net forums
- **37** Dark Net markets
- **~50** Ransmoware group leak sites
- **> 4000** telegram channels

Key Takedowns

The Hive ransomware group, notorious for its widespread cyber attacks, was effectively neutralized in a sophisticated operation by the FBI. This operation, involving advanced cyber tactics, resulted in the dismantling of the group's infrastructure and the arrest of key members, marking a significant victory against cybercrime and ransomware activities.

Breach Forums, an illicit forum catering to English speakers, was poised to succeed Raid Forums. Launched by threat actor 'Pompompurin' on March 16, 2022, it quickly turned into a prime destination for hackers looking to purchase or vend compromised data. On March 15, 2023, it was disclosed that Conor Brian Fitzpatrick was the individual behind 'Pompompurin,' leading to his arrest.

Genesis Market, a prominent invite-only dark market known for selling stolen credentials, was recently dismantled. This market, over its five-year operation, accumulated data from over 1.5 million computers and 80 million account credentials. The takedown, named 'Operation Cookie Monster,' was a significant effort by the FBI and European law enforcement. They successfully arrested over 100 individuals connected to the market and shut down its web domains, marking a notable crackdown on cybercrime and illicit data trading

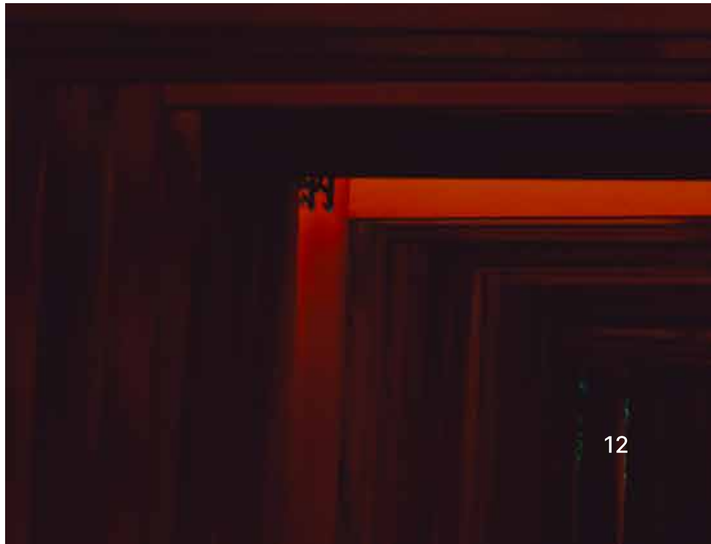
The EncroChat encrypted mobile communications platform, offering unbreakable encryption and anonymity, was brought down by a significant European law enforcement operation in 2020. This sophisticated infiltration led to the arrest of over 6,600 individuals and the seizure of $979 million in illicit funds. The takedown was a result of cracking the platform's encryption, analyzing millions of messages between about 60,000 users. Law enforcement agencies were able to confiscate large quantities of drugs, weapons, vehicles, and other assets. The majority of EncroChat users were involved in organized crime and drug trafficking, leading to thousands of years of cumulative prison sentences for the arrested individuals

Dark Web: New Methods and Shifts

Despite the takedowns, the “space doesn’t like emptiness”. It is filled with replacements. A significant shift towards Telegram can be seen.

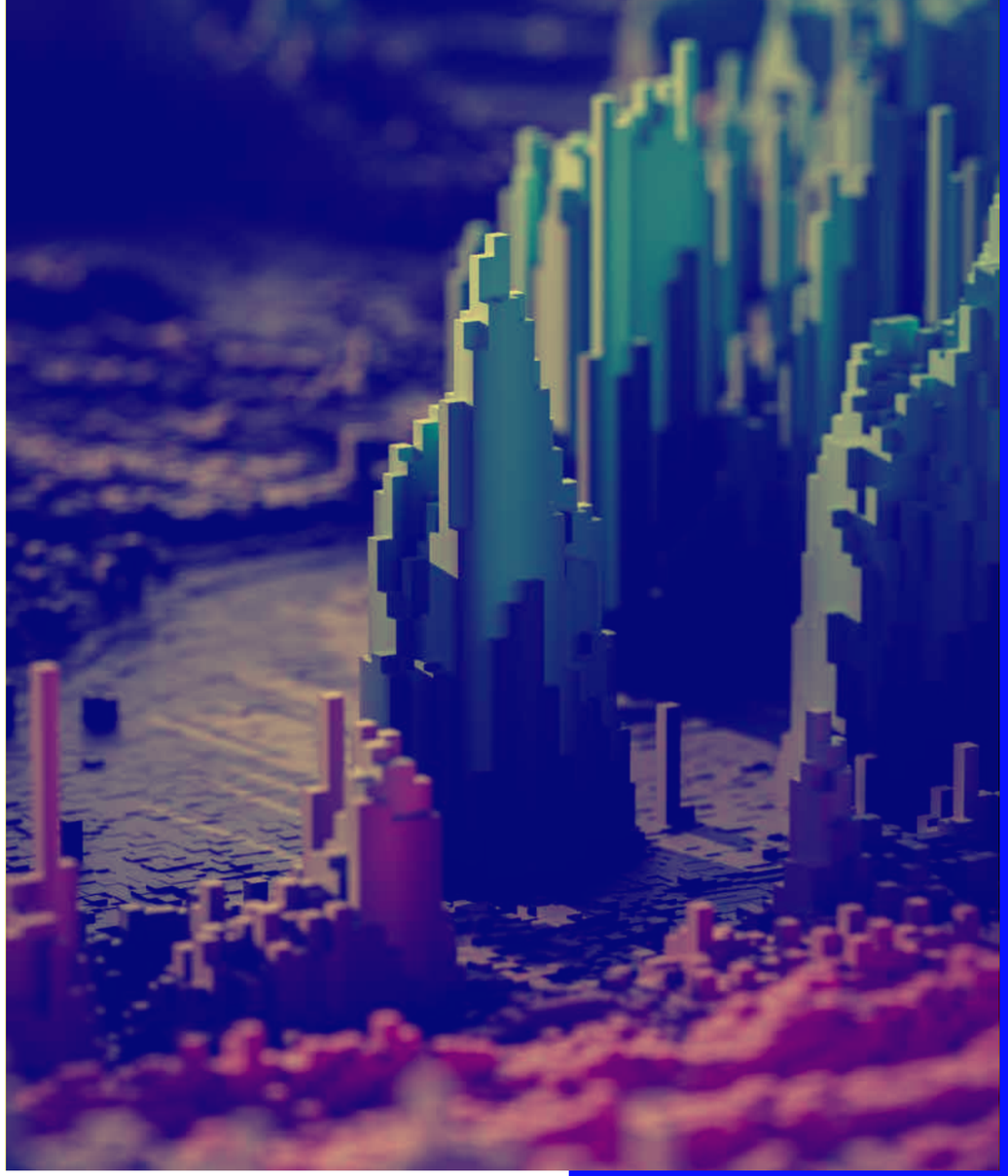
A newly established dark web marketplace, **STYX**[5], launched earlier this year, is rapidly developing into a popular center for illicit transactions, including the purchase and sale of illegal services and stolen data. This platform offers a range of unlawful services such as money laundering, identity theft, DDoS attacks, circumvention of two-factor authentication, distribution of counterfeit or stolen IDs and personal information, malware leasing, cash-out operations, extensive email and telephone harassment, identity searches, among other criminal activities.

Telegram's hacking channels have evolved into a central point for distributing stolen data, cybercrime tools, and unauthorized guides. Those channels can’t be easily taken down like the websites. The secure messaging platform has recently turned into a bustling online marketplace for cybercriminal activities due to these factors.



KEY PERSPECTIVES & TRENDS FOR 2024

Smarttech
YOUR 24/7 SECURITY PARTNER



MACRO TRENDS

In the dynamic landscape of cybersecurity, the next 12 months are poised for transformative shifts driven by strategic initiatives from CISOs and Senior Security executives. Security leaders will be adopting attack surface management mindsets as well as more targeted offensive and defensive tactics. Organizations will also actively consolidate security vendors, streamlining operations, and prioritizing integrated solutions. 2024 will witness a heightened focus on a human-centric approach to cybersecurity awareness training and other key initiatives, reflecting a departure from static methodologies. Additionally, trends such as enhanced Operational Technology (OT) security measures, increased automation in incident response, and heightened controls in data security are indicative of a concerted effort to secure against evolving cyber threats.

Attack Surface Management

One prominent trend revolves around the adoption of a holistic approach to managing the entire security ecosystem. CISOs are increasingly viewing their organization's security posture through the lens of attack surface management. This entails a thorough examination and fortification of all potential entry points and vulnerabilities across the infrastructure. In the past, an IT asset was typically just a computer on the network, often identified by an IP address or as a separate host. Today, assets encompass a much broader spectrum, including IPs, network services, technology stacks, SaaS platforms, domains, identities and their credentials, web and mobile applications, mobile devices, and IoT and OT components. This expanded scope underscores the need for a nuanced and thorough approach to security. Consequently, organizations will prioritize investments in tools and strategies that provide a unified view of their entire attack surface, fostering a more comprehensive and proactive defense against cyber threats.

Cybersecurity Validation

Another noteworthy trend involves the evolution of cybersecurity validation efforts, with a shift towards a red team–blue team approach. Organizations are intensifying their cybersecurity validation by incorporating simulated attacks (red team) to identify vulnerabilities and weaknesses, followed by defense and response exercises (blue team) to enhance incident response capabilities. This signifies a broader embrace of both offensive and defensive tactics within cybersecurity strategies. Companies will allocate resources towards training and technologies that strenghten the detection and response aspects of their cybersecurity programs.

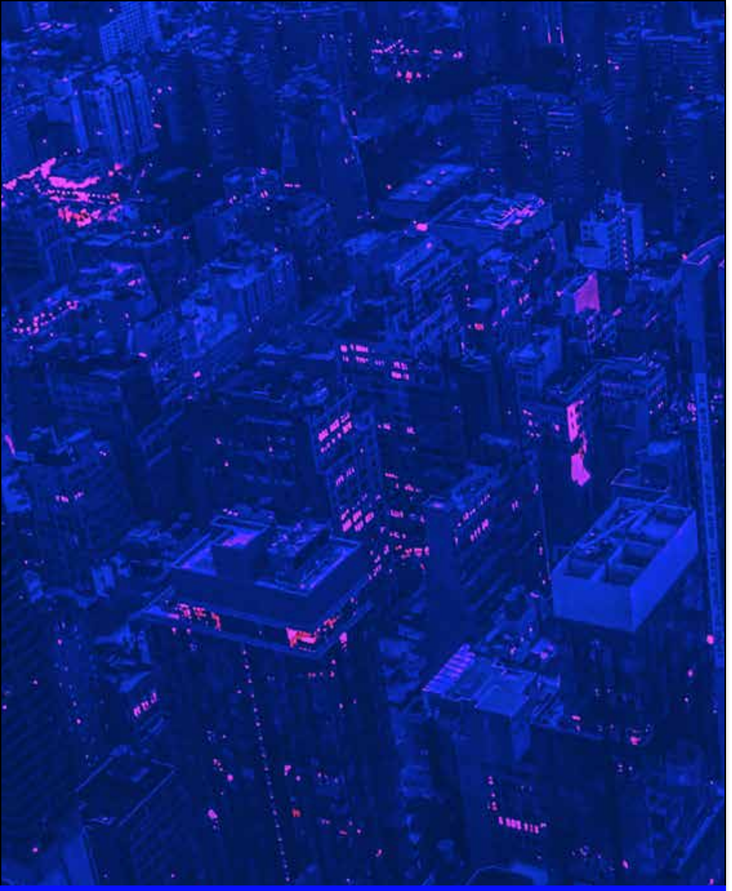
Vendor Consolidation and Removing Complexities

We all know it. Cybersecurity is a complex industry and in our conversations with internatinaol organizations and their CISOs, one trend is alarmingly clear: security operations are lacking efficiency. Organizations have to deal with too many tools, report on complex metrics and drive security operations models with limited resources. There is a discernible trend towards the consolidation of security vendors and the simplification of security operations. Organizations are actively seeking to reduce complexity, improve operational efficiency, and gain a clearer understanding of dependencies. This consolidation effort will manifest in the form of using fewer, more integrated security tools and approaches. While this streamlining of operations is expected to enhance overall efficiency, organizations will also need to exercise caution in managing and monitoring the associated risks stemming from a reduced number of vendors and tools. The cybersecurity landscape is poised for a wave of mergers and acquisitions as companies strive to provide more comprehensive solutions to address the evolving threat landscape.

Less Machine, More Human

In tandem with these strategic shifts, the overarching theme is a more human-focused approach to cybersecurity. This is evident in the changing landscape of cybersecurity awareness training, where organizations are recognizing the limitations of static, one-way-led approaches. Companies are now actively involving users in a more participatory manner, seeking their feedback on the effectiveness of security awareness programs. As a result, the next 12 months will likely witness a continued emphasis on human-centric cybersecurity approaches that acknowledge the evolving nature of cyber threats and the importance of an engaged and informed user base.

> “ Organizations are actively seeking to reduce complexity, improve operational efficiency, and gain a clearer understanding of dependencies.



> “The threat landscape is driving a real demand for 24/7, always-on monitoring, triage and incident response - not just for IT but for OT, too.

Automation in Incident Response

Broad adoption of digital transformation has pushed IT from the backroom to be an integral part of the supply chain and so increasing the stakes when things go wrong. Coupled with increasing regulatory and disclosure requirements, a heightened threat landscape is driving a real demand for 24/7, always-on monitoring, triage and incident response.

Organizations are increasingly demanding Incident Response that is over and above hand-holding requesting fully automated incident response with increasing demand for advanced incident response including containment, forensics investigation and communication support.

This is supported by a growing awareness of the need for Incident Response planning and understanding of the unique characteristics of cyber incidents compared to traditional DR and BC events.

OT Security

The fundamental drive across all sectors to transform our economy digitally has not escaped the traditional supply chain. OT systems are increasingly being connected to office environment, to suppliers and to external systems. While this challenge is not new, it has traditionally been the focus of the automation community and CISOs are increasingly being tasked with bringing the entire IT/OT stack into a single governance, risk and control view. This is driven both by the threat environment and increased regulation.

Again, resourcing and tooling are critical here with different technologies and business impacts driving demand. This is also complicated by the multi-site, multi-national impact of cyber attacks where traditional BC and DR strategies have been country or site-based.

Data Security

The development of the CISO from being a strong technical architect of security controls to being a senior leadership team/ boardroom player is now being further challenged by the increasing requirements around data security. The complexity of data to be considered from PII, to PHI to IP to source code, the array of stakeholders from IT to the data owners (i.e. business leaders) to regulatory and compliance stakeholders means the CISO has to increasingly corral a multitude of stakeholders in a multi-faceted program to agree what is important, identify it, find it, classify and label it and put the necessary controls in place.

This is compounded by what we are seeing as, the real need for fundamental awareness about intellectual property ownership and responsibility at an individual level across most organizations. Too often are we hearing “I thought I owned that data”. We will see wider adoption of holistic data security governance approaches, with more organizations looking to handle their data loss prevention, data classification, encryption and security of data in a modern way.

10 GLOBAL CYBERSECURITY PERSPECTIVES

For 2024 and beyond

1. SHIFTING PARADIGMS IN VULNERABILITY MANAGEMENT: FROM CVSS SCORES TO BUSINESS-CENTRIC RISK ASSESSMENT

In the ever-evolving landscape of cybersecurity, vulnerability management is undergoing a significant transformation. Historically, vulnerability management largely relied on Common Vulnerability Scoring System (CVSS) scores obtained from vulnerability scans, leading to a primarily reactive approach. However, the field is now transitioning towards a more proactive stance, with a stronger emphasis on business risk, vulnerability exploitability, and threat surface management.

Vulnerability management has long been an essential component of cybersecurity, aimed at identifying and mitigating security weaknesses in an organization's IT environment. Traditionally, CVSS scores have been the cornerstone of this process. While CVSS scores offer valuable insights into the technical severity of vulnerabilities, they do not provide a comprehensive understanding of the actual risk they pose to the business.

Instead, in the last 12 months we have seen organizations pivoting from a reliance on CVSS scores to an approach that factors in business/asset risk, vulnerability exploitability, and threat surface management. The approaches are also changing due to the challenges posed by limited budgets and a shortage of skilled experts, as these factors necessitate a more refined prioritization of remediation efforts.

The Reactive Nature of CVSS Scores

The CVSS is a well-established system for rating the severity of vulnerabilities on a scale of 0 to 10, with a higher score indicating a more severe vulnerability. While CVSS scores provide a baseline for understanding the technical impact of vulnerabilities, they have inherent limitations. This approach has primarily been reactive in nature, focusing on:

Technical Severity
CVSS scores assess the technical impact of vulnerabilities, such as the ease of exploitation and potential consequences. However, they often lack context about how a particular vulnerability could affect the organization's business operations.

Patch Prioritization
Organizations often use CVSS scores to prioritize patching based solely on severity. This can lead to a "patch all the high-severity vulnerabilities" approach without considering the actual business impact.

Overlooking Threat Landscape
CVSS scores don't account for the evolving threat landscape, where the likelihood of a vulnerability being exploited is influenced by factors like its relevance to attackers and the availability of exploits.

New Metrics Gaining Traction

To address the weakness in CVSS, and align more with a risk-based approach, newer metrics are gaining traction in the field of vulnerability management:

Exploitability-Probability Severity Score (EPSS): EPSS combines traditional severity metrics with elements of exploitability, asset value, and threat intelligence. This approach provides a more nuanced view of vulnerabilities, enabling organizations to prioritize remediation efforts more effectively.

Vulnerability Priority Rating (VPR): VPR is another evolving metric that takes into account factors like the threat landscape, asset value, and availability of exploits. It provides a holistic view of vulnerability risk, helping organizations allocate their resources wisely. It is proprietary to Tenable, a vulnerability platform provider.

Vulnerability Management: Key trends for 2024

SHIFTING TO A RISK-CENTRIC APPROACH

The transition towards a risk-centric vulnerability management approach underscores the importance of aligning security with the organization's business objectives. This approach factors in business risk by considering the following:

Impact on Business Operations: Vulnerabilities are assessed not only for their technical severity but also for their potential impact on business continuity, data confidentiality, and compliance.

Asset Valuation: Criticality and value of assets are weighed when prioritizing vulnerability remediation. High-value assets receive greater protection.

Compliance Requirements: Organizations must meet various compliance standards, and these requirements are integrated into vulnerability management processes.

EVALUATING VULNERABILITY EXPLOITABILITY

The focus on exploitability aims to understand how likely it is that a vulnerability will be exploited in the wild. This requires a broader view of the threat landscape, taking into account:

Threat Intelligence: Regularly updated threat intelligence is essential for identifying emerging threats and vulnerabilities actively targeted by attackers.

Historical Data: Analyzing past incidents and breaches provides insights into which vulnerabilities are frequently exploited.

Attack Surface Analysis: An in-depth analysis of an organization's attack surface helps identify potential entry points for attackers.

THREAT SURFACE MANAGEMENT IS VULNERABILITY MANAGEMENT

The shift towards a more comprehensive vulnerability management approach also encompasses the organization's threat surface.
This involves:

Asset Discovery: An accurate inventory of assets and their criticality, including those in cloud environments and IoT devices, is critical for an effective threat surface assessment.

Third-Party Risks: Evaluating vulnerabilities in third-party dependencies, such as software vendors and service providers, is an integral part of threat surface management and understanding where risks to the organization may reside.

Zero Trust Architecture: Adopting Zero Trust principles, which involve continuous monitoring and least privilege access, helps reduce the threat surface and potential impact of vulnerabilities.

OTHER KEY VULNERABILITY MANAGEMENT TRENDS FOR 2024

Integration of Vulnerability Management with DevOps: Recognizing the inadequacy of traditional security practices in rapid software delivery environments, there is a trend towards seamlessly incorporating security into the DevOps pipeline. This paradigm shift enhances security, fosters collaboration between development and security teams, streamlines processes, and ensures that security is not sacrificed for speed.

Cloud Integration: With the increasing migration to the cloud, there is a heightened focus on cloud security. Organizations are adapting vulnerability management strategies to address cloud-native vulnerabilities and configurations, recognizing the unique security challenges introduced by cloud environments.

Artificial Intelligence and Machine Learning Integration: The integration of AI and ML technologies into vulnerability management is revolutionizing security approaches. These advanced technologies enable more accurate and efficient identification of vulnerabilities, automate repetitive tasks, and enhance a company's ability to protect its assets effectively.

Continuous Vulnerability Assessment and Remediation: Continuous, real-time monitoring of security posture for vulnerabilities and malware has replaced periodic scans. This practice allows organizations to swiftly identify and address emerging threats, aligning with the need for proactive defense and immediate remediation.

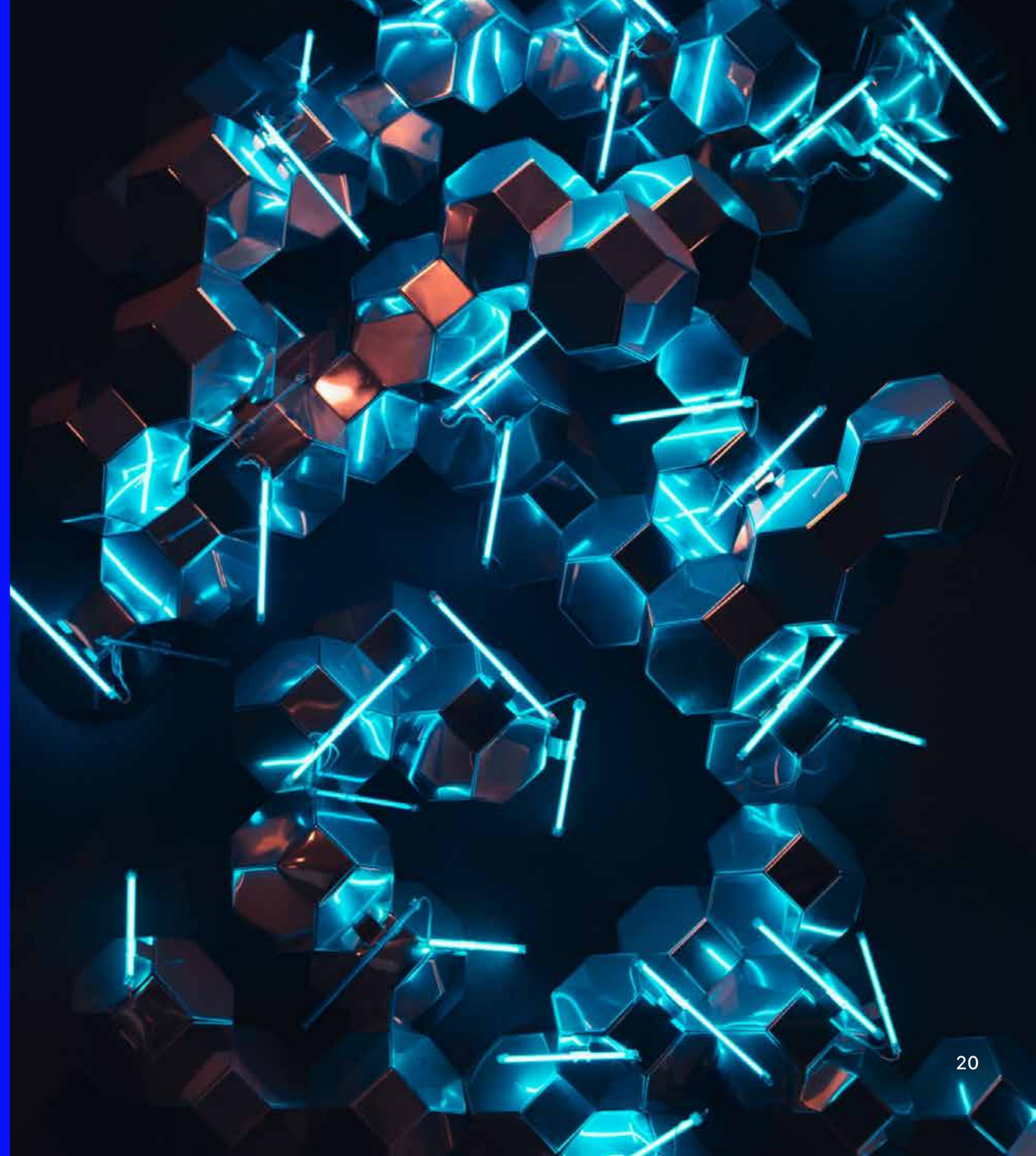
Asset Management and Prioritization: The complexity of digital infrastructures has led to the essential practices of asset management and prioritization. Statistics indicate that 75% of organizations will use asset management to prioritize vulnerabilities by 2024, highlighting the increasing recognition of the importance of understanding the criticality of assets and focusing resources where they matter most.

> "75% of organizations will use asset management to prioritize vulnerabilities by 2024

The shift from a reactive CVSS-based vulnerability management approach to one that considers business risk, vulnerability exploitability, and threat surface is pivotal for organizations to enhance their security posture. This transformation is particularly relevant in the face of limited budgets and skilled expert shortages.

By embracing this new approach and leveraging emerging metrics like EPSS and VPR, organizations can maximize the impact of their vulnerability management efforts, effectively mitigating risks and safeguarding their digital assets in an ever-evolving threat landscape. Moreover, when looking at vulnerability management, it is important to understand that budget and skills constraints have an impact on organizations' ability to tackle their vulnerability challenges.

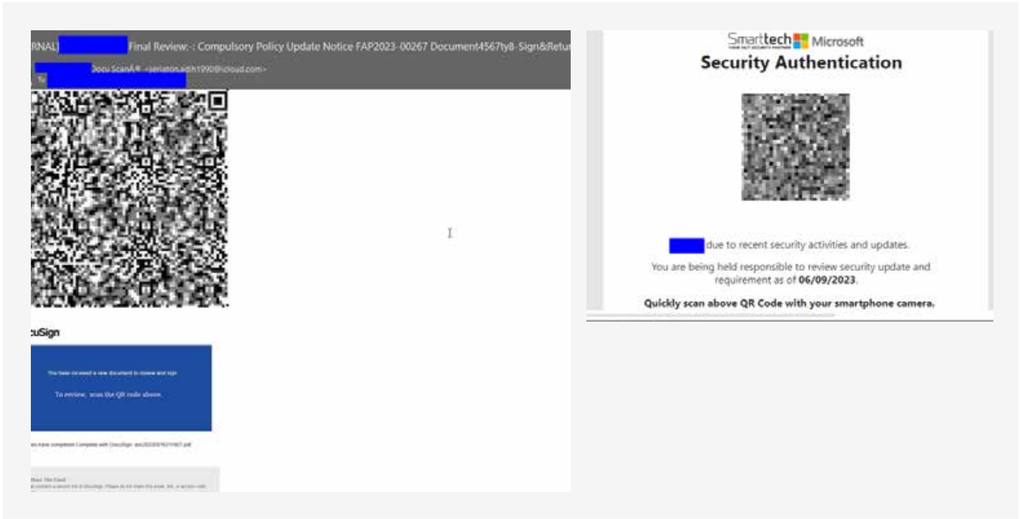
Organizations may struggle to find or afford cybersecurity experts. However, by adopting a risk-based approach, organizations can simplify vulnerability management by providing a more nuanced and prioritized view of vulnerabilities. EPSS incorporates factors like exploitability, asset criticality, and threat intelligence, enabling organizations to make more informed decisions to reduce risk with a limited budget. Leveraging automation in vulnerability management can mitigate the impact of skill shortages. Automated tools can help identify and prioritize vulnerabilities while also implementing patches or mitigations as needed, allowing a resource-thin team to focus on more challenging resolutions.



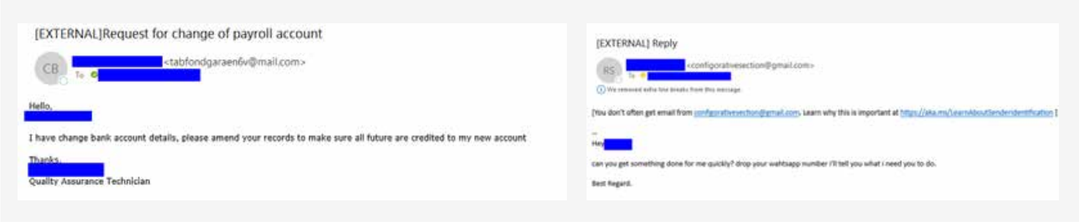
2. SOCIAL ENGINEERING IN 2024: AI-POWERED PHISHING, DEEPFAKE DECEPTIONS, AND THE USER DEFENSE EVOLUTION

In 2023, there has been a significant surge in phishing attacks, and what is particularly alarming is the evolving sophistication of these attacks. In our Threat Intelligence Centers, we have noted a 60% increase from 2022 in phishing attacks, with a primary target being the healthcare industry. Cybercriminals have increasingly demonstrated their capability to bypass conventional security email tools, rendering them less effective in safeguarding against these malicious campaigns.

Attackers are now employing a range of methods that go beyond traditional phishing tactics. This includes the use of QR codes, which can be employed to lure victims into unwittingly accessing malicious websites or downloading harmful content. This tactic exploits the trust users place in QR codes for convenience.

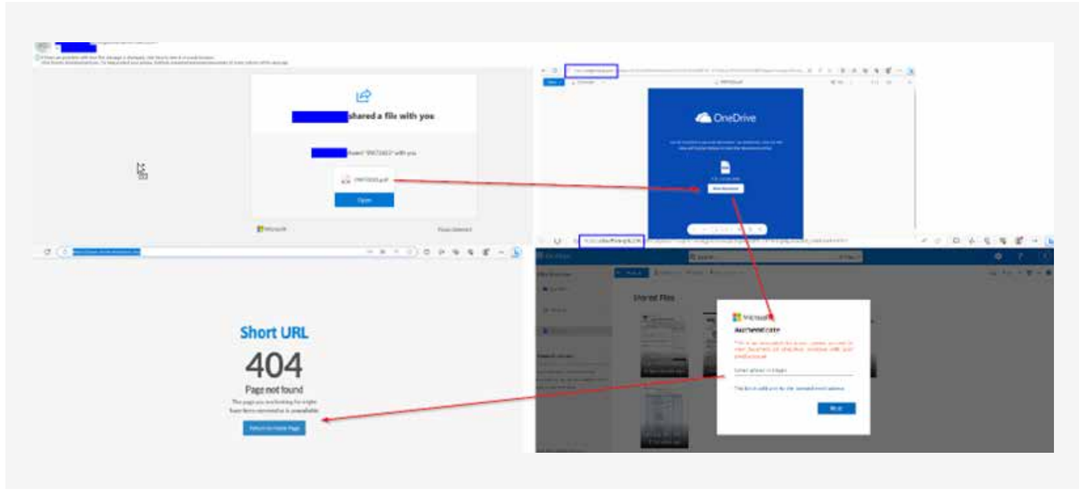


Furthermore, attackers are opting for simplicity by using just plain text in their phishing attempts, a method that can be surprisingly effective. This minimalistic approach often evades the scrutiny of email filters, relying on the recipient's trust in seemingly benign messages.



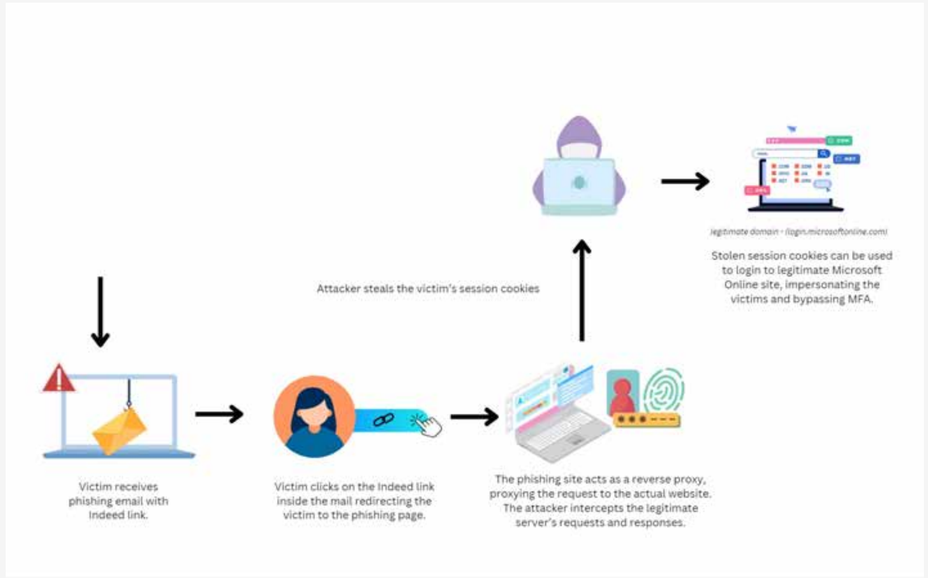
Redirects – A Lucrative Method

Another technique in the attackers' arsenal is the utilization of redirects. By employing these, they can lead victims through a maze of web pages before ultimately landing on a phishing page or malicious download link, making it more challenging for security tools to track and block such activities.



Advanced MFA Bypass

Beyond these techniques, the attackers are also developing more advanced Multi-Factor Authentication (MFA) bypass methods. These include the use of social engineering tactics to trick users into revealing their authentication codes or one-time passwords. Additionally, attacks that target the weaknesses in hardware tokens or mobile authentication apps are on the rise, compromising the integrity of MFA systems.



Mirroring the genuine website in a phishing attack imparts an illusion of authenticity to the scheme, as the victim perceives themselves to be interacting with the actual site via the attacker's proxy server. Nonetheless, despite the victim's engagement with the legitimate website, deviations in the URL and TLS certificate can serve as telltale signs of deception, as they diverge from the original source. Moreover, when a user accesses the legitimate site via the proxy, this inadvertently prolongs the longevity of captured Multi-Factor Authentication (MFA) session cookies, thereby affording the attacker an extended window of opportunity for executing malicious activities.

Phishing: Key Trends for 2024

In the phishing threat landscape for 2024, we anticipate a rise in AI-powered attacks as malicious actors leverage artificial intelligence and machine learning to craft more convincing and contextually relevant phishing emails. This could significantly increase the difficulty for users to discern between legitimate and malicious messages.

Deepfake technology is likely to be exploited in phishing campaigns, with attackers using realistic audio or video messages to deceive individuals into divulging sensitive information. Cloud services may become a prime target, with phishing attacks focusing on compromising credentials for cloud-based applications, storage, or collaboration tools due to the widespread adoption of these services.

Supply chain attacks are expected to grow, with attackers targeting vendors or service providers to gain access to a broader network of potential victims. This could lead to more sophisticated and widespread phishing campaigns. Additionally, phishing attacks may increasingly exploit zero-day vulnerabilities in popular applications, making detection and mitigation more challenging.
The combination of social engineering and malware delivery is likely to become more prevalent in phishing campaigns, with malicious attachments or links deploying sophisticated malware. New attack vectors beyond email may emerge, such as exploiting vulnerabilities in emerging technologies like IoT devices or utilizing alternative communication channels.

As phishing attacks continue to evolve and grow in sophistication, it's essential for individuals and organizations to remain vigilant and employ a combination of advanced security tools, user education, and robust cybersecurity practices to mitigate these emerging threats effectively. But how should tackle this challenge in a more effective way? Revamping user training is key, considering the current methods are outdated and often lack a human-centric approach in addressing evolving phishing threats. Instead of relying on traditional training, it's essential to adopt a more modern, user-focused strategy that aligns with the dynamic nature of cyber threats. This entails moving away from rigid structures and embracing interactive, engaging, and personalized training modules that cater to the diverse learning styles and experiences of individuals within the organization. By doing so, we can ensure that users are not just educated on the latest phishing tactics but are empowered through a learning experience that resonates with them on a more human level.

Here are a few ideas on how to tackle Phishing challenges:

Implement simulated phishing with a little extra. For example, in order to enhance engagement, incorporate gamification elements into the training program. Interactive challenges, quizzes, and rewards for milestones not only make learning enjoyable but also increase retention.

Customize training paths based on user roles within the organization. Tailored content ensures that individuals receive information relevant to their specific responsibilities. Utilize interactive learning platforms offering videos, modules, and assessments to accommodate various learning styles and reinforce key concepts.

Introduce managed phishing response tools to simplify incident reporting. These tools streamline the process, allowing for quick analysis and remediation of reported incidents. Create a collaborative environment where users actively contribute to the organization's cybersecurity defense.

Simplify the reporting process with user-friendly mechanisms, such as one-click reporting buttons in email clients, encouraging prompt reporting without disrupting users' workflows. Foster a culture of continuous communication by regularly sharing information about the latest phishing trends, recent attacks, and success stories of users thwarting phishing attempts.

Establish reward and recognition programs to acknowledge individuals or teams demonstrating exceptional vigilance. Positive reinforcement motivates users to actively participate in the organization's cybersecurity efforts, creating a positive and proactive cybersecurity culture. In essence, combining effective training, gamification, and managed phishing response tools is key to empowering users as a crucial line of defense against phishing threats.

3. AI'S EVOLUTION AND DOMINANCE IN 2024

The year 2023 has witnessed unprecedented advancements in the field of Artificial Intelligence (AI), bringing transformative changes across industries. “Generative AI” entered the general lexicon, and the Cambridge Dictionary updated the entry for “hallucinate”. If 2023 was dramatic, then 2024 promises to bring even more substantial changes as companies catch up with the technology.

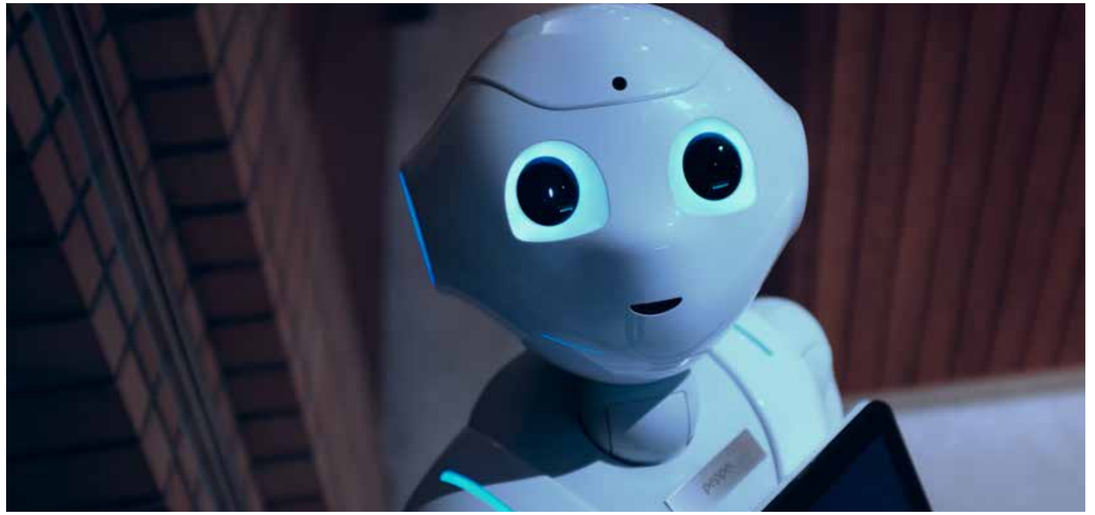
Release of ChatGPT- OpenAI's release of ChatGPT-4 marked a significant milestone in natural language processing. This model, more advanced than its predecessor GPT-3, showcased enhanced understanding and generation of human-like text, making it a valuable tool for businesses and educators alike.

Release of Custom GPTs - The OpenAI release of custom GPTs, allows ChatGPT to be customized for specific use cases. However, this requires more detailed knowledge and will likely lead to additional accidental data leaks for organizations.

First generation of Malicious AI as a service - In 2023, a disturbing trend emerged with the advent of "Malicious AI as a Service". This development marked a new era in cyber threats, where advanced AI tools designed for malicious purposes were offered as a service on the dark web. These services included AI-driven phishing attack generators, malware creation tools, and systems for automating social engineering attacks. 2024 will bring even more sophisticated Malicious AI.

AI Dangers

Despite the benefits, AI's rise is not without risks. As AI systems become more integral to our lives, understanding and mitigating these dangers is critical.



1. AI HALLUCINATIONS

AI hallucinations refer to the phenomenon where AI systems generate false or misleading information. For CISOs, this poses a challenge in ensuring data integrity and reliability, where people inside their organizations make decisions based on inaccurate data.

2. AI POISONING

AI poisoning, where malicious actors feed AI systems with corrupted data to skew results or decision-making processes, is a growing concern. This can lead to compromised security systems or erroneous business decisions.

3. UNINTENDED BIAS

AI systems can inadvertently perpetuate biases present in their training data, leading to unfair or unethical outcomes. Ensuring AI ethics and fairness is a significant challenge for developers and users alike.

AI: Key Trends for 2024

Looking ahead to 2024, several trends and developments are likely to shape the AI landscape.

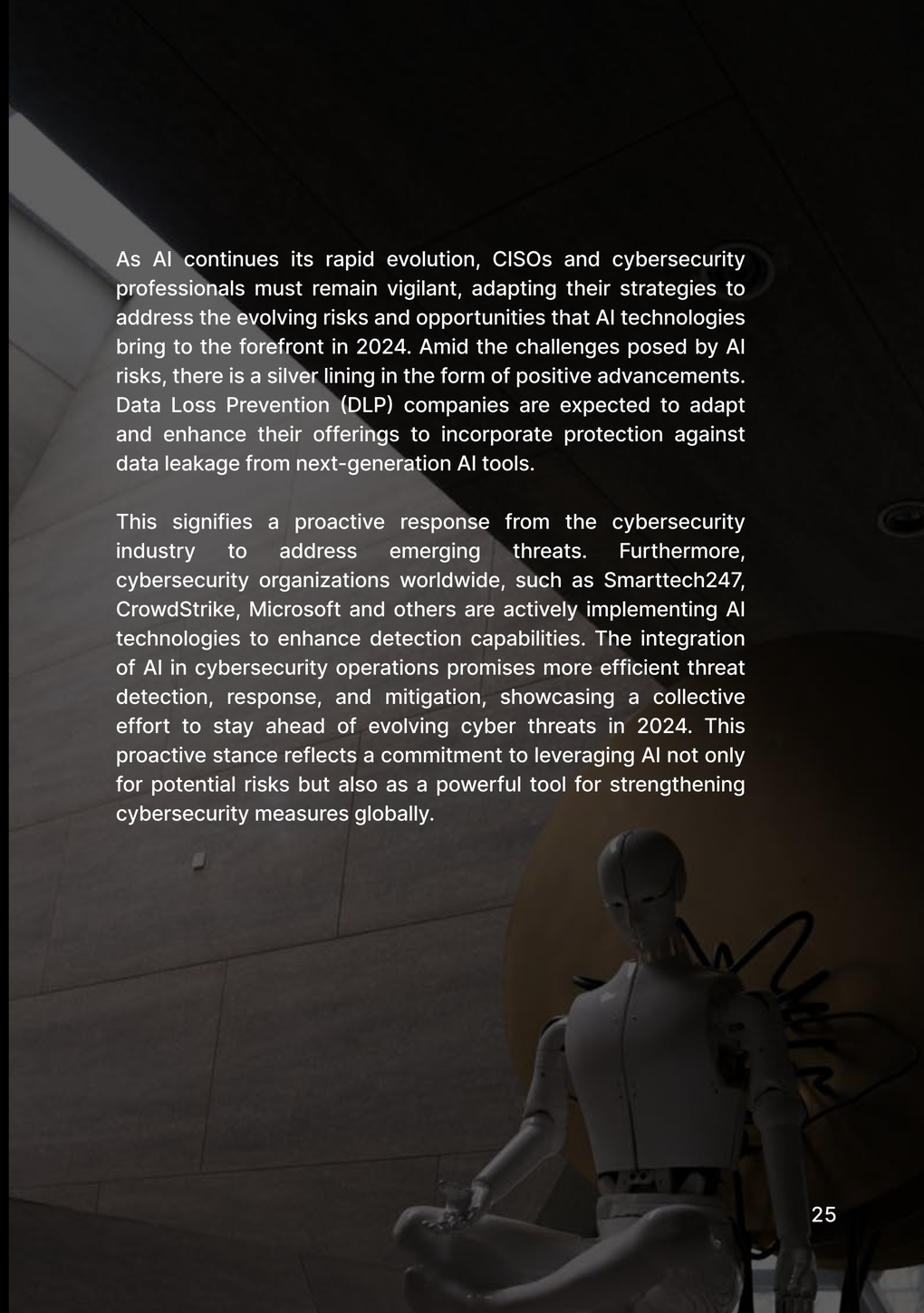
1. Enhanced AI Regulation: The year 2024 is expected to witness a significant uptick in the scrutiny and regulation of AI technologies, with a heightened focus on aspects such as data privacy, ethical use, and accountability. Governments and regulatory bodies are likely to introduce more stringent measures to ensure responsible AI deployment. For instance, regulations might mandate transparent AI algorithms, necessitating organizations to disclose the logic behind AI decisions. Additionally, there could be increased emphasis on AI ethics committees to assess and validate the ethical considerations of AI applications, especially in sensitive domains like healthcare and finance.

2. Growth in AI-as-a-Service (AIaaS): The AIaaS model is poised for substantial growth in 2024, providing businesses with accessible and scalable AI solutions without the need for extensive in-house expertise. This expansion, however, comes with a flip side. The proliferation of Malicious AI as a Service is anticipated to be a growing concern. Cybercriminals may increasingly leverage AIaaS platforms to deploy sophisticated attacks. As a countermeasure, organizations will see a heightened need for robust Data Loss Prevention (DLP) solutions to safeguard against potential malicious activities facilitated by AI.

3. AI Will Cause Major Data Leaks: With the increasing reliance on AI and the sharing of vast amounts of data, the potential for major data leaks is a looming concern in 2024. Unstructured and possibly unauthorized data sharing with AI systems could lead to substantial security vulnerabilities. For instance, envision a scenario where an attacker gains access to an internal AI system, exploiting it for reconnaissance and data exfiltration. This risk is reminiscent of past incidents, such as public S3 buckets, and is expected to manifest in the AI landscape. The cybersecurity landscape will witness a surge in the demand for proactive measures, including robust authentication mechanisms and comprehensive data access controls, to mitigate the risks associated with unauthorized data sharing and potential AI-enabled data breaches.

As AI continues its rapid evolution, CISOs and cybersecurity professionals must remain vigilant, adapting their strategies to address the evolving risks and opportunities that AI technologies bring to the forefront in 2024. Amid the challenges posed by AI risks, there is a silver lining in the form of positive advancements. Data Loss Prevention (DLP) companies are expected to adapt and enhance their offerings to incorporate protection against data leakage from next-generation AI tools.

This signifies a proactive response from the cybersecurity industry to address emerging threats. Furthermore, cybersecurity organizations worldwide, such as Smarttech247, CrowdStrike, Microsoft and others are actively implementing AI technologies to enhance detection capabilities. The integration of AI in cybersecurity operations promises more efficient threat detection, response, and mitigation, showcasing a collective effort to stay ahead of evolving cyber threats in 2024. This proactive stance reflects a commitment to leveraging AI not only for potential risks but also as a powerful tool for strengthening cybersecurity measures globally.



4. REGULATIONS WILL DRIVE RESILIENCE AND PROACTIVE PRACTICES

Regulatory initiatives in 2023 reflect an increasing awareness of the necessity for international collaboration in addressing global cybersecurity challenges. We have seen a notable trend towards stricter data protection regulations, with a particular emphasis on safeguarding individuals' privacy and ensuring responsible data handling practices. With new legislation like DORA, in financial services and NIS2, we see standards and frameworks becoming regulations with real teeth and timelines coming on the back of GDPR.

Additionally, in 2023, regulatory measures have placed a heightened emphasis on protecting critical infrastructure from cyber threats. The Biden administration's Executive Order on Improving the Nation's Cybersecurity addresses critical infrastructure resilience. It includes provisions for enhancing the security of critical software, establishing a Cybersecurity Safety Review Board, and implementing incident response and remediation requirements. The focus on critical infrastructure aligns with global initiatives such as the NIST Cybersecurity Framework, illustrating a commitment to safeguarding essential systems from cyber risks.

New SEC requirements, effective in 2023, have introduced enhanced cybersecurity measures for public organizations with periodic reporting obligations under federal securities law. Effective from July 26, 2023, the amendments to Form 8-K mandate registrants to report specific details of a material cybersecurity incident within four business days of confirming its significance. Foreign private issuers, using Form 6-K, must promptly provide information on a material cybersecurity incident under specified conditions. Annual reports for all registrants are now required to include disclosures on cybersecurity risk management, strategy, and governance.

Furthermore, in 2023, New York implemented new reporting requirements specifically tailored for financial organizations. These regulations demand stringent cybersecurity practices and reporting protocols to fortify the resilience of the financial sector. Financial institutions operating in New York are required to conduct regular cybersecurity risk assessments, implement robust data encryption measures, and adhere to comprehensive incident response plans.

Regulations: Key Trends for 2024

Evolving Cybersecurity Practices in Financial Services

In 2024, the financial services sector is expected to witness a continued evolution in cybersecurity practices, primarily driven by the adoption of the DORA (Digital Operational Resilience Act) framework. As financial organizations embrace DORA, there will be a structured and reference-based approach, particularly in incident response. This adoption signifies a shift towards a more standardized and proactive cybersecurity stance, providing a clear framework for organizations to enhance their incident response capabilities. The financial industry will leverage DORA to strengthen its core competence in cybersecurity, ensuring a robust defense against emerging cyber threats.

Emphasis on Incident Response in Critical National Infrastructure (CNI)

Critical National Infrastructure (CNI) sectors, guided by NIS2 (Network and Information Systems Directive), will place a heightened emphasis on incident response in 2024. NIS2, with its renewed focus on incident response capabilities, will drive CNI entities to enhance their readiness to combat cyber threats. The directive's emphasis on resilience and response strategies will lead to the development of more sophisticated incident response plans, ensuring the quick and effective mitigation of cyber incidents. This trend reflects a recognition of the evolving threat landscape and the need for CNI entities to continually fortify their cyber defenses

Impact of Standards and Regulation on Cybersecurity Practices

The evolving standards and regulations in cybersecurity, such as DORA and NIS2, will continue to shape the industry landscape in 2024. Organizations in the cybersecurity domain will perceive these developments as either a valuable ally or a potential source of stress. The best practice observed is that organizations are leaning into these regulations, actively seeking early buy-in from the business. By demonstrating both the business benefits and compliance requirements, companies can align their cybersecurity practices with the evolving standards. This approach not only ensures regulatory compliance but also fosters a culture of cybersecurity that is integrated into the overall business strategy.

Proactive Approach to Cybersecurity Compliance

Anticipating the evolving cybersecurity landscape, organizations will adopt a proactive stance towards compliance in 2024. Rather than viewing regulations as a reactive necessity, companies will invest in staying ahead of emerging standards and regulatory requirements. This proactive approach involves continuous monitoring of regulatory developments, early adoption of best practices, and regular updates to cybersecurity protocols.

Cybersecurity remains a paramount concern for the European Commission. Recent years have seen a staggering surge in software supply chain attacks, targeting small businesses and critical institutions like hospitals daily. Ransomware attacks occur every 11 seconds, estimated to cost €20 billion annually. In 2021 alone, cyber criminals executed around 10 million distributed denial of service (DDoS) attacks worldwide, rendering websites and online services inaccessible to users. These alarming statistics underscore the urgency for enhanced cybersecurity measures.

Against this backdrop, the European Commission has recently endorsed a significant milestone, the Cyber Resilience Act. This act introduces universal cybersecurity standards mandating that all digital devices, from everyday gadgets to critical infrastructure, must adhere to specific criteria. Notably, it implements a risk-tailored approach, subjecting less than 10% of products to third-party testing.

The Cyber Resilience Act holds implications that directly benefit consumers and businesses across the EU. By addressing emerging cyber threats, it ensures that all products entering the EU market meet stringent cybersecurity standards. Moreover, it empowers users by compelling manufacturers to provide timely security updates, fostering transparency and enabling informed consumer choices.

Enforcement measures outlined in the Act cover the entire lifecycle of products. This includes mandates for the CE marking to denote compliance with the Act's requirements and eligibility for sale within the EU. Manufacturers will also be legally bound to provide consumers with timely security updates for several years following purchase, aligning with the product's expected duration of use.

The Cyber Resilience Act is now subject to formal approval by both the European Parliament and the Council. Upon adoption, it is expected to take effect within 20 days of publication in the Official Journal. Manufacturers, importers, and distributors will have 36 months to adapt to the new requirements, with a more limited 21-month grace period concerning manufacturers' reporting obligations for incidents and vulnerabilities.

This legislative effort builds upon the foundation laid by the 2020 EU Cybersecurity Strategy and the 2020 EU Security Union Strategy. It complements existing legislation, such as the NIS2 Framework adopted in 2022, and reflects the European Commission's commitment to a digitally secure Europe.

In light of the evolving threat landscape and the imperative to fortify cybersecurity measures, the Cyber Resilience Act signifies a crucial step forward. Its implementation promises to elevate the standard of cybersecurity across digital products, safeguarding consumers, businesses, and critical infrastructure within the EU against a rapidly growing array of cyber threats.

5. ORGANIZATIONS WILL HEIGHTEN EFFORTS TO TACKLE THE CYBERSECURITY SKILLS SHORTAGE

Reports indicate a staggering 3.5 million open positions within the cybersecurity industry, underscoring a critical skills shortage that continues to escalate. This scarcity is not merely a product of insufficient interest but is exacerbated by the expanding array of tools deployed in the cybersecurity landscape. Notably, cybersecurity providers are capitalizing on this demand, with a trend towards platform consolidation. Companies are strategically reducing tool complexity, fostering a more integrated approach between Security and IT Operations to efficiently navigate the intricate cyber threat landscape.

Shift Towards Managed Security Services: The skills gap, particularly evident during non-business hours, is steering organizations towards Managed Security Services. A paradigm shift is observable, with 24/7 Monitoring and Incident Response topping the agenda for companies seeking external support. This surge in reliance on MSSP/MDR/SOC providers, however, brings forth concerns regarding the management overhead associated with these services. Companies are grappling with the challenge of seamlessly integrating these external services into their existing functions and processes.

Consolidation and Commonality: The demand for cybersecurity skills is intricately linked to the accelerating pace of technological evolution. Microsoft and Splunk, as industry leaders, are reaping the rewards of this demand through the consolidation of security platforms. Organizations are now realizing the benefits of reducing tool complexity, striving for commonality between their Security and IT Operations. This strategic shift not only addresses the immediate skills shortage but also positions companies for a more streamlined and cohesive cybersecurity approach.

Transparency and Proactive Service Delivery: With the rising reliance on external security services, there is a growing demand for increased transparency and proactive engagement from service providers. Organizations are not only seeking technical expertise but also expect MSSPs to act as an extension of their internal functions. The management of cybersecurity services should not be a burden but an enhancement to existing processes. In 2023, the industry is witnessing a shift towards service providers who proactively align with an organization's objectives, offering a seamless integration that goes beyond mere incident response.

“A paradigm shift is observable, with 24/7 Monitoring & Incident Response topping the agenda for companies seeking external support.

Cybersecurity Skills: Key Trends for 2024

Looking ahead to 2024, the trajectory of cybersecurity dynamics suggests a continued surge in demand for skilled professionals. The skills shortage is unlikely to abate, prompting organizations to further invest in Managed Security Services. However, there will be a discernible evolution in expectations, with companies increasingly prioritizing service providers that not only bridge the skills gap but also act as collaborative partners. Transparency, integration, and proactive service delivery will be the hallmark of successful cybersecurity collaborations, shaping a landscape where organizations and service providers work seamlessly in unison to counter emerging threats.

In the next twelves months, we will also see a paradigm shift in talent management strategies as companies grapple with the persistent skills shortage. Recognizing the urgency of attracting and retaining skilled professionals, organizations will increasingly invest in innovative approaches to attract and retain talent. Beyond traditional recruitment practices, companies will emphasize creating appealing work environments, fostering continuous learning opportunities, and implementing mentorship programs. Cybersecurity talent will not only be enticed by competitive salaries but also by a commitment to professional growth and a supportive workplace culture.

As the demand for cybersecurity experts intensifies, corporations will recognize the importance of investing in social projects to cultivate a future-ready workforce. Collaborations with educational institutions, vocational training programs, and initiatives to bridge the diversity gap in the industry will become more prevalent. By actively participating in community-building endeavors, companies will not only contribute to addressing the skills shortage but will also bolster their corporate social responsibility initiatives.

In response to the persistent skills shortage, the cybersecurity industry will witness increased collaboration through industry-wide initiatives. Shared resources, knowledge-sharing platforms, and joint training programs will become more prevalent. Companies will realize the collective strength of the industry in addressing common challenges and will actively participate in collaborative efforts to fortify the global cybersecurity workforce.

2024 will mark a definitive turning point where companies will adopt more automation and artificial intelligence to augment their cybersecurity capabilities. From threat detection and response to routine tasks, automation will streamline operations, allowing human professionals to focus on complex problem-solving and strategic initiatives. This symbiotic relationship between human expertise and technological prowess not only ensures a more robust defense against evolving threats but also signifies a forward-looking approach to navigating the dynamic landscape of cybersecurity in the years to come.

6. GEOPOLITICAL DYNAMICS WILL CONTINUE TO IMPACT THE CYBERSECURITY LANDSCAPE

The evolving global landscape continues to witness an alarming surge in cyber warfare and state-sponsored attacks. Recent global conflicts have served as a stark revelation of states' readiness to deploy cyber assaults targeting both military and civilian infrastructure. Looking ahead, it appears inevitable that military operations worldwide will invariably intertwine with cyber warfare strategies.

Moreover, in the last twelve months, we have noted a rise in hacktivism as a result of global tensions. Geopolitical instability inevitably fuels hacktivist activities, predominantly through Distributed Denial-of-Service (DDoS) attacks strategically aimed at causing substantial disruption. A notable trend is the increasing overlap between hacktivism and commercial interests. Threat actors now leverage ransomware attacks to generate revenue, potentially funding various other clandestine activities.

Against this backdrop of heightened geopolitical tensions, the UK's National Cyber Security Centre (NCSC) has issued warnings regarding enduring and substantial threats posed by state-aligned groups to critical infrastructure. Recognizing the direct impact of geopolitical dynamics on national security, this necessitates a swift enhancement of cyber resilience across sectors globally, pivotal to the nations' well-being, including water, electricity, transportation, and communication networks.

A notable trend is the increasing overlap between hacktivism and commercial interests.

In the realm of cybersecurity, the significance of safeguarding critical infrastructure extends beyond immediate physical consequences. The interconnected nature of these systems makes them attractive targets for state-sponsored cyber espionage. Recent incidents, such as the Sellafield breach, further illustrate the alarming convergence of critical infrastructure vulnerabilities and state-sponsored cyber espionage. The breach at Sellafield, assumed to involve actors from China and Russia, underscores the potential motivations behind these attacks. While the exact motives remain complex and multifaceted, they may range from gaining insight into nuclear technologies for strategic advantage to geopolitical posturing and fostering a climate of uncertainty. China, Russia, and Iran continue to emerge as notable actors in cyber espionage and attacks. China's state-affiliated cyber actors exhibit sophisticated capabilities targeting critical infrastructure on a global scale. Similarly, Russia remains a prominent force in global cyber activities, including attacks against Ukraine and ransomware operations impacting the UK. While less sophisticated, Iran employs digital intrusions for theft and sabotage, primarily targeting specified sectors such as academia, defense, government organizations, NGOs, journalists, and activists.

Geopolitical Dynamics: Key Trends for 2024

Looking ahead to 2024, the repercussions of ongoing geopolitical tensions are expected to significantly contribute to escalating cyber threats. The rise of AI as a tool in cyberattacks, coupled with the increasing prominence of political hacktivism and misinformation, is anticipated to amplify cybersecurity risks throughout the year.

As cyber warfare escalates, critical infrastructure sectors such as energy, transportation, and healthcare may face increased targeting. State actors may exploit vulnerabilities in these sectors to disrupt services, causing economic damage and potential harm to civilians. Nations will need to bolster their cybersecurity measures to safeguard essential services.

Cyber warfare will become an integral component of hybrid warfare strategies, where nations leverage both conventional and cyber capabilities simultaneously. This may involve the integration of cyber attacks with conventional military actions, making attribution more challenging and exacerbating the potential impact on targeted nations.

Geopolitical tensions often accompany disinformation campaigns aimed at shaping public opinion. In 2024, we can expect an increase in sophisticated disinformation efforts orchestrated by nation-states, leveraging social media platforms and other online channels to influence perceptions, manipulate narratives, and create internal discord within targeted nations.

Nation-states will continue to invest in cyber espionage to gather intelligence on geopolitical rivals. Advanced persistent threat (APT) groups affiliated with nation-states may target government agencies, military organizations, and private enterprises to gain a strategic advantage in geopolitical negotiations and conflicts. Furthermore, nations will prioritize the development and enhancement of offensive cyber capabilities as a means of maintaining a competitive edge in global power struggles. This may involve the creation of more sophisticated malware, zero-day exploits, and advanced persistent threats designed to infiltrate and compromise adversaries' networks. Nations may employ cyber proxies—non-state entities with advanced cyber capabilities—to carry out attacks on their behalf. This strategy allows states to maintain a degree of deniability while still achieving their geopolitical objectives through cyber means.

In response to the evolving cyber threat landscape, governments may introduce or enhance cybersecurity regulations to protect national interests. Industries deemed critical to national security may face stricter cybersecurity requirements, and companies could be mandated to adopt robust measures to mitigate the risk of cyber attacks.

DEFENDING DEMOCRACY

In 2024, strengthening election security on a global scale emerges as a paramount imperative, resonating with the echoes of past challenges and triumphs. The integrity of democratic processes has faced unprecedented scrutiny in recent years, as nations grapple with the multifaceted threats posed by cyber adversaries, misinformation campaigns, and evolving technologies.

Examples from the recent past, such as the interference in the 2016 United States presidential election and the attempted manipulation of various electoral processes worldwide, serve as stark reminders of the vulnerabilities inherent in modern democracies. These incidents have not only underscored the pressing need for robust election security measures but have also catalyzed a paradigm shift in how nations approach the protection of their democratic foundations. The NCSC's Annual Review emphasizes a concerning trend of targeted attacks on the personal email accounts of influential political figures. These attacks represent a persistent effort aimed at obtaining sensitive information, indicating a shift from mass campaigns to pinpoint targeting.

STRENGTHENING ELECTION SECURITY IN 2024

Global Collaboration for Cyber Resilience:
Recognizing the transnational nature of cyber threats, nations will increasingly engage in collaborative efforts to share intelligence, best practices, and technological solutions. International alliances focused on election security will emerge, fostering a collective response to emerging threats and bolstering the resilience of democratic processes.

Could Blockchain Solutions for Secure Voting be the future?
In pursuit of enhanced transparency and trust, some nations may experiment with blockchain technology to secure the integrity of their electoral systems. The decentralized and tamper-resistant nature of blockchain holds the potential to mitigate concerns related to fraud, manipulation, and unauthorized access.

Rise of AI-Powered Threats:
As artificial intelligence continues to advance, the use of AI-driven cyber threats targeting election infrastructure is expected to escalate. From deepfake technologies manipulating public perception to sophisticated automated attacks on voting systems, nations will confront the challenge of staying ahead in the cybersecurity arms race.

Heightened Focus on Voter Education and Awareness:
Beyond technological controls, there will be a growing emphasis on educating voters about the importance of cybersecurity hygiene. Governments and non-governmental organizations will collaborate to raise awareness about potential threats, misinformation, and steps individuals can take to ensure the sanctity of their democratic participation.

Regulatory Frameworks for Digital Campaigning:
Recognizing the influence of digital platforms in shaping public opinion, governments may implement comprehensive regulatory frameworks to monitor and control political advertising and campaigning on social media. Stricter measures may be enacted to curb the spread of misinformation and foreign interference through online channels.

Red Teaming and Simulations: To proactively identify vulnerabilities in election systems, governments will increasingly invest in red teaming exercises and simulations, which is very welcome. These proactive measures will help assess the resilience of electoral infrastructure and enable authorities to address weaknesses before they can be exploited.

7. NEXT-LEVEL RANSOMWARE

The year 2023 has proven to be a pivotal period in the relentless evolution of ransomware threats, witnessing a substantial surge in incidents. Prominent ransomware strains such as Lockbit, ALPHV (BlackCat), and Bian Lian have emerged as top performers, dominating the global scene. Their prevalence in Ransomware as a Service (RaaS) and extortion attacks has cast a shadow over various victim organizations, with a special emphasis on the Manufacturing sector. The choice of this sector as a primary target reveals a strategic focus on disrupting manufacturing processes and seizing control of critical infrastructure, making it an attractive prospect for cybercriminals.

In the global perspective, the United States has surfaced as a primary hotspot for ransomware attacks. Lockbit, in particular, has targeted a significant number of victims in the country, capitalizing on its diverse industries, critical infrastructure, and large corporations. The concentration of nearly half of all recorded ransomware incidents worldwide in the United States underscores the attractiveness of the nation for cybercriminals seeking substantial ransoms.

In the intricate web of ransomware activities, Cl0p stands out as a notable player. Employing advanced tactics, Cl0p orchestrated a successful GoAnywhere campaign, infiltrating and compromising a staggering 104 organizations. The group's strategic exploitation of zero-day vulnerabilities in widely-used file transfer software, GoAnywhere MFT and MOVEit Transfer, further emphasizes the evolving nature of ransomware tactics.

Moreover, a noteworthy shift has been observed in the monetization strategy of ransomware groups. The Hospital for Sick Children and Olympia Community Unit School District 16 incidents serve as compelling examples. In these cases, Lockbit, responsible for the attacks, surprisingly released free decryption tools and issued apologies. This demonstrates a nuanced approach by ransomware groups, acknowledging self-imposed rules and restrictions on certain targets due to potential life-threatening consequences.
Furthermore, emerging trends such as "Franken-ransomware" and the dominance of URL-based attack vectors reveal the adaptability and sophistication of contemporary ransomware threats. The rise of data extortion as a primary method for ransomware attacks, as observed with groups like RansomHouse and Karakurt, highlights a strategic shift toward exploiting sensitive information to coerce victims.

Ransomware: Key Trends for 2024

Ransomware threats are poised to evolve significantly in 2024, with a notable emphasis on stealthy attack methodologies. The rise of "living off the land" techniques, leveraging legitimate system tools, poses challenges for detection, highlighting the crucial need for sophisticated threat prevention strategies. Despite enhanced defenses, the risk of data loss or leakage remains high, amplified by the reliance on SaaS platforms storing sensitive information, creating fresh vectors for exploitation.

Foreseeing the evolution of tactics, ransomware operators are likely to diversify their extortion methods beyond the conventional realms of encryption and data exfiltration. The landscape may witness the introduction of innovative approaches, such as threats to reach out to clients, suppliers, or regulatory bodies. By targeting these external entities, threat actors aim to amplify the impact of their actions, compelling organizations to comply with their demands under the threat of damaging relationships, supply chains, or regulatory standing.

Additionally, there may be an uptick in tactics involving the manipulation of critical data integrity, coercion through the exposure of sensitive information, or threats of reputational damage.

The landscape of ransomware attacks is expected to become more targeted and sophisticated in 2024. Threat actors will focus on critical infrastructure and high-value targets, demanding substantial ransoms. Practical examples of this evolution can be seen in potential scenarios where ransomware attackers target the control systems of power grids, leading to widespread blackouts. Similarly, disrupting transportation infrastructure through ransomware could result in chaos and economic downturns. Additionally, compromising healthcare systems could impact patient care, medical records, and even the availability of critical medications and treatments.

Moreover, ransomware actors are increasingly leveraging newer programming languages like Nim, Rust, and Golang to create sophisticated and evasive malware. The simplicity, concurrency, and memory management features of these languages make them attractive to cybercriminals. This shift adds complexity to malware analysis due to the lack of comprehensive security tooling for these languages.

8. ENHANCED FOCUS ON SUPPLY CHAIN SECURITY

The term "supply chainpocalypse," coined by Verizon in its 2022 Data Breach Investigations Report, now resonates as 2023 unfolds with significant cyber onslaughts. The Log4j vulnerability, though initially perceived as a mere ripple, set the stage for a cascade of supply chain attacks, with 3CX and MOVEit marking 2023 as a pivotal year. Log4j's impact reverberated beyond expectations, revealing that 73% of cases involved espionage and 26% were linked to organized crime. The subsequent emergence of 3CX and MOVEit showcased the vulnerabilities that persist within our interconnected supply chains. These attacks, targeting well-established providers like 3CX and MOVEit, exemplify the sophistication and audacity of cybercriminals in exploiting weaknesses. The recent Okta incident serves as a stark reminder of the pervasive threats organizations face. In a disconcerting turn of events, Okta, a prominent identity management company, found itself entangled in a supply chain compromise. The breach, stemming from a third-party vendor, exposed Okta user data and although, initially, the scope of the incident was uncertain, the plot thickened in November when after a thorough investigation, the organization revealed that all users had been affected.

Supplier Risks: Key Trends for 2024

Looking ahead to 2024, several strong predictions emerge. First, there will be a heightened focus on software supply chain security. Organizations will invest heavily in scrutinizing and fortifying the entire software development lifecycle, implementing rigorous code integrity checks, and adopting secure coding practices. As defenses against traditional supply chain attacks strengthen, threat actors will evolve their tactics, increasingly employing advanced techniques such as AI and ML.

The surge in high-profile supply chain breaches will likely lead to stricter regulatory measures focused on supply chain security. Compliance frameworks will evolve to incorporate specific guidelines for software supply chain security. Blockchain technology will see widespread adoption to enhance supply chain integrity, offering decentralized and tamper-resistant records for greater visibility and traceability.

A significant development for 2024 will be the proliferation of Software Bill of Materials (SBOMs). Recognizing the critical role of software in supply chain security, organizations will prioritize creating and sharing comprehensive SBOMs. This transparency will empower organizations to assess and manage risks effectively, becoming a fundamental requirement in supplier relationships.

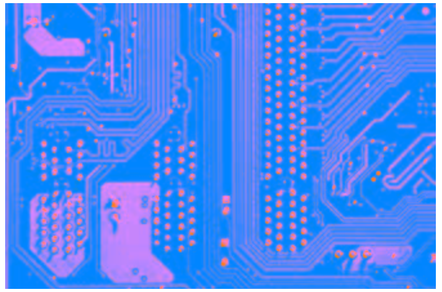
When a company like Okta gets breached, the Board Members start asking tough questions. Supply chain security and third-party risk assessments will be on the board agenda for many organizations around the world and these assessments will become the norm in 2024. Automation will play a pivotal role in streamlining these assessments, offering efficiency and accuracy.

As organizations grapple with the evolving nature of supply chain security threats, proactive measures, emerging technologies, and regulatory frameworks are converging to strengthen the resilience of global supply chains in 2024. The trajectory outlined involves the integration of AI-driven security orchestration, which will automate incident response, threat intelligence analysis, and anomaly detection, enabling cybersecurity teams to identify and mitigate potential risks more efficiently.

9. OT/ICS SECURITY TEAMS WILL SHARPEN THEIR FOCUS IN 2024

In the dynamic landscape of Operational Technology (OT) security, in 2023 we noted a series of impactful cyber attacks, leaving an indelible mark on critical sectors. Notable incidents, including the Johnson Controls International (JCI) breach, the Lumila Attack, and cyber incident targeting Yamaha, Trèves Group, and Toyota, underscored the heightened vulnerabilities faced by industrial and manufacturing environments. These attacks illuminated the evolving tactics of cyber adversaries, revealing the potential consequences of breaches within OT systems. The top attacked industries were Manufacturing, Automotive, Power and Energy, Electronics and Utility, Food and Beverage.

As we navigate through the landscape of Operational Technology (OT) security risks in 2023, a critical dimension that intertwines with these concerns is the rapidly evolving realm of Internet of Things (IoT) cybersecurity. The synchronicity of these two domains is imperative, given that the year 2024 brings forth not only tremendous opportunities but also growing challenges in the IoT cybersecurity sphere. The proliferation of IoT devices, projected to exceed 207 billion worldwide, signifies a paradigm shift where devices embedded with artificial intelligence (AI) capabilities become commonplace. However, this evolution also introduces significant vulnerabilities that cyber attackers are poised to exploit, amplifying the complexities of OT security.



One of the primary concerns in IoT security revolves around the increased interconnectivity among devices, creating numerous entry points for cyber attackers. The rise of AI-powered cyber threats, especially in the context of remote and distributed workforces, underscores the urgency of ensuring device security.

This interconnectedness becomes a critical facet in the broader conversation about OT security risks, as compromised IoT devices can potentially serve as gateways for attacks on operational technology networks. Establishing secure networks for smart devices and connected technology is paramount not only for maintaining customer and workforce trust but also for safeguarding the integrity of digital ecosystems in industrial environments.

The impact of IoT on specific sectors, such as healthcare, is noteworthy. Remote patient monitoring and AI-assisted diagnostics revolutionize patient care and research, making IoT a transformative force in the medical landscape. However, as the IoT healthcare market is projected to reach a valuation of $289 billion by 2028, the intersection of healthcare IoT and AI-augmented IoT (AIOT) introduces new dimensions of security concerns.

In addressing the security challenges posed by IoT, leading experts emphasize the need for increased regulations and standards. Initiatives like the GSMA IoT SAFE standards and the US Cyber Trust Mark aim to strengthen the security of IoT applications and restore consumer trust in technology. Despite these efforts, risks persist, including weak login credentials, command injection vulnerabilities, and flaws in third-party components.

OT/ICS Security: Key Trends for 2024

Exploring the evolving landscape of OT security trends in 2024 reveals pivotal shifts shaping the cybersecurity dynamics within industrial, production, and manufacturing domains. Operational environments are embracing more and more IoT technologies, which means we will see a shift from confining incidents to administrative networks to widespread malware infections. The interconnected networks, now digitally transformed, expose all facets to potential risks, impacting both company downtime and the physical safety of employees. We will also see a massive shift to a focus on the manufacturing industry as the last 6 months have proven this sector to be a lucrative one.

A paradigm shift is observed in the objectives of cyberattacks, moving beyond causing business interruptions to posing physical threats. The spillover of malicious activities from IT to OT is evident, with attackers targeting essential services and utilities like raw materials, energy, water, and infrastructure. Operational technology environments are weaponized, as seen in global conflicts like the Russia-Ukraine war, escalating geopolitical threats to OT systems and emphasizing the potential for physical harm and human casualties.

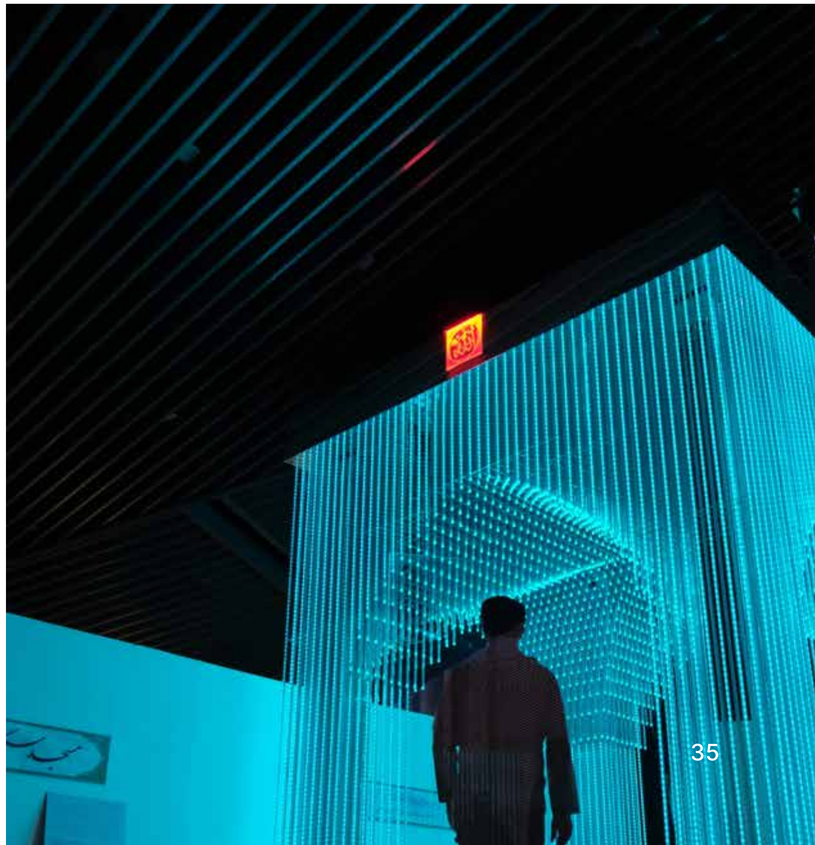
In tandem with these geopolitical dynamics, hacktivism gains momentum, exemplified by politically motivated cyberattacks during conflicts. This trend is anticipated to intensify and evolve in 2024, as illustrated by recent events such as DDOS attacks impacting Israel and Palestine during hostilities

Some good news, too! A proactive approach to OT security compliance emerges with the NIS2 Directive. Enterprises falling under its ambit are required to enhance cybersecurity measures before October 2024. NIS2 significantly impacts OT environments by enforcing stricter cybersecurity requirements and expanding the scope to include more sectors. Compliance involves adopting robust security practices, enhancing incident reporting, managing supply chain risks, and fortifying resilience against cyberattacks. This regulatory push aims to elevate the overall security posture of OT environments within the EU, recognizing their critical role in ensuring the safety and reliability of essential services.

The proliferation of IoT connections introduces a myriad of challenges. Companies are integrating diverse IoT technologies into their networks, ranging from passive RFID to security sensors. However, the lack of inherent security measures in numerous IoT devices heightens vulnerability to large-scale DDoS botnet attacks. The diverse communication protocols utilized by these devices, including Wi-Fi, cellular systems, mesh networks, and NFC, amplify the threat landscape.

Operational technology, traditionally a low-priority area, is witnessing a notable shift in attention. Governments and companies are gearing up to bolster OT security in response to growing threats. Recognizing the significance of fostering a dedicated culture of IT and OT security, organizations will be investing in extensive end-user training. The focus extends to the reevaluation of training programs to enhance user awareness of the latest social engineering schemes. Governments, including the US and the EU, contribute to these efforts through new regulations and the promotion of customized detection, scanning, and security tools.

As the complexity and frequency of cybersecurity risks surge, the demand for skilled IT talent surpasses the available supply. To address this shortage, an increasing number of organizations are considering alternatives like outsourcing for managing core cybersecurity functions, including OT security.



10. INCREASED DIGITAL TRANSFORMATION WILL ACCELERATE THE ADOPTION OF ZERO-TRUST FRAMEWORKS AND SASE TECHNOLOGIES

If you haven’t included SASE in your 2024 strategy, now it’s time to do so. Secure Access Service Edge (SASE) solutions are on an upward trajectory, set to continue their growth in adoption over the upcoming year. According to Gartner's projections, in 2024, more than 40% of enterprises will have explicit strategies in place for SASE adoption, a significant leap from the mere 1% in 2018. This surge is attributed to the increasing permanence of remote work and the rampant proliferation of cloud-based applications, rendering SASE ever more crucial in safeguarding modern network architectures.

The landscape of IT networks is undergoing fundamental shifts, presenting unparalleled security challenges. Hybrid cloud environments, the prevalence of cloud-based applications, the surge in personal devices, and the rise of remote work have made the traditional network perimeter obsolete. The conventional security solutions, designed to secure this perimeter, fall short in addressing the complexities inherent in highly distributed networks and the array of cyber threats targeting them.

As network perimeters vanish, the conventional method of routing network traffic through a centralized data center for threat inspection and security policy enforcement is impractical. As organizations increasingly migrate computing resources and operations to the cloud and network edge, the demand intensifies for security solutions that can function in close proximity to users, devices, and cloud resources. Simultaneously, there's a pressing need for a centralized system capable of managing security policies across both cloud and on-premises infrastructure.

SASE solutions tackle this challenge by consolidating networking and security functions into a unified solution that revolves around authenticating identities rather than solely defending a perimeter. Moreover, SASE technology shifts the focus from reliance on physical hardware, paving the way for scalable, flexible, cloud-based solutions that cater to the agility required by today's highly distributed enterprises.

Digital Transformation: Key Trends Driving The Adoption of SASE in 2024

The increasing prevalence of remote work and the ongoing digital transformation initiatives are key factors influencing the adoption of SASE technologies. As organizations embrace distributed work environments, the need for secure and scalable network solutions becomes paramount. SASE, with its capability to provide secure access from anywhere, aligns seamlessly with the requirements of businesses adapting to remote work and digital transformation trends.

An accelerated migration of applications and infrastructure to the cloud is another influential trend shaping the adoption of SASE. With businesses embracing cloud services, there is a growing demand for network solutions that can effectively integrate with cloud-native architectures. SASE's cloud-centric design positions it as an attractive choice for organizations seeking a unified approach to networking and security in the era of cloud computing.

The rise of mobile workforces and the implementation of Bring Your Own Device (BYOD) policies are contributing to the adoption of SASE technologies. SASE is designed to offer secure access to resources regardless of the user's location or device, addressing the security challenges associated with diverse endpoints and remote access. This trend reflects the changing dynamics of the modern workplace, where flexibility and mobility are increasingly valued.

The growing adoption of Zero Trust security models is influencing organizations to explore SASE solutions. SASE aligns with the principles of Zero Trust by adopting a "verify-first" approach to security. As businesses transition from traditional perimeter-based security to Zero Trust architectures, SASE's emphasis on identity verification and continuous monitoring supports this evolving security paradigm.

The continuous evolution of the cybersecurity threat landscape is a significant driver for the adoption of SASE. With the dynamic nature of cyber threats, organizations require adaptive and comprehensive security measures. SASE solutions often integrate advanced threat intelligence, real-time analytics, and AI-driven capabilities to detect and mitigate evolving threats, making them well-suited to address the evolving challenges in the realm of cybersecurity.

RECOMMENDATIONS FOR AN ELEVATED SECURITY POSTURE 2024

Smarttech
YOUR 24/7 SECURITY PARTNER

IMPLEMENT AI AND AUTOMATION

Harness the power of artificial intelligence (AI) and automation to fortify your cybersecurity defenses. Employ advanced AI-driven anomaly detection mechanisms that continuously analyze user behavior, network traffic, and system activities. This proactive approach enables the identification of potential security threats in real-time, empowering security teams to respond swiftly and effectively. Additionally, automate routine security tasks, such as log analysis and vulnerability scanning, allowing security professionals to focus on strategic initiatives and threat mitigation.

Go beyond looking at just misconfiguration, enforce a Zero Trust model for secure access.

ADOPT A ZERO TRUST METHODOLOGY

Embrace a Zero Trust methodology to redefine your organization's security architecture. Implement continuous authentication, requiring users and devices to continually verify their identity, and adopt micro-segmentation to compartmentalize network access. Enforce the principle of least privilege, granting minimal access based on job responsibilities. Adopting a Zero Trust approach means assuming no implicit trust, even within the network, and thoroughly verifying every user and device attempting to connect to resources.

STRENGTHEN YOUR CLOUD SECURITY POSTURE

In the last year, more than a third of businesses experienced a data breach in their cloud environment. Go beyond looking at just misconfigurations, enforce a Zero Trust model for secure access, extending it to Software-as-a-Service (SaaS) applications and integrating robust API security measures. Employ continuous monitoring, threat detection, and Data Loss Prevention (DLP) to ensure the security of cloud environments.

MEASURE YOUR CYBER RISK EFFECTIVELY

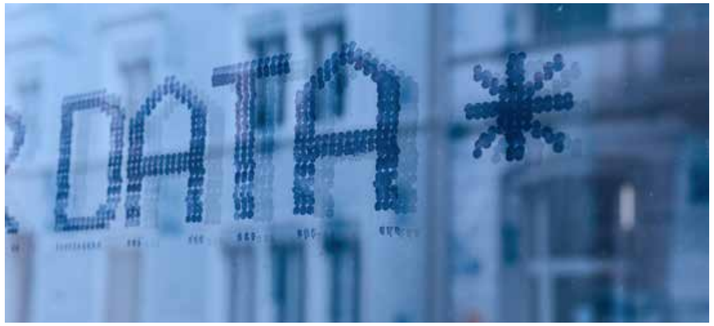
Establish a robust risk management framework based on industry standards, such as the National Institute of Standards and Technology (NIST) guidelines. This framework provides a structured approach to identifying, assessing, and prioritizing security risks. Regularly conduct risk assessments to evaluate the evolving threat landscape and measure the maturity of your security program over time. By incorporating a risk management framework, organizations can make informed decisions, allocate resources efficiently, and continually enhance their cybersecurity posture.

ASSET VISIBILITY AND CRITICALITY

Asset visibility is on every CISO’s agenda in 2023 and will continue in 2024. Elevate your organization's security posture by enhancing asset visibility and classifying assets based on criticality so that you can protect the most vital components of your infrastructure. If you’re running Operational Technology (OT) systems, conduct regular assessments to identify and mitigate vulnerabilities in industrial control systems, ensuring the resilience of critical operational assets. Extend your current SOC monitoring to include OT for wider visibility.

DISASTER RECOVERY PLANNING

Reevaluate and enhance your disaster recovery plans to ensure swift and effective response in the face of security incidents. Regularly test incident response plans through simulated scenarios, engaging with business stakeholders to measure and improve response times. Collaborate with cross-functional teams to identify potential weaknesses and refine the incident response strategy. By thoroughly planning and testing disaster recovery procedures, organizations can minimize downtime, reduce the impact of security incidents, and maintain business continuity.



DATA SECURITY STRATEGY

Develop a comprehensive data security strategy that encompasses data posture management, Data Loss Prevention (DLP), and access control. Implement automated tools to classify and monitor sensitive data, ensuring that encryption protocols are enforced consistently. Establish granular access controls based on user roles and responsibilities, limiting data access to authorized personnel. By adopting a holistic data security strategy, organizations can protect sensitive information, maintain regulatory compliance, and mitigate the risk of data breaches.

THIRD-PARTY SECURITY MANAGEMENT

Conduct thorough and ongoing assessments of third-party security practices to effectively manage supply chain risks. Utilize automated tools for continuous monitoring, complemented by regular security audits of third-party vendors. Ensure that these vendors adhere to established security standards and protocols, and collaborate closely to address any identified vulnerabilities promptly. A proactive approach to third-party assessment helps organizations maintain a resilient supply chain and minimizes the risk of security breaches originating from external partners

ADOPT INNOVATIVE USER AWARENESS TRAINING

Revolutionize user awareness training programs by incorporating elements of rewards and gamification. Develop engaging and interactive training modules that encourage active participation from employees. By integrating gamification principles, such as challenges, competitions, and rewards, organizations can create a positive and competitive environment that motivates employees to adopt and retain security best practices. This innovative approach enhances overall security awareness and fosters a culture of continuous learning and vigilance

PROACTIVE ENGAGEMENT WITH SECURITY PARTNERS

Foster a strategic and proactive partnership with security vendors to enhance overall cybersecurity defenses. Engage security partners in ongoing risk assessments, threat intelligence sharing, and joint incident response planning. Encourage a collaborative approach that goes beyond a reactive stance, allowing security partners to actively contribute to the organization's security strategy. By leveraging the expertise of security partners in a proactive manner, organizations can stay ahead of emerging threats, bolster their defenses, and navigate the evolving cybersecurity landscape with confidence. In other words, make sure you get more from your current MDR provider!

GETTING BUSINESS BUY IN

Finally, in 2023, we have observed CISOs excelling in two key areas: employing real-world scenario exercises to enhance awareness and securing business support to position cybersecurity as a brand enhancer rather than a cost. When executed effectively, a well-managed and pertinent Incident Response exercise serves as a profound revelation for senior leadership, immersing them in the intricacies of a cyber attack as opposed to a conventional DR scenario. In a matter of hours, we've witnessed the transformation of cyber skeptics.

Frameworks and standards persist in offering a benchmark for both internal and external stakeholders concerning an organization's relative security maturity. Forward-thinking CISOs are adept at leveraging these frameworks to contribute actively to solutions rather than being perceived as obstacles. They empower their organizations to stand out by not only meeting but surpassing these standards, subsequently promoting and publicizing their achievements.

10-STEP PLAN FOR A CISO'S FIRST 90 DAYS

1. UNDERSTAND BUSINESS OBJECTIVES

- Conduct meetings with key stakeholders to understand the organization's business objectives and critical assets.
- Identify the role of cybersecurity in supporting these objectives.

2. ASSESS CURRENT SECURITY POSTURE

- Identify vulnerabilities, gaps, and areas for improvement in policies, processes, and technology.
- Perform a comprehensive assessment of the current cybersecurity posture.

3. BUILD RELATIONSHIPS

- Establish strong relationships with key departments, including IT, legal, compliance and executive leadership.
- Collaborate with other business units to ensure a holistic approach to cybersecurity.

4. REVIEW POLICIES & PROCEDURES

- Evaluate existing cybersecurity policies and procedures.
- Update or create policies to align with industry standards and regulatory requirements.

5. SECURITY AWARENESS TRAINING

- Implement a security awareness training program for all employees.
- Foster a culture of cybersecurity awareness and responsibility throughout the organization.

6. INCIDENT RESPONSE PLANNING

- Review and enhance incident response plan.
- Conduct tabletop exercises to ensure the organization is prepared to respond effectively to security incidents.

7. VENDOR RISK MANAGEMENT

- Evaluate and enhance vendor risk management program.
- Identify and assess cybersecurity risks associated with third-party vendors.

8. TECHNOLOGY ASSESSMENT

- Evaluate the effectiveness of current cybersecurity technologies.
- Identify areas of improvement and implement necessary upgrades or changes.

9. ESTABLISH KEY PERFORMANCE INDICATORS

- Define and implement KPIs to measure effectiveness of the cybersecurity program.
- Regularly assess and report on key metrics to track progress and areas of improvement.

10. COMMUNICATION AND REPORTING

- Develop a communication plan for reporting cybersecurity updates to leadership.
- Provide regular updates on cybersecurity initiatives, incidents, and risk management.

ELEVATE YOUR SECURITY

ABOUT US

SMARTTECH247

Smarttech
YOUR 24/7 SECURITY PARTNER

Smarttech247 is a multi-award-winning expert Managed Detection & Response (MDR) company and a market leader in Security Operations. Trusted by world's largest global organizations, our expert MDR and AI-enabled unified VisionX MDR platform provides continuous monitoring, advanced threat detection, investigation & response capabilities, 24/7.

WHAT WE DO

At Smarttech247, we help you protect against constant cyber threats and significantly reduce your Security Operations (SecOps) complexities. Our 24/7 expert led managed detection and response (MDR) is geared towards enhancing your cyber resilience and significantly improving your security efficiency.

Get the support that you need to enhance your cyber defenses and improve your security posture.

- **24/7 Managed Detection & Response**
- **Data & Information Security**
- **Governance , Risk & Compliance**
- **Security Validation**

VISION X
KEEPING YOU SECURE

RESPOND TO THREATS FASTER THAN EVER!

Led by human expertise and powered by the VisionX platform, Smarttech247 provides a 24/7 unbeatable Managed Detection and Response (MDR) capability giving you transparent and consolidated security solutions.

- **Extended Visibility across entire attack surface**
- **Seamless & Powerful SIEM & SOAR Integration**
- **Risk Scoring & Advanced Threat Intelligence**

REQUEST A DEMO TODAY!

Tech Excellence Awards – Managed Security Service Provider of the Year
ISO 9001:2015 Certified Company
ISO 27001:2013 Certified Company
IBM Managed Security Service Provider of the Year
Deloitte. 50 Technology Fast 50 2023 IRELAND
Chambers Ireland Cybersecurity Company of the Year 2023
CYBER ESSENTIALS
it@cork Leaders Awards Winner

Are you ready to elevate you security with Smarttech247?

Contact Us

www.smarttech247.com

info@smarttech247.com

Smarttech
YOUR 24/7 SECURITY PARTNER

zerodaycon
powered by Smarttech247

EVOLVE 2024

6 March, 2024

Dublin Convention Centre

ENTER INTO A NEW ERA OF BUILDING CYBER RESILIENCE

Join us at Zero Day Con 2024, taking place at Dublin's Convention Centre on March 6th. As the premier gathering for cybersecurity leaders, this event attracts over 500 C-level IT executives annually from across the globe. Get ready to immerse yourself in an unrivalled platform for networking, collaboration, and cutting-edge insights.

Check out the website for a list of confirmed speakers and sponsors.

Don’t miss this opportunity to join us at Zero Day Con 2024 and be part of the evolution in cybersecurity.

Register now to secure your spot and be at the forefront of cyber resilience.

Exclusive Offer: Use code **ZDC25** for a **25% DISCOUNT** on **Zero Day Con** tickets!

This year, under the theme of "Evolve," Zero Day Con recognizes that change is the only constant in cybersecurity. Through shared knowledge, collaborative solutions, and innovative insights, we equip ourselves to evolve and safeguard the digital future.

🔍 Key Highlights:

- Meet like-minded cybersecurity leaders and global experts
- Explore the newest trends and innovations in cybersecurity
- Engage with visionary sponsors showcasing revolutionary tech solutions
- Dive deep into critical topics: Leadership in Cybersecurity, Geopolitical Dynamics, AI's Impact, Boardroom Engagement in Cyber Risk Communication

Zero Day Con offers interactive learning sessions, demonstrations, keynotes, and panel discussions, fostering an environment for learning and idea exchange. Discover groundbreaking solutions, products, and strategies shaping the digital frontier.

🚀 What to Expect:

- Understand today’s complex cyber threat landscape and revamp your security strategy
- Gain unique insights from industry experts on security threats, vulnerabilities, and risks
- Network with peers, speakers, and executives throughout the event

Global Cybersecurity Perspectives and Trends for 2024

Smarttech
YOUR 24/7 SECURITY PARTNER

This Cybersecurity Perspectives Report has been crafted under the careful guidance of our esteemed senior executive team, including the leadership of our CEO. Their collective expertise and strategic insights have played a pivotal role in shaping the content of this report, ensuring its relevance and reliability. The commitment of our leadership team to advancing cybersecurity knowledge underscores the importance of the information presented herein. We express our gratitude for their valuable contributions in steering our organization toward a deeper understanding of evolving cyber threats and effective mitigation strategies.

Many others across Smarttech247 have also contributed to the report:

Alexandru Sandu
Alin Curcan
Andrei Constantinescu
Ben Hellis
Ciaran Coulstock
David Sandor
Edward Skraba
Gavan Egan
Joe O'Dowd
Ken Sheehan
Robert Kehoe
Sweta Patnaik