CYBERFORCE

THREAT INTELLIGENCE

A YEAR IN REVIEW 2023

www.cyberforceq.com

TABLE OF CONTENTS

2023 ANNUAL REPORT

Introduction

Welcome to the 2023 Annual Threat Intelligence Recap. Since the launch of our Monthly Threat Intelligence Bulletin in 2022, the report has quickly become a key reference guide to the cybersecurity risks associated with our findings in our Collective Security Operations Center. This report is widely used by cybersecurity professionals, including CISO's, security managers, technology directors, and decision makers to stay informed of the latest cybersecurity threats and challenges affecting various industries and platforms.

In this annual recap our security team examines the challenges to government and public entities, vulnerabilities in the healthcare sector, educational institutions, and the importance of safeguarding the infrastructure.

Here are some of the highlights:

Phishing Trends continue to be a significant threat in our clients' environments. The QR Code Phishing trend saw a 587% increase. Funds Transfer Fraud is a continued attack vector on users with urgent action words to catch the user's attention. Typo-Squatting is getting harder and harder to spot with the advanced sophistication of the attacker.

The need for **Detection in Depth & Importance of Identity Protection** surged in response to ransomware groups gaining access in the infrastructure of organizations.

Techniques Most Prevalent in Clients Environments ranged from Active Scanning, Brute Force and User Execution of Malicious Files.

We extend our gratitude to our clients, whose collaborative engagement has been instrumental in making this report possible. The joint sessions with our clients not only enhance their capa-bilities but also result in measurable improvements, contributing to the ongoing enhancement of their cybersecurity posture.

Furthermore, our security team excels in responding to alerts, consistently surpassing the average alert response time. Our commitment to promptly addressing an alert within a short timeframe enables real-time actions within our Security Operations Center (SOC), ensuring swift response and efficient case management leading to effective resolution for our clients.

We hope you find value in the detailed and actionable data presented in this report.

2023 A YEAR IN REVIEW

Phishing Trends

In 2023, cybersecurity threats increased significantly, with most being phishing attacks. While the cybersecurity community often directs its attention towards sophisticated and complex cyber-attacks, it is crucial to acknowledge the critical role that seemingly mundane phishing campaigns play in the initial stages of a breach. These campaigns, although not directly linked to advanced persistent threat groups, serve as the primary method for unauthorized access and entry into secure systems. What is particularly concerning is that these campaigns can manifest themselves long before any actual incident occurs, making them a potent and stealthy threat that organizations must confront.

Phishing attacks capitalize on human fallibility, leveraging social engineering techniques to deceive unsuspecting individuals and elicit sensitive information. By impersonating trusted entities or creating compelling scenarios, cyber-criminals manipulate their victims into divulging confidential data, such as passwords or financial details. The repercussions of falling victim to a phishing attack can be devastating, ranging from financial loss to compromised personal and professional reputations.

Given the increasingly widespread nature of phishing attacks, organizations and individuals alike must adopt a proactive and multi-faceted approach to cyber-security. This includes implementing email filters, strong multi-factor authentication (MFA) technology, and employee training programs. Additionally, fostering a culture of cybersecurity awareness and vigilance can empower individuals to identify and report potential phishing attempts promptly.

Below are some key phishing trends that our team observed throughout the year.

QR Code Phishing (Quishing)

A particularly novel trend in credential phishing emails that emerged in 2023 was QR code phishing, sometimes referred to as *quishing*.

QR codes, which are two-dimensional barcodes, have become increasingly popular and are commonly used in various applications such as advertising, business cards, and contactless payments. These codes can be easily scanned by a smartphone camera to quickly access information or a website. However, threat actors have found a way to exploit this technology for their malicious purposes.

In QR code phishing, threat actors create QR codes with malicious URLs, which often directs users to fraudulent login portals. When users scan these QR codes, they unknowingly expose themselves to the risks of unknowingly providing their login credentials to the threat actors.

This new form of phishing poses a significantly higher risk to users because they may not have a way of knowing where the QR code will take them until they scan it. Furthermore, they may not be able to verify the authenticity of the link, making it easier for threat actors to deceive them.

2023 A YEAR IN REVIEW

Funds Transfer Fraud (FTF)

Funds Transfer Fraud (FTF) is a type of cybercrime that involves the unauthorized transfer of funds from one account to another through fraudulent means. This fraudulent activity is typically carried out by individuals who impersonate others to gain access to sensitive financial information. This type of fraud is particularly effective because the perpetrator is likely already familiar with the internal workings of the organization, allowing them to make their impersonation more convincing. They often use information about the victim's coworkers, clients, and other internal details to make the email appear legitimate.

The perpetrators commonly use fake email accounts from providers like Gmail to impersonate high-level employees within the company. They then request changes to the direct deposit payroll accounts of end-users, aiming to extract sensitive banking information by persuading the end-user to comply with their request.

Common email subject lines often include words like "changes" or "request" to grab the recipient's attention — a standard social engineering technique — and encourage them to open the email. For example, a subject line might read "I HAVE A REQUEST" or "Urgent request for information" or "UPDATE PAYROLL". By using language that suggests the email contains important or urgent information, the sender hopes to convince the recipient to open the email and take the desired action.

2023 A YEAR IN REVIEW

HTML Attachments

During 2023, our team observed a trend in a sophisticated form of credential phishing known as HTML smuggling.

Traditional phishing attempts typically involve sending an email that prompts the recipient to click a link to a fake website, masquerading as a reputable company, to trick them into providing their login information. However, email security scanners have become increasingly adept at identifying and blocking these malicious URLs before the emails reach the user's inbox.

To counter this, phishers started using HTML attachments more frequently in their emails. HTML, or Hypertext Markup Language, is a legitimate and commonly used language to format and structure emails, including the inclusion of images, text styling, and links. However, it is possible to create HTML files that are designed to mimic real login portals. These attachments are included in emails that prompt recipients to take action related to domain account verification, such as resetting passwords or confirming personal information.

Since these types of attachments are not typically blocked by email security scanners, phishers can use them to sneak in fake login pages. Once the user opens the HTML attachment, they are taken to the login page. JavaScript is embedded in the file, so that when an email and password are submitted, the credentials are captured by an external server controlled by the phisher.

JavaScript is a programming language used to add interactivity and dynamic behavior to websites and applications, such as auto-saving an email draft or triggering automatic file downloads. While JavaScript powers many of today's internet platforms, it presents both significant benefits and potential security risks.

Typo-Squatting

Our team observed a growing trend in the use of typo-squatting in phishing emails. Typo-squatting is a technique where malicious actors register domain names that are similar to popular websites or brands but contain deliberate typos. The goal is to deceive users into visiting these fraudulent websites and providing their login credentials for business services like Microsoft Office 365. Registered domain names can be modified by adding or removing letters, adding hyphens, or using subdomains and top-level domains (TLDs), among other options.

For example, below are typo-squatted domains closely resembling Wells Fargo and Chase Bank:

> wellc-fargo[.]com
> secure[.]chase-onilne-us[.]com
> secure[.]chase-bakn[.]com

Typically, the emails will prompt the recipient to click a link to view a document related to banking. However, the sender, domain, and the domain's server have no affiliation with the actual company. The document serves as a lure to trick the recipient into logging in through a fake login portal. Additionally, the sender may use a service account, such as Google Shares, to send the email. This is done to make the email appear more legitimate and trustworthy to the recipient, while also bypassing standard email security filters.

Steps to Mitigate Risk

QR Code Phishing (Quishing)

Educate end users on how to spot and report phishing attempts. Additionally, be cautious of business authentication related emails containing a QR code.

Establish policies and procedures for handling emails requesting personal or sensitive information.

Implement phish-resistant MFA for all user accounts and systems to prevent unauthorized access through stolen credentials.

Funds Transfer Fraud

Educate employees about the threat of impersonation scams and encourage them to be cautious when receiving requests for sensitive information, especially when the request comes from someone they do not know or trust.

Implement strict security protocols for verifying the identity of employees before granting access to sensitive information, such as requiring two-factor authentication or using digital signatures.

Regularly review and update security policies and procedures to ensure that they are effective at protecting against impersonation scams and other forms of cyber-crime.

Steps to Mitigate Risk

HTML Attachments

Regularly educate employees on how to identify and report suspicious emails, particularly those containing .html file attachments that may ask for login information and foster a culture where reporting them is encouraged.

If HTML files do not serve a legitimate business purpose, consider enforcing mail flow rules or Group Policy for Outlook to strip .html and .htm file types. This will reduce the likelihood of these attachments from reaching the intended recipient's inbox.

Implement phish-resistant multi-factor authentication (MFA) for all employee login accounts, which can effectively protect against unauthorized access, even if login credentials are compromised.

Typo-Squatting

ICANN (Internet Corporation for Assigned Names and Numbers) has a Trademark Clearing House that allows website owners to monitor how their names are used with different domains. Regularly check in on how names like your brand or domain are used.

Report typo-squatted domains to relevant authorities such as ICANN or the domain registrar. They may have the ability to suspend or remove the fraudulent site.

Regularly educate employees on how to identify and report emails using typo-squatted domains.

2023 A YEAR IN REVIEW

Detection in Depth & the Importance of Identity Protection

Threat identification of any kind is fundamental to safeguarding sensitive information and protecting systems from a successful compromise. More specifically, though, is the importance of identifying potentially malicious activity as early as possible. The steps in an attack chain may vary widely.

> However, in 2023, there was a surge in ransomware groups gaining initial access to organizations' internal networks worldwide by focusing on compromising user credentials.

This trend represents a significant change as threat actors increasingly exploit LOLBAS (Living off the Land Binaries and Scripts). Identity compromise is just one aspect of it.

LOLBAS refers to a technique used by threat actors to leverage legitimate and built-in system tools, such as binaries and scripts, to carry out malicious activities without raising suspicion. These activities can be easily mixed with regular administrative tasks, making it difficult for security monitoring tools to differentiate between legitimate and malicious use. Detecting malicious use of LOLBAS typically requires behavioral analysis and an understanding of the context. This approach is more complex than signature-based detection. Performing this analysis may necessitate the use of advanced security solutions augmented with Machine Learning (ML) and Artificial Intelligence (AI), and the expertise of skilled personnel. Gaining access to an organization’s network through a valid user account is likely to generate the least amount of system noise, because it may blur the line between legitimate and unauthorized user activity.

2023 A YEAR IN REVIEW

> As the saying goes, "identity is the new perimeter," this statement underscores the fundamental shift in the cybersecurity landscape brought about by the increasing prevalence of a remote and flexible workforce.

With more and more employees working from different locations and using various devices to access company resources, the traditional notion of a physical perimeter as the primary line of defense is no longer sufficient. Instead, organizations must recognize that identity has become the new focal point for securing their digital assets.

This paradigm shift has been driven by the need to adapt to the changing dynamics of the modern workplace. The rise of remote work has brought many benefits, such as increased productivity and flexibility. However, it has also introduced new vulnerabilities and challenges when it comes to ensuring the security of sensitive information. With employees accessing corporate networks and resources from outside the traditional confines of the office, the attack surface has expanded, providing more opportunities for cybercriminals to exploit weaknesses and gain unauthorized access.

In this context, cyber protection measures must not only keep up with the evolving trends but also stay one step ahead of potential threats. It is no longer sufficient to rely solely on traditional security measures like firewalls and antivirus software. Instead, organizations must adopt a multi-layered approach that encompasses not only network security but also robust identity protection mechanisms.

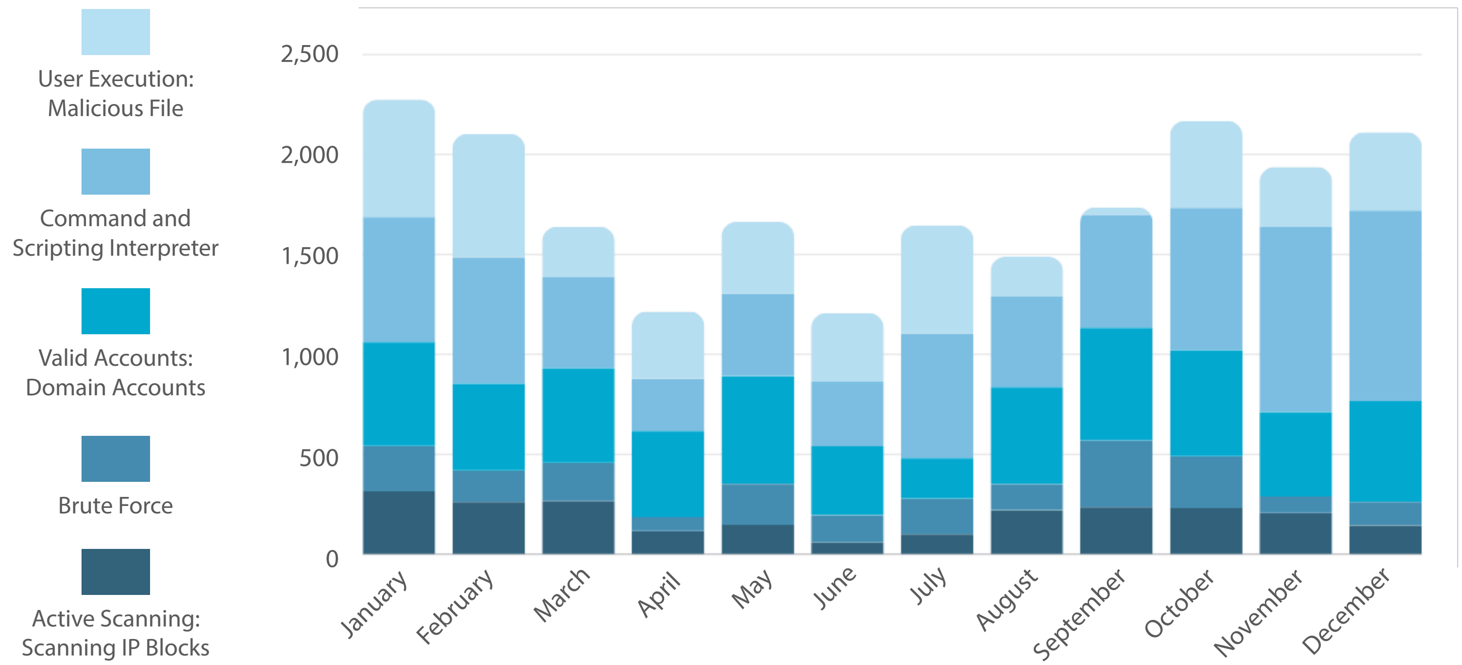
By focusing on identity as the new perimeter, organizations can gain a more comprehensive view of user activity and detect anomalies and potential threats with greater granularity. This approach involves monitoring various factors such as usernames and passwords, multi-factor authentication (MFA), geolocation, role-based access control (RBAC), account manipulation, and user endpoint telemetry. Analyzing these identity-related data points through a robust detection scheme enables organizations to effectively identify unauthorized access attempts and take appropriate action to mitigate the risk. This emphasizes the importance of prioritizing identity protection as a core component of organizations' cybersecurity strategy, allowing them to safeguard their valuable digital assets.

2023 A YEAR IN REVIEW

Techniques Most Prevalent in Client Environments: A Closer Look

The heat map below illustrates the five techniques that were most prevalent in 2023 within our client environments.

It is important to note that these techniques correspond to specific detection analytics and may not necessarily indicate the presence of adversary behavior, but rather the occurrence of the techniques themselves.



Active Scanning: IP Blocks [T1595.001} - Adversaries may scan victim IP blocks to gather targeted information. By scanning IP blocks, adversaries gather victim network information such as active IP addresses and detailed host information. Scans can be simple pings or more advanced to reveal host software/versions through server banners or network artifacts. This information can uncover opportunities for reconnaissance, resource establishment, or initial access.

2023 A YEAR IN REVIEW

Brute Force [T1110] — Adversaries may attempt to gain unauthorized access to accounts by using brute force techniques such as guessing passwords or using previously acquired password hashes. They can do this by interacting with a service that verifies the credentials' validity or by offline attacks against stored password data.

Valid Accounts – Domain Accounts [T1078.002] -- Adversaries may acquire and misuse domain account credentials to gain initial access, maintain persistence, escalate privileges, or evade defense mechanisms. Domain accounts are managed by Active Directory Domain Services and have access and permissions configured across systems and services within the domain. Adversaries can compromise domain accounts, including those with elevated privileges, through techniques such as OS credential dumping or password reuse. This allows them to access privileged domain resources.

Command and Scripting Interpreter [T1059] -- Adversaries may exploit command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages facilitate interaction with computer systems and are available on different platforms. Most systems include a built-in command-line interface and scripting capabilities. For example, macOS and Linux have Unix Shell, while Windows has the Windows Command Shell and PowerShell.

User Execution: Malicious File [T1204.002] — An adversary may exploit a user's action of opening a malicious file to gain execution privileges. Users can be targeted through social engineering techniques, tricking them into opening files that ultimately execute malicious code. Additionally, malicious extensions can be installed in a browser through deceptive app store downloads, posing as legitimate extensions.

As we discussed earlier, identity protection plays a crucial role in mitigating the risks associated with many of these prevalent techniques. The Valid Accounts – Domain Accounts [T1078.002] and Command and Scripting Interpreter [T1059] techniques, represented by the most prominent parts of the heat map, exploit pre-existing resources and technology in the target environment.

By compromising domain accounts, including those with elevated privileges, adversaries can gain access to privileged domain resources. Furthermore, by using command and scripting interpreters, adversaries can easily disguise their actions as regular administrative tasks. This makes it challenging for security monitoring tools to differentiate between legitimate and malicious use.

Without comprehensive visibility into various aspects of user and entity behavior analytics (UEBA), organizations may face challenges in effectively detecting and responding to these techniques.

2023 A YEAR IN REVIEW

Understanding the Limitations of IOCs: Summitting the Pyramid

In cyber threat intelligence, indicators of compromise (IOCs) refer to observable artifacts or traces of known malicious activity, used to indicate an intrusion or threat to a system or network.

Generally, these include IP addresses, domain names, hashes of malware files, and patterns in network traffic, among others. Analyzing and tracking IOCs is an important part of detecting and responding to cyber-attacks. However, organizational focus on IOCs as part of a threat intelligence program can sometimes lead to a "whack-a-mole" approach.

Instead of merely responding to incidents after they occur, organizations must strive to anticipate and mitigate potential risks before they manifest. Teams should prioritize analyzing the root cause of a problem or incident and gaining a comprehensive understanding of the extent of an adversary's access. Instead of solely addressing individual symptoms or incidents as they occur, this approach enables a more effective response. Taking a constantly reactive approach can result in a cycle of recurring issues. This approach only addresses the immediate symptoms, while the underlying causes remain unresolved, and the adversary continues to have access to the environment. Such an approach often leads to inefficient resource utilization and can prolong the resolution process. New problems continue to arise, and the adversary remains present in the environment.

2023 A YEAR IN REVIEW

To shift away from a reactive approach, it is crucial to implement detection analytics that focus on invariant behavior, along with the utilization of extended detection and response (XDR) and security orchestration, automation, and response (SOAR) solutions. Invariant behavior is a fundamental activity in adversary techniques that does not change when the procedural implementation of that technique is altered.

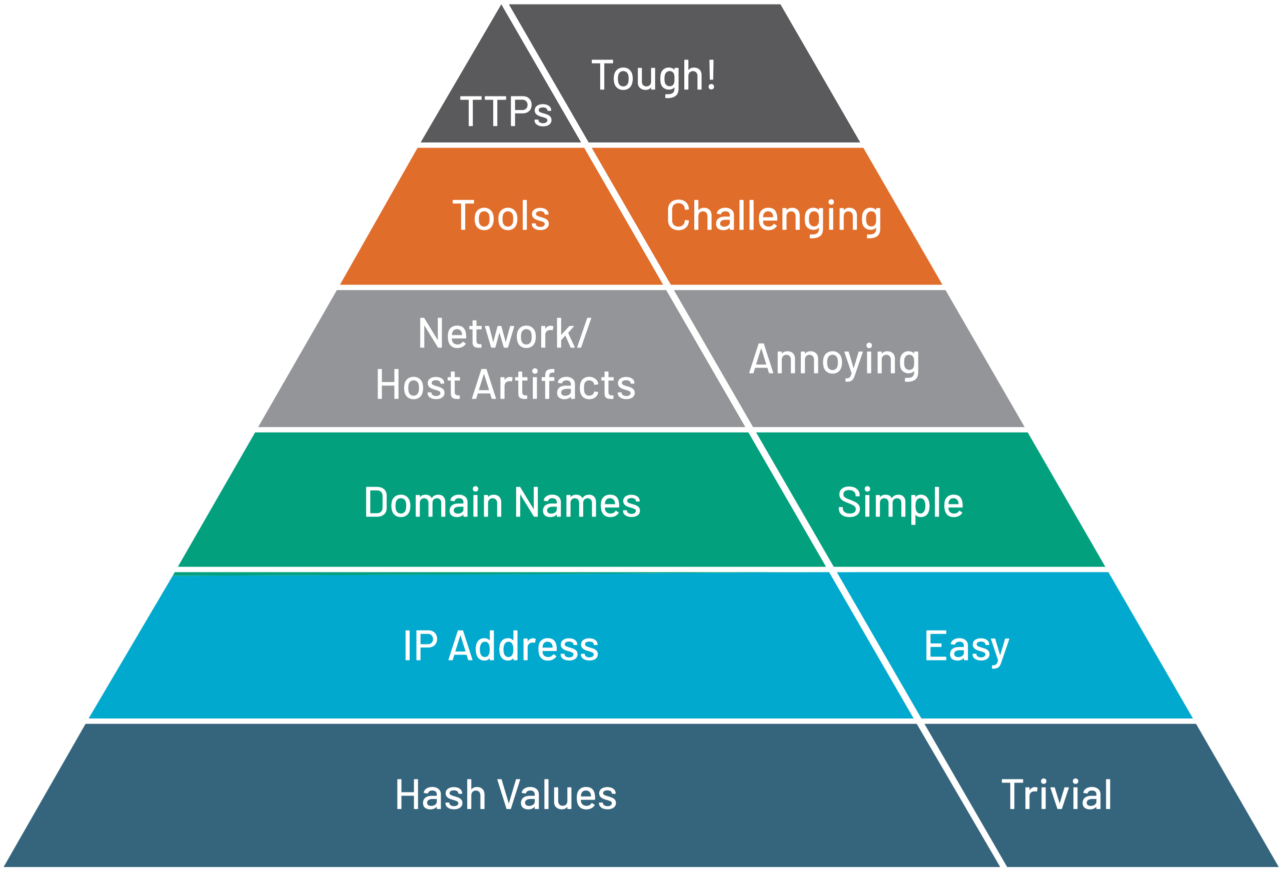
These analytics should be tailored to specifically identify and detect techniques that are commonly used by potential threat actors who are most likely to target your business. Additionally, the use of XDR and SOAR products can greatly enhance an organization's ability to detect and respond to potential threats effectively. These solutions provide advanced analytics and automation capabilities, allowing for quicker and more accurate threat detection and response. By focusing on these techniques, organizations can effectively address the security and integrity of their business's assets by prioritizing threats based on their likelihood of occurrence.

While IOCs generally originate from external network environments, modern adversary network intrusions increasingly rely on existing technologies and utilities native to the organization's internal network environment to achieve their goals. The term tactics, techniques and procedures (TTPs) is often used to refer to working within these environmental limitations. In many cases, the malicious use of these resources by a threat actor is technically considered a legitimate use for them.

For instance, if a threat actor creates a remote scheduled task on an internal endpoint to periodically execute a malicious script, this scheduled task may not necessarily be triggered as suspicious, but rather as a legitimate task. Therefore, organizations should also focus on the abuse of legitimate operating system features, rather than solely relying on IOCs. This proactive and effective approach to threat intelligence allows for a strategy that goes beyond reacting to each new indicator as it appears. By doing so, the risk of an intrusion can be decreased, or at the very least, the time malicious activity occurs within the network can be greatly limited.

2023 A YEAR IN REVIEW

The Pyramid of Pain model, shown below, describes the concept that indicators of compromise (IOCs) are the least valuable form of threat intelligence, while tactics, techniques, and procedures (TTPs) are the most valuable.



In many scenarios, a threat actor could very well achieve their operational objectives without being detected by using hash values, domain names, host artifacts, or external tools as malicious observables. On the other hand, TTPs represent the behaviors and methods used by threat actors, which are more difficult to change and can provide valuable insights into how they tend to interact with the system's resources already present in their target environment. This approach allows organizations to gain a deeper understanding of the techniques employed by threat actors, identify detection gaps, and develop more effective countermeasures.

2023 A YEAR IN REVIEW

Proven Cybersecurity Program Advancement

Average Case Response Time, 2023

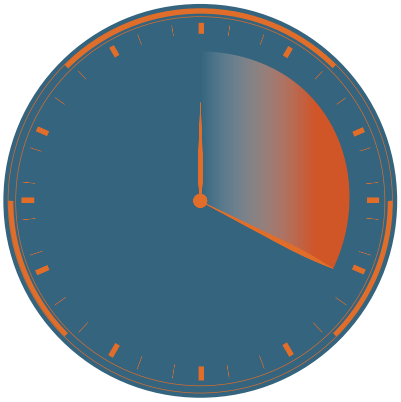
1.3 MINUTES

The time to respond to SOC alert queue events. The desired outcome is to promptly respond to SOC alert queue events within client service level agreement (SLA) times, per our contractual requirements. The goal is to respond to a case within 3 minutes.

Average Case Handling Time, 2023

20 MINUTES

The time it takes from a case reaching our SOC to closure or handoff. It is part of the client service level agreement (SLA) regarding time to investigate and turnover events. The goal is to keep case handling time under 1 hour.



Our Services

COSOC

Collective Cyber Ops

Q|FRAME

Cyber Program Management

PIVOT

Red Team Validation

TADA

Program Advancement

2023 A YEAR IN REVIEW

Cited Sources

Active Scanning: Scanning IP blocks, Sub-technique T1595.001 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1595/001/

Brute Force, technique T1110 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1110/

Valid Accounts: Domain Accounts, Sub-technique T1078.002 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1078/002/

Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1059/

User Execution: Malicious file, sub-technique T1204.002 - Enterprise | MITRE ATT&CK®.
https://attack.mitre.org/techniques/T1204/002/

2023 A YEAR IN REVIEW

Closing Remarks

As we look back on the past year, it is crucial to reflect on the threats we faced and the strides we made in mitigating them. The threat landscape is ever evolving, demanding our constant vigilance and proactive efforts to safeguard our organization and customers.

In this year's threat intelligence report, we have highlighted significant trends and advancements in the cybersecurity realm. We hope the insights and information provided will enhance your understanding and preparation for future challenges. We encourage you to utilize this report as a valuable resource and reference, while staying updated on the latest threats and best practices in the field. As we move forward into the new year, it remains imperative to closely monitor and analyze the threat landscape. Let us collaborate as a team to devise and implement effective strategies to mitigate these threats.

At CyberForce|Q, we unite like-minded organizations to address current cybersecurity challenges and strategically tackle these situations for proactive system protection. Through the exchange of security intelligence, every participant contributes to strengthening the collective while bolstering their individual security posture. Daily meetings and group training exercises enable participating organizations to achieve greater progress than they could alone.

CyberForce|Q stands apart from competitors by employing a distinctive collective model that no one else offers. Participants have achieved tangible results through the tactical and strategic sharing of expertise, resources, diverse perspectives, and innovative ideas. This collective model empowers participants to advance their capabilities at an accelerated pace and continuously enhance their cybersecurity.

If you have any inquiries or wish to learn more about our services, please contact us.

Phone
Office: 248.837.1400
Fax: 248.837.1401

Office Address
47911 Halyard Drive, Suite #110
Plymouth, MI 48170

Email
solutions@cyberforceq.com

Website
www.cyberforceq.com

CYBERFORCE|Q