Navigating the Evolving Cybersecurity Landscape

2022 SUCCESSES AND 2023 CHALLENGES

BLUE TEAM ALPHA

This white paper was written based on conversations with Blue Team Alpha cybersecurity experts: Dan Wolfford, Chief Information Security Officer (CISO); Joe Wright, Incident Response Lead; and Sean Sullivan, Security Operations Center (SOC) Manager.

Contents

Introduction

The world has seen an unprecedented surge in cybercrime in recent years, as the digital realm expands and diversifies. As such, it's crucial to understand the significance of cybersecurity. This white paper covers the activities of Blue Team Alpha, one of the leading cybersecurity firms in the industry. This paper has two primary sections; the first section presents a recap of the cybersecurity issues that Blue Team Alpha resolved in 2022 and the service updates it made. The second section will provide a cybersecurity industry look-ahead, focusing on the challenges the industry will face in 2023, where the cybersecurity market is headed, and the changes made by Blue Team Alpha to its services and approach.

As the world becomes more interconnected, cybersecurity threats continue to evolve, creating new challenges for organizations of all sizes. In this paper, we will explore the changing landscape of cybersecurity and the challenges facing the industry in 2023. We will then take a closer look at Blue Team Alpha, a leading cybersecurity firm that has been helping companies stay ahead of the ever-evolving threat landscape. We will examine the impact of Blue Team Alpha's services, its enhancements to its incident response methodology and SOC technology, and its plans for future tooling capabilities.

Blue Team Alpha's Impact and Service Enhancements

Blue Team Alpha has been a trusted cybersecurity firm that has assisted several government and independent entities in responding to incidents that necessitated complete network rebuilds. Blue Team Alpha aims to offer services accessible to all companies, regardless of size or maturity. Unlike other companies that require a minimum endpoint count for their solutions, Blue Team Alpha’s objective is to ensure that every company benefits from effective cybersecurity measures to protect its assets and data.

In 2022, Blue Team Alpha expanded its services by partnering with Palisade, its sister company, to provide integrated or managed IT services, functioning as a managed security service provider (MSSP). Blue Team Alpha’s customers can now benefit from the integration, as they no longer need to work with multiple vendors or tools, making it easier for them to manage their cybersecurity needs. Blue Team Alpha’s priority is business continuity regarding incident response, unlike other incident response companies. When Blue Team Alpha is put on a case by its insurance partners, its priority is to return companies to operations without paying the ransom.

> “ **Blue Team Alpha’s objective is to ensure that every company benefits from effective cybersecurity measures to protect its assets and data.**

Blue Team Alpha has enhanced its incidence response (IR) methodology by incorporating an updated process checklist, and a comprehensive response framework drawn from past encounters to guarantee that its handling of incidents is more effective than ever. It has also upgraded its security operations center (SOC) technology with the addition of new tools such as dark web ID monitoring. Furthermore, it has established new detection protocols and a playbook to manage specific alerts. Blue Team Alpha has expanded its tooling capabilities and plans to renovate them again in 2023, focusing on enhancing vulnerability management capabilities, allowing it to streamline its operations and provide more comprehensive reports to its clients.

2023 Cybersecurity Outlook:

RISING THREATS AND SOLUTIONS

As we move into 2023, the cybersecurity industry faces several challenges that threaten to undermine the progress made in recent years. Here are some of the main challenges we can expect to encounter:

DOWNSIZING OF SECURITY TEAMS

INCREASED CYBERATTACKS FROM NATION-STATE HACKERS

RANSOMWARE-AS-A-SERVICE (RAAS)

EXTORTION, DATA THEFT, AND SOCIAL ENGINEERING

CYBER INSURANCE VOLATILITY

SEGREGATION OF SILICON TECHNOLOGY

THE RISE OF CHATGPT

2023 Cybersecurity Outlook

DOWNSIZING OF SECURITY TEAMS

With the worsening economy and tech bust, many companies have downsized their teams, and security teams are often the first to go due to their high cost. Company leadership may not fully understand cybersecurity's return on investment (ROI), particularly if the chief information security officer (CISO) fails to make a compelling case for the investment. This downsizing elevates the risk for a company by reducing its security measures. In all probability, outsourcing security assistance will be the solution, as teams will be underfunded, understaffed and under high stress.

INCREASED CYBERATTACKS FROM NATION-STATE HACKERS

Foreign economies are likely to be negatively impacted by the declining US economy, prompting their citizens to search for alternative ways to make money. As a result, we can expect the countries responsible for producing most nation-state hacking, such as Russia, North Korea, Iran and China, for increasing their cyberattack volume. Cybercriminals find ransomware to be a lucrative option for generating significant profits. Ransomware attacks will persist if companies neglect their cybersecurity practices. In a new phase, some ransomware attacks are now targeting company IP addresses, demanding multiple payments in a single incident – one for the decryption key and another to prevent the leak of the company’s IP.

RANSOMWARE-AS-A-SERVICE (RAAS)

The rapid growth of RaaS is expected to continue. In this model, two parties collaborate, with one group carrying out the initial breach and selling the access to another group to "finish the job" by deploying the ransomware and leaving the ransom note. Ransomware is a business, and just like any business, minimizing risk while growing is the preferred approach. RaaS exemplifies this; the threat actor performing the initial breach lowers their risk because they get paid regardless of whether the attacked company pays the ransom.

2023 Cybersecurity Outlook

EXTORTION, DATA THEFT, AND SOCIAL ENGINEERING

These tactics will continue to be a problem. Cybercriminals are scoping their attacks based on how likely companies are to pay, which includes factoring in cyber insurance and any premiums or limits. These attackers are determined to get the highest payment possible.

CYBER INSURANCE VOLATILITY

Cyber insurance will remain a volatile industry. Insurance companies are trying to innovate to minimize loss. Agencies want companies to recover without paying the ransom because it is expensive.

SEGREGATION OF SILICON TECHNOLOGY

The segregation of silicon technology will compel nations to obtain this type of technology, increasing the probability of breaches in this industry.

THE RISE OF CHATGPT

ChatGPT by Open AI is expected to cause both disruption and innovation. It represents the most significant step in human evolution since Bitcoin, with the potential to disrupt industries across the board, including marketing, sales, business, manufacturing, education, security, travel and more. It can be considered a "calculator" for human language, reading and writing. Just as the calculator allows for faster and more accurate calculations, ChatGPT can summarize, write, read, understand written language and provide reasonable responses based on its data set. The API version is unfiltered, unlike the web version, which is filtered to identify and block harmful users. This is significant because cybercriminals with high technical aptitude are the most likely to use the API version. Some individuals have already used this tool for malicious purposes, such as creating undetectable malware, ransomware or phishing emails.

Cybersecurity Market Outlook: GROWTH AND PROJECTIONS

As the world becomes more digital, the cybersecurity market is expected to grow rapidly. According to a report by MarketsandMarkets, the global cybersecurity market is projected to reach $266.2 billion by 2027, up from $173.5 billion in 2022.

One trend that is gaining traction in the market is the adoption of Security Operations Centers (SOCs) across multiple sectors. SOCs provide a central location for organizations to detect, investigate, and respond to security incidents. The Department of Defense (DoD) mandates that government agencies have actively monitored networks by SOCs. Similarly, private sector organizations, including those in oil, gas and silicon manufacturing, will likely turn to SOCs, if they haven't already, as they begin to prioritize cybersecurity.

Another trend in the market is the shift in mindset from preparing for a possible cyberattack to preparing for when an attack occurs. Companies are recognizing that no matter how strong their defenses are, breaches can still occur. Therefore, it is essential to have an incident response plan in place to minimize the damage and quickly return to normal operations. Blue Team Alpha is assisting organizations in transitioning from vulnerability hunting to attack preparedness.

In addition, the cybersecurity industry is expected to continue to face challenges such as downsizing of security teams, foreign economies being impacted by the declining US economy, and the rise of Ransomware as a Service (RaaS). Cybercriminals will continue to find ways to exploit vulnerabilities in technology and use social engineering to trick employees into giving up sensitive information. It is crucial for organizations to stay vigilant and invest in robust cybersecurity measures to prevent and respond to cyberattacks.

$266.2 BILLION

Projected value of the global cybersecurity market by 2027.

Overall, the cybersecurity market is poised for significant growth as companies prioritize cybersecurity and adopt new technologies protect their data and assets. As the industry evolves, companies will need to stay ahead of the curve to protect themselves from emerging threats and minimize the impact of cyberattacks.

Transforming Cybersecurity Services:

OUR NEW FOCUS AND CAPABILITIES

Blue Team Alpha has made significant changes in its approach and services to ensure that it provides the necessary cyber hygiene for the 16 critical infrastructure sectors in the United States (the sectors are seen in Figure 1). While the company does not decline work from other industries, it remains focused on providing security services to these sectors, starting with compliance and expanding to vulnerability scanning, penetration testing, phishing training, and simulations.

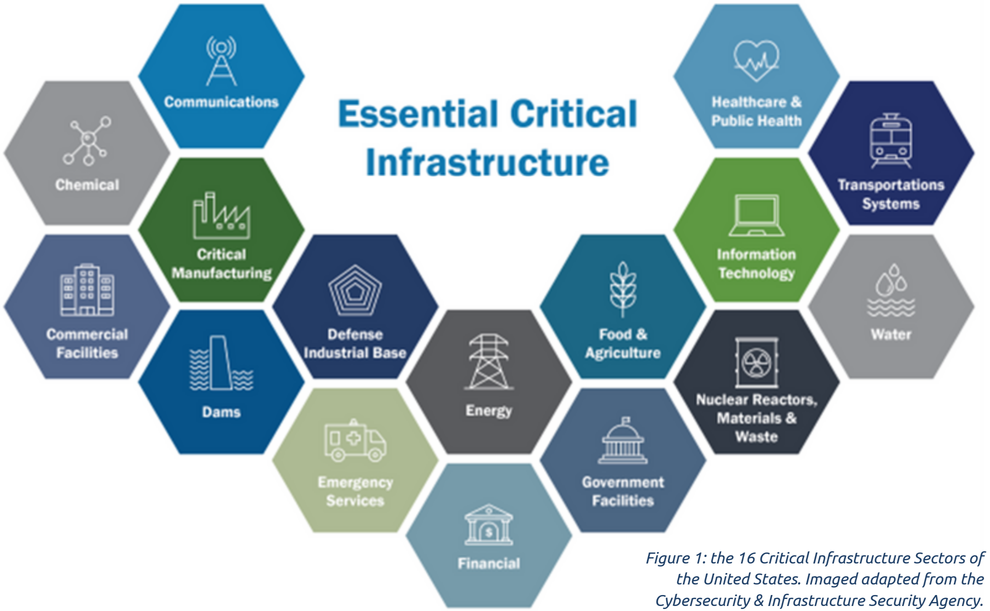

Figure 1: the 16 Critical Infrastructure Sectors of the United States. Imaged adapted from the Cybersecurity & Infrastructure Security Agency.

COMPLIANCE FRAMEWORK

Blue Team Alpha follows the Center for Internet Security's (CIS) Critical Security Controls compliance framework. The CIS Critical Security Controls Implementation Group 1 (IG1) is the foundation for cybersecurity, and smaller or newer companies can begin with it before advancing their security practices. Companies without effective cyber hygiene are vulnerable and more likely to be compromised. Therefore, Blue Team Alpha recommends that companies implement proper cyber hygiene to prevent attacks and minimize recovery costs.

Transforming Cybersecurity Services:

OUR NEW FOCUS AND CAPABILITIES

MODERN TOOLS & PROCESSES

Blue Team Alpha is upgrading its tools and capabilities to better serve its clients, particularly in security operations centers (SOCs) and vulnerability management. The company is revamping its incident response (IR) strategy by updating procedures and implementing a designated personnel approach, including an onsite incident coordinator. Blue Team Alpha is also incorporating new equipment and upgraded technology to enhance its capabilities and expedite response resolution.

SOC IMPROVEMENTS

The company is actively seeking to expand the range of services and capabilities it offers in its SOC, specifically aiming to provide dark web ID monitoring to help companies search for leaked credentials and identify potential security threats.

DOD SKILLBRIDGE PROGRAM

Blue Team Alpha is proud to launch the DOD SkillBridge Program, an opportunity for veterans to gain valuable civilian work experience through industry training, apprenticeships, or internships during their last 180 days of service. This program allows Service members to apply their military skills in the civilian workforce while also connecting them with industry partners in real-world job experiences. As a veteran-owned company, Blue Team Alpha understands the importance of providing resources to help veterans transition into civilian life and successful careers. Implementing this program is an extension of its commitment to supporting Service members.

Conclusion

In conclusion, the rise of cyberthreats poses a significant risk to businesses and individuals alike. As we have seen, the cybersecurity industry will face several challenges in 2023, with higher stakes than ever. However, with challenges come opportunities for innovation and growth. By partnering with trusted cybersecurity firms such as Blue Team Alpha, companies can gain the support they need to keep their operations secure and protect their valuable assets. We must all work together to promote a culture of cybersecurity and take proactive steps to safeguard our digital lives. As we move forward, let us remember that cybersecurity is not a one-time investment but a continuous process that requires ongoing attention and effort.