BEYONDSOFT®
beyond your expectations

Get the Framework to

Strengthen your Security Operations Center

Table of Contents

Cybersecurity

The Present Landscape

Organizations of all sizes have been working at a global scale for decades to safeguard themselves against threats in cyberspace. There has been a consistent and considerable investment made in enhancing and expanding security solutions through research and development within organizations as well as through partnerships, collaborations, and outsourcing.

This white paper endeavors to provide a comprehensive understanding of the various cybersecurity threats prevailing in the digital landscape and outlines the roadmap that you can take to shield from cyberthreats.

Identify and Understand Cybersecurity Threats

The first few steps in tackling any threats are to identify, categorize, and understand them. Cyberthreats today can be broken down into five distinct categories:

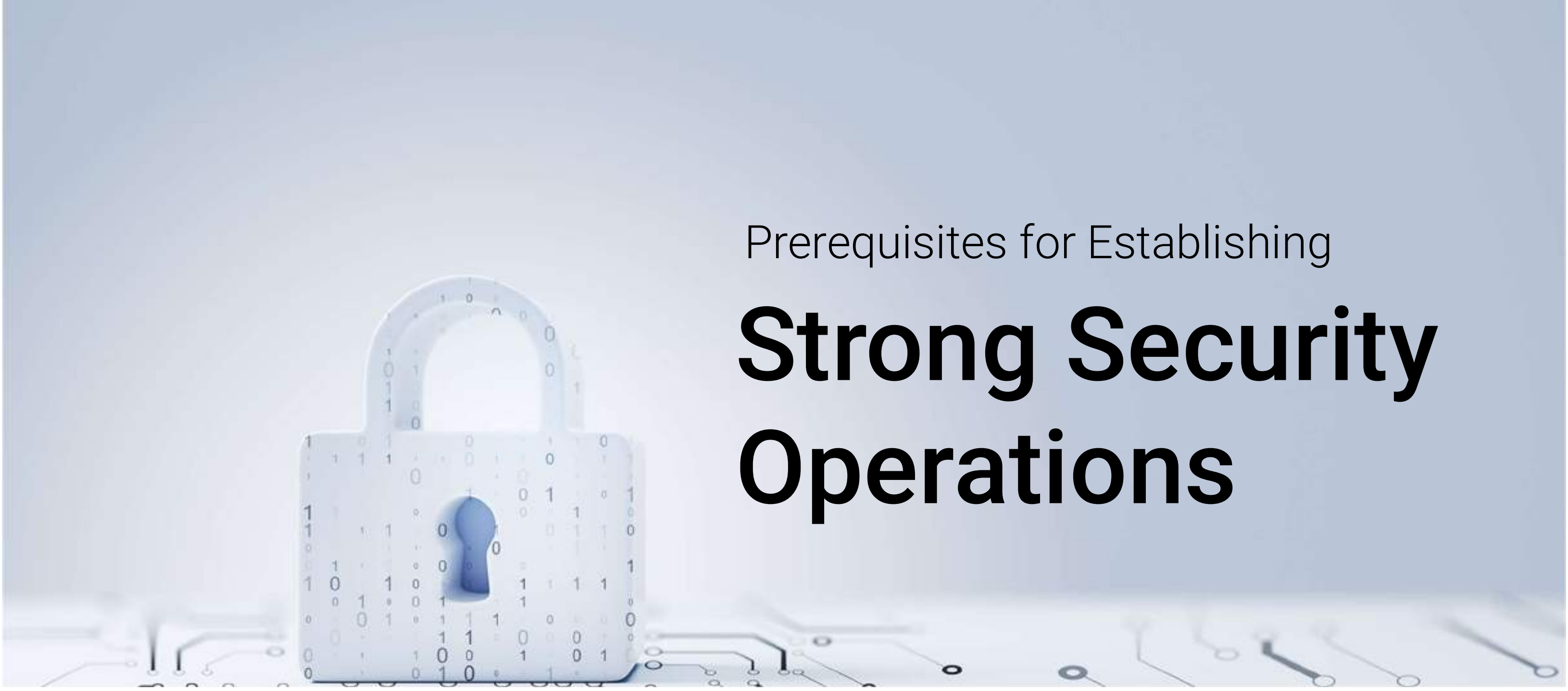
- Phishing
- Ransomware attacks
- Data breach of personal or confidential data
- Brute force attacks
- Attacks against cloud platforms

Cybersecurity or IT security (information technology security), involves the protection of digital systems and networks from attack by malicious entities.

The consequences of these attacks could be data theft, damage to hardware or software, business disruption, a complete shutdown of your operations, or even damage to your company's reputation. Large organizations with physical and digital assets spread across multiple geographies are more vulnerable to such attacks. Whenever there is a new threat, organizations generally respond by adopting additional security tools and software. While the approach only seems natural and certainly addresses the immediate threat, it comes with an inherent risk of governance, maintenance, and talent-based issues in keeping them operational in the distant future.

Recent developments on the geopolitical front and the changing needs because of hybrid work culture have added an extra element of uncertainty to an already complex landscape. Below are a few of the key factors why cyberattacks will continue and spread with time:

- Economic Distress
- Increased Business Email Compromises
- AI-driven Information Warfare
- Geopolitical Instability
- Emergence of Disruptive Technologies
- Cloud Security



Prerequisites for Establishing

Strong Security Operations

Before you decide to build, buy, expand your talent pool, or bring in a partner to help in security operations, here are some prerequisites that you can consider:

1. **Develop a Deep Understanding of Your Organization's Overall Attack Surface**

   One of the most important pillars of any organization's cybersecurity posture is understanding the breadth of the attack surface. This is critical from the planning perspective. Without having complete awareness of your organization's attack surface, any operational planning to secure the assets will fail. Many times, these devices are deployed and stored at places that can be accessed by many users.

   - How many devices are exposed to the perimeter?
   - How many workstations are running outdated operating systems?
   - How many servers are being hosted on premises?

   These questions illustrate the importance of asset management in an organization's overall security posture. By creating a full inventory of assets in the environment, your organization can gain a better understanding of the overall attack surface while determining which assets are exposed to the perimeter.

   Your assessment will also enable your organization to prioritize and refine your security operations program with precision and develop a stronger vulnerability detection and security posture management program. Along with creating an inventory of assets, implementing endpoint monitoring across the environment will help your organization review public ports, disable unnecessary ports, and restrict port destinations. This type of monitoring is crucial to provide visibility into actions taken by potential threat actors. While other types of log sources can complement this type of visibility, they cannot replace it.

2. **Monitor Critical Log Sources for Security Threats**

   We also recognize that a lack of visibility allows security threats to go unnoticed and can cause severe damage to an organization's reputation. For example, log monitoring is extremely critical to detect major threats. This includes logs from various sources like firewalls, Endpoint Detection and Response (EDR) solutions, Identity Access Management (IAM) systems, Intrusion Detection Systems (IDS)/Network Detection and Response (NDR) systems, and the cloud-hosted services used in enterprise environments.

3. **Implement Multi-Factor Authentication (MFA)**

   By requiring multiple forms of authentication, it becomes much more difficult for unauthorized individuals to gain access to sensitive systems and data within a network or system. We recommend your organization consider your overall MFA configuration against diverse types of threats. These countermeasures include rate limiting of authentication requests, adding a step after the authentication prompt, and end-user security awareness training.

4. **Instill a Zero-Trust Security Culture and Strategy**

   As your organization adopts several cloud-based services to manage your team's workload needs and gives them access to a remote or hybrid environment, establishing a Zero-Trust culture and robust security strategies are important decisions for your company. Zero-Trust will focus on the user, not the perimeter, and limits all access unless it can be verified.

   There are multiple ways to implement Zero-Trust strategies, including implementing multi-factor authentication and other identity management tools. Utilizing a Zero-Trust strategy and other relevant solutions will reduce the risk of account takeovers and will provide additional security for organizations.

5. **Understand the Shared Responsibility Model and Eliminate Misconfiguration**

   It is important to recognize where a cloud provider's security responsibilities end, and where your organization's responsibilities begin.

   This is also known as the shared responsibility model. In this model, the cloud provider is responsible for the security of the cloud, while you are responsible for the security within the cloud. The specifics of this responsibility can vary depending on the cloud service model your organization uses, such as IaaS, PaaS, or SaaS.

   Without a firm grasp of these concepts, setting up cloud security can be complicated and confusing, which can result in incorrect configurations or a lack of adequate cloud security. It is vital for you to know where data is being transferred to the cloud, and establish secure protocols and encryptions to be deployed once it is in the cloud. These protocols should include a knowledge of, and restrictions to, who can access the data and applications within the cloud environment.

6. **Establish a Comprehensive Security Awareness Program/Cybersecurity-minded Culture**

   By establishing a comprehensive security awareness program, users can understand how they are targeted and how they can act as a critical line of defense against threat actors and breach attempts. A strong program includes regular training on current trends and topics — such as password management, browsing habits, social engineering tactics, and how to report and respond to suspicious activity.

Given the increasing frequency and complexity of cyberattacks, it is no longer a matter of if an attack will occur, but rather when. Setting up a Security Operations Center (SOC) is ideal to address the "when" question of the cyberattack and to strengthen your organization's resilience against cyberthreats and minimize the impact in the event of a compromise.

> "
>
> *Beyondsoft plays a vital role in helping you establish robust and proactive security operations that enhance your cybersecurity posture and defend against evolving threats effectively.*
>
> **MengKhong Tong, President & COO**
> NABG team at Beyondsoft

Five Advantages of a

Security Operations Center

- Proactive Threat Hunting
- Improved Incident Detection & Response Time
- Cost Savings
- Increased Security Visibility and Centralized Management of Incidents
- Regular Auditing of Systems

While most organizations are not completely lacking in the development of a cybersecurity framework, many of them also admit that they are not equipped for the in-house staffing of a 24/7 workforce for the Security Operations Center (SOC). Cybersecurity is one of the most sought-after fields these days and has a very severe resource shortage, and that also impacts many organizations' ability to hire the right skilled resources.

Cybersecurity is a team sport and that is why Beyondsoft has created an ecosystem of experts who bring their different expertise together for the benefit of our customers. We understand that no organization can protect itself in isolation. Therefore, we as an ecosystem rely on each other for sharing, learning, and providing expertise. It's almost impossible to go it alone in today's threat landscape. We belie

Framework of a Successful

Security Operations Center

We help you in setting up your Security Operations Center (SOC) by providing a range of expertise, services, and support throughout the process. An SOC is a critical component of your organization’s cybersecurity infrastructure, responsible for monitoring and responding to security threats in real time. Here is our framework:

Assessment and Planning

We conduct an initial assessment of your existing cybersecurity posture and infrastructure. We work with you to understand your security needs, risk profile, and business objectives. Based on this assessment, we create a comprehensive roadmap for setting up your SOC, outlining the required processes, technology platforms, and most importantly the skilled resources.

SOC Design and Architecture

We design the SOC’s architecture to ensure optimal performance and scalability. We will consider factors such as data collection, correlation, analysis, and incident response workflows to create a robust and efficient SOC design.

Tools/Technology Selection

We design the SOC’s architecture to ensure optimal performance and scalability. We will consider factors such as data collection, correlation, analysis, and incident response workflows to create a robust and efficient SOC design.

Processes and Workflows

We help develop incident response plans, standard operating procedures (SOPs), and workflows for the SOC team. This ensures that SOC analysts can effectively respond to security incidents in a timely and coordinated manner.

Implementation and Integration

With close to 3 decades of experience in implementation solution deployments, we assist in the implementation and integration of the chosen security technologies and tools. Our team of experts will configure the systems to work together seamlessly, ensuring that all necessary data sources are connected to the SOC for effective threat monitoring.

Governance and Continuous Improvement

We support your SOC in continuously improving its operations. This means focusing on regular assessments, performance monitoring, and refining processes based on lessons learned from past incidents.

Next Step

Along with helping our customers to set up their SOC, we also provide managed services for security operations services. We offer managed SOC services where the end-to-end operation of your SOC will be managed by us or in collaboration with a few dedicated partners. This approach gives you back time to focus on your core business while you have Beyondsoft and our partners’ cybersecurity expertise.

Let us work together to strengthen your security posture.

About Beyondsoft

As a global IT company with over 30,000 associates, Beyondsoft leverages emerging technologies and a proven delivery method, enabling customers in every industry to take an agile and forward-thinking approach to business. For nearly three decades, Beyondsoft has provided a broad range of high-quality IT services, including AI, cloud, big data and analytics, business process outsourcing, custom software solutions, test automation, digital enablement, and other software engineering services.

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used in this website are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

DESIGN BY ZAMSTARS