

2024

Service offer

Cybersecurity as a Service



A comprehensive digital security solution

As a company, our specialty lies in offering thorough cyber security solutions that adhere to current guidelines and standards. Our services encompass a broad spectrum of options ranging from basic support to full management.

Security systems, all offered by a team of seasoned technicians with extensive experience. This method enables us to promptly address the specific requirements of our clients and guarantee the utmost protection for their information systems and data.

Security services

<p>Vulnerability Management</p> <p>NIS2 ISO 27001</p> <p>MANDATORY A.8.8 / A.8.19</p> 	<p>Security Awareness Training</p> <p>NIS2 ISO 27001</p> <p>MANDATORY A.6.3</p> 	<p>Password Management</p> <p>NIS2 ISO 27001</p> <p>MANDATORY A.5.17</p> 
<p>Log Management</p> <p>NIS2 ISO 27001</p> <p>MANDATORY A.8.15</p> 	<p>Penetration Testing</p> <p>NIS2 ISO 27001</p> <p>MANDATORY A.8.8</p> 	
<p>Microsoft Security</p> <p>NIS2 ISO 27001</p> <p>RECOMMENDED MULTIPLE</p> 	<p>Cyber Consulting</p> <p>NIS2 ISO 27001</p> <p>RECOMMENDED MULTIPLE</p> 	<p>Cloud WAF & DDoS</p> <p>NIS2 ISO 27001</p> <p>RECOMMENDED A.8.21 / A.8.22</p> 

Cyber TBD

Our company offers exceptional services in the realm of cybersecurity, drawing on the extensive expertise and wealth of knowledge possessed by our skilled team. We specialize in holistic security solutions for enterprises of varying scales, ranging from small firms to major corporations with numerous employees and devices. Furthermore, our proficiency extends across various pivotal sectors such as critical infrastructure, healthcare, banking, and travel.

The abbreviation TBD (To Be Done) underscores the perpetual nature of safeguarding cybersecurity, highlighting the need for continual enhancement and adjustment. This perspective aligns with our belief that security protocols should consistently evolve to address current threats and advancements in technology.

In our organization, this approach entails not only consistent updates and advancements of our services and solutions, but also ongoing education and growth of our professionals to confront the most recent challenges in the realm of cybersecurity. Dedication to TBD (To Be Done) represents for us a dedication to excellence, continual enhancement, and delivering superior protection for our clientele.

cybertbd.com →



Advantages of selecting our firm:

Experienced and certified personnel:

Our specialists possess globally acknowledged certifications from top cybersecurity organizations such as CompTIA Security+, Microsoft (SC-900, MS-900), NUKIB - Cybersecurity Manager, Qualys, Skybox Security SCPS+, Tenable, Zabbix, First CVSS, Elasticsearch, Cisco, Palo Alto. This proficiency guarantees the utmost quality of our services.

Demonstrated expertise in pivotal sectors:

Our experience in critical infrastructure, healthcare centers, and technology leaders in the travel industry enables us to offer specialized solutions that precisely meet the unique needs of these sectors.

Thorough understanding of legislation:

We possess a profound comprehension of the NIS2 directive and its present interpretation, allowing us to assist our clients in fulfilling all legal and regulatory obligations.

Flexibility and adaptability:

Our expertise in assuming services and integrating new technologies enables us to adapt flexibly to clients' specific requirements, ensuring a seamless transition and incorporation of innovative solutions.

Global Reach:

Our capacity to operate globally and a vast network of collaborators enable us to provide services where required, with local comprehension and assistance.

Vulnerability Management

A vulnerability management service is an essential component of cybersecurity, offering organizations vital tools to detect, analyze, and address vulnerabilities in their information systems. This service enables organizations to methodically scan and assess vulnerabilities in their infrastructure, crucial for robust protection against cyber threats. Through consistent identification and analysis of vulnerabilities, businesses can preemptively thwart attacks, reducing the likelihood of data breaches, financial harm, and reputational damage.

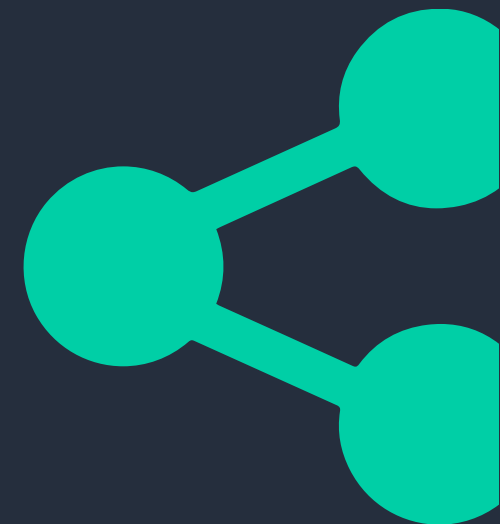
One of the primary advantages of a vulnerability management service is aiding organizations in complying with diverse cybersecurity regulations and standards, encompassing GDPR, NIS, NIS2, and PCI DSS.

Organizations are required to implement and maintain sufficient security measures. Effective vulnerability management ensures that organizations not only meet these standards but also avoid potentially costly penalties for violations.

Another crucial aspect of this service involves overseeing updates and addressing vulnerabilities. Methodical implementation of security updates is vital for safeguarding corporate networks and endpoints against new threats. This procedure not only enhances the organization's cyber resilience but also bolsters its credibility and standing with clients, partners, and regulatory bodies.

Benefits

- Proactively identifying and resolving vulnerabilities
- Preventing data leakage and financial losses
- Regulatory compliance
- Enhancing credibility and reputation
- Efficient updating and patching management
- Enhancing cyber resilience



[Request a service →](#)

Security Awareness Training

Cybersecurity training is crucial to ensure that employees are well-informed about constantly evolving security risks, regulations, and efficient defense strategies. In the current digital era, where cyber threats evolve rapidly, regularly updating employees' knowledge and skills is not just advised but imperative. Our training offers employees a thorough understanding of all essential facets of cybersecurity, covering basic principles to cutting-edge defense methods, empowering them to comprehend and adeptly address potential threats.

Employees are commonly known as the "first line of defense" in an organization's cybersecurity, based on their capacity to recognize

Recognizing phishing emails, appropriately addressing suspicious system behavior, and effectively utilizing and overseeing passwords can significantly enhance the company's overall security. Insufficient training leaves employees more susceptible to attacks, increasing the risk of severe security breaches that could have devastating consequences for the organization.

Cybersecurity training enhances employees' capacity to identify and address cyber threats, fostering a security culture within the organization.

Benefits

- **Raising awareness of security risks**
- **Enhancing understanding of laws and established protocols**
- **Application of knowledge**
- **Ongoing testing and assessment**
- **Enhancing employee engagement**
- **Enhancing internal security**



[Request a service →](#)

Password Management

A password manager is a crucial tool for contemporary organizations, consolidating the storage, management, and security of passwords for accessing different applications and services. This system provides significant advantages including safeguarding sensitive data, user-friendly interface, and auditing and monitoring features, empowering organizations to maintain password compliance with internal policies. Automatically generated passwords are securely stored, eliminating the necessity for users to remember multiple passwords and decreasing the likelihood of data breaches and insider threats.

Our service provides centralized management and transparency to streamline auditing and monitoring of access rights, enhance user productivity, and guarantee regulatory and security compliance.

With these characteristics, your organization can efficiently handle access permissions and safeguard vital information from unauthorized access.

Our proficient team will assist you in the successful deployment of a password manager and provide comprehensive training to your users to enable effective system utilization. Through our post-implementation support, you will receive a reliable solution that enhances data security, streamlines auditing and access monitoring, and boosts productivity across your organization.

Benefits

- **Protection of sensitive data**
- **Centralized management and transparency.**
- **User-Friendliness**
- **Possibility of audits and monitoring**
- **Adherence to regulations and standards**
- **Preventing data leakage**
- **Mitigating insider threats**
- **Enhanced productivity**



[Request a service →](#)

Log Management

Our services in log management and SIEM offer a comprehensive solution for efficiently collecting, storing, analyzing, and managing log records and security events from different systems and applications. This integration enables organizations to centralize and standardize data from various sources into a unified repository, simplifying the monitoring, assessment, and response to security incidents.

Our specialists create unique parsers, connectors, and control mechanisms to guarantee optimal value and efficiency in both log management and SIEM systems.

Thanks to our services, clients who possess these systems but do not utilize them can.

Realize significant enhancements in reporting and data analysis by maximizing its full potential. We assist in developing informative case studies showcasing the tangible advantages of implementing and optimizing SIEM systems effectively.

Our service aims to convert extensive data volumes into valuable and succinct information, offering valuable insights for managerial decision-making. The objective is to minimize the occurrences necessitating intervention from thousands to mere dozens or units, facilitating quicker and more precise responses to actual threats, thereby enhancing an organization's security stance. This effectiveness not only saves time but also markedly diminishes the expenses linked to the operational security of the IT infrastructure.

Benefits

- **Centralization of data management**
- **Sophisticated analysis and reporting**
- **Optimization of existing systems**
- **Efficient threat response**
- **Enhancing decision-making and strategic planning.**
- **Cost reduction and process streamlining**
- **Adhering to the regulations**



[Request a service →](#)

Penetration Testing

Our penetration testing service provides a comprehensive and proactive security assessment of your information systems. In contrast to vulnerability management, which concentrates on detecting and remedying network vulnerabilities, penetration testing actively replicates real-world attacks to breach your systems. This methodology enables our skilled professionals to not only reveal potential weaknesses but also evaluate the efficacy of your existing security protocols against genuine threats.

During penetration testing, our specialists methodically analyze your information systems, encompassing applications and network infrastructure, to pinpoint vulnerabilities exploitable by attackers. The procedure entails a sequence of controlled attacks emulating cybercriminal activities and is intended to reveal vulnerabilities that may be exploited.

The outcome of these assessments is a comprehensive report comprising an analysis of the discovered vulnerabilities, an evaluation of the risks linked to each, and suggestions for enhancing security protocols. This report offers crucial insights to assist in securing your systems and safeguarding sensitive data against real-world threats.

Benefits

- **Detection and patching of vulnerabilities**
- **Simulation of authentic cyber threats**
- **Enhancing security measures**
- **Mitigating the risk of data breaches and monetary losses.**
- **Regulatory compliance**
- **Enhancing customer and partner trust.**



[Request a service →](#)

Microsoft Security

Microsoft Security offers expert guidance and assistance for every facet of the Microsoft 365 environment, covering planning, deployment, management, and optimization. Our focus lies in implementation management, utilizing established practices to enhance system configuration for optimal Microsoft 365 utilization and improved return on investment.

In order to guarantee the utmost level of cybersecurity for our clients, we provide an integrated security solution utilizing tools like Microsoft Defender and Azure Sentinel. These tools deliver strong protection against a broad spectrum of cyber threats and facilitate proactive real-time monitoring, detection, and response to security incidents.

Emphasizing the implementation of standard operating procedures (SOPs) and adherence to industry standards is crucial for ensuring compliance with best practices and regulatory requirements. SOPs establish clear rules and procedures that standardize security and information management operations, promoting consistency and minimizing human risk.

Microsoft enhances security operations to provide substantial advantages to organizations utilizing their technologies through ongoing enhancements to security features and mechanisms. The company prioritizes investing in the advancement and maintenance of its security tools and services to safeguard its products and customers from constantly changing cyber threats.

Benefits

- **Detection and patching of vulnerabilities**
- **Simulation of authentic cyber threats**
- **Enhancing security measures**
- **Mitigating the risk of data breaches and monetary losses.**
- **Regulatory compliance**
- **Enhancing customer and partner trust.**

Request a service →

Cyber Consultancy

Our cyber consulting service offers organizations specialized expert guidance and assistance in the realm of cyber security. It is tailored to detect, assess, and mitigate security threats and risks encountered by organizations. Our expertise covers multiple facets of cyber security, such as strategy development, risk mitigation, security technology deployment, and incident response.

Outsourcing critical positions like the Cyber Security Manager (CMS) and Cyber Security Architect (CSA) enables organizations to leverage the knowledge and skills of an external team without the need to allocate resources to internal staffing and management. This results in cost savings, enhanced efficiency, and improved flexibility in addressing security issues.

Through our consulting services, organizations can access top experts and methods in the cyber security field, enhancing their defenses, mitigating risks related to cyber threats, and safeguarding their information systems and data. Our services offer a customized cybersecurity solution to address the unique requirements and objectives of each organization.

Benefits

- **Expertise access**
- **Cost reduction is the revised text.**
- **Advance security**
- **A versatile and expandable solution**
- **Proactive risk mitigation**
- **Protection of sensitive data and systems**
- **Adherence to legislative and regulatory mandates**

[Request a service →](#)

Cloud WAF & DDoS

Our Cloud WAF and DDoS protection services are crafted to offer thorough security for web applications and networks against a broad spectrum of cyber threats.

Cloud WAF provides a strong cloud-based security solution safeguarding web applications from various attacks like SQL injection, cross-site scripting (XSS), and other exploits. It features a user-friendly interface for simple security rule configuration, traffic monitoring, and real-time security event analysis. This solution aids in early detection and mitigation of security threats to prevent potential damage.

DDoS protection aims to prevent DoS (Denial of Service) and DDoS attacks.

Distributed Denial of Service (DDoS) attacks aim to overwhelm web applications or networks with a high volume of requests, rendering them inaccessible to legitimate users. Our DDoS protection features sophisticated detection and filtering mechanisms that continuously monitor and counter potential attacks, ensuring the availability of your services even amidst extensive attack campaigns.

Both services are crafted for easy management and scalability, enabling tailored protection based on your organization's specific needs and size. Our cloud-based services are swiftly deployable without the need for complex infrastructure or significant initial investment, making them ideal security solutions for businesses of all sizes seeking efficient and cost-effective online asset protection.

Benefits

- **Thorough safeguard**
- **Security monitoring proactivity**
- **Intuitive interface for simple setup**
- **Scalability**
- **Financial loss prevention**
- **Adherence to safety standards and regulations**
- **Rapid execution**



[Request a service →](#)



CYBER  TBD

cybertbd.com

sales@cybertbd.com

ID: 21414432 | CZ21414432

D-U-N-S: 984089981