2024

Service offer

Cybersecurity as a Service

CYBERTBD

A comprehensive digital security solution

As a company, our speciality 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 approach enables us to promptly address the specific requirements of our clients and guarantee the utmost protection for their information systems and data.

Security services

Vulnerability Management

NIS2 MANDATORY
ISO27001 A.8.8 / A.8.19

Security Awarenes Training

NIS2 MANDATORY
ISO27001 A.6.3

Password Management

NIS2 MANDATORY
ISO27001 A.5.17

Log Management

NIS2 MANDATORY
ISO27001 A.8.15

Penetration Testing

NIS2 MANDATORY
ISO27001 A.8.8

Monitoring Service

NIS2 MANDATORY
ISO27001 MULTIPLE

Microsoft Security

NIS2 RECOMMENDED
ISO27001 MULTIPLE

Cyber Consulting

NIS2 RECOMMENDED
ISO27001 MULTIPLE

Skybox Security

NIS2 RECOMMENDED
ISO27001 MULTIPLE

Cloud WAF a DDoS

NIS2 RECOMMENDED
ISO27001 A.8.21 / A.8.22

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 specialise 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 organisation, 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 commitment 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 organisations 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 centres, and technology leaders in the travel industry enables us to offer specialised 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.

Reference

Our company has established a strong position in the digital security market in a relatively short time. Our portfolio includes prominent companies across various sectors, including finance, telecommunications, healthcare, and industry.

Companies that protect the sensitive data of thousands of customers daily and whose operations rely on secure and reliable IT systems have placed their trust in our services.

The services we currently provide are validated not only by a wide range of clients but also by their long-term satisfaction and successful outcomes in preventing and addressing cyberattacks.

Satisfied clients

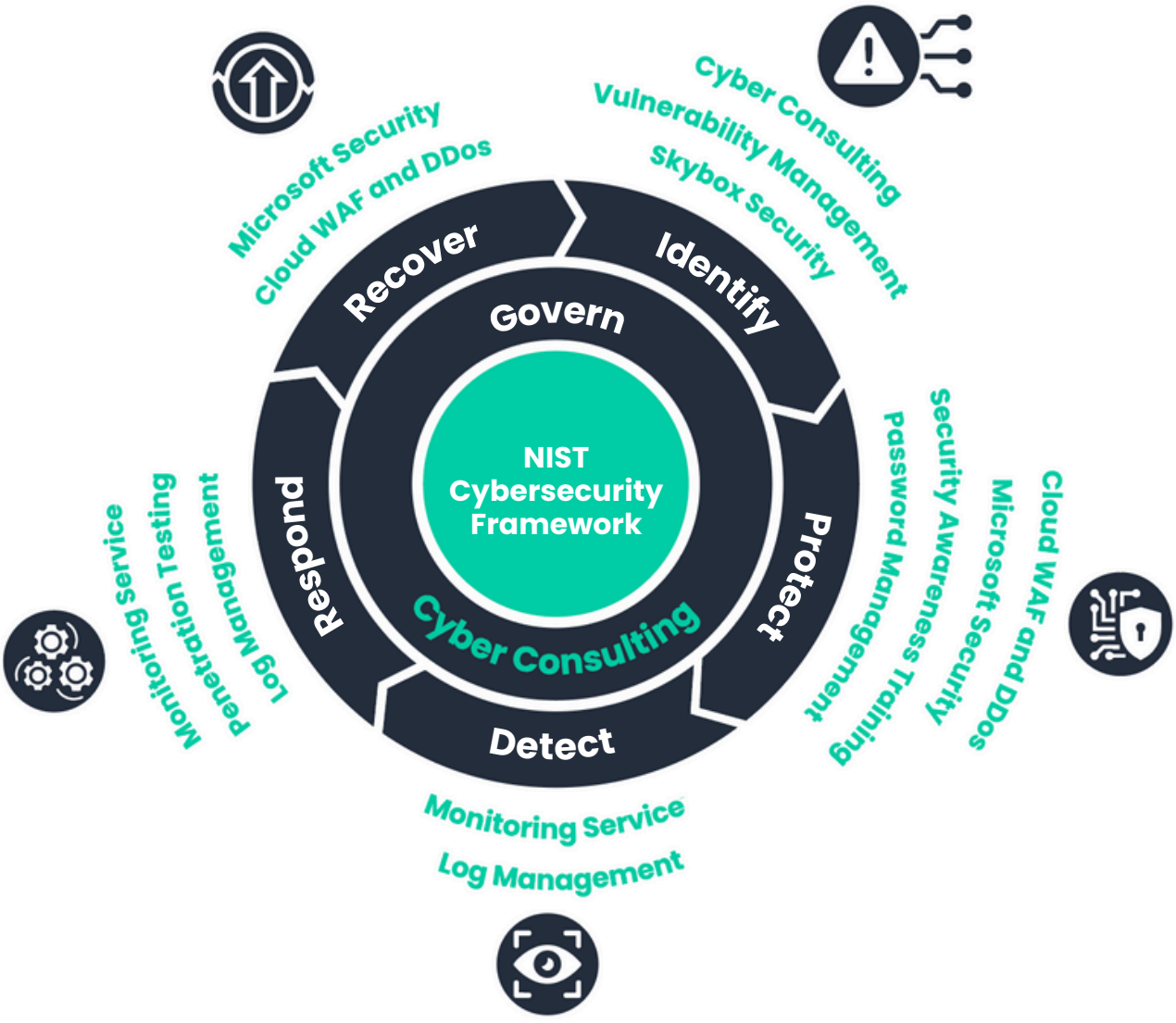
Place your trust in us →

Mapping NIS 2 with the NIST Cybersecurity Framework

The NIS 2 Directive establishes extensive obligations but does not provide specific steps. Adopting the NIST Cybersecurity Framework helps organizations effectively meet the requirements of NIS 2.

The framework includes six key functions:

GOVERNANCE: Establishing policies for effective cybersecurity governance.
IDENTIFICATION: Asset management and risk assessment.
PROTECTION: Protection of networks, access, and data.
DETECTION: Detection of incidents and anomalies.
RESPONSE: Incident response planning.
RECOVERY: Recovery and business continuity planning.



NIS2 MANDATORY
ISO 27001 A.8.8 / A.8.19

Vulnerability Management

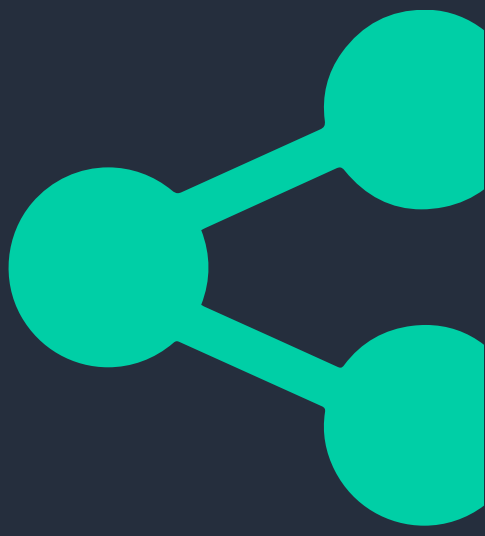
A vulnerability management service is an essential component of cybersecurity, offering organisations vital tools to detect, analyse, and address vulnerabilities in their information systems. This service enables organisations to **methodically scan and assess vulnerabilities in their infrastructure**, 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 organisations in complying with diverse cybersecurity regulations and standards, encompassing **GDPR, NIS, NIS2, and PCI DSS**. organisations are required to implement and maintain sufficient security measures. Effective vulnerability management ensures that organisations 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 organisation'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 ⟶

NIS2 MANDATORY
ISO 27001 A.6.3

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 organisation's cybersecurity, based on their capacity to **recognise phishing emails, appropriately addressing suspicious system behavior, and effectively utilising 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 organisation.

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

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 →

NIS2 MANDATORY
ISO 27001 A.5.17

Password Management

A password manager is a crucial tool for contemporary organisations, **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 organisations 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 **centralised management and transparency** to streamline auditing and monitoring of access rights, enhance user productivity, and guarantee regulatory and security compliance.

With these characteristics, your organisation can efficiently handle access permissions and safeguard vital information from unauthorised 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 utilisation. 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 organisation.

Benefits

- **Protection of sensitive data**
- **Centralised 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 →

NIS2 MANDATORY
ISO 27001 A.12.4

Log Management

Our services in **log management and SIEM** offer a comprehensive solution for **efficiently collecting, storing, analysing, and managing log records and security events from different systems and applications.** This integration enables organisations to centralise and standardise 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 utilise them can.

Realise significant enhancements in reporting and data analysis by maximising its full potential. We assist in developing informative case studies showcasing the tangible advantages of implementing and optimising 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 minimise the occurrences necessitating intervention from thousands to mere dozens or units, facilitating quicker and more precise responses to actual threats, thereby enhancing an organisation'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

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

Request a service →

NIS2 MANDATORY
ISO 27001 A.8.8

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 analyse 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 ⟶

NIS2 MANDATORY
ISO 27001 MULTIPLE

Monitoring Service

Monitoring IT infrastructure is essential for maintaining continuous and efficient operation of all your systems, servers, networks, and applications.
It allows real-time monitoring of the infrastructure's status and performance, identifying issues before they escalate, and responding to them immediately. **A properly configured monitoring system ensures efficient resource management, performance optimisation, and minimises the risk of downtime.**

The deployment and management of such a system require advanced expertise. Our company specialises in providing comprehensive services in IT infrastructure monitoring. Our team of qualified experts with extensive experience will assist you with the design, implementation, and management of monitoring solutions **to ensure your infrastructure operates flawlessly.**

In addition, we will train your IT specialists to fully utilise personalised dashboards and efficiently work with triggered events. This way, your experts will be able to proactively respond to potential issues before they affect operations, **minimising the risk of downtime and ensuring the reliable performance of your systems.**

Benefits

- **Professional deployment of the monitoring system**
- **Continuous management and support**
- **Performance optimisation**
- **Fast and efficient incident resolution**
- **Proactive solutions**
- **Improved decision-making and planning**
- **Compliance with regulatory requirements**
- **Increased trust of customers and partners**

Request a service ⟶

NIS2
ISO 27001

RECOMMENDED
MULTIPLE

Microsoft Security

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

In order to guarantee the utmost level of cybersecurity for our clients, we provide an integrated security solution utilising 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.

Emphasising 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 standardise security and information management operations, promoting consistency and minimising human risk.

Microsoft enhances security operations to provide substantial advantages to organisations utilising their technologies through ongoing enhancements to security features and mechanisms. The company prioritises 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 →

NIS2
ISO 27001

RECOMMENDED
MULTIPLE

Cyber Consultancy

Our **cyber consulting service** offers organisations specialised expert guidance and assistance in the realm of cyber security. It is tailored to **detect, assess, and mitigate security threats and risks** encountered by organisations. 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 organisations 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, organisations 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 customised cybersecurity solution to address the unique requirements and objectives of each organisation.

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 ⟶

NIS2 RECOMMENDED
ISO 27001 MULTIPLE

Skybox Security

The deployment and management of Skybox Security require expertise. Our certified team provides comprehensive services from deployment and configuration, through the management of specific modules, to full platform management. **Proper management of Skybox** is essential for optimal performance of all its functions and maximum security benefits.

Our services include:

- **Deployment and complete management of Skybox**
- **Support and consulting**
- **Training and education**
- **Integration into corporate processes**

This ensures **the efficient use of Skybox** in your organisation, leading to a significant increase in security and risk management.

Skybox Security is an advanced cybersecurity management platform that helps organisations optimise their security infrastructure. By integrating data from various security systems, **Skybox provides a comprehensive view of the entire network**, identifies vulnerabilities, analyses risks, and supports strategic security decision-making. The platform includes tools for attack simulation, security policy analysis, firewall management, and a dynamic network map, enabling proactive threat protection.

Benefits

- **Complete deployment and configuration of Skybox**
- **Specialised project services for specific modules**
- **Thorough management and regular maintenance of the platform**
- **Maximum utilisation of all Skybox functionalities**
- **Enhanced security and reduced risks in network infrastructure**
- **Cost optimisation and process efficiency**

Request a service →

NIS2
ISO 27001

RECOMMENDED
A.8.21 / A.8.22

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 organisation'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 →

CYBERTBD

cybertbd.com
sales@cybertbd.com

ID: 21414432 | CZ21414432
D-U-N-S: 984089981