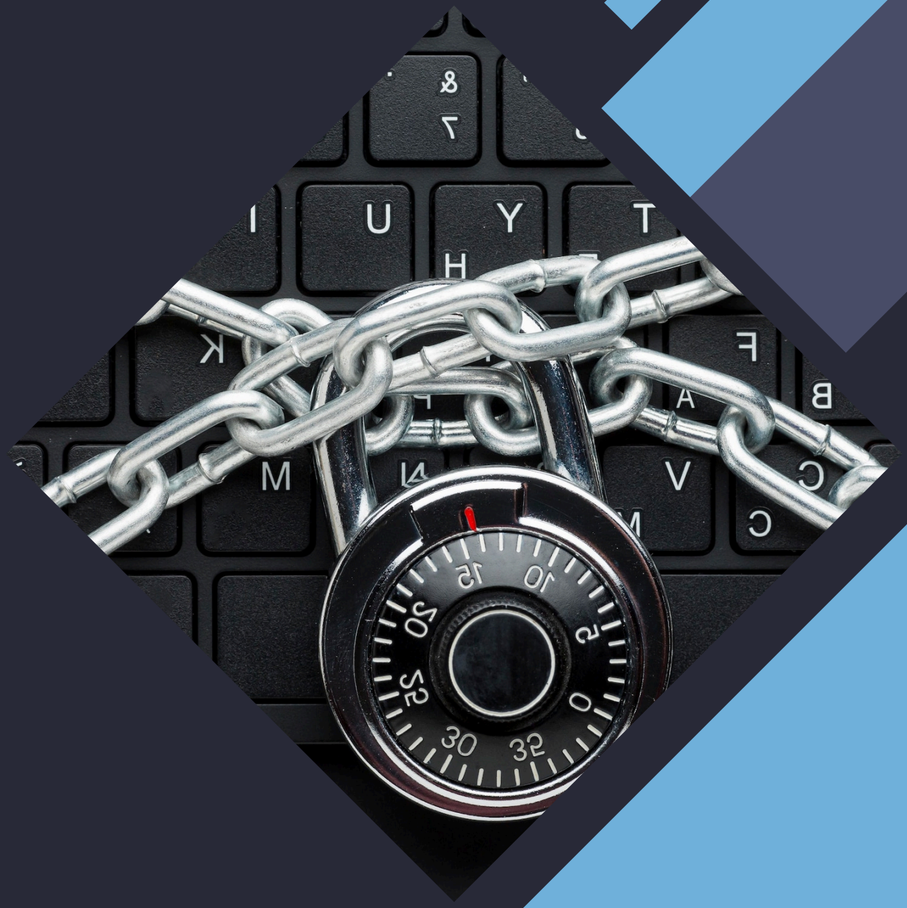
Fortifying Digital Defenses: A Comprehensive Approach to Cyber Security Systems

Introduction

The temporary period of society's existence in terms of the use of weapons of mass destruction in wars and conflicts can be conditionally divided into two stages – before 2010 and after.

The first stage is characterized by a relatively "soft" attitude towards the concepts of "cyber weapon," "cyberattack," and "cybersecurity." The virtual space was perceived as a parallel space to the everyday realm of life and human interaction.

The second stage is marked by the emergence of combat computer viruses such as Stuxnet, Duqu, Flame, Gauss, and similar ones. In mid-June 2010, the Stuxnet virus intrusion was discovered in the computers of the Iranian nuclear plant in Bushehr. The virus consists of two parts: the first penetrates the system controlling the operating mode of uranium enrichment centrifuges, potentially allowing it to provoke even an explosion of these devices, while the second part ensures that all control devices (even the plant operator) receive signals that everything is functioning normally, and all elements are working within specified parameters. The damage caused by a nuclear explosion at the plant to the surrounding environment can be comparable to the harm that would have been inflicted by conventional nuclear weapons. Therefore, this virus can reasonably be classified as a weapon of mass destruction. The analysis of the situation led to the conclusion that cyberspace is no longer just a medium for human communication, gaming, or knowledge storage. Cyber tools (cyber weapons) represent an independent type of armament capable of delivering an effective strike comparable in outcome to a nuclear attack while remaining undetected and invisible to the enemy. Thus, the modern world has realized that the era of underestimating cyber tools is over, and a serious approach is required for studying and countering them. Currently, a genuine cyber arms race is unfolding globally, and any delay in studying and developing effective countermeasures to cyber weapons is simply unacceptable. The modern world demands constant improvement of cybersecurity measures and ensuring state control over information security. We live in an era of unprecedented cybercrime. The number and complexity of attacks on digital systems continue to grow year by year, as hackers constantly invent new methods of crime and actively use advanced technologies. The emergence of powerful artificial intelligence further necessitates a more comprehensive approach to combating cyber weapons and hackers.

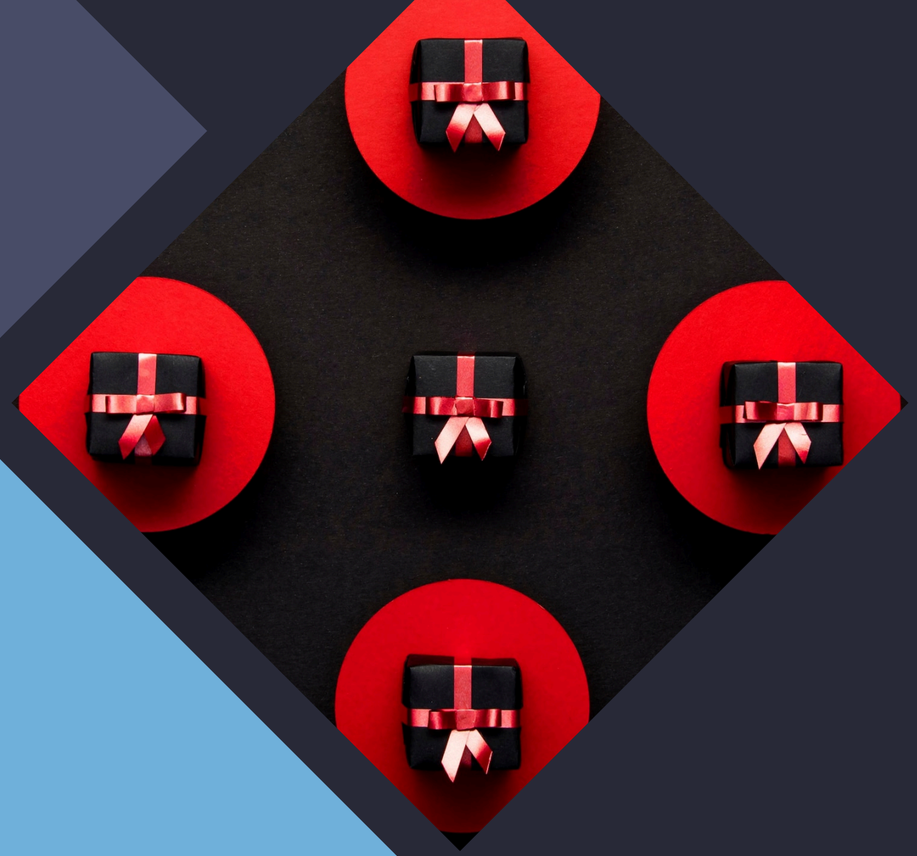


Purpose

Our goal is to assist the government and directive bodies in developing a national cybersecurity strategy, propose solutions for ensuring cybersecurity, and provide strategic insights into cybersecurity issues, cyber readiness, and resilience. We aim to offer a useful, flexible, and convenient foundation for understanding the context and current state of the country's cybersecurity and to help directive bodies develop a strategy that considers the specific situation in the country, its cultural and social values, and encourages the creation of secure, resilient, ICT-based, and integrated communities.

Our Vision

Demonstrate the advantages of a comprehensive approach to designing and developing a national cybersecurity strategy, as well as how it can take different forms with varying levels of detail depending on the country's goals and cyber readiness level. Emphasize that early definition of the concept, goals, and priorities allows the government to consider cybersecurity comprehensively within its national digital ecosystem, rather than just at the level of a single economic sector, specific goal, or response to a particular risk, which in turn enables strategic action. The priorities of the national cybersecurity strategy may vary significantly depending on the challenges the country is currently facing. The project's task is to design, develop, and implement its own cybersecurity defense system.



Understanding Cyber Threats

By identifying national digital assets, both public and private, their interdependencies, vulnerabilities, and threats, as well as by assessing the likelihood and potential impact of cybersecurity incidents. These efforts are related to the principle of risk management and resilience, according to which risk management is crucial for fully realizing the benefits of the digital environment for socio-economic development. Additionally, this initial risk assessment can serve as the basis for future, more specific risk assessments. The aim of this stage is to develop the strategy text by engaging key stakeholders from the public sector, private sector, and civil society through a series of public consultations and working groups. This expanded group of stakeholders, coordinated by the project management body, will be responsible for defining the overall concept and scope of the strategy, formulating shared goals, assessing the current situation, setting priorities for impact on society, citizens, and the economy, and ensuring the necessary financial resources.

Main Threats

Tracking and remote control

The proliferation of the Internet of Things (IoT) and smart devices means that almost every aspect of our lives can be tracked and managed remotely. While this level of connectivity is convenient, it exposes us to an increased risk of cyberattacks.

Data breaches

Large-scale data breaches (especially in government financial institutions, healthcare facilities, and large corporations) have demonstrated the potentially catastrophic consequences of cyberattacks. Theft of personal data, financial losses, and reputational damage are just a few of the negative outcomes.

Economic impact

As the global economy is interconnected, a single cyberattack can impact multiple sectors, leading to significant financial losses. Let's consider possible scenarios of specific cyberattacks. In this context, it is important to note that the realm of cyber threats is vast and continually expanding. Malicious actors are using increasingly sophisticated methods to breach security systems and the data stored within them.

Common attack types

Malware
Viruses and ransomware can infiltrate systems, steal data, and block access to the affected systems.

Phishing and social engineering
Malicious actors use deceptive emails or messages to trick users into revealing private information, such as passwords and financial data.

Denial of Service (DoS) attacks
Cybercriminals overload a system or network with excessive traffic, making it unavailable and disrupting the operation of services.

Man-in-the-Middle (MITM) attacks
Hackers intercept communications between two parties, allowing them to eavesdrop, manipulate, or steal information.

Zero-day attacks
Hackers exploit new vulnerabilities in software that are not yet known to the community.

Countering, detecting, and neutralizing the above-mentioned threats are the primary goals of establishing a cybersecurity system.

Services

- Data access control
- Ensuring the security of information from unauthorized access
- Protection against data interception by unauthorized users
- Verification of data sources
- Implementation of additional controls for information obtained from the internet or other unverified sources
- Training of personnel
- Conducting audits and reporting
- Assessment of cyber risks
- Testing the ability of malicious software to penetrate the internal perimeter of the organization

Employee Training and Awareness

We provide a full range of professional services in the field of cybersecurity, including documentation development and comprehensive training for personnel at various levels of access. Our expertise ensures effective information protection and enhances employee skills in line with current security requirements.

Essential for Government Enterprises

Cybersecurity is extremely important for government enterprises, as it ensures data security, enhances employee productivity, helps protect their reputation, supports compliance with laws and regulations, and is cost-effective.

Cybersecurity involves protecting systems, networks, and data from cyber threats such as malware and unauthorized access. Proper cybersecurity ensures that data is preserved and prevents it from falling into the hands of malicious actors who might use it for harmful purposes, such as stealing personal information. Data managed by government enterprises, from customer information to financial records, must always be protected. Cybersecurity measures, such as access control and the requirement for strong passwords, protect this information from unauthorized access and data breaches. By effectively safeguarding confidential data, financial losses can be prevented and the trust of stakeholders and clients can be maintained.

Cybersecurity not only protects government enterprises from external threats but also creates a secure environment for employees and their productivity. For instance, using certain cybersecurity tools can help employees securely access accounts without the need to repeatedly create support tickets when they forget passwords. Security breaches can also completely disrupt the operations of a government enterprise. However, by implementing cybersecurity measures, the risk of downtime in the event of a cyberattack can be reduced. Cybersecurity for government enterprises is not just an investment in protection but also economic efficiency. Although the costs of implementing cybersecurity solutions and methods may seem excessive, the potential consequences of a cyberattack can be far more devastating financially.

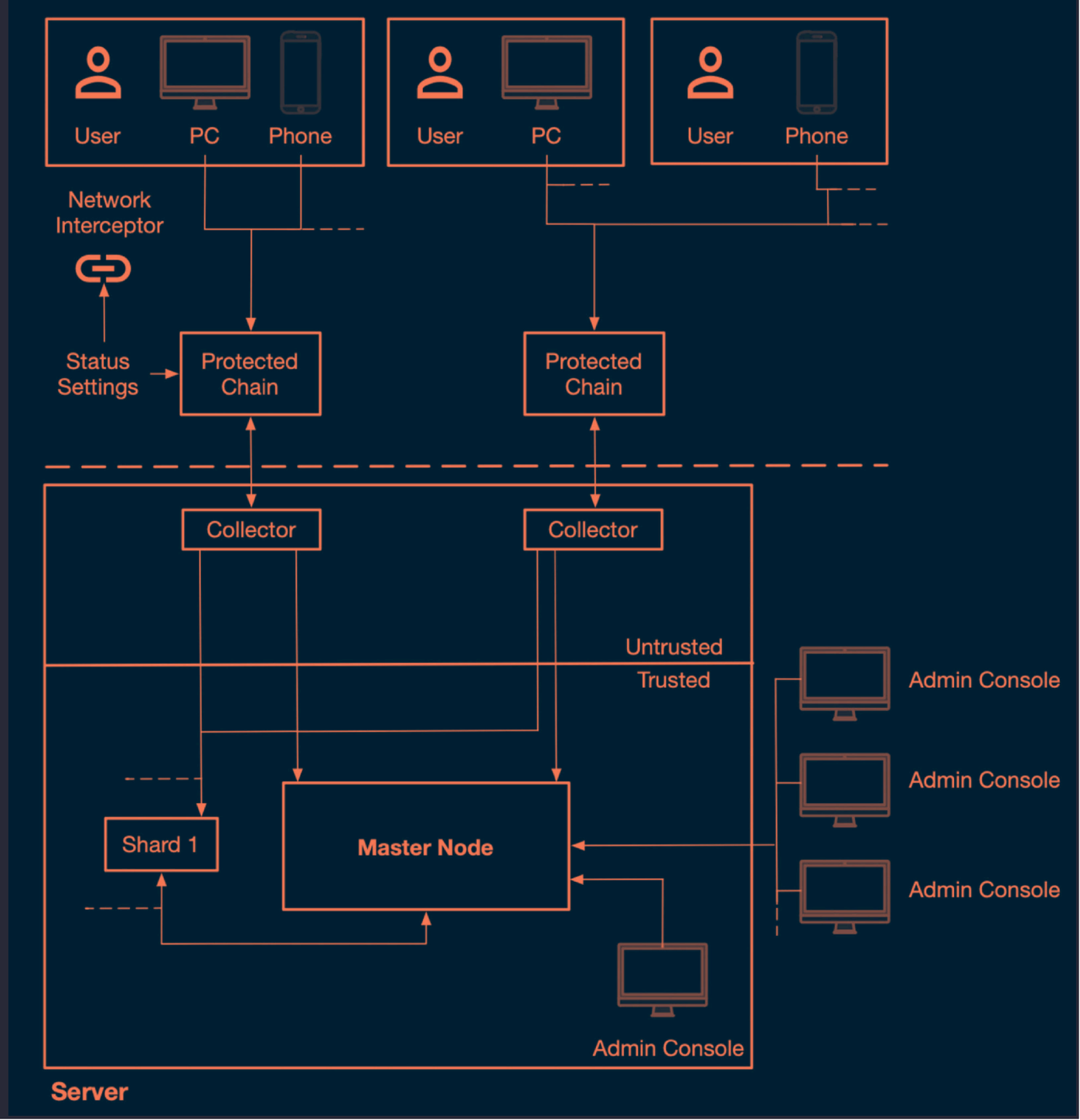
For example, some costs associated with data breaches include compensation to clients, legal expenses, and operational downtime. According to the only Keeper`s Security 2023 Cybersecurity Report in the US, private companies with stolen funds due to cyberattacks lost an average of over $395,000, excluding costs related to the aftermath of the attacks. Thus, by implementing cybersecurity measures, government enterprises can significantly reduce the risk of cyberattacks and the associated financial burden.

Peculiarity of the solution

The proposed cybersecurity system is a solution that supports and, if necessary, can dynamically adjust the developed cybersecurity strategy to align with current cyber threats. This is achieved through active and passive investigation, interception, and analysis of user traffic data. The cybersecurity system is self-learning, collecting and analyzing traffic data, sending results to a distributed database for decryption, storage, and further learning. After this, the cybersecurity system disseminates updated security policy settings to end users. The self-learning mode can also be disabled or significantly restricted if needed. The cybersecurity system operates transparently (invisibly) to the end user and fully controls traffic within the internal network perimeter.

Architecture

Base architecture of the solution



Short Description of components

Protected Chain
A secure chain, consisting of geographically distributed groups, checks and analyzes traffic from user devices and redirects the collected data to protect servers from remote attacks. To enhance protection, multiple secure chains can be configured, each with its own strategy. Each chain leads to a single data collector.

Collector
A data collector, one per secure chain. Each data collector has three services installed:

- **Collector:** collects user traffic data that has been sent through the secure chain.
- **Carrier:** sends data to Shards (distributed storage) and Master Node (main node).
- **Network Controller:** receives the status of the secure chain and conducts audits, sending updates and new security policy settings.

Firewall
Firewall, provides additional protection for the trusted environment (where data is processed and stored) from the untrusted environment (where data is collected).

Admin Console
Administration, monitoring, and analysis console used by cybersecurity system administrators.

Master Node
The Master Node represents the core of the cybersecurity system server. It manages data flows, the status of components, and includes the first section of the distributed database (Shard 0). This shard contains a Worker service for decoding user traffic data before it is stored in the database, and a Monitor service for overseeing all components of the architecture, including the Master Node, and sending alerts via email and various messaging applications in case of alarms.

Network Interceptor
A stationary hardware component, it performs analysis and interception operations in user HTTP connections. It communicates with the data collector (Collector) and its secure chain (Protected Chain) to send data and receive rules and security policy settings.

Shard 1,2,3...N
Additional sections of the cybersecurity system's distributed database. Shard 0 is included in the Master Node. It also includes a Worker service for decoding data and storing it in the database.

Stages of project implementation.

- Description of the main requirements for the cybersecurity system.
- Creation of an informational model of the cybersecurity system.
- Formalization of input data.
- Design of the cybersecurity system architecture.
- Design of the database model for the cybersecurity system.
- Development of the cybersecurity system.
- Modular, functional, and load testing of the cybersecurity system.
- Determination of the final hardware requirements for the cybersecurity system based on load testing results.
- Testing the cybersecurity system for compliance with the chosen protection strategies.
- Writing technical documentation.
- Writing the user manual for the cybersecurity system.

Implementation plan.

- Conducting an on-site cybersecurity audit
- Analysis of the cybersecurity audit, identification of 'weak points,' and development of a cybersecurity strategy.
- Deployment of the cybersecurity system.
- Configuration of the cybersecurity system according to the strategy.
- Launch of the cybersecurity system.
- Penetration testing of the internal network perimeter after the launch of the cybersecurity system.
- Analysis of penetration testing of the internal network perimeter and post-deployment adjustments to the cybersecurity system.
- Conducting basic cybersecurity training for employees.
- Conducting training on working with the cybersecurity system for system administrators.
- Providing technical documentation for the cybersecurity system.
- Maintenance of the cybersecurity system.

Hardware requirements.

Recommended Requirements:

- Number of instances: 4
- Operating System: Linux/Unix/Windows 7-11
- Processor: 2x Intel/AMD 18 Core 3.5GHz, 30MB Cache
- RAM: 32GB
- Storage: 1x SSD 250GB, 2x HDD 1TB (Raid 1)

Optimal Requirements:

- Number of instances: 6
- Operating System: Linux/Unix/Windows 7-11
- Processor: 2x Intel/AMD 24 Core 4.0GHz, 45MB Cache
- RAM: 64GB
- Storage: 1x SSD 250GB, 2x HDD 1TB (Raid 1)

It should be noted that the aforementioned hardware can be either physical or virtual. It is also important to emphasize that all instances within the chosen configuration must be of the same configuration, as they will be combined into a high-performance cluster.