Cybersecurity threatscape in the Middle East

2022–2023

Contents

Main cybersecurity issues in the Middle East region

The Middle East region has one of the most tense areas of cyberspace in the world. The combination of a thriving economy and high rates of digitization is attracting the attention of malicious actors from around the globe. The losses suffered by Middle Eastern countries from cyberattacks are increasing every year: according to IBM data for 2020, the average cost of a cyberattack on an organization in Saudi Arabia and the United Arab Emirates was $6.53 million, which is 69% more than the global average. According to ResearchAndMarkets, the size of the cybersecurity market in the Middle East is expected to reach almost $30 billion by 2025, with an average annual growth rate of 14%.

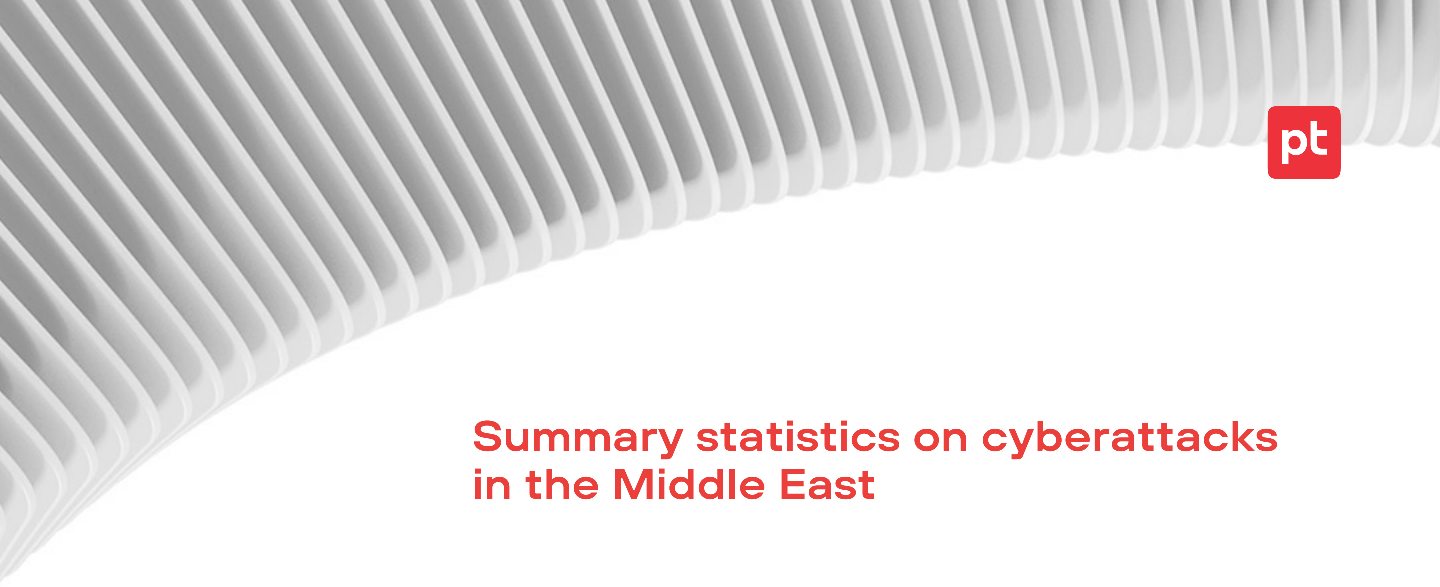
In addition to the growing cybercrime, there are several cybersecurity issues that can significantly affect an organization's achievement of its operational and strategic goals or the security of an entire country:

- ## Cyberattacks on critical infrastructure

The Middle East is one of the most important regions in the world in terms of oil and gas production (for example, Saudi Arabia produced almost 11 million barrels of oil per day in 2021), as well as the transportation of extracted resources. This makes the region particularly vulnerable to cyberattacks on critical infrastructure, such as oil and gas fields, power plants, ports, and airports. Kaspersky analysts reported that in 2022, the Middle East was one of the top five regions in the world with the highest percentage of malware blocked in industrial control systems (ICS).

- ## Cyberwarfare, cyberespionage, and hacktivism

The geopolitical tensions in the region give rise to the constant activity of well-trained groups of attackers (advanced persistent threats, APT), who carry out targeted cyberattacks and conduct cyberespionage. Furthermore, in the Middle Eastern countries, there is a relevant threat from hacktivists—groups of cybercriminals whose attacks are not aimed at financial gain or data collection but rather at drawing public attention to various social or political issues through massive DDoS attacks and website defacement.

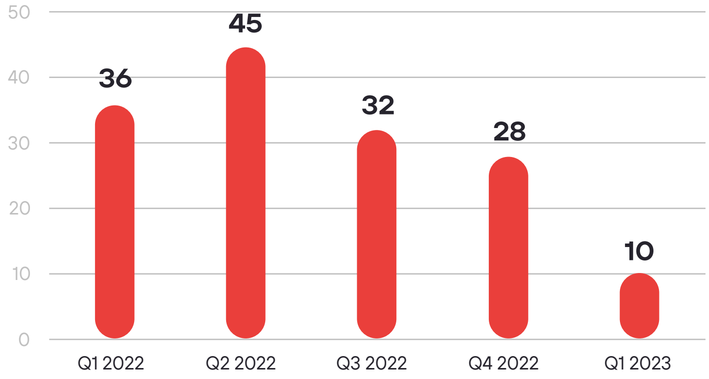


Summary statistics on cyberattacks in the Middle East

83%

of successful cyberattacks were targeted attacks

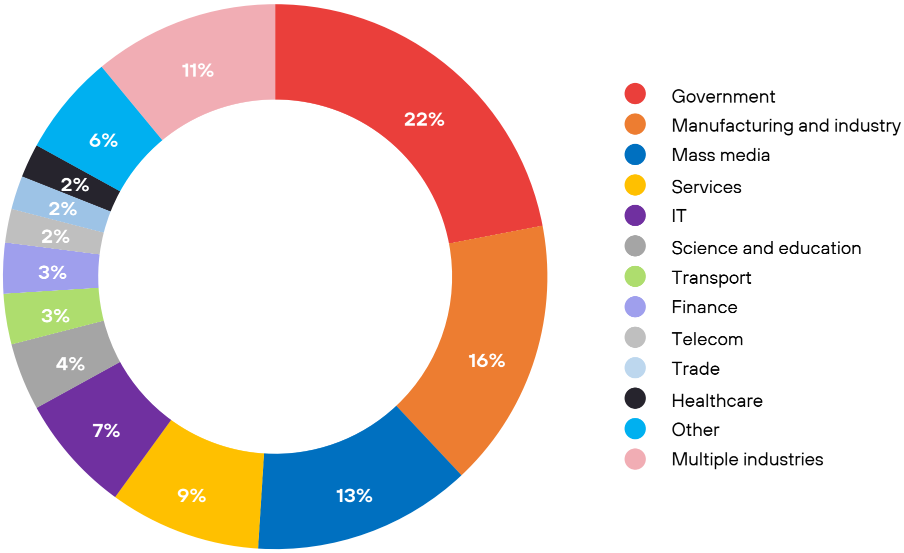
Figure 1. Number of successful cyberattacks in the Middle East region (by quarter)



20%

of attacks were targeted at individuals

Figure 2. Categories of victim organizations



Government agencies

In the countries of the Middle East, government agencies are the most attractive targets for cybercriminal attacks, accounting for 22% of the total number of attacks on organizations. A distinguishing feature of attacks on Middle Eastern government agencies is that they are mainly carried out by APT groups (56%), covertly establishing themselves in the victim's infrastructure for an extended period of time for the purpose of cyberespionage. These attackers are highly skilled and possess a whole arsenal of malware and exploits to compromise systems and exfiltrate data. An interesting type of attacks using social engineering methods was demonstrated by the TA456 group: the attackers created a fake profile of an attractive girl to gain the trust of government employees in their correspondence and distribute spyware. The main consequences of cyberattacks on state institutions are the disruption of core activities (36%) and the leakage of confidential information (28%).

Industrial organizations

Industrial sector organizations constitute a significant portion of the GDP of Middle Eastern countries, are highly valued in the market, and accumulate a large amount of confidential data, thereby attracting the attention of malicious actors: they rank second among the most targeted industries (16%). Attackers gain access to the systems of their victims through attacks on users via social engineering channels (33%); in 62% of attacks using malware, remote administration tools (RATs) were used, as well as wipers (31%).

Current objects and methods of cyberattacks in the Middle East

78% of cyberattacks on organizations in the Middle East region target computers, servers, and network equipment. This is due to the activity of APT groups that target end devices and servers, as well as ransomware groups. Attacks on users (41% of organizations, 96% of individuals) are one of the most widespread current attack methods; the human factor was the cause of more than 80% of hacks in 2022 according to the Verizon's annual report, including in the Middle East. Web resources complete the top three most targeted objects among organizations—attackers exploit web vulnerabilities and steal user data. Additionally, web applications are the target of defacement and DDoS attacks by hacktivists.

Figure 3. Attack targets (share of attacks)

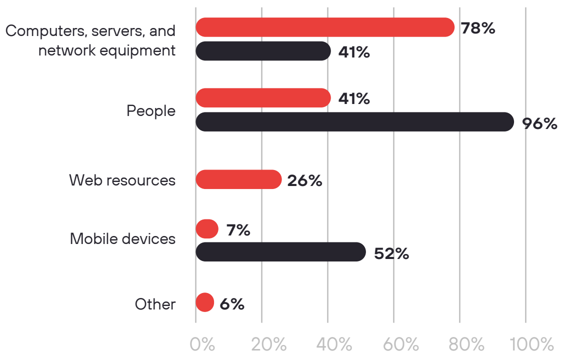
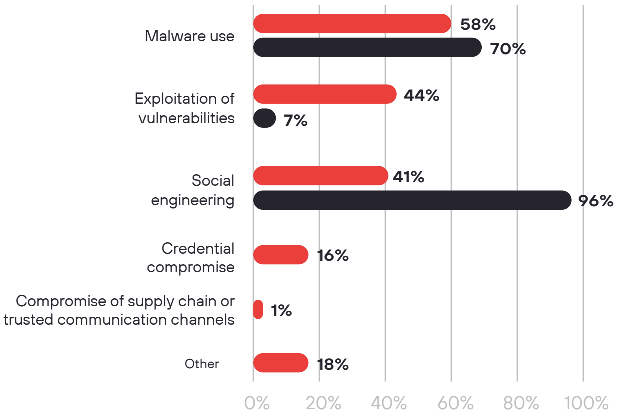


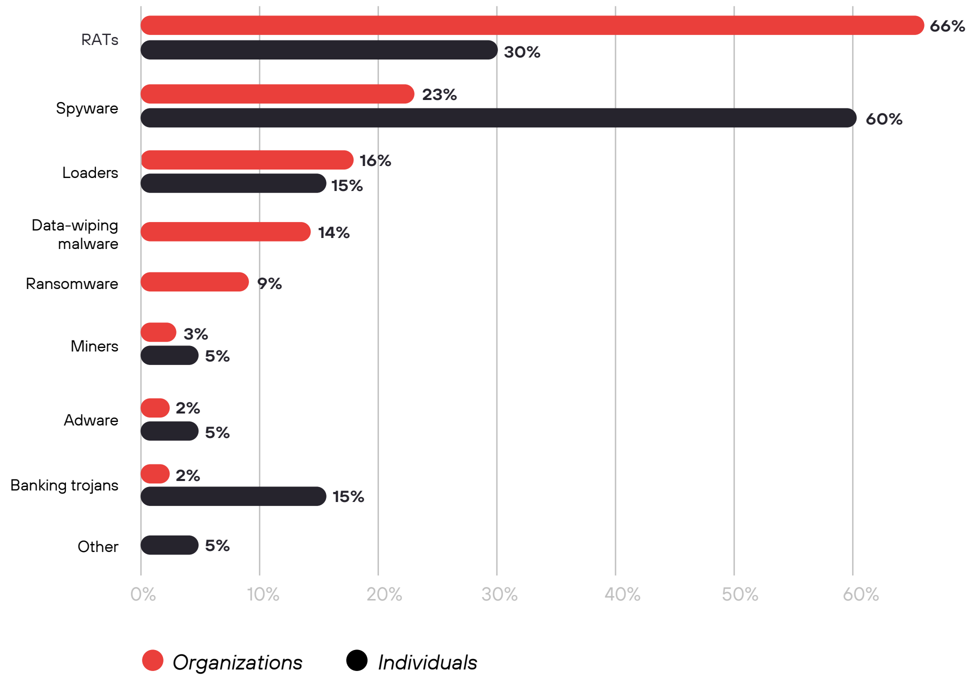
Figure 4. Attack methods (share of attacks)



● *Organizations* ● *Individuals*

Malware used in attacks in the Middle East

Figure 5. Types of malware (percentage of malware attacks)



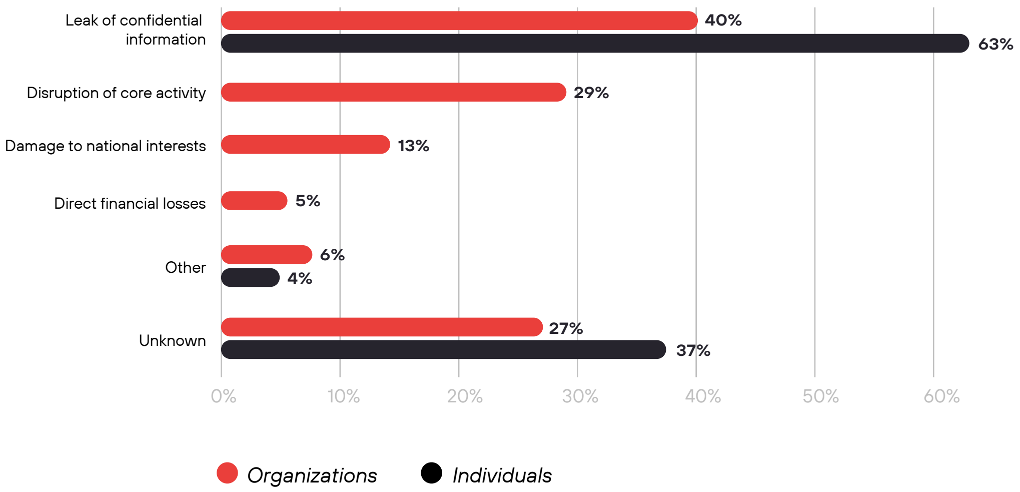
Almost two-thirds of attacks on organizations in the Middle East use malware of various types. are the most popular type of malware in attacks on organizations, and for good reason—they provide attackers with almost complete control over compromised devices, disable security tools, and ensure persistence within the infrastructure. This type of malware is popular among all types of threat actors, particularly APT groups.

Spyware has become widespread in malware attacks on individuals. Most often, attackers distribute it under the guise of legitimate applications, such as VPN services or applications for creating virtual phone numbers.

Ransomware groups are one of the major threats worldwide at the moment, including in the Middle East: the activity of ransomware groups increased by 77% in the first quarter of 2023 compared to the same period in 2022. According to the Group-IB "Hi-Tech Crime Trends 2022/2023" report the most targeted countries in the Persian Gulf region were the UAE (33%), Saudi Arabia (29%), and Kuwait (21%).

A regional feature of the Middle East is the use of wipers by malicious actors in attacks using malware. When this malware infects a device, it erases all user and system files, causing the device to crash. A particularly dangerous scenario is when wipers infect ICS equipment, since its failure can lead to disruptions in the technological process and even to emergency situations. In the second quarter of 2022, there was a major attack on three Iranian steel plants, resulting in disruptions to the production processes. At one of the plants, the attackers managed to tip over a container of molten steel, causing a fire on the factory floor.

Figure 6. Attack consequences (share of attacks)



Following the global trend of information theft, the majority of criminals have been focused on stealing confidential information, conducting cyberespionage, and disrupting the core operations of organizations. Due to the region's relatively high level of secrecy regarding its internal affairs, and the poor coverage of cases of cyberattacks, the consequences of a high proportion of incidents remain unknown.

Figure 7. Types of data stolen (in attacks on organizations)

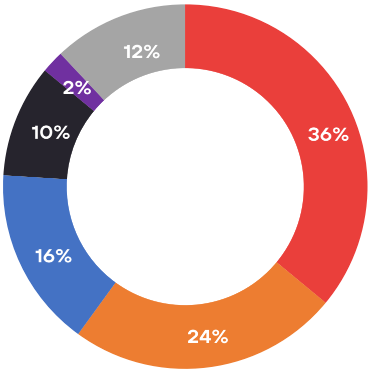
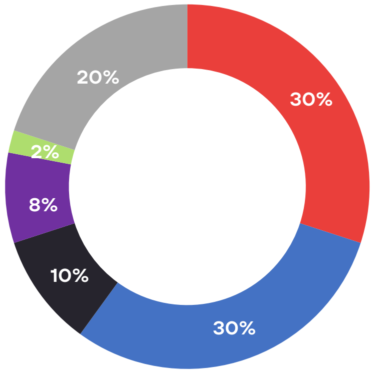


Figure 8. Types of data stolen (in attacks on individuals)

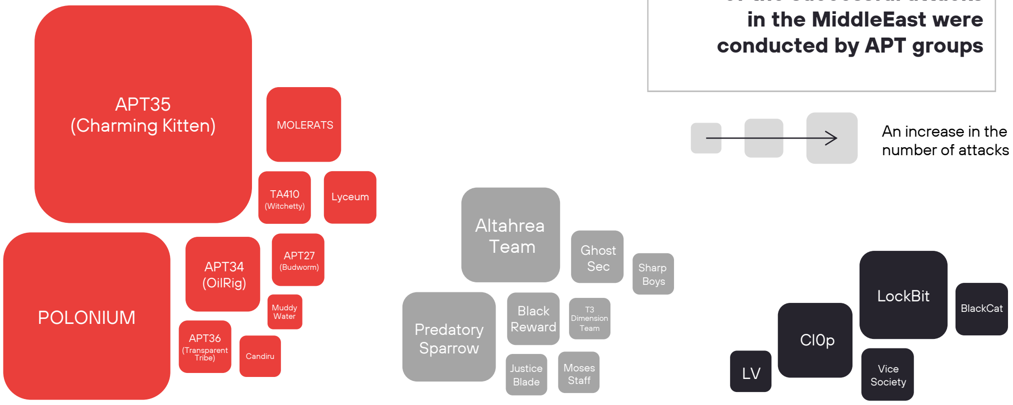


● Personal data	● Payment card data	● Other
● Intellectual property	● Correspondence	
● Credentials	● Medical data	

Groups that attacked organizations and individuals in the Middle East

40%

of the successful attacks in the MiddleEast were conducted by APT groups



🟥 **APT groups**

Organized groups of highly skilled and well-equipped cybercriminals. The main objective of their attacks is cyberespionage

⬜ **Hacktivists**

Criminals whose cyberattacks are aimed not at gaining financial benefit but at drawing public attention to various social or political issues

⬛ **Ransomware attackers**

Criminals who use malicious software to encrypt and exfiltrate data in order to demand a ransom for the decryption and non-disclosure of the data

How to solve cybersecurity problems in the Middle East

When it comes to cyberattacks, the Middle East is in a unique and potentially vulnerable position. It is a region rich in oil, and its countries are rapidly pursuing large-scale digitization, introducing innovative technologies into government processes and key sectors of the economy. In 2023, it will become one of the most attractive targets for ransomware attackers, scammers, APT groups, and hacktivists. Based on data from open sources and our own statistics, we can conclude that the majority of successful cyberattacks in the Middle East are and will be carried out using social engineering methods, the spread and deployment of malware, and the exploitation of web and software vulnerabilities.

The most significant security threats to countries in the Middle East region in 2023 are:

- **Cyberattacks on government organizations.** Cybercriminals or APT groups may aim to compromise government systems to obtain confidential data, conduct cyberespionage, disrupt operations, or influence decision-making processes.

- **Constant attacks on critical infrastructure.** Attacks on critical infrastructure can have the most serious consequences for both the organization itself and the economy or security of the country. To achieve this, attackers may target organizations in the energy, telecommunications, and financial sectors, as well as healthcare or transportation.

- **Phishing and social engineering.** Attacks based on phishing and social engineering methods will be carried out to gain access to the systems of organizations in all sectors of the economy and individuals.

- **Distribution of malware.** Attacks using malware (remote access trojans, spyware, ransomware) will remain a serious threat to organizations and individual users.

- **Hacktivism.** Hacktivists can use website defacement, DDoS-attacks, or malware injection to damage information systems and gain unauthorized access to confidential information. They are also capable of conducting cyberpropaganda and spreading false information in order to influence public opinion.

The increase in the number of criminal groups and, consequently, the number of cyberattacks has increased the need for cybersecurity in organizations in the Middle East. According to the International Data Corporation's forecast, security spending in the Middle Eastern region in 2023 will increase by nearly 8% annually, with the largest share of spending (41%) allocated to software.

The leadership of the Middle Eastern countries fully recognizes the seriousness of cyberthreats and is establishing a regulatory framework to regulate activities in cyberspace:

- Qatar has implemented provisions for organizations in accordance with Law No. 13 of 2016 on Personal Data Privacy Protection to ensure the protection and security of user data.

- Bahrain enacted the Personal Data Protection Law (PDPL) on August 1, 2019. It was modeled after the European Union, and offenders can face a penalty of up to one year of imprisonment.

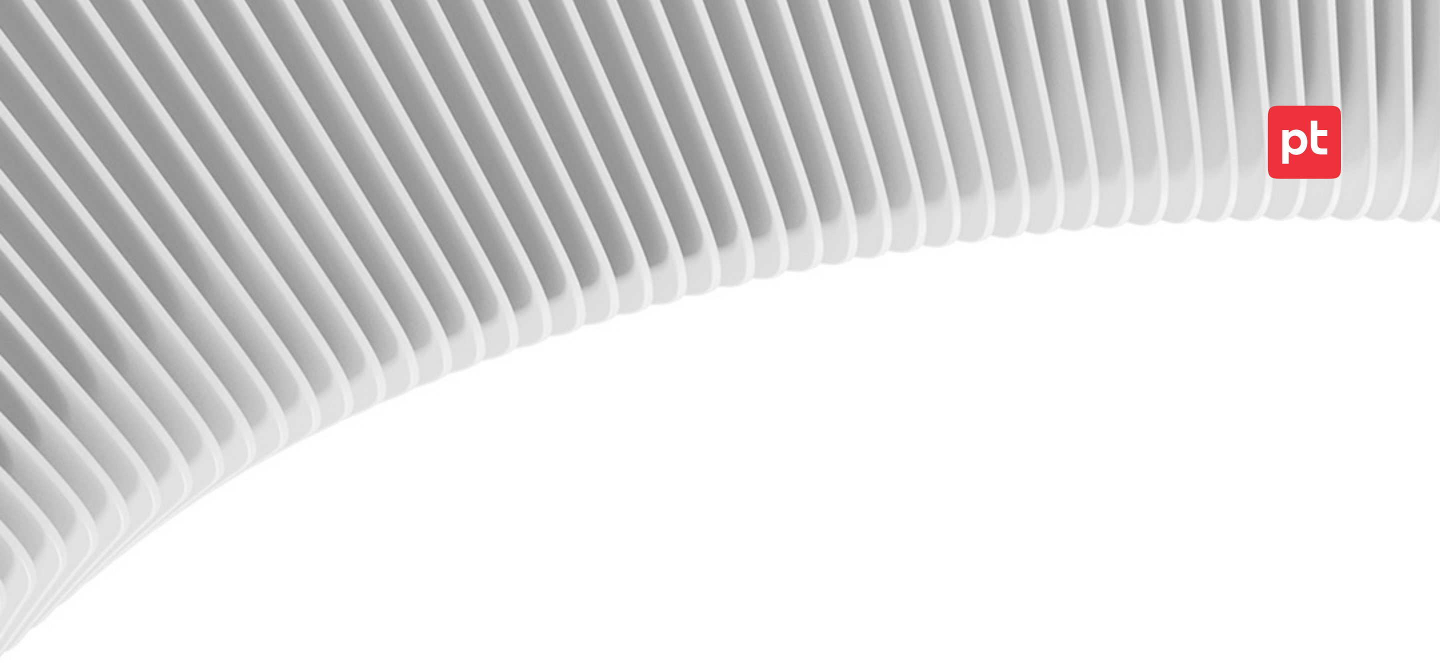
- In November 2021, the United Arab Emirates issued Federal Law No. 45 (UAE Data Protection Law), which establishes stricter privacy and data protection standards and defines the rights and duties of all parties concerned in processing of personal data.

Because of the increased activity of cybercriminals and the severity of the consequences of successful cyberattacks, organizations in the Middle East must prioritize cybersecurity. They need to implement tools, services, and practices that can empower their ability to monitor and respond to information security incidents and increase the awareness and vigilance of their employees to prevent cyberattacks. One of the relevant methodologies for addressing core security issues is a comprehensive approach to effective cybersecurity, which aims to establish a continuous and automated system for protecting the entire IT infrastructure, taking into account the specific activities and business processes of the organizations.

To build such a system, organizations need to identify and assess the information assets that require protection, as well as determine the events that could occur as a result of a cyberattack and hinder the achievement of the organization's operational and/or strategic objectives or significantly disrupt their core operations (non-tolerable events).

Once the assets and non-tolerable events have been identified, measures must be taken to assess the security of systems (cyberexercises, pentests) and actually implement (verify) the non-tolerable events.

Based on the assessment of the organization's security, select those protection components that will ensure the three key elements of effective cybersecurity:



Monitoring

A real-time security system should be aware of what is happening with the protected assets and how well the infrastructure elements comply with secure settings.

Implementing SIEM (security information and event management) systems allows security teams to monitor and analyze security events, detect attacks, and assess the compliance of protected infrastructure elements with security requirements.

Response

The system must understand the attacker's intent in order to respond quickly and effectively to incidents and prevent non-tolerable events.

The combination of XDR (extended detection and response) and SIEM solutions makes it possible to detect attacks in the infrastructure and respond to them both manually and automatically. Threat detection and response capabilities can be enhanced by using a sandbox for the statistical and dynamic analysis of threats such as advanced malware. In the case of expert incident investigations, NTA (network traffic analysis) solutions are used for deep traffic analysis and detecting malicious activity. NTA solutions also act as SIEM sensors to display network status information and serve as a tool for proactive threat hunting.

Asset Management

One of the main functions of a security system is keeping a constant inventory of assets and their classification, taking into account non-tolerable events for the organization and ways that cyberattacks could develop.

VM (vulnerability management) systems automate the processes of asset management and the detection and fixing of vulnerabilities in infrastructure components, depending on their severity level. VM systems also monitor the level of infrastructure protection against vulnerabilities exploited in real-world attacks.

In case an organization is engaged in the development of software products and web applications, it is necessary to implement and adhere to secure software development processes and use source code analysis tools to identify vulnerabilities and design flaws during the development phase.

Bug bounty platforms can help organizations establish a continuous security analysis process for their services and optimize security costs.

Employees are the main asset of any organization and, at the same time, one of the main vectors for attacks on corporate systems. It's necessary to increase employees' awareness in the field of information security (security awareness) when building reliable company protection. Compliance with digital hygiene rules reduces the likelihood of endpoints being compromised. Users who are aware of current threats will not fall for the tricks of malicious actors and open attachments from suspicious emails or connect unfamiliar devices. Instead, they will report suspicious activity and attack attempts to the security operation center (SOC).

A combination of properly configured information security tools, an experienced team of cybersecurity specialists, and process continuity, all within the framework of an effective approach, enables the maximum automation and centralization of the organization's security management processes, and the achievement of the main goal: protection against non-tolerable events.

About the report

This report contains information about current information security threats in the Middle East region, based on Positive Technologies' own expertise, as well as data from reputable sources. The term "Middle East" in this report refers to the following countries: Bahrain, Egypt, Israel, Jordan, Iraq, Iran, Yemen, Qatar, Cyprus, Kuwait, Lebanon, United Arab Emirates (UAE), Oman, the State of Palestine, Saudi Arabia, Syria.

We estimate that most cyberattacks are not made public due to reputational risks. As a consequence, even companies specializing in incident investigation and analyzing hacker activity are unable to calculate the precise number of threats. Our research seeks to draw the attention of companies and ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

This report considers each mass attack (for example, phishing emails sent to multiple addresses) as one incident, not several. For explanations of terms used in this report, please refer to the Positive Technologies glossary.