MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATIONS, ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING SYSTEMS

ADMIT TO DEFENCE
Head of the Department

_____ R. Odarchenko
«_____»_____ 2022

DIPLOMA WORK

(EXPLANATORY NOTE)

BACHELOR'S DEGREE GRADUATE
BY SPECIALITY "TELECOMMUNICATIONS AND RADIO ENGINEERING"

Topic: «Cybersecurity system for enterprise telecommunications resources»

Performer: _____ Topala R.R
(signature)

Supervisor: _____ I. Terentieva
(signature)

N-controller: _____ D.Bakhtiiarov
(signature)

Kyiv 2022

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigations, electronics and telecommunications
Department of telecommunication and radio engineering systems
Speciality: 172 "Telecommunications and radio engineering"
Educational professional program: Telecommunication systems and networks

ADMIT TO DEFENCE
Head of the Department

R. Odarchenko
«__» _____ 2022

TASK
for execution of bachelor diploma work

Topala Roman Romanovich
(full name)

1. Topic of diploma work: «Cybersecurity system for enterprise telecommunications resources»

Approved by the order of the rector from «25» April 2022 № 433/ст.

2. The term of the work: from 23.05.2022 to 17.06.2022.

3. Initial work Data: Telecommunication cybersecurity systems; building a corporate network of an enterprise; Network security methods

4. Explanatary note content: Construction and analysis of corporate network cybersecurity. Checking the reliability and stability of the constructed network. Identification of the pros and cons of the constructed network and the selected protection methods

5.Work schedule

№ п/п	Task	Term implementation	Performance note
1.	Develop a detailed content of the sections of the diploma	25.05.2022-26.05.2022	*Done*
2.	Introduction	25.05.2022	*Done*
3.	Research of security systems of corporate net-works and their problems	26.05.2022-29.05.2022	*Done*
4.	Analysis of modern cybersecurity systems for corporate networks	30.05.2022-01.06.2022	*Done*
5.	Building an enterprise corporate network and testing its vulnerabilities	02.06.2022-05.06.2022	*Done*
6.	Elimination of shortcomings of the thesis	05.06.2022-08.06.2022	*Done*
7.	Electronic version of the report, illustrative material of the report	08.06.2022-17.06.2022	*Done*

7. Date of issue of the assignment: “20” May 2022

Supervisor _____ I. Terentieva
(signature) (full name)

Accepted task for execution _____ R. Topala
(signature) (full name)

ABSTRACT

Graduate work on the topic “Cybersecurity system for enterprise telecommunications resources”. It contains 62 p., 19 Figures., and 40 sources.

The object of the study is the Cybersecurity system.

The thesis aims to build an enterprise cybersecurity system for the protection of their telecommunication resources.

Research of methods – computer design and special cybersecurity software.

This work presents one of the most relevant Cybersecurity systems that are based on the endpoint protection method. These systems provide the one of most complicated detective and response probability for their users.

Considered systems conclude many components that help to find and neutralize threats. Such as rules mode that users can edit for the most needed situation. All of these mechanisms help to simplify threat protection.

The telecommunication systems were built in Cisco Packet Tracer. The other part of the work was tested with help of the Cortex XDR on the Windows operating system platform.

Materials of these works are recommended to be used in different kinds of research, educational process, etc.

ЗМІСТ

LIST OF ABBREVIATIONS

API – Application Programming Interface

CPU – Central Processing Unit

CSS – Cascading Style Sheets

DNT – Do Not Track

HTML – HyperText Markup Language

HTTP – Hyper Text Transfer Protocol

HTTPS – Hyper Text Transfer Protocol Secure

IP – Internet Protocol

JVM – Java Virtual Machine

RTC – Real-Time Communications

URL – Uniform Resource Locator

VPN – Virtual Private Network

WebGL – Web Graphics Library

INTRODUCTION

Relevance of the topic is that this work draws attention to the new generation of firewalls that have recently taken over the market. This cybersecurity system has a number of innovations that help fight virus threats. It is based on the relatively recently introduced concept of endpoint security. And it provides the search and investigation of incidents using the latest technology.

Connection of work with scientific programs, plans, themes.

The purpose and objectives of the study

To achieve this goal, the following scientific problems are solved.

1) Research of corporate network security systems and their problems
2) Analysis of modern cybersecurity systems for corporate networks
3) Building an enterprise corporate network and testing its vulnerabilities

The object of study - the Cybersecurity system.

The subject of research **-** to build an enterprise cybersecurity system for the protection of their telecommunication resources

Research methods. To achieve the goals in the work used: Commputer modeling methods, Analytic methods, Construction methods, etc.

Scientifi nolti of the obtained results.

The novelty of the obtained scientific data is to determine the effectiveness of the software that ensures network security

The practical significance of the results obtained.

This cybersecurity system can be used by enterprises of almost any scale. The possibilities of application are practically unlimited, except for the resources of the company itself

SECTION 1.
RESEARCH OF SECURITY SYSTEMS OF CORPORATE NETWORKS AND THEIR PROBLEMS

Nowadays, building a secure network is one of the most common problems for engineers. Since at the stage of designing and implementing a project, various problems may arise that both indirectly and directly affect the security of the network. In this section, corporate networks and their problems will be considered [4]. Types of networks and ways to build them will be given, the difficulties that may arise with them and how to deal with them as far as possible. The main pros and cons of networks and ways to implement them are also considered [3].

1.1. Principles of building corporate networks

Corporate data networks are one of the most useful tools for the development of medium and large businesses. Since such networks are very helpful in establishing business infrastructure and providing communication between different departments. They also reduce the delay in processing various requests and solving problems.

One of the main requirements for networks of this kind is that they must provide all types of telecommunications and information services. Also, the costs of creating and maintaining the network should not exceed the optimal ones.

The networks under consideration are for different purposes. For example, local and global, the main differences between these networks, as the name implies, is the unification of local units that are located on the same territory or units located at a certain distance from each other. Depending on the type of network we have chosen, the need to rent communication lines or build a virtual communication line between two departments is determined.

Also, an important nuance in the construction of the networks under consideration is the choice of equipment. As you know, equipment can be divided into

two classes: main and peripheral. Backbone equipment is installed in those cases when leased communication lines are involved, or they create their own access nodes. In other situations, global means of information transfer take on this role. It is also necessary to pay attention to the fact that the backbone equipment is always subject to increased requirements in terms of reliability, scalability and performance. As for the peripheral equipment for this class of special tools, the requirements are much lower, which affects some nuances of building a network.

Especially important is the definition of the topology on which the network will be built. At the moment, there are only four types of topologies. Some key features depend on the choice of topology, for example, the cost of building a network and its location [8]. Four main types of topologies will be considered next:

1) The first type of topology is Bus. It is also called a linear bus, it uses only one cable to which the endpoints or computers of the segment are connected. In this topology, the connection is sent to all network endpoints, regardless of who the destination is. In this network, any device checks each packet to understand who it is addressed to, if it is addressed to another device, then the current station will reject it.

One feature of this network structure is the main bus cable or backbone. The trunk has plugs at both ends to prevent signal reflection. Without properly installed plugs, network operation will be unreliable or impossible at all. At figure 1.1 shows an example of Bus topology.

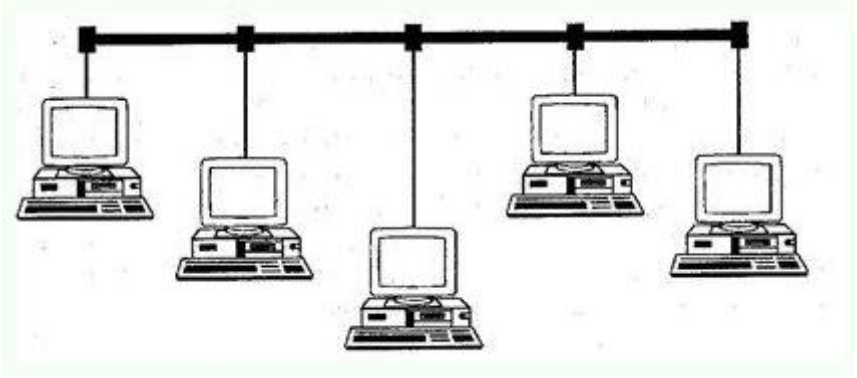

Fig 1.1 Bus topology

Bus topology is a quick and easy way to set up a network. It requires the least amount of materials in terms of equipment and cabling compared to other network structures. It is ideal for small networks, usually no more than a dozen stations. Most often used as a temporary network.

It is worth mentioning the main disadvantages of this network. One of the most pronounced disadvantages is situations in which the failure of a station or other component is difficult to isolate from the entire network. Sometimes this can lead to network infection or other unpleasant consequences. The second, but no less important, disadvantage is that if the backbone is damaged, the entire network fails.

2) The topology of the ring is shown below (Figure 1.2). Commonly used in token ring and fiber optic networks. In a physical Ring topology, the data line actually forms a logical ring to which all computers on the network are connected. Unlike a bus topology, which uses a contention scheme to allow stations to access network media, media in a ring is accessed via logical tokens that are passed around from station to station, enabling them to resend the package if needed. This gives every computer on the network an equal opportunity to access the media and therefore send data over it. The computer can only send data when it owns the token [10].

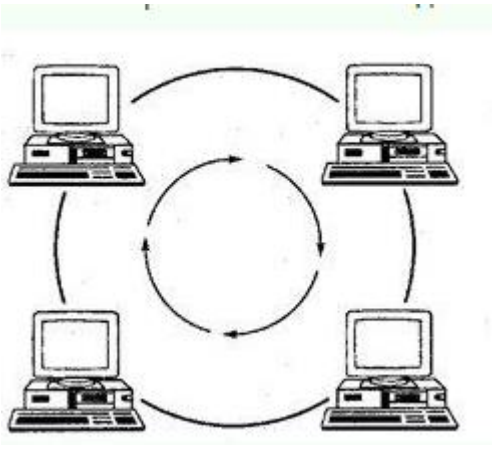

Fig 1.2 Ring topology

Since each computer in this topology is part of the ring, it has the ability to forward any data packets it receives to another station. The resulting refresh makes the

signal strong and avoids the need for repeaters. Since the ring forms an endless loop, plugs are not required.

The ring topology is relatively easy to install and configure, requiring minimal hardware. The physical ring topology has several disadvantages. As with a line bus, failures in one station can bring down the entire network. Maintaining a logical ring is difficult, especially on large networks. In addition, if you need to configure and reconfigure any part of the network, you will have to temporarily disable the entire network. Ring topology will give all computers equal access to network media [7].

3) In a star topology, all computers on the network are connected to each other using a central hub (Figure 1.3). All data that the station sends is sent directly to the hub, which then forwards the packet towards the recipient. As with a bus topology, a computer in a star network can try to send data at any time. However, in reality, only one computer can send a message at a time. If two stations send signals to the hub at exactly the same time, both sends will fail and each computer will have to wait a random amount of time before attempting to access the media again [17]. Networks with a Star topology generally scale better than other types.

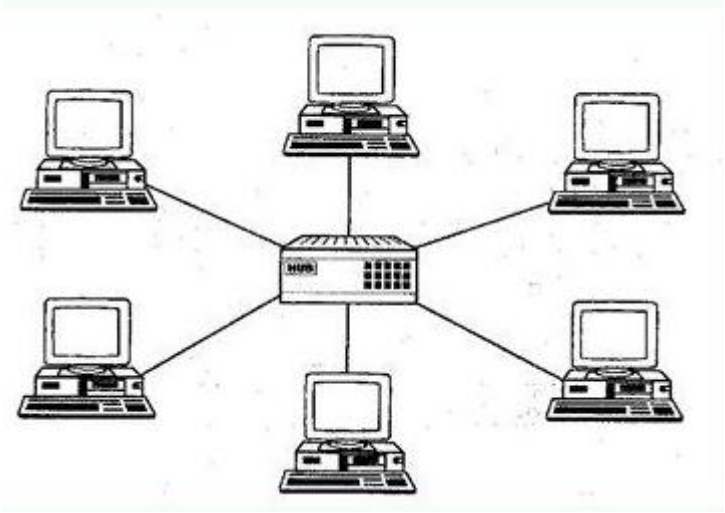

Fig. 1.3 Star topology

The main advantage of implementing a star topology is that, unlike a linear bus, failures in one station will not bring down the entire network. In networks with this

topology, it is easier to find cable breaks and other faults. This makes it easier to detect cable breaks and other problems. In addition, having a central hub in a star topology makes it easier to add a new computer and reconfigure the network. The star topology has several disadvantages. First, this type of configuration requires more cable than most other networks due to the separate lines that connect each computer to the hub. In addition, the central hub performs most of the functions of the network, so the failure of this one device will shut down the entire network.

4) And the last topology considered will be a mesh topology that connects all computers in pairs (Fig. 1.4). Mesh networks use significantly more cable than any other topology, making them more expensive. In addition, such networks are much more difficult to install than other topologies. However, the mesh topology is fault tolerant. Fault tolerance refers to the ability to operate in the presence of damage. On a network with a damaged segment, this means segment bypass. Each computer has many possible ways to connect to another computer over the network, so that a single cable break will not result in a loss of connection between any two computers.

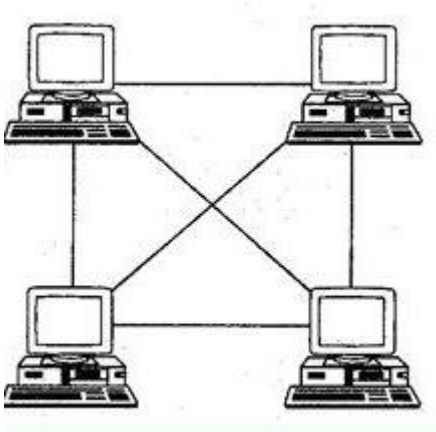

Fig. 1.4 Mesh topology

Based on the information above, we can conclude that when building a corporate network, based on the available space for deployment and the allocated budget. We choose the topology that suits us, but an important point is that the chosen topology corresponds to the technical task. Thus, the following basic principles of building a network are distinguished. Based on the information above, we can conclude that

building a corporate network depends on the available space for deployment and the allocated budget. Therefore, we choose the topology that suits us, but the critical point is that the selected topology corresponds to the technical task. Also, software and hardware methods for protecting the network itself at the design stage are being worked out; if the search for vulnerabilities at the network development stage is not carried out, it can be quite challenging to eliminate them during the network operation.

The following essential aspect has already been mentioned above. It is worth checking whether the planned network corresponds to the standard requirements for networks. After all, if the basic needs are not met, for the most part, further construction of the network is irrational. The main network requirements will be discussed below. Primary requirements:

- Performance;
- Reliability and safety;
- Extensibility and scalability;
- Clarity;
- Support for different types of traffic;
- Controllability;
- Compatibility;

As you can see above, the list of requirements is quite extensive. Therefore, each of the points will be discussed in more detail below to clarify aspects of each of these requirements.

The first requirement considered is performance. Performance is a characteristic of the network; it allows you to evaluate how quickly the information of the transmitting station reaches the receiving station. Network performance can be affected by the following factors:

- Configuration;
- Channel access method;
- Network topology;

When network performance drops, the administrator can resort to various troubleshooting tools or fine-tuning to improve performance. One way to eliminate performance degradation is to reconfigure the network so that the network's structure is more appropriate for the flow of information. You can also switch to a different distribution application building model to reduce overall network traffic. One extreme option may be to replace the switches with higher-speed ones. But the most radical solution in such a situation would be to switch to a faster technology. If the network uses traditional Ethernet or Token Ring technology, switching to fast Ethernet or similar technology will immediately increase the channel bandwidth ten times.

With the growth of the scale of networks, there is a need to improve their performance. One way to achieve this was to micro-segment them. It allows you to reduce the number of users per segment, reduce broadcast traffic, and thus improve network performance. Initially, routers were used for micro-segmentation, which, generally speaking, are not very suitable for this purpose. Solutions based on them were pretty expensive and were distinguished by a significant time delay and low throughput. Switches have become more suitable devices for the micro-segmentation of networks. Due to their relatively low cost, high performance and ease of use, they quickly gained popularity. Thus, networks began to be built based on switches and routers. The former provides high-speed traffic forwarding between segments of the same subnet, while the latter transmits data between subnets, limits the distribution of broadcast traffic, solves security problems, etc. Virtual LANs (VLANs) provides the ability to create logical groups of users on a corporate network scale. Virtual networks allow you to organize your networking more efficiently.

The next requirement to be considered will be Reliability and safety of the network. The essential characteristic of computer networks is reliability. Improving reliability is based on the principle of preventing malfunctions by reducing the rate of failures and failures through the use of electronic circuits and components with a high and ultra-high degree of integration, reducing the level of interference, lighter modes of operation of circuits, ensuring thermal modes of their operation, as well as by

improving methods of assembling equipment. Fault tolerance is such a property of a computing system that it provides it, as a logical machine, with the ability to continue the actions specified by the program after a malfunction occurs. The introduction of fault tolerance requires redundant hardware and software.

Directions related to the prevention of faults and fault tolerance are the main ones in the reliability problem. On parallel computing systems, both the highest performance and, in many cases, very high reliability are achieved. Available redundancy resources in similar techniques can be flexibly used for performance and reliability. It should be remembered that the concept of reliability includes hardware and software. The main goal of increasing the reliability of systems is the integrity of the data stored in them. Security is one of the main tasks solved by any standard computer network. The security problem can be viewed from malicious data corruption, the confidentiality of information, unauthorized access, theft, etc. It is always easier to protect the information in a local network than if a company has a dozen autonomously working computers. In practice, you have one tool at your disposal - backup. For simplicity, let's call this process redundancy. Its essence is to create a complete copy of the data in a safe place, updated regularly and as often as possible. For a personal computer, floppy disks are more or less secure media. It is possible to use a streamer, but this is an additional cost for equipment

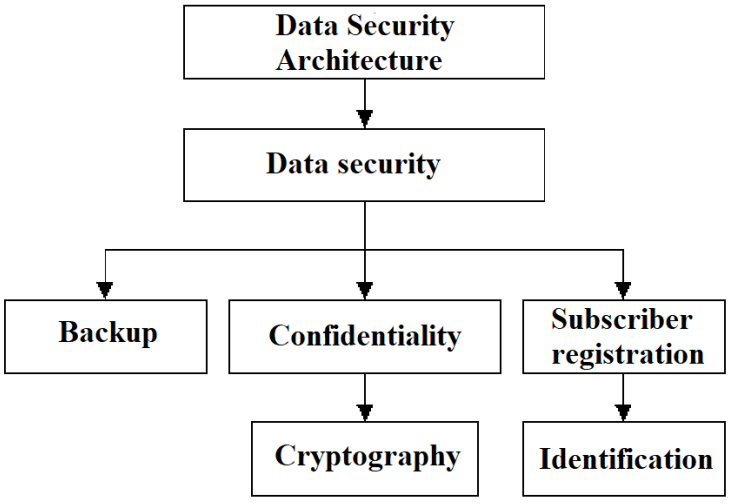

Fig. 1.5 Data Security Challenges

The easiest way to ensure data protection from various troubles is in the case of a network with a dedicated file server. All the most critical files are concentrated on the server, and saving one machine is more accessible than ten. The concentration of data also facilitates redundancy since it does not need to be collected throughout the network. Shielded lines improve network security and reliability. In addition, shielded systems are much more resistant to external RF fields.

Transparency is a state of the network when the user does not see it while working on the web. A communication network is transparent concerning information passing through it if the output bitstream is the same as the input stream. But the network can be opaque in time if, due to the changing sizes of the queues of data blocks, the time of passage of various blocks through the switching nodes also changes. Network rate transparency indicates that data can be transferred at any desired rate. If information and control (synchronizing) signals are transmitted along the same routes, then the network is said to be transparent concerning signal types. If the transmitted data can be encoded, the network is evident to any encoding methods. An exemplary network is a simple solution that uses the Plug-and-play principle to interconnect local networks located at a considerable distance from each other. Transparent connection. The Transparent LAN Service provides an end-to-end relationship between remote LANs. The attractiveness of this solution lies in the fact that this service unites nodes remote from each other at a considerable distance as part of a local network. Therefore, there is no need to invest in studying new technologies and creating geographically distributed networks (Wide-Area Network - WAN). Users only need to maintain a local connection, and the Transparent Network Service Provider will ensure that nodes communicate seamlessly over the Metropolitan-Area Network (MAN) or WAN. Transparent LAN services have many benefits. For example, a user can quickly and securely transfer large amounts of data over long distances without the hassle of WANs.

Support for different types of traffic. Traffic in the network is formed randomly, but it also reflects some patterns. As a rule, some users working on a standard task (for

example, employees of one department) most often make requests either to each other or to a shared server. Sometimes, they need to access the resources of computers in another department. Therefore, the network structure should correspond to the design of information flows. Depending on network traffic, computers on the network can be divided into groups (network segments). Computers are combined into a group if most of the messages they generate are addressed to computers in the same group. Bridges and switches are used to divide the network into segments. They shield local traffic within a part by not passing any frames outside of it, except for those addressed to computers located in other elements. Thus, the network breaks up into separate subnets. This allows you to more rationally choose the bandwidth of available communication lines, taking into account the intensity of traffic within each group and the activity of data exchange between groups. However, traffic localization using bridges and switches has significant limitations.

On the other hand, using the virtual segment mechanism implemented in LAN switches leads to complete traffic localization; such segments are entirely isolated from each other, even for broadcast frames. Therefore, computers with different virtual elements do not form a single network in networks built only on bridges and switches. To effectively consolidate various types of traffic in the ATM network, special preliminary preparation (adaptation) of data of a different nature is required: frames for digital data, pulse-code modulation signals for voice, and bitstreams for video. Effective traffic consolidation also requires taking into account and using statistical variations in the intensity of different types of traffic.

ISO has made a significant contribution to the standardization of networks. The network management model is the primary tool for understanding the main functions of network management systems. This model consists of 5 conceptual areas:

- Performance management;
- Configuration management;
- Resource usage accounting management;
- Fault management;

- Data protection management.

Performance management aims to measure and enforce various aspects of network performance to maintain internetwork performance at an acceptable level. Examples of efficiency variables that could be provided are network throughput, user response time, and line utilization. Performance management includes several stages:

- Collection of performance information on those variables that are of interest to network administrators;
- Analysis of information to determine regular (baseline) levels;
- Determining appropriate performance thresholds for each essential variable such that exceeding those thresholds indicates a problem in the network worthy of attention.

The purpose of configuration management is to control network and system configuration information so that the impact on network performance of different versions of hardware and software elements can be monitored and managed. Because all hardware and software elements have operational deviations and errors (or both) that can affect the operation of the network, such information is essential to maintain the smooth operation of the network. Each device on the web has various version information associated with it. Configuration management subsystems store this information in a database to provide easy access. This database can be searched for clues that might help solve the problem when a problem occurs.

Resource usage accounting management. The purpose of resource usage accounting is to measure the usage of a network so that it can be appropriately managed by individual or group users. Such regulation minimizes the number of problems in the network (since network resources can be divided based on the source's capabilities) and maximizes the fairness of the web for all users.

Fault management. The purpose of fault management is to identify, fix, notify users, and (to the extent possible) automatically fix network problems to keep the network running efficiently.

Because failures can lead to network downtime or unacceptable degradation, fault management is probably the most widely used element of the ISO network management model. Fault management involves several steps:

- Determining the symptoms of the problem;
- Isolating the problem;
- Troubleshooting;
- Verification of troubleshooting on all critical subsystems;
- Recording the discovery of a problem and its solution.

Data protection management. Data protection management aims to control access to network resources by following local guidelines to prevent unauthorized persons from sabotaging the network and accessing sensitive information. For example, one of the data protection management subsystems can control the registration of users of a network resource, denying access to those who enter access codes that do not match the established ones.

Data protection management subsystems work by separating sources into authorized and unauthorized areas. For some users, access to any network source is inappropriate. Data protection management subsystems perform the following functions:

- Identify sensitive network resources;
- Mappings are defined between sensitive network sources;
- Control access points to sensitive network resources;
- Register inappropriate access to sensitive network resources.

And the last requirement considered is compatibility. The concept of software compatibility was first applied on a large scale by the IBM/360 system developers. The main task in designing the entire range of models of this system was to create an architecture that would be the same from the user's point of view for all system models, regardless of the price and performance of each of them.

The enormous advantages of this approach, which allows you to keep the existing software backlog when moving to new (usually more productive) models,

were quickly appreciated by computer manufacturers and users. Since then, almost all computer equipment suppliers have adopted these principles by supplying a series of compatible computers.

It should be noted that over time, even the most advanced architecture inevitably becomes obsolete, and there is a need to make radical changes in the architecture and ways of organizing computing systems.

One of the most critical factors determining current trends in the development of information technology is the orientation of computer equipment supplier companies to the market of applied software. This transition put forward several new requirements. First of all, such a computing environment should allow flexible changes in the number and composition of hardware and software by solving the changing needs of the tasks. Secondly, it should provide the ability to run the same software systems on different hardware platforms, i.e., ensure software portability.

Thirdly, this environment must guarantee the possibility of using the same human-machine interfaces on all computers included in a heterogeneous network. In the fierce competition between manufacturers of hardware platforms and software, open systems have been formed, which is a set of standards for various components of the computing environment designed to ensure the mobility of software within a heterogeneous, distributed computing system.

1.2. Study of problem areas in the Cybersecurity of corporate networks

In this section, problem areas will be explored in ensuring the cybersecurity of a corporate network. As can be seen from the paragraphs above, there are various pros and cons to security software and network architectures. Also, an integral nuance of security is the human factor.

It turns out to be a somewhat risky situation, which engineers can usually avoid using various tools. Therefore, these tools will also be discussed in this section.

1.3.1. The main cyber threats to the corporate network.

To begin with, we should understand what is, all the same, responsible for security. Security responsibility refers to an action or event that can represent the destruction, distortion, or unauthorized use of network resources, including stored, perceived and processed information and software and hardware [2].

Threats are divided into:

- Unintentional or accidental;
- Intentional.

Let's take a closer look at these threats. To begin with, Random threats arise as a result of errors in software, hardware failure, incorrect actions of users or a network administrator, etc. But Deliberate threats are aimed at causing damage to users and subscribers of the network and, in turn, are divided into active and passive.

Passive threats are aimed at unauthorized network information resources but do not affect their functioning. An example of a passive threat is receiving information circulating in the network channels through listening [3].

In turn, active threats aim to disrupt the normal functioning of the network through a targeted impact on its hardware, software and information resources. Operational hazards include, for example, destruction or electronic jamming of communication lines, disablement of a computer or operating system, distortion of information in user databases or system information, etc.

The main security threats include:

- disclosure of confidential information;
- information compromise;
- unauthorized exchange of information;
- refusal of information;
- denial of service;
- unauthorized use of network resources;

Threats of disclosure of confidential information are implemented through unauthorized access to databases. Information is compromised by making unauthorized changes to databases.

The unauthorized use of network resources means disclosing or compromising information and harms users and network administration. Erroneous use of resources is a consequence of local area network software errors.

The unauthorized exchange of information between network subscribers makes it possible to obtain information to which access is prohibited, i.e., it essentially leads to information disclosure. Refusal of data consists of non-recognition by the recipient or sender of this information of the facts of its receipt or sending. Denial of service is a common threat that originates from the network itself. Such a failure is hazardous in cases where a delay in providing network resources can lead to severe consequences for the subscriber.

1.3.2. Methods for protecting corporate networks.

The key to a successful fight against unauthorized access to information and data interception is a clear understanding of the channels of information leakage. Integrated circuits, on which computers are based, create high-frequency changes in the level of voltages and currents. Oscillations propagate through wires and can not only be transformed into an understandable form but also intercepted by particular devices. For example, devices can be installed on a computer or monitor to block information displayed on the monitor or entered from the keyboard. Interception is also possible when data is transmitted via external communication channels, for example, via a telephone line [21].

In practice, several groups of protection methods are used, including:

- An obstacle in the way of the alleged kidnapper, which is created by physical and software means;
- Management, or influencing the elements of the protected system;
- Masking, or data transformation, usually by cryptographic means;

- Regulation, or the development of rules and a set of measures aimed at encouraging users interacting with databases to behave appropriately;
- Coercion, or the creation of such conditions under which the user will be forced to comply with the rules for handling data;
- Inducing or creating conditions that motivate users to behave appropriately.

Each of the methods of information protection is implemented using various categories of means. Fixed assets - organizational and technical.

Organizational means of information protection. The development of a set of organizational information security tools should be within the competence of the security service [20].

Most often, security professionals:

- Deploy documentation that establishes the rules for working with computer equipment and confidential information;
- Conduct training and screening procedures for personnel; initiate the signing of additional provisions to the employment contract, which specifies liability for disclosure or misuse of evidence that has become permissible at work;
- Delimit coverage areas to cover situations where the most common data available to one of the employees is most common; organize work in large workflow programs and track to get important files not stored outside of using disks;
- Implement software products that protect data from sale or destruction by individuals, including top management of the organization;
- System recovery plans in case of an outage from a building around the world.

If the company does not have a dedicated information security service, the way out will be to invite a security specialist to outsource. A remote employee will be able to audit the company's IT infrastructure and give recommendations on how to protect

it from external and internal threats. Outsourcing in information security also involves the use of special programs to protect corporate information.

The group of technical means of information protection combines hardware and software.

Main of them:

- Backup and remote storage of the most important data arrays in a computer system - on a regular basis;
- Duplication and redundancy of all network subsystems that are important for data safety;
- Creation of an opportunity to redistribute network resources in cases of malfunction of individual elements;
- Ensuring the ability to use backup power systems;
- Ensuring safety from fire or water damage to equipment;
- Installing software that protects databases and other information from unauthorized access.

The set of technical measures also includes measures to ensure the physical inaccessibility of computer network objects, for example, such practical methods as equipping a room with cameras and alarms.

1.3.3. Impact of a cyberthreat on the network.

In today's world, cyber threats are an integral part of life. Both in business and everyday life. People often do not even think about the need to keep their devices safe in everyday life. Most people do not even use basic means of ensuring their cybersecurity. Double authentication or the usual linking of an email address to an account is often overlooked. Because of this mostly irresponsible behavior, more global and complex difficulties follow. For example, the business sector can observe the biggest impact of cyber threats. Most people don't even realize that something as seemingly insignificant as computer problems due to a virus can cause problems for dozens or even hundreds of people [21]. Cyberthreats can lead to a variety of

difficulties. For example, difficulties in logistics and even equipment breakdowns due to improper functioning of systems. Some particularly sophisticated cyberattacks can even threaten the comfortable life of entire cities, etc. Clever hackers can get a person's whereabouts and credit history from the comfort of their desk. All it takes is the user's inattention and a weak firewall. The detrimental effect on the network, as well as on the users of this network, is a very broad topic. We can talk about the detrimental effect on the technology itself, on the network bandwidth, and the complexity of the user's interaction with the network. After all, viral and not only threats penetrate and can interfere with work on almost every layer of the OSI model. This paper will consider the impact of cyber threats on the operation of the network itself, the operation of the equipment, and in particular, what difficulties the user may experience when working with the equipment [22].

Let's look at the first and most banal thing that can paralyze the work of many devices at once (in this situation, personal computers), namely ransomware programs. Ransomware that penetrates the system can block the interaction with the endpoint and thereby paralyze the work of an entire department in a large company. For the most part, such programs are quite easy to overcome, but it takes time, which in turn can have a very detrimental effect on the operation of the company's apparatus as a whole. When viewed from the side of the network itself, infected components (servers, etc.) can spread the threat to all connected devices. Thus, the example of the most elementary cybersecurity threats shows the detrimental effect on the entire network and, in general, on the key points of the network and the user of this network.

1.3. Statement of research objectives

Based on the above information, a conclusion is made, building a network, selecting equipment and setting up network security is a very painstaking process. It is for this reason that, in order to understand all the details, further in this work a study will be carried out, the purpose of which can be established as follows:

- Build a model of an enterprise corporate network;
- Configure the security of this network
- Test the network, namely to determine its strengths and weaknesses by analyzing the operation of the software selected by the main firewall.

CONCLUSION TO SECTION 1

Based on the above and having considered in more detail the topologies that are used in the construction of networks, a mixed topology was chosen.

Mixed topology is a network topology that prevails in large networks with arbitrary connections between computers. In such networks, it is possible to single out separate arbitrarily connected fragments (subnets) that have a typical topology; therefore, they are called networks with a mixed topology.

Also, after analyzing the market for XDR products, the cortex XDR was chosen to protect our network, namely its endpoints.

The Cortex XDR from Palo Alto Networks is, according to the manufacturer, the first system in the world that natively integrates network, end device and cloud data to prevent sophisticated attacks. It uses behavioral analytics (Behavioral IOC), and profiling identifies unknown and hard-to-detect threats to the network. Sandbox integration is available for dynamic and non-mediated (bare-metal) analysis. Machine learning and artificial intelligence models that work locally identify threats from any source, including managed and unmanaged devices, enabling rapid investigations. Several specialized technologies prevent the exploitation of vulnerabilities on endpoints, and the focus rules of behavioral analysis protect against ransomware. Cortex XDR prioritizes threats and assists in incident response by providing a complete picture of each danger, automatically identifying its root cause, and providing a wide range of actions against the station under attack.

Also, the main cyber threats for corporate networks were considered, as well as methods of protection against them.

The main security threats include:

- disclosure of confidential information;
- information compromise;
- unauthorized exchange of information;
- refusal of information;
- denial of service;

In practice, several groups of protection methods are used, including:

- An obstacle in the way of the alleged kidnapper, which is created by physical and software means;
- Management, or influencing the elements of the protected system;

SECTION 2
ANALYSIS OF MODERN CYBERSECURITY SYSTEMS FOR CORPORATE NETWORKS

This section will consider modern cyber security systems as telecommunication and not only systems. Since their application is comprehensive, they can help secure an entire corporation or a small network. These systems are state of the art on the market and can provide maximum data protection on virtually any web. All these systems belong to the branch of XDR(Extended Detection and Response) systems.

Products of the XDR class are a completely new branch of information security systems that emerged in 2018. As a continuation of the evolution of EDR (Endpoint Detection and Response) products, they offer more options for analyzing and detecting network attacks at all levels, not just at endpoints. Let us consider the current situation in the global and domestic markets for these products.

Even though XDR systems are new-generation products, they did not appear from scratch but became a logical continuation of EDR class systems. We have previously reviewed the EDR market.

EDRs are effective at endpoints but lack the functionality to detect threats at other levels of the infrastructure, such as the network, which severely limits their functionality. The XDR class proposed a fundamentally new protection model, which includes monitoring endpoints and events in other areas using its agents and network sensors, as well as firewalls, security gateways, IDS / IPS, NTA mail and DLP-systems, IDM / IAM, SIEM. All this information is analyzed in a single complex, and besides, you can configure the response to a possible attack at any level. XDR also allows for a deeper investigation of incidents starting from “zero action,” i.e., an attacker's first step when trying to penetrate the infrastructure. This makes it possible to almost completely control all possible channels to implement threats in the enterprise infrastructure. Since the XDR direction appeared on the market not so long ago, only

a few vendors were able to develop their products and enter the market with it. In some cases, vendors offer several of their products as a single XDR platform.

2.1. XDR systems

XDR systems combine multiple tools to form a single platform for detecting and responding to security incidents [29]. XDR allows you to comprehensively control possible attacks on the enterprise infrastructure by collecting historical and current data at the following levels:

- access points,
- network layer (security gateways,
- FW, IPS, WAF, network sensors),
- sandboxes,
- vulnerability scanners,
- cloud environments and virtualization,
- mail traffic,
- access control systems,
- DLP systems, etc.

The information collected at these levels goes through several stages. First, it is normalized according to predetermined parameters; then, the material enters the so-called Data Lake. The next step is data correlation, followed by a response and, if necessary, investigation [30].

The general scheme of XDR operation is similar to that of SIEM. The main difference is the combination of many events received from different sources into a common attack history. Thus, you can easily see all the attack stages and determine what the first action was and from which penetration into the enterprise network began. This can be done through a single console without using different, most often unrelated administration systems. Event collection and analysis processes are built on automatic

system actions and machine learning, which reduces the number of security administrators responsible for responding to and investigating incidents.

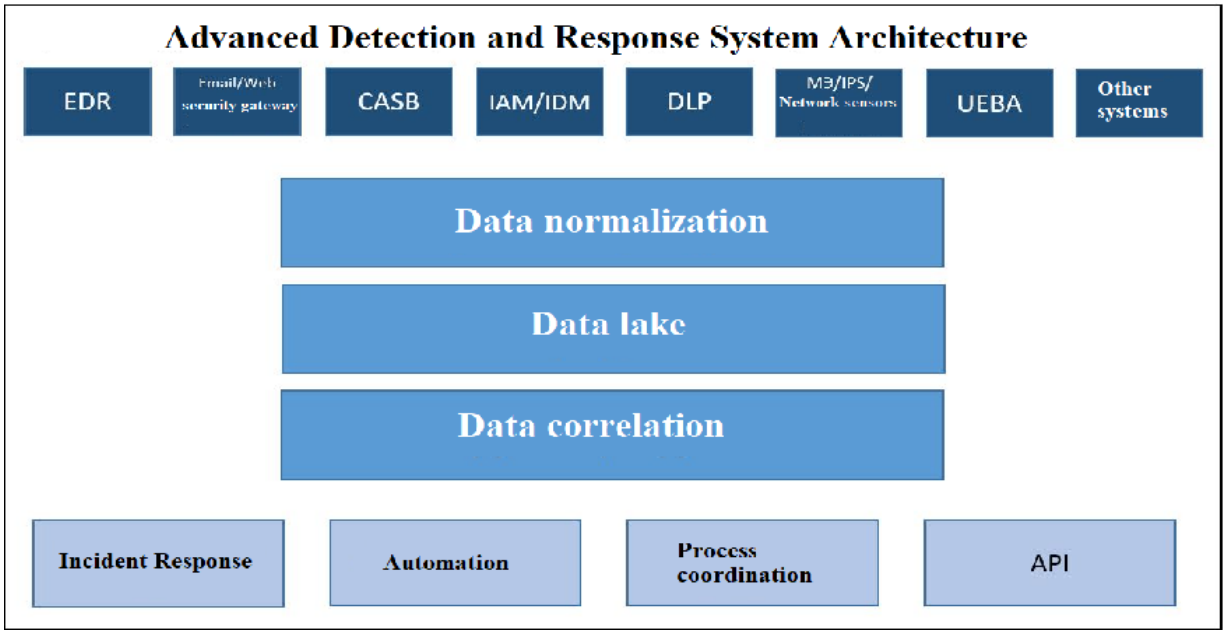

Fig 1.6 General scheme of XDR

2.2 Global XDR market

In 2020, Gartner published an article titled "Gartner Top 9 Security and Risk Trends for 2020", in which they named the use of XDR as one of the nine information security trends [29].

Gartner identifies three critical requirements for an XDR system:

- Centralized collection of normalized data, but mainly from the elements of the XDR system.
- Correlation of events and generation of notifications ("alerts") for security administrators in case of detection of incidents.
- Availability of a centralized incident response system that combines individual security products.

XDR can secure data centers using tools such as cloud workload protection platforms, cloud security management products, and Web Application Firewall. We

can also say that another important task of XDR will be to improve the performance of the security monitoring and control center (SOC) and its accuracy in detecting threats. The concept involves integrating systems and products that can identify the problem and inform the response to incidents in familiar attack chains. Combining security tools that are not typically involved in the same chain of attacks will be of less value. As for the prospects for this concept, Gartner, in the article "Hype Cycle for Security Operations, 2020," suggested that XDR is currently in the first phase of the cycle, at the stage of technological breakthrough, and will reach maturity, i.e., will reach the "plateau productivity," in about 5-10 years [30]. According to analysts, this class of products in 2020 had a low level of penetration into the information security market (the market share is less than 1%).

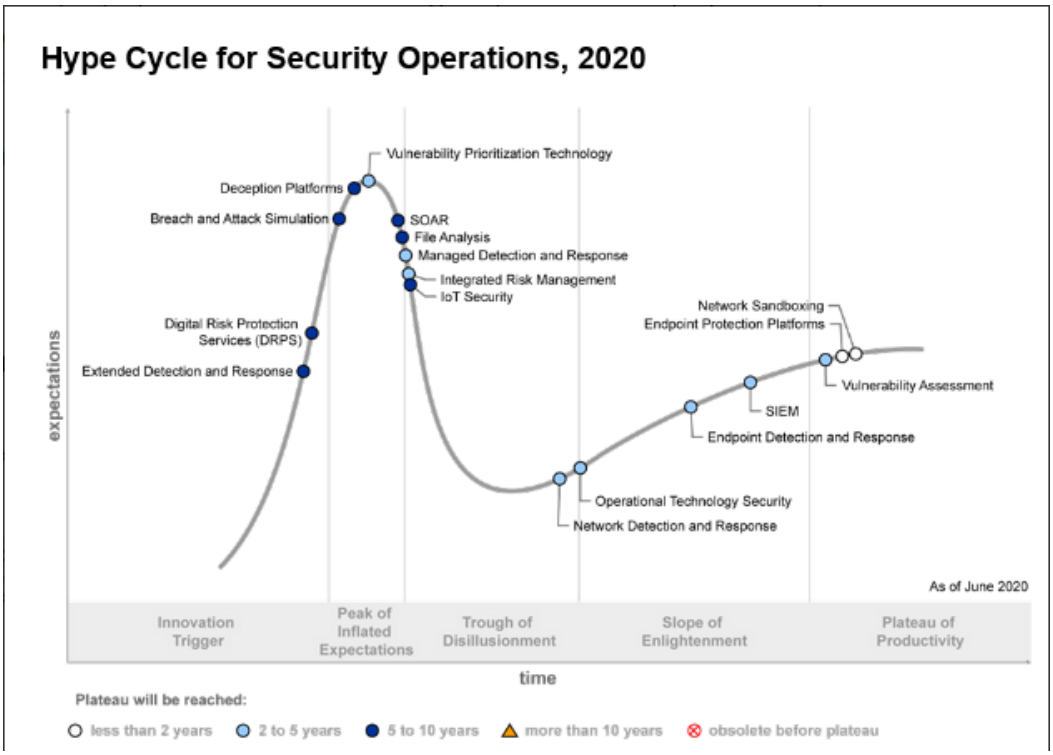

Fig. 1.7 Curve "Hype Cycle for Security Operations, 2020"

Currently, XDR systems are mainly offered by those security solution providers with a portfolio of infrastructure protection products unified by their management platform. This group also includes vendors that currently have products of the EDR class and network protection. Another feature of XDR is mono-vendor: the system shows the most efficient operation when one vendor's products interact.

The XDR concept addresses many threat detection and response needs and looks like a modern "SOC in a box" designed to integrate controls, telemetry normalization, advanced analytics, and response automation. However, according to experts, three big problems could hinder the development of XDR. The first problem is deployment difficulties. Today's security technology infrastructure is a collection of various point tools. Many organizations use multiple software products from different vendors for endpoint security, network security, leak control, etc. XDR vendors will have to convince security teams to move away from a set of “motley” tools in favor of a longer-term vision for cybersecurity technologies [33].

The second problem is a possible confrontation with the SOC. XDR assumes that organizations either do not have existing SOC components (e.g., SIEM, SOAR, threat intelligence platforms, etc.) or can replace them. However, this will be a problem for large enterprises that have already spent heavily on establishing a monitoring center and employee training. Instead of competing with SOC, interaction with it seems to be a more intelligent solution.

The third problem is competition with MDR / MSSP (Managed Detection and Response / Managed Security Service Provider) services. As threat detection and response becomes more complex, many organizations are actively hiring external vendors willing to take complete control of the threat detection and response process. Likely, XDR providers will also provide services using their products or interact with existing MDR/MSSP services. Trend Micro analysts believe that XDR systems have several advantages. Specifically, it is multi-vector control that spans email, endpoints, servers, cloud workloads, and networks. It allows you to provide a more practical search for threats and responses to them [26].

Another feature is a wide range of analytical functions that correlate data in the client environment and global threat intelligence; this makes it possible to provide fewer warnings but more certainty. A single console for managing and conducting investigations makes it easier to present an attack as a chain of events at different levels of security with the ability to respond from the same console.

Gartner, in the article “Innovation Insight for Extended Detection and Response,” suggested that the following vendors would become potential suppliers of XDR products: Cisco, Fortinet, Fidelis Cybersecurity, McAfee, Microsoft, Palo Alto Networks, Symantec, Trend Micro, FireEye, Rapid7 and Sophos. These vendors already have their understanding of the relationships in the source data. They can provide private APIs to provide more efficient automation of actions than trying to integrate products from multiple vendors. The big attraction of these XDR products will be the fast payback through built-in integration between components and pre-configured detection mechanisms in system elements.

In this paper, the following products of the global XDR market will be considered:

- Cortex XDR (Palo Alto Networks);
- SecureX (Cisco);
- SentinelOne Singularity XDR (SentinelOne).

2.3 Overview of XDR systems

Cisco SecureX. SecureX is a cloud-based platform for integrating Cisco Secure solutions with a customer's infrastructure. This system allows you to simplify managing security, centralize all controls and significantly increase operational efficiency through workflow automation. In addition,

SecureX organizes the process of online threat neutralization in the network and reduces the number of manual tasks. The XDR system, which is part of SecureX, collects and correlates data at email, end devices, servers, cloud workloads, networks, web proxies, next-generation firewalls, cloud-based information security systems (SASE) and other sources [11].

This data is used to monitor, analyze, and detect complex threats (Threat Hunting) and enable rapid and automated response (Orchestration). SecureX also offers a feature-rich analytics module.

SecureX supports a variety of Cisco and non-Cisco products. At the endpoint level, Cisco Secure Endpoint, Cisco Secure Email, and Cisco Secure Web Appliance can be used. The networking layer uses Cisco Secure Firewall and Cisco Secure Network Analytics. Finally, for cloud environments, you can use Cisco Umbrella.

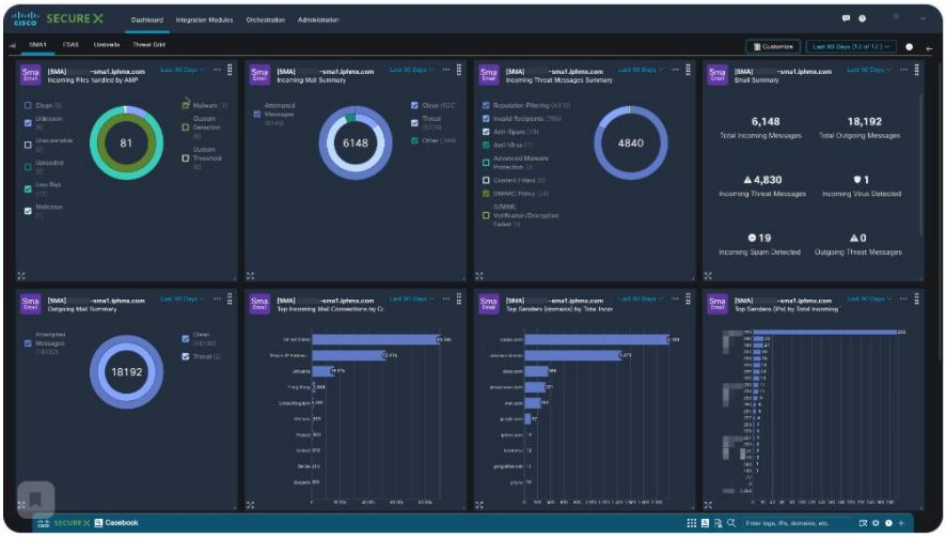

Fig. 1.8 SecureX Administration Console

The developer has a ready-made Cisco Secure Malware Analytics product to analyze potentially malicious files. In addition, the architecture capabilities of this system make it easy to integrate other products, the list of which is constantly growing. For example, it already has developments from Google, IBM, Microsoft, Gigamon, Radware, ServiceNow, VirusTotal, and Qualys [29].

Benefits of Cisco SecureX:

- Support for cloud-based information security systems (SASE).
- Existence of function of detection of complex threats (Threat Hunting).
- Possibility of interoperability with other products besides Cisco developments.

The next Cortex XDR from Palo Alto Networks is, according to the manufacturer, the first system in the world that natively integrates network, end device and cloud data to prevent sophisticated attacks. It uses behavioral analytics (Behavioral IOC), and profiling identifies unknown and hard-to-detect threats to the network. Sand-

box integration is available for dynamic and non-mediated (bare-metal) analysis. Machine learning and artificial intelligence models that work locally identify threats from any source, including managed and unmanaged devices, enabling rapid investigations. Several specialized technologies prevent the exploitation of vulnerabilities on endpoints, and the focus rules of behavioral analysis protect against ransomware. Cortex XDR prioritizes threats and assists in incident response by providing a complete picture of each danger, automatically identifying its root cause, and providing a wide range of actions against the station under attack [32].

The system combines various types of data and simplifies analysis. Tight integration of XDR with endpoint security systems, next-generation firewalls (not only Palo Alto but also third-party ones), as well as various platforms, such as Threat Intelligence, automatically builds MITER attack coverage, allows you to use data obtained from the investigation of previous incidents to detect similar attacks in the future is helpful for Threat Hunting.

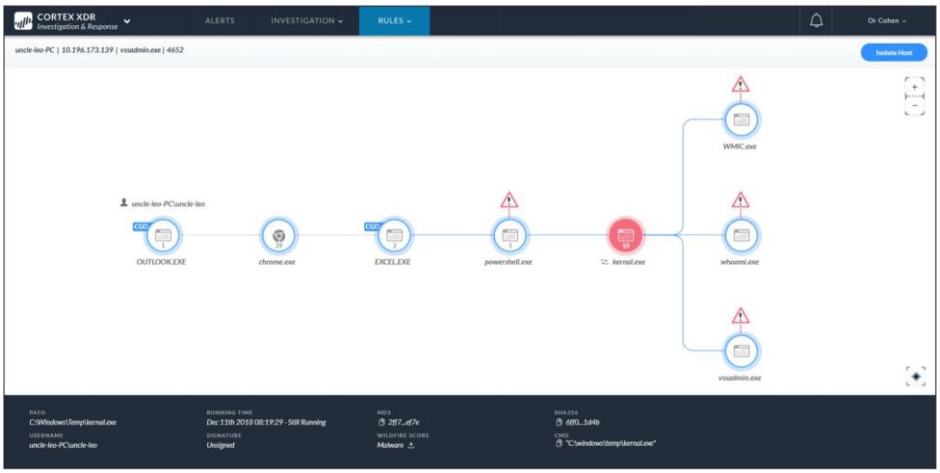

Fig. 1.9 Process launch chain in the Cortex XDR administration console

Included with Cortex XDR, the XDR agent is designed to protect endpoints and provide a comprehensive approach to preventing malware attacks and exploits. The agent also allows you to control the device and its USB connections, such as blocking webcam infections.

The cloud-based Cortex XDR system will enable you to quickly organize the deployment of an information protection system, eliminating the need to install new local data collection services and controls. The latter uses existing Palo Alto Networks products. In addition, a particular local proxy broker can be used for networks with limited access to the Internet [23].

Advantages of Cortex XDR:

- Availability of Behavioral IOC behavioral analytics module;
- Using machine learning and artificial intelligence models;
- Ability to control USB connections.

Last but not least, SentinelOne's Singularity Platform, from developer SentinelOne, combines next-generation antivirus, attack detection, handling, and prevention tools, and AI-based proactive threat hunting across endpoints, and containers, clouds, and IoT devices in a single standalone XDR platform.

This system allows you to provide complete visibility and transparency regarding everything that happens on the network, reflecting each attack at each stage of the threat life cycle. The heart of SentinelOne Singularity is the patented Storyline technology. Each SentinelOne agent builds a real-time model of its endpoint and its behavior. A group of related events in this model is assigned a Storyline ID. When an abnormal event is detected, the system administrator uses the Storyline ID to quickly find all associated processes, files, threads, events, and other data with a single query. Attack storylines are constantly updated in real-time as new telemetry becomes available, providing a complete picture. After detecting malicious activity, the analyst can mark the line as unfavorable and automatically roll back all changes made to the system within it.

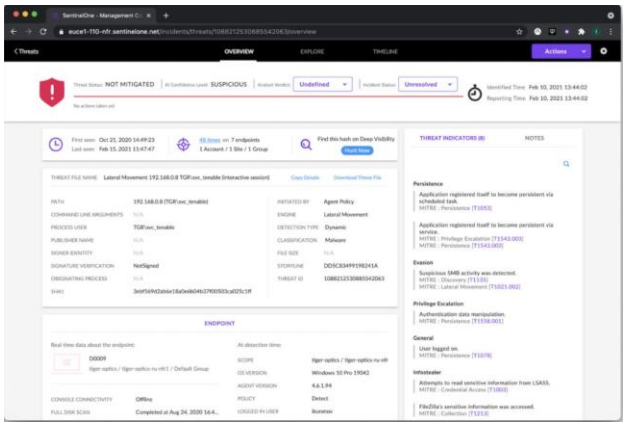

Fig. 1.10 Singularity XDR management console

Singularity XDR also has the following additional features: flexible authentication and authorization system (SSO, MFA), storage of data with incidents and threats for 365 days, built-in SentinelOne cyber intelligence and MITER ATT&CK indicators, highly customizable notifications, Singularity API-based integration with SIEM, sandboxes, messengers like Slack, cyber intelligence (Threat Intelligence), etc. Built-in static and behavioral analysis based on artificial intelligence prevents or detects a wide range of attacks in real time before they cause damage [17].

The SentinelOne Singularity platform is SaaS-based by default. Potential customers have a choice between using the system in the Amazon AWS cloud or on-premises as a virtual appliance. It should be noted that prevention, detection, and response actions are performed locally on the agent, so SentinelOne's capabilities are cloud-agnostic. At the same time, it should be noted that SentinelOne provides only endpoint control through its products without the use of network sensors. To control the network layer, you will need integration with third-party network systems.

Benefits of Singularity XDR:

- Availability of patented technology Storyline;
- Integration with SIEM, sandboxes, messengers, and cyber intelligence of other vendors;
- The presence of built-in SentinelOne cyber intelligence.

CONCLUSIONS TO SECTION 2

XDR is a promising direction in the information security market. This is because this concept is a logical continuation of the development of EDR systems, but now with coverage of the enterprise's entire infrastructure, and not just endpoints. XDR allows you to provide control over the network layer, virtual devices and clouds, including hybrid ones. XDR also boasts a multifunctional analytical engine for detecting incidents and responding to them, convenient tools for investigating attacks.

Furthermore, a new concept of “data lake” has appeared, describing a specific core in which data are collected, correlated and normalized and which allows you to filter out “garbage” and routine actions, leaving only those events that have become stages of an incident or attack. However, it should be noted that since this is an entirely new class of systems, there are not many products of this kind on the market.

Those developments that are now available to customers continue to develop and update. For XDR products to be more effective, integration with other systems such as SIEM, SOAR, DLP, IAM / IDM, UEBA, SASE, CASB, etc., is necessary. XDR has a great future since, on the one hand, this class successfully fits into the global trend of combining and centralizing various information security tools to build a more efficient and functional information protection system that allows you to respond to attacks and investigate incidents automatically. On the other hand, it is a logical continuation of the development of EDR class products. Also, a significant advantage of these systems is an attempt to relieve the burden on security administrators through machine learning and automation of many processes.

SECTION 3.
BUILDING AN ENTERPRISE CORPORATE NETWORK AND TESTING ITS VULNERABILITIES

In this section, you will develop an enterprise network model and test its robustness in terms of cybersecurity. In this model of the network, it will be a conditional formality that the reliability of the network and its performance was checked earlier.

From the side of cyber security, it will be held as a conditional briefing of personnel on security measures to ensure maximum safety of the network network.

There will also be a division of employees into certain "castes" in order to divide them into those who will have access only to work with limited functionality of the equipment (both personal computers and servers), as well as to separate access to the hardware part of the equipment of some employees .

3.1. Enterprise Network Modeling

In this section, modeling of the enterprise network will be carried out, the purpose of the system itself, the purpose of creating the system will be described. The characteristics of the system as a whole and the characteristics of the nodes (objects, subsystems) of the network will also be considered [5].

3.1.1. Purpose of the System.

The corporate network of the Enterprise is designed to ensure the functioning of distributed complexes of software (computer) applications used in the implementation of commercial, industrial and economic activities of the enterprise within the framework of an agreed and approved technical information policy and information security policy.

The object of automation is the commercial, industrial and economic activities of the enterprise's divisions, as well as a number of tasks related to the activities of head structures, related and subsidiaries.

3.1.2. Goals of creating the System.

The main goal of creating the System is to minimize production, commercial and other risks, the magnitude of which may depend on the efficiency of the corporate network and the applications using it. To achieve this goal, it is necessary to ensure the most reliable operation of all network nodes and its communication lines [24], which, in turn, determines the need to perform the following tasks:

- Ensuring fault tolerance of the System at the functional level of the local area network core (hereinafter - LAN);
- Organization of physically dedicated fault-tolerant LAN segments with increased security requirements (third-party organizations, workshop structures for monitoring and managing technological processes, etc.) and ensuring the connection of these segments with the rest of the network infrastructure using specialized secure gateway devices;
- Modernization of LAN nodes related to the distribution level to ensure fault-tolerant operation of this functional level;
- Modernization of critical sections of the LAN of the functional access level in order to reserve network connections used by servers;
- Retrofitting network equipment and infrastructure with interface modules and cable communication lines - to ensure fault tolerance at the physical level;

3.1.3. Characteristics of the system as a whole.

The proposed configuration of the local area network effectively provides the current and planned corporate business requirements, namely:

• integration of applications and data at the corporate level;

• sharing secure use of consolidated data;

• work of users of applied systems in real time and high degree of availability of network resources;

• guaranteed access to information and applications 24x7x365;

• High resource access performance, fast response time, adequate throughput, sufficient bandwidth reserve for future growth.

In order to ensure the reliable functioning of an integrated information system and guaranteed high-speed access for all categories of users to its information and computing resources [19], the proposed solutions for building a LAN are based on modern data transmission technologies and provide for the implementation of the following main features:

• ensuring the throughput of the network backbone sufficient for data exchange within corporate application systems, tasks and services, taking into account the fact that in order to ensure load balancing, the throughput of connecting servers and the backbone of the network should exceed the throughput of connecting workstations of network users by an order of magnitude;

• necessary and sufficient redundancy of the data transmission medium at the physical and logical levels in order to increase the degree of operational reliability and network stability against damage to communication channels, hardware failures and software failures, eliminating a "single point of failure";

• application of a structured cabling system (SCS);

• providing users with access to corporate resources and applications based on communication protocols of the TCP/IP stack;

• organization of virtual networks on the basis of a coordinated policy of differentiation of access rights and protection against unauthorized access;

• LAN connection to external telecommunication networks;

• provision of remote access to network resources for mobile users through the public telephone network;

• connecting external communication channels and providing users of the local area network with access to the resources of the Internet and Intranet networks, integration into a single information space;

The LAN deployed as a result of this project will provide support for the following services:

• file service;

• print service;

• e-mail service;

• HTTP and FTP services;

• Dynamic Host Configuration Protocol (DHCP) service;

• Domain Name Server (DNS) service;

• implementation of centralized maintenance, administration and monitoring.

The successful functioning of corporate application systems depends significantly on the degree of intelligence of the network infrastructure. This implies the need to provide the network administrator with the tools and procedures to allocate and prioritize network resources across different applications and user groups. Within the framework of this project, it is planned to implement the Policy Networking architecture, which includes the following functional components:

• Intelligent Network - intelligent network infrastructure devices, ie. routers, switches, access servers, with unified middleware;

• Policy Services - tools and technologies for converting business requirements into network configuration and activating quality of service (QoS) policies, network security and other network services;

• Registration and Directory Services - tools and technologies for dynamic registration of a network address, application profile, user name and other information in directories;

• Policy Administration - means and technologies for providing centralized management based on the rules of the network services control policy.

LAN hardware and software implement the following mechanisms and tools:

• quality control of QoS service to control data exchange rate and delays;

• active identification and authorization of users in the network, implementation of predefined registration rules, real-time control of user activity, protection against unauthorized access to the network;

• registering the name, virtual network, IP address and MAC address of the user, as well as the port of the access switch when the user connects;

• support for all types of switches available in the network;

• dynamic interaction with Dynamic Host Configuration Protocol (DHCP) and Domain Name Server (DNS) services;

• automatic configuration of ports of access switches;

• control of users by various attributes of registration rules and provision of this information to other components of the system, in particular for configuring virtual networks by usernames;

• redundancy of the registration subsystem;

• provision of integrated DNS and DHCP services, management of the IP address space to provide user identification, authorization and registration functions;

• automating the development, verification, configuration and implementation of policies and tools to ensure the quality of service QoS;

• definition of different traffic classes for different applications;

• verification of the developed QoS policy before its implementation, taking into account the types of devices, interfaces, software versions and supported technologies;

• activation of the network congestion prevention service;

• a simplified and reliable procedure for propagating the QoS policy within the administrative domain of the network;

• IP traffic filtering and access control to network infrastructure devices in accordance with Access Lists.

To achieve the best characteristics in terms of performance, reliability, manageability and scalability of the local area network, an approach was used that provides for the development of a "multi-level" architecture shown on next figure.

The multilayer LAN model includes 4 layers:

• access layer (Access Layer) – layer 2 switches of the OSI model;

• distribution layer (Distribution Layer) – layer 2 switches of the OSI model;

• core layer (Core Layer) – layer 3 switches of the OSI model;

• server farm (Server Farm) – switches of levels 2/3 of the OSI model;

• The use of switches as active network-forming equipment instead of traditional hubs and routers ensures maximum network performance, since all the main functions in the switches are implemented at the hardware level.

Layer 2 switching is a hardwired bridge. In particular, the transmission of frames is carried out by specialized equipment called the Application-Specific Integrated Circuit (ASIC). Layer 2 switches replace repeater hubs in LAN communication nodes.

Layer 3 switching is hardware-based routing. In particular, specialized devices (ASICs) are engaged in packet transmission. Depending on protocols, interfaces, and supported features, Layer 3 switches can be used in LANs instead of routers.

Layer 4 switching consists of hardware analysis of the traffic generated by various types of user applications. In the data streams created by the TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols, the port of a particular application is contained in the header of each packet. There is a set of functions for parsing layer 4 protocol information that allows you to manage data flows based on Access Lists.

In one physical device (switch) it is possible to simultaneously implement several or all logical switching levels (2, 3, 4).

Modernization of the corporate network of the Enterprise will be carried out with the reservation of the main communication lines for 2000 jobs. This will take into account the ratio between the number of jobs located in the office premises of the administrative buildings (70%) and the number of computers connected to the network located in the workshops (30%). Routing and switching centers of the core of the network will be located in different buildings. The primary routable protocol on the network is IP.

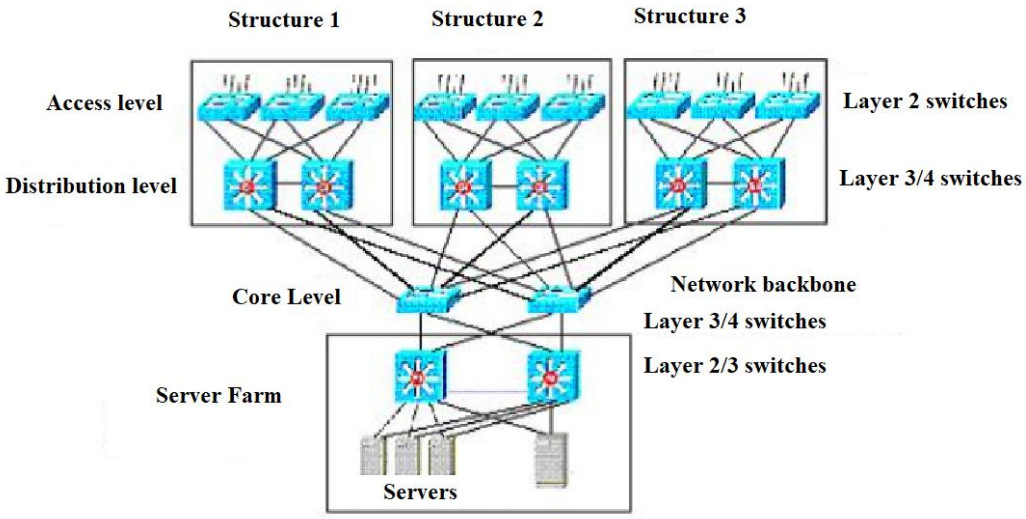

Fig. 3.1 An example of a "layered" corporate LAN architecture

The designed network will be resistant to accidental and deliberate attempts to violate information security, such as unauthorized connection, unauthorized access to data and the generation of network activity leading to a denial of service (Denial of Service) from servers and (or) active network equipment related to core and distribution levels.

3.1.4. Characteristics of nodes (objects, subsystems) of the network.

An additional center for routing and switching at the level of the network core is supposed to be located in the building (APCS). Switching centers of distribution and access levels, located on the sites "Management", "Departments of shops 1,2,4,3". In production premises and network sections owned by third parties, it is planned to organize physically and (or) logically allocated fault-tolerant LAN segments. The connection of these segments with the rest of the network is supposed to be organized using specialized secure gateway devices [20].

The routing and switching centers of the core and distribution levels will be interconnected by redundant fiber-optic communication channels, passing, if possible, through different physical routes, with the declared bandwidth of the data link layer protocol of at least 1 Gbps. Redundancy and configuration of equipment at the core

and distribution levels, as well as redundancy of communication lines at these levels will ensure complete fault tolerance of the System at all levels of the LAN. The failure of one routing and switching center or any of its elements will not affect the work of end users.

3.1.5. Technical conditions for building a fault-tolerant solution

The following picture shows the constructed enterprise network

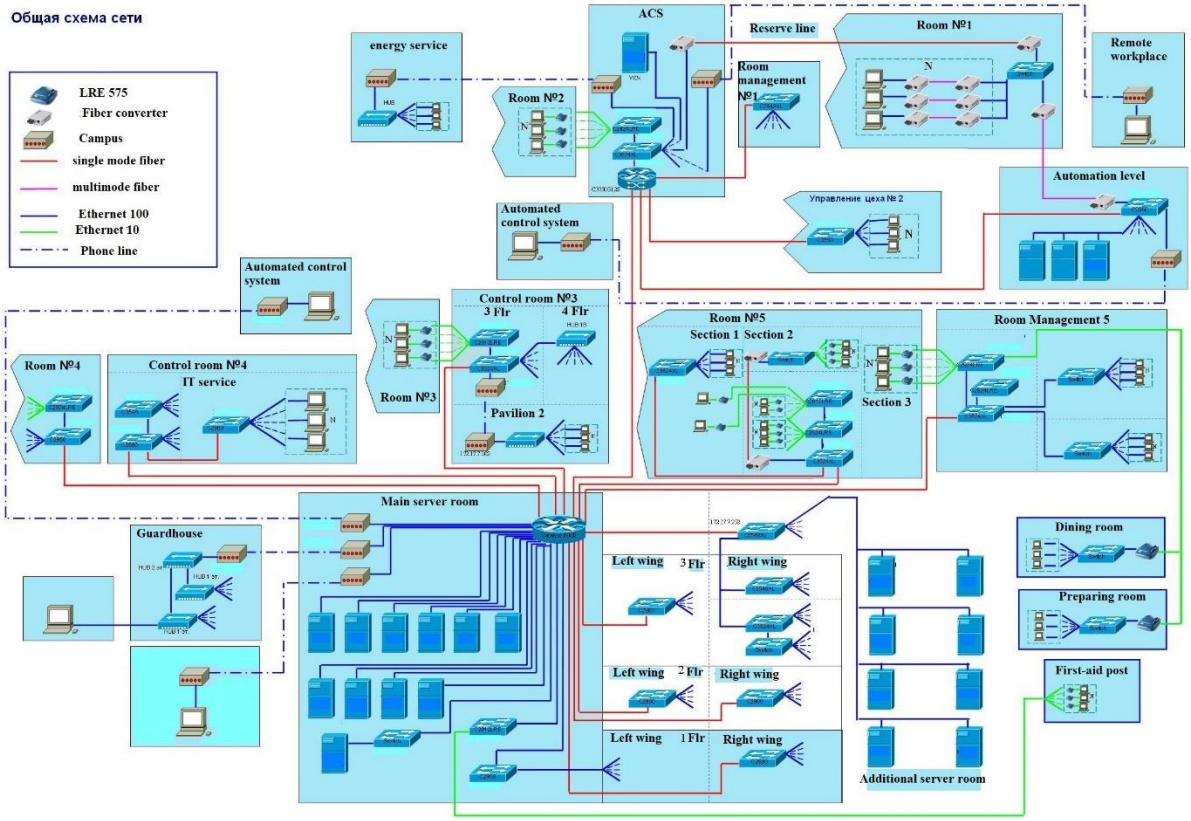

Fig 3.2 Model of enterprise network

At the access layer, fault tolerance is provided by stacking access switches. In this case, the failure of a separate switch or the breakage of one of the channels ascending to the core of the network does not lead to the failure of the access module. Users connected to this module retain the ability to work on the network. At the distribution level, fault tolerance is provided by the presence of optical links from each core switch to each distribution node. The failure of any channel or channel-forming equipment does not lead to a failure, since the network equipment automatically

activates the backup route. At the network core level, fault tolerance is provided by redundant processor modules (SUP 720-3B) and power supplies of the Cisco 6509 core switch. Failure of one of the processor modules or failure of one power supply does not lead to the termination of the network core. By having two independent power feeders connected to separate core switch power supplies, fault tolerance is achieved when power is lost on one of the feeders. At the server connection level, fault tolerance is achieved by connecting the server's two Ethernet ports (Dual-Home) to two separate 1000BaseT core switch modules. The failure of one of the ports or the breakage of one of the connections does not interrupt the availability of the server on the network.

The use of Cisco StackWise technology in floor switches increases fault tolerance, simplifies operation, and increases the efficiency of stackable switches. Cisco StackWise technology allows you to combine up to 9 Cisco Catalyst 3750 series switches as part of a single switching unit with a throughput of 32 Gb / s.

3.1.6. Structure and functioning of LAN nodes of the Enterprise

Active network equipment of the core and distribution layers are high-performance switches capable of operating at the network layer of the OSI model (the third layer of the OSI model, hereinafter referred to as L3), providing switching of high-speed communication channels and supporting the maintenance of a sufficient number of virtual local area networks (VLANs). The nodes of the network core level use L3 switches of modular design, the configuration of which provides for a uniform load on both routing centers and automatic load switching to one of them when the other fails. At distribution level nodes, L3 switches with a fixed configuration are allowed. The choice of a specific switch model was made on the basis of technical feasibility and the requirements of the security subsystem.

Active network equipment of the access layer is a switch that provides connection to the network of end users. Taking into account the fact that the hierarchical three-level model assumes the division of network nodes according to a functional attribute, it is allowed to implement several functional levels on one physical piece of equipment. In this case, it is allowed to include users directly in the switches

of both the access level and the distribution level. Therefore, the equipment of nodes higher in the hierarchy provides for the availability of spare ports and a margin of performance for connecting end users.

Preference is given to switches operating at the link layer of the OSI model (the second layer of the OSI model, hereinafter referred to as L2).

The project allows the use of existing active equipment installed at the nodes of the existing network, provided that the requirements for the network are met in full.

The configuration of the communication nodes of the network serving the sites where the servers are located provides for maximum fault tolerance for such sites in terms of equipment and communication lines. To achieve this goal, it is proposed to use active network equipment L2 and L3 as switches at the level of the server complex.

3.2. Building a cybersecurity system for the corporate network of an enterprise

In this section, we will consider the construction of cyber defense of the corporate network built above. In this case, the protection system will be based on the protection of endpoints (computers, servers, etc.). Cortex XDR was chosen as the software that will provide protection for devices. At the moment this software is one of the wired ones on the market. In this work, further emphasis will be placed on the deployment of the network and the detection of threats in it.

3.2.1. Compatibility and Reliability.

It should be noted that the selected software supports almost all common operating systems (Windows, Android, Linux), except for the operating system from apple (MacOS). Compatibility with major systems (Windows, Android, Linux) allows you to deploy a fairly extensive network, which will include different platforms (smartphones, desktop and compact computers, servers and even tablets, etc.). In this work, the network will be deployed below mainly on servers, desktops and laptops.

This is due to the fact that most modern networks will include these devices. In other words, they are the most common, and it will not be so significant to consider some less frequently used devices. Since, most often, attacks occur precisely through the most accessible points, and everything else is either special cases or a small amount of chance. Unfortunately, the architecture of some operating networks limits the functionality of most of these programs, but in this situation, the next generation firewall was chosen, which provides almost the maximum functionality possible. Some of these features will be discussed in more detail below. In addition, the general operations and procedures adopted to ensure the security of the network will be considered.

The reliability of the security system built further is ensured by the program itself, namely by the chosen approach of the developers. Since our firewall clients will be installed on computers, and their management console is located in the cloud storage, and users only have the opportunity to check the status of client synchronization with the management console. As for the safety of the program itself from various viruses, etc. She is at the highest level. An ordinary user, like an administrator, does not have the ability to remove a client from a device without a special authorization code and special software. This is due to the fact that the cortex is, as it were, "sewn" into the system.

3.2.2. Client installation and configuration.

To install the Cortex XDR agent on the endpoint for the first time, you must first create an agent installation package. After you create and download an installation package, you can then install it directly on an endpoint, or you can use a software deployment tool of your choice to distribute the software to multiple endpoints. On next picture shown the Cortex XDR setup window (Fig. 2.1).

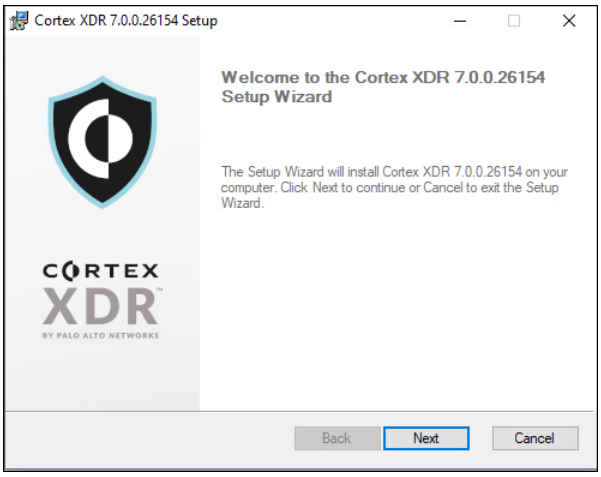

Fig. 3.3 Setup window.

To install the Cortex XDR agent software, you must use a valid installation package that exists in your Cortex XDR management console. On the next figure shown the Cortex XDR client in the tray.

Fig. 3.4 Cortex XDR in tray

If you delete an installation package, new agents installed from this package are not able to register to Cortex XDR, however existing agents may re-register using the Agent ID generated by the installation package. To create a new installation package:

Step 1: From Cortex XDR, select Endpoints > Agent Installations.

Step 2: Create a new installation package.

Step 3: Enter a unique Name and an optional Description to identify the installation package

Step 4 Select the Package Type (In this work selected Standalone Installers is used for fresh installation and upgrade existing's agents of software).

Step 5: Specify the installation package settings (Windows/Always deploy with latest agent version/cortex-xdr/Node Selector/Broker Service).

Step 6: Create the installation package.

Step 7: Download installation package on PC and run it (example of installed client is shown on figure 2.3).

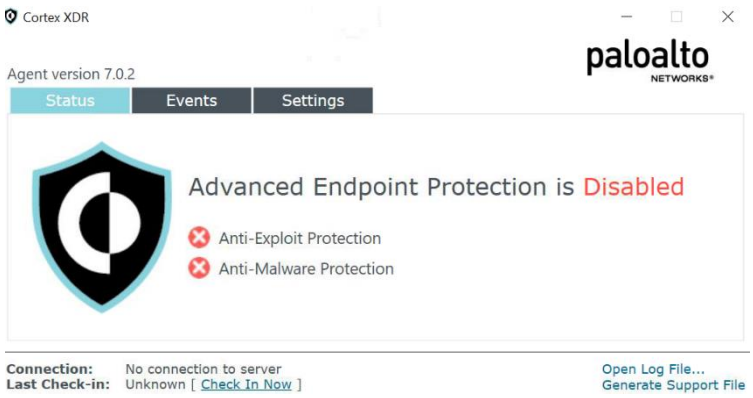

Fig.3.4 Installed Cortex XDR client.

At this point, a complete deployment of the system was carried out on all necessary devices. After everything is installed and configured, you just need to monitor the status of the network, which will be discussed in the next steps of work.

3.2.3. Organizational practices applied to security.

In this work above, some organizational security methods have already been considered. But it is necessary to discuss the methods of informing and so on. which were applied in the case under study.

- To begin with, employees were informed that it was forbidden to browse social networks and public Internet places through work devices.
- Also, briefing on general Internet literacy was made. In particular, about phishing methods and other fraudulent schemes.
- On most devices, USB ports have been disabled where possible and does not interfere with workflows.

- A pass mode was set and access to servers, etc. was limited. a number of employees who do not need such access.

The methods of informing and trite caution are elementary means of ensuring preventive security. Without them, the number of cyber threats will increase many times over. Since, even in the modern network structure, the human factor is one of the most vulnerable places. This is worth looking at as closely as possible.

3.2.4. Using a ready-made security network.

Everything was installed and running. Now you only need to check the status of all connected devices. At the next figure 2.4 shown the Cortex XDR cloud console. The status of all devices can only be checked through the cloud console, which can be accessed through the gateway. Login data is generated by the vendor of this product. Many tools are available in this console to combat, prevent and eliminate the consequences of complexities caused by cyber threats. On this page we see a graph of the ratio of closed incidents to those under investigation. We also see the total number of agents, both connected and disconnected. We can view the latest events that occurred on our devices and inspect them in more detail. At the moment, you can see that all devices are connected. Also, recent events reflect a high-risk event that happened quite a long time ago. That is, now the network is safe and nothing threatens it, it is in a stable state.

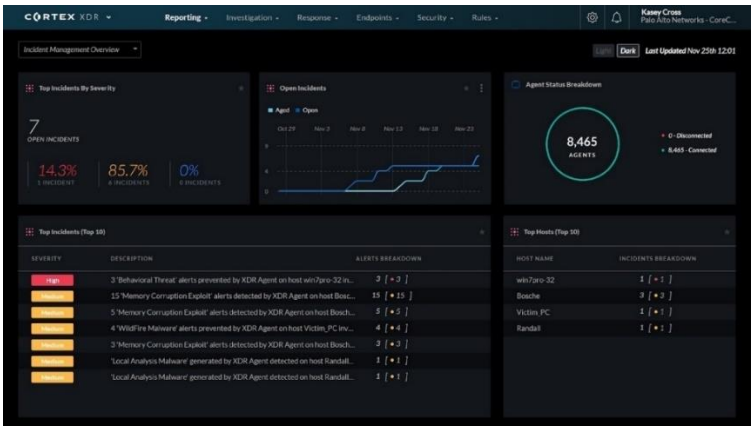

Fig. 3.5 Cloud console of Cortex XDR

3.2.5. Testing the security response to a threat

At this stage, we will check the performance of the system by trying to carry a "threat to the device. The attempt will be made in the most usual way, the infected file will be downloaded from a public file sharing service on the Internet. For example, the site (https://example.threat.com/u/2/downloadvirus) will be taken.

Since downloading is allowed, our security system does not notify us of difficulties and a possible violation of its sovereignty. But after the unknown infected file is launched, we can see the following on figure 2.5.

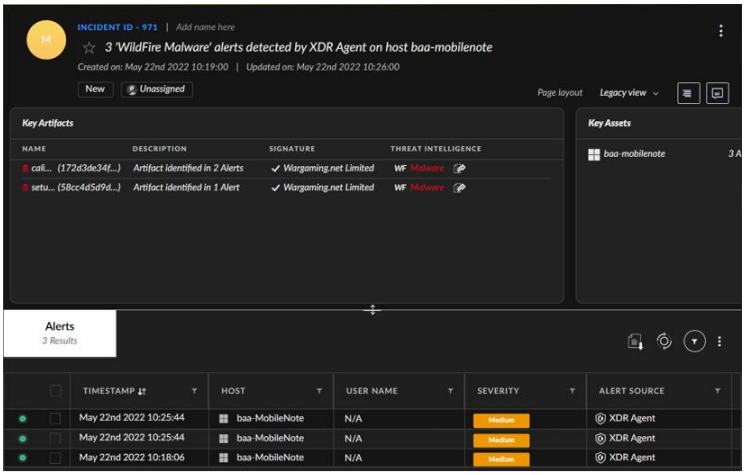

Fig.3.6 Alert in Cortex console

Since our security system has policies configured, it additionally checks the file in the sandbox. Since our security system has policies configured, it additionally checks the file in the sandbox. And then it gives us in the console the exact information that we managed to get from it, this can be seen in the picture 2.6.

Fig. 3.7 Detail information about the file

As for the user, he will be able to see a small notification on his device and will not be able to run this file to work. What you can see in picture 2.7

Fig.3.8 Example of alert that can see user on PC

As you would expect, the system is fully operational and ready to withstand the test of time and many penetration attempts.

3.2.6. Recommendations for the operation and maintenance of the security system

There is nothing complicated in the operation of this system, the interface is as friendly as possible, and the program itself is easy to use and practically does not affect the operation of the device on which it is located. There are only a few simple but effective solutions or recommendations for this kind of system:

- Always check the relevance of the software.
- Provide regular briefings to personnel about potential hazards

And do not delay the response to incidents on devices. Since it is necessary to check the slightest encroachments in the protection, especially sophisticated attackers are always trying to find a loophole in the protection.

CONCLUSIONS TO SECTION 2

The conclusion that we can draw from the above information can be drawn as follows. Nowadays, security systems and other technologies do not stand still, but unfortunately attackers do too. They are looking for both technical and non-technical ways to infiltrate our network or information.

You should always remember about the safe use of the Internet, and especially its most common places. Since intruders are on the alert, they will always try to get into the most secure places. But, such programs as Cortex and others will always come to our rescue. In this paper, we looked at how to deploy a network that can help us protect data. And it turns out to be surprisingly simple, but it also has its drawbacks. In such a scheme of work, most often a special employee is needed who will monitor the console, process data and report on all difficulties.

But most often, vendors provide the services of their specialists in this area, the only catch may be the price of a subscription to this software. In this case, the security system shows itself perfectly, so there is no doubt about its work. Even if the client is not connected to the management console, it will perform its immediate functions. With such software, the network will be safe in 85% of cases.

CONCLUSION

Based on the above and having considered in more detail the topologies that are used in the construction of networks, a mixed topology was chosen.

Mixed topology is a network topology that prevails in large networks with arbitrary connections between computers. In such networks, it is possible to single out separate arbitrarily connected fragments (subnets) that have a typical topology; therefore, they are called networks with a mixed topology.

Also, after analyzing the market for XDR products, the cortex XDR was chosen to protect our network, namely its endpoints.

The Cortex XDR from Palo Alto Networks is, according to the manufacturer, the first system in the world that natively integrates network, end device and cloud data to prevent sophisticated attacks. It uses behavioral analytics (Behavioral IOC), and profiling identifies unknown and hard-to-detect threats to the network. Sandbox integration is available for dynamic and non-mediated (bare-metal) analysis. Machine learning and artificial intelligence models that work locally identify threats from any source, including managed and unmanaged devices, enabling rapid investigations. Several specialized technologies prevent the exploitation of vulnerabilities on endpoints, and the focus rules of behavioral analysis protect against ransomware. Cortex XDR prioritizes threats and assists in incident response by providing a complete picture of each danger, automatically identifying its root cause, and providing a wide range of actions against the station under attack.

Also, the main cyber threats for corporate networks were considered, as well as methods of protection against them.

The main security threats include:

- disclosure of confidential information;
- information compromise;
- unauthorized exchange of information;
- refusal of information;

- denial of service;

In practice, several groups of protection methods are used, including:

- An obstacle in the way of the alleged kidnapper, which is created by physical and software means;
- Management, or influencing the elements of the protected system;

XDR is a promising direction in the information security market. This is because this concept is a logical continuation of the development of EDR systems, but now with coverage of the enterprise's entire infrastructure, and not just endpoints. XDR allows you to provide control over the network layer, virtual devices and clouds, including hybrid ones. XDR also boasts a multifunctional analytical engine for detecting incidents and responding to them, convenient tools for investigating attacks.

Furthermore, a new concept of “data lake” has appeared, describing a specific core in which data are collected, correlated and normalized and which allows you to filter out “garbage” and routine actions, leaving only those events that have become stages of an incident or attack. However, it should be noted that since this is an entirely new class of systems, there are not many products of this kind on the market.

Those developments that are now available to customers continue to develop and update. For XDR products to be more effective, integration with other systems such as SIEM, SOAR, DLP, IAM / IDM, UEBA, SASE, CASB, etc., is necessary. XDR has a great future since, on the one hand, this class successfully fits into the global trend of combining and centralizing various information security tools to build a more efficient and functional information protection system that allows you to respond to attacks and investigate incidents automatically. On the other hand, it is a logical continuation of the development of EDR class products. Also, a significant advantage of these systems is an attempt to relieve the burden on security administrators through machine learning and automation of many processes.

LIST OF USED LITERATURE

1. Corporation P. T. E-Tech 2004: An IEEE Student Branch, Ned University of Engineering and Technology International Multi-Topic Conference. Institute of Electrical & Electronics Enginee, 2004. 129 p.

2. Cybersecurity Guide / I. ALECU et al. Romanian Association for Information Security Assurance (RAISA), 2021. URL: https://doi.org/10.19107/cybersec.2021.ro (date of access: 29.05.2022).

3. DeLaet G., Schauwers G. Network Security Fundamentals. Cisco Press, 2004. 480 p.

4. Du D.-Z., Huang S. C. H., MacCallum D. Network Security. Springer, 2014. 292 p.

5. Ellis R., Mohan V. Rewired: Cybersecurity Governance. Wiley & Sons, Incorporated, John, 2019. 352 p.

6. Hulick K. Cybersecurity Careers. Referencepoint Pr Inc, 2018. 80 p.

7. Marchette D. J., Verma R. M. Cybersecurity Analytics. Taylor & Francis Group, 2019. 340 p.

8. Mathematical modelling for information technology: Telecommunication transmission, reception, and security. Chichester : E. Horwood, 1988. 214 p.

9. Pacemaker Cybersecurity / A. Baranchuk et al. Circulation. 2018. Vol. 138, no. 12. P. 1272–1273. URL: https://doi.org/10.1161/circulationaha.118.035261 (date of access: 29.05.2022).

10. Patterson W., Winston-Proctor C. E. Behavioral Cybersecurity. Boca Raton : Taylor & Francis, CRC Press, 2019. : CRC Press, 2019. URL: https://doi.org/10.1201/9780429461484 (date of access: 29.05.2022).

11. Petrakis G. J. Management of computer security and telecommunication systems. Brown & Benchmark Publ, 1998. 172 p.

12. Publishing C. G. Don't Panic! I'm a Professional Senior Cybersecurity Analyst : Customized 100 Page Lined Notebook Journal Gift for a Busy Senior

Cybersecurity Analyst: Far Better Than a Throw Away Greeting Card. Independently Published, 2020. 102 p.

13. Ratnayake D. Cybersecurity. ITNOW. 2022. Vol. 64, no. 1. P. 37. URL: https://doi.org/10.1093/itnow/bwac019 (date of access: 29.05.2022).

14. Security U. S. C. H. C. o. H. The XDR tuberculosis incident: A poorly coordinated federal response to an incident with homeland security implications : full hearing before the Committee on Homeland Security, House of Representatives, One Hundred Tenth Congress, first session, June 6, 2007. Washington : U.S. G.P.O., 2009. 100 p.

15. Stephenson P. Global Network Security. M & T Books, 1996. 864 p.

16. Union I. T. Fixed service HF systems. Geneva : International Telecommunication Union, 1998.

17. Union I. T. Study of the costs of providing and operating telecommunication services between industrialized and developing countries. Geneva : International Telecommunication Union, 1988. 20 p.

18. Waschke M. Personal Cybersecurity. Berkeley, CA : Apress, 2017. URL: https://doi.org/10.1007/978-1-4842-2430-4 (date of access: 29.05.2022).

19. Bennett L. Cyber Security Strategy. ITNOW. 2012. Vol. 54, no. 1. P. 10–11. URL: https://doi.org/10.1093/itnow/bws003 (date of access: 29.05.2022).

20. Brandreth D., Ophoff J. Investigating Customer-Facing Security Features on South African E-commerce Websites. Information and Cyber Security. Cham, 2020. P. 144–159. URL: https://doi.org/10.1007/978-3-030-66039-0_10 (date of access: 29.05.2022).

21. Cohen F. Managing network security: Simulating network security. Network Security. 1999. Vol. 1999, no. 4. P. 6–13. URL: https://doi.org/10.1016/s1353-4858(00)80009-4 (date of access: 29.05.2022).

22. Committee P. I. T. A. Cyber security: A crisis of prioritization. Arlington, VA : National Coordination Office for Information Technology Research and Development, 2005. 58 p.

23. Cyber Security and Information Security. International Journal of Recent Technology and Engineering. 2019. Vol. 8, 3S. P. 372–374. URL: https://doi.org/10.35940/ijrte.c1079.1083s19 (date of access: 29.05.2022).

24. Ellis S. R. Cyber Forensics. Managing Information Security. 2013. P. 223–274. URL: https://doi.org/10.1016/b978-0-12-416688-2.00009-x (date of access: 29.05.2022).

25. (GCSCC) G. C. S. C. C. Global Cybersecurity Education Needs Assessment: Discussion Resource Paper. SSRN Electronic Journal. 2020. URL: https://doi.org/10.2139/ssrn.3660010 (date of access: 29.05.2022).

26. Govender I., Watson B. Theorising Information Security Policy Violations. Information and Cyber Security. Cham, 2020. P. 131–144. URL: https://doi.org/10.1007/978-3-030-43276-8_10 (date of access: 29.05.2022).

27. Gupta N. MDR and XDR Tuberculosis. Jaypee Brothers Medical Publishers (P) Ltd., 2015. URL: https://doi.org/10.5005/jp/books/12516 (date of access: 29.05.2022).

28. Humeniuk I. V., Basaraba M. S., Nekrilov O. V. METHODS OF ENSURING CYBER SECURITY OF CRITICAL COMPONENTSNETWORKS OF INFORMATION AND TELECOMMUNICATION SYSTEM. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2020. No. 18. P. 101–110. URL: https://doi.org/10.46972/2076-1546.2020.18.10 (date of access: 29.05.2022).

29. Irvine W. M. XDR. Encyclopedia of Astrobiology. Berlin, Heidelberg, 2015. P. 2657–2658. URL: https://doi.org/10.1007/978-3-662-44185-5_5124 (date of access: 29.05.2022).

30. O'Connell M. E. Cyber Security without Cyber War. Journal of Conflict and Security Law. 2012. Vol. 17, no. 2. P. 187–209. URL: https://doi.org/10.1093/jcsl/krs017 (date of access: 29.05.2022).

31. Perez A. Network Management. Network Security. Hoboken, NJ, USA, 2014. P. 133–154. URL: https://doi.org/10.1002/9781119043942.ch6 (date of access: 29.05.2022).

32. Rosário A. T. Internet of Things, Security of Data, and Cyber Security. Advances in Wireless Technologies and Telecommunication. 2022. P. 148–185. URL: https://doi.org/10.4018/978-1-7998-9312-7.ch007 (date of access: 29.05.2022).

33. Snyman D., Kruger H. A Management Decision Support System for Evaluating Information Security Behaviour. Information and Cyber Security. Cham, 2020. P. 15–27. URL: https://doi.org/10.1007/978-3-030-43276-8_2 (date of access: 29.05.2022).

34. The TCP/IP Protocol Stack. Network Security. 2005. P. 319–333. URL: https://doi.org/10.1016/b978-012311633-8/50013-4 (date of access: 29.05.2022).

35. Vancouver C. Cyber Security in an Information Warfare Age. The Journal of Intelligence, Conflict, and Warfare. 2018. Vol. 1, no. 2. P. 9. URL: https://doi.org/10.21810/jicw.v1i2.652 (date of access: 29.05.2022).

36. XDR tuberculosis / J. van Ingen et al. The Lancet Infectious Diseases. 2011. Vol. 11, no. 8. P. 585. URL: https://doi.org/10.1016/s1473-3099(11)70200-6 (date of access: 29.05.2022).

37. Yermalovich P., Mejri M. Risk Forecasting Automation on the Basis of MEHARI. Information and Cyber Security. Cham, 2020. P. 34–49. URL: https://doi.org/10.1007/978-3-030-66039-0_3 (date of access: 29.05.2022).