

**The Czech University of Life Sciences**

**The Faculty of Economics and Management**

**Economics and Management (EM)**



**Wireless network security in critical infrastructure business in  
Kazakhstan: A comparative analysis of intrusion detection systems  
using MCDA**

Bachelor thesis

Author: Adylkhanov Akbar

Thesis supervisor: John Phillip Sabou, PhD.

Prague 2022

## **Summary of the Thesis**

**Title:** Wireless network security in critical infrastructure business in Kazakhstan: A comparative analysis of intrusion detection systems using MCDA

**Author:** Adylkhanov Akbar

**Supervisor:** John Phillip Sabou, PhD.

**Level:** Bachelor Thesis in Economics and Management

**Keywords:** MCDA, intrusion detection systems, critical infrastructure business, wireless network security, ransomware

**Purpose:** This thesis will problematize the use of three intrusion detection systems to the case sample, *Kaztransoil*, an oil export company in Kazakhstan. Intrusion detection systems or “IDS” are necessary tools to protect critical infrastructure from malicious computer infections and worms that can harm not only businesses, but also access to wireless networks and related equipment. Threats such as malware and, especially, ransomware, are real concerns for business in developing countries that may not access to the same intrusion detection systems that developed nations do.

**Literature review:** The consequence of studying the long-term experience of the company's employees and previous research on information security in wireless networks. The work will contain the experience of recent years so as not to lose relevance.

**Method:** Multi-Criteria Decision Analysis, Scoring Method.

**Practical part:** The research aims to determine the importance of implementing threat detection systems in the wireless segment of a large, critical infrastructure company. It also aims at determining the most optimal security threat detection system for a large company through *multi-criteria decision analysis*.

## Table of Contents

1.1. Introduction.....	1
1.2. Premise of the study .....	1
2. Literature review .....	2
2.1. Wireless network. Principle of operations. ....	3
2.1.1. Benefits of Wi-Fi.....	4
2.1.2. Disadvantages of Wi-Fi.....	4
2.1.3. Wireless Vulnerabilities, Threats and Countermeasures of Big Company	5
2.2. Potential Threats and attacks of Wireless network .....	6
2.2.1. Accidental association.....	6
2.2.2. Malicious association .....	6
2.2.3. Ransomware .....	7
2.2.4. Procedures to identify the problems.....	8
2.3. Intrusion detection systems .....	8
2.3.1. Principle of operation of Intrusion Detection Systems .....	9
2.3.2. Detection Methodology.....	10
2.3.3. Intrusion detection system for the Large Companies.....	12
2.4.2.a. <i>Snort</i> Intrusion detection system.....	12
2.4.2.b. <i>Suricata</i> Intrusion detection system.....	15
2.4.2.c. <i>Bro (Zeek)</i> Intrusion Detection System .....	16
3. Practical part .....	17
3.1. Special market research .....	17
3.2. Methodology .....	18

3.3. Focus Group Discussion .....	19
3.3.1. Organizing Focus Group Material and Defining a Unit of Analysis .....	20
3.3.2. Focus-Group Questions.....	20
3.4. EMPIRICAL ANALYSIS .....	22
3.4.1. Research Approach .....	22
3.4.2. Target population .....	22
3.4.3. Questionnaire Design .....	22
3.4.4. Collecting data.....	23
3.5. The Weighted Scoring Method .....	28
3.5.1. The Weight percentage.....	28
3.5.2. Calculations analysis .....	33
3.5.3. Discussion .....	37
3.6. Analyzing Data for Multi-Criteria Decision Analysis .....	38
3.7. Multi-Criteria Decision Analysis .....	42
3.7.1. The first stage .....	42
3.7.2. The second stage (The Use of Resources Calculations) .....	46
3.7.3. The third stage .....	51
4. Conclusion .....	53
5. References.....	54
6. Appendix.....	57
7. Appendix II: Interview chart.....	60

## List of Figures and Tables

Figure 1: Snort Intrusion Detection System components. ....	14
Figure 2: Suricata Intrusion Detection System components.....	15
Figure 3: Bro Intrusion Detection system Components.....	17
Figure 4: Time of processing testing results in a chart .....	39
Figure 5: The difference in the number of alarms for each of the intrusion detection systems .....	40
Figure 6: Formula of linear normalization for further calculations in Multi-Criteria Decision Analysis.....	43
Figure 7: Formula of linear normalization for further calculations in Multi-Criteria Decision Analysis.....	47
Figure 8: An example of a questionnaire, an employee wished to remain anonymous. ....	57
Table 1: Pros and cons of intrusion detection methodologies. ....	11
Table 2: Closed-ended interview questions and answers .....	24
Table 3: Weight determination for the weighed scoring method .....	29
Table 4: The Weighted Scoring Methods Calculations .....	33
Table 5: The percentage of consumed processor resources.....	41
Table 6: The entered data for each of the criteria for further analysis.....	42
Table 7: Determination of the formula suitable for each of the criteria based on Linear Normalization.....	43
Table 8: Multi-Criteria Decision Analysis Calculations.....	45
Table 9: The final results of the calculations: Ranking/Score .....	46
Table 10: The percentage of RAM and CPU resource utilization for each intrusion detection system. ....	47

Table 11. Determination of the formula suitable for each of the criteria based on Linear Normalization .....	48
Table 12: Multi-Criteria Decision Analysis Calculations.....	49
Table 13: The final results of the calculations, the ranks .....	50
Table 14: Scores on two separate analyses .....	51
Table 15: Multi-Criteria Decision Analysis Calculations.....	51
Table 16: The final results of the calculations, the ranks .....	52

## **1.1. Introduction.**

On September 19, 1994, the first record (.kz) appeared on the Internet Assigned Numbers Authority (IANA) database for the (ccTLD). In 1994 “Kaznet” was born. “Kaznet” is essentially the infrastructure that hosts internet access on the territory of the Republic of Kazakhstan. With the advent of Kaznet, IT development in Kazakhstan has increasingly involved security in combating cybercrime. At the moment, cybersecurity plays a vital role in the IT development of Kazakhstan.

The priority of Kazakhstan in the global economics stage currently focuses on competitiveness with other developed countries. A project was introduced to expand the workability and security of information within the Kaznet network. This project was named "The Third Modernization," which included an entirely new concept for 2017 in the field of cybersecurity and was named "Cyber Shield." (Shumatov, 2018, p.108).

The concept defines the main directions for implementing state policy in protecting electronic information resources, information systems, and telecommunication networks, ensuring the safe use of information and communication technologies. In addition to these innovations, generally accepted laws have been adopted to ensure network security. Personal data protection status in the Republic of Kazakhstan now focuses on:

- Regulation of public relations in the field of personal data.
- Features regarding protecting personal data in electronic form for state systems are defined in the “Law of the Republic of Kazakhstan: On Informatization” (Gabdyzhamalov N.M. 2010).
- Implementation of law enforcement for violations regarding the legislation of the Republic of Kazakhstan on personal data and their protection. (Gabdyzhamalov N.M. 2010).

## **1.2. Premise of the study**

The thesis is oriented around the exploration of three intrusion detection systems (software) that are available to critical infrastructure businesses in the Republic of Kazakhstan. Intrusion detection systems or “IDS” are necessary tools to protect critical infrastructure from malicious computer

infections and worms that can harm not only businesses, but also access to wireless networks and related equipment. Threats such as malware and, especially, ransomware, are real concerns for business in developing countries that may not access to the same intrusion detection systems that developed nations do.

Therefore, this thesis will problematize the use of three intrusion detection systems to the case sample, *Kaztransoil*, an oil export company in Kazakhstan. This company, along with many others in the country, regularly suffer from intrusion attempts via their wireless networks, and thus, the selection of their IDS is a priority consideration for their business continuity. Considering that, this study will compare their selection with two other known IDS software's using *Multi-Decision Criteria Analysis* and recommend the best one. The provided selection, as well as the methods used to determine it can be applied to other critical infrastructure business in developing countries.

## 2. Literature review

Information security exists to protect the confidentiality, unity, and availability of computer system data from malicious intent. Before embarking on research, it is essential to understand its purpose. The goal of introducing information security in the business area is to ensure the stable operation of the company and reduce the potential damage caused to the company by preventing and combating the impact of harmful threats and attacks. "Fraud or misuse of IT is often due to a lack of basic controls, with half of the detected frauds being discovered by accident" (Audit Commission Report, 1998, p.73).

According to Mordasova (2015), data loss is the most dangerous for any company's internal processes and software. Common threats, such as computer viruses, computer hacks, and denial of service attacks, are becoming more common, ambitious, and sophisticated. A model of three components often follows the standard security model:

- Confidentiality is a state of information in which access to it is carried out only by subjects who have the right to it.
- Integrity - avoidance of illegal modification and changes in information.



- Accessibility - avoiding temporary or permanent hiding of information from users who have received access rights.

Companies' access to the internet puts companies at high risk of fraudulent activity, targeted cyber-attacks, data corruption and theft, and the spread of malware. Not all violations and threats result from targeted harmful effects; inadvertent misuse and human error also leave a mark. Malware is by far the most popular form of system damage. (Yaseneva V.N. 2017). They can cause irreparable harm on a par with fire. Poor oversight and control of processes and lack of proper secure authorization procedures are often the root cause of security problems. Companies then have to resort to securing information within their systems. Each company approaches the prevention of security breaches individually. It all depends on the literacy of the company's IT departments. Someone prohibits anything that makes it difficult to perform day-to-day access tasks; others are too weak and allow access to everyone, exposing themselves to a high degree of risk. It is not enough to know how to deal with a threat and malware; it is equally essential to detect it at the time before it is too late. (Yaseneva V.N. 2017).

### **2.1. Wireless network. Principle of operations.**

The transmission of radio waves determines the principle of operation of wireless networks; In terms of physical characteristics, a wireless network is close to radio communication. Wi-Fi can have one or more access points in chips to connect multiple users to an access point. The radio transmitters and receivers of the same Wi-Fi network operate on the same frequencies and use the same type of data modulation into radio waves. Wi-Fi networks operate on specific 2.4 and 5 GHz radio frequency bands that have been published, optimized, and approved around the world. (Marshall Brain, 2004, p. 2). These frequencies are officially called unlicensed radio services. Access to these frequencies is possible without a radio access license. Generally, the functioning of large companies is dependent on wireless networks. Almost every department of large modern companies uses laptops, tablets, mobile devices, and wireless devices to operate regular business activities. A wireless network is an indispensable part of a business, except for individual departments where network access is not required or prohibited.

### 2.1.1. Benefits of Wi-Fi

Aside from the apparent dependencies that modern businesses face with regards to network access and security, Şeymanur Cantav (2014) highlighted the main benefits of using wireless networks:

- Wi-Fi creates the ability to use the network for many users without laying cables and reduces the cost of deploying and expanding network access. For instance, locations where the cable cannot be installed, such as outdoors and in buildings of historical value, can be served by wireless networks.
- Wi-Fi devices are widespread in the market. At the moment, almost every new device is equipped with the ability to use Wi-Fi. Devices from different manufacturers can interact at the basic level of services.
- Wi-Fi is a set of global standards. Unlike cell phones, Wi-Fi equipment can work in different countries around the world.

### 2.1.2. Disadvantages of Wi-Fi

In addition to the advantages, when working with wireless networks, many problems can be encountered. Bornstein (2015), in his writings on the use of Wi-Fi, noticed that in mechanical use, high power consumption is often encountered compared to other standards, which shortens the battery life and increases the temperature of the device. The overlap of signals from a closed or encrypted access point and an open access point operating on the same or adjacent channels can interfere with access to other access points. This problem can arise with a high density of access points, for example, in large business centers, where offices are owned by different independent companies and have Wi-Fi access points.

Additionally, Wi-Fi has a limited range. A typical office Wi-Fi 802.11b or 802.11g router has a range of 45m indoors and 90m outdoors. A microwave oven or mirror between Wi-Fi devices will weaken the signal. Distance also depends on frequency (Jon Edney, 2014). Regarding the devices themselves, regardless of routers, incomplete interoperability between devices from different manufacturers or incomplete compliance with standards may result in limited connectivity or reduced speed.

The most important issue is the security vulnerability, as the most popular encryption standard, WEP, can be relatively easily compromised even with the correct configuration due to the weak strength of the algorithm. Although newer devices support the more advanced WPA encryption protocol, many older access points do not support it and need to be replaced. The adoption of the IEEE 802.11i standard in June 2004 made a more secure scheme available in new equipment. Both schemes require a stronger password than those typically assigned by users.

Many organizations use additional encryption (like VPN) to protect against intrusions (Jon Edney, 2014). It can also be attributed to disadvantages overload of equipment when transmitting small data packets due to the attachment of a large amount of service information since this can significantly reduce the company's efficiency. Another disadvantage is the low suitability for applications using real-time media streams (for example, the RTP protocol used in IP telephony). The quality of the media stream is unpredictable due to possible high data transmission losses caused by several factors beyond the user's control (atmospheric interference, landscape, and others, in particular, those listed above). Despite this drawback, much VoIP equipment is produced based on 802.11b \ g devices, also targeted at the corporate segment. However, in most cases, the documentation for such devices contains a clause that the quality of communication is determined by the stability and quality of the radio channel. (Kellogg, 2016).

### 2.1.3. Wireless Vulnerabilities, Threats and Countermeasures of Big Company

Before understanding potential threats, it is necessary to understand what vulnerabilities in the wireless network can serve as a conduit for attacks and threat penetration into the company's internal systems. Wireless networks have four main components:

1. Data transmission using radio frequencies.
2. Access points that provide connection to the organization's network.
3. Client devices (laptops, PDAs, et cetera).
4. Users.

These components can be vulnerable to an attack that could violate one or more of the three primary security objectives - confidentiality, integrity, and availability. (P.V Gayarti, 2009, page 9).

## **2.2. Potential Threats and attacks of Wireless network**

Wireless offers many benefits to organizations and users, such as portability and flexibility, increased productivity and lower installation costs. Wireless technologies cover a wide range of capabilities, tailored to different applications and needs. Wireless networks allow data transfer and application sharing between devices. Wireless functionality also eliminates cables for connecting the printer and other peripherals. Pocket devices such as personal digital assistants (PDAs) and mobile phones, tablets, and small computers enable remote users to synchronize personal databases and provide access to network services such as wireless email, web browsing, and Internet access. Moreover, these technologies can offer significant cost savings and new opportunities for a variety of applications. However, in addition to the pros, there are also risks that come with any wireless technology. Some of these risks are similar to those of a wired network; some are exacerbated by wireless connections; some are new. (Tom Karygiannis, 2002).

### **2.2.1. Accidental association**

Unauthorized access to wireless and wired networks of a large company can happen entirely in different ways and with different intentions. This may not always happen on purpose, but the company's private information may be at risk. This method is called "accidental association." When the user turns on the computer and connects to a wireless access point from an overlapping network of a neighboring company, he may not even know that this has happened. However, it is a security breach in that the company's private information is affected, and a link may exist from one company to another. This is especially true if the laptop is also connected to a wired network. (Min-kyu Choi, 2008).

### **2.2.2. Malicious association**

"Malicious associations" is when wireless devices are intentionally connected to a company's wireless network by attackers to connect to the corporate network through their compromised laptop

instead of company access points. These laptops are known as “soft APs” used when the intruder launches specially crafted software that makes the wireless network card look like a legal access point. Once a cracker has gained access, he can steal passwords, launch so-called attacks on the wired network, or install virus programs. Since wireless networks work Layer 2, Layer 3 security such as network authentication and virtual private networks (VPNs) offer no barriers. 802.1x wireless authentication helps with protection but is still vulnerable to hacking. The idea behind this type of attack could be not about hacking a VPN or other security measures (Min-kyu Choi, 2008).

### 2.2.3. Ransomware

Ransomware is currently one of the most widespread and dangerous threats to businesses and large companies. Historically, ransomware was initially focused on petty theft of funds of individual users. However, with the evolution of technology and the fight against threats, ransomware programs are aimed at large companies to get more profit. The first ransomware was discovered in 1989 and is known as the AIDS Trojan or Computer Cyborg. This ransomware was developed by Dr. Joseph L. Popp (Richardson & North, 2017). This program was created to obtain ransom from personal computers and distributed through third-party downloads over the internet. Although the first ransomware proved to be quite helpful, AdamYoung and Moti Jung took the initiative to present the prototype of asymmetric ransomware in 1996 (Gorman & McDonald, 2012).

One of the first modern ransomware programs called GPCoder was developed and presented to the IT community in 2015. This ransomware was sent through spam email attachments that included job application emails (Richardson & North, 2017). Users who opened attachments were required to pay the ransom. Ransomware is a ransomware strategy. Malicious software is designed to hold a computer system user and even entire servers of large companies’ hostage until the so-called ransom is paid.

It is also not uncommon for theft of classified company data, followed by a ransom demand so that the data is not published on the network. Ransomware attackers are often asked to buy back bitcoin due to the anonymity of encryption transactions. The software blocks users and servers for a limited time, after which the refund or user data is destroyed or published on the network. (A. Tandon, 2019). The importance of my research lies in the timely detection of malware data through the Intrusion detection systems implementation tool.

#### 2.2.4. Procedures to identify the problems

Intrusion into the company's network is extremely dangerous because the personal data of employees and the entire company's database are at risk. This puts ordinary users of the wireless network and the company's system at risk. It is necessary to understand what procedures are used to identify the problem promptly and what intrusion detection systems are worthwhile, are the most effective, convenient to use, and have a reasonable cost of implementation.

### 2.3. Intrusion detection systems

Security is one of the highest priorities for all networks of large companies. Typically, IT departments of businesses and organizations are focused on preventing intrusions into the internal systems. However, with the advancement of technology in terms of protection and security, cyber-crimes have also evolved. (Rebecca Bace, 2001). For instance, fraudsters can provide penetration intrusion into a business' network infrastructure via the internet through firewalls, encryption, et cetera. The intrusion detection system is a detection technology that is widely regarded in developed countries but is still costly for developing nations and industries, e.g., critical infrastructure businesses in the Republic of Kazakhstan. The main purpose of these systems is to detect intrusions into the internal networks of such businesses. (Rebecca Bace, 2001). The role of these detection systems in networks is to assist departments, and computer systems prepare and resolving network attacks. Intrusion detection systems include:

- Monitoring and analysis of user and system actions.

--This means that the threat detection system will monitor communication activity.

- Configuration and vulnerability analysis system

--Threat Detection analyzes and points out internal security gaps.

- Rating system and file honesty.

--Files are continuously scanned, and suspicious files with possible threats are given a low rating.

- Ability to recognize patterns typical of attacks.

--The threat detection systems themselves contain attack patterns created with experience in combating cybercrime.

- Analysis of patterns of abnormal activity.

--As well as templates, exceptional levels of network traffic may indicate a threat to the system's security.

- Tracking violations of user rules.

--Also, if company employees follow a third-party link to dubious sites, the threat detection system detects this, utilizing warnings and blocking to prevent the user from accessing the link (Asmaa Shaker Ashoor, 2011).

The main goal of Intrusion detection systems is to help computer systems and IT departments on how to respond and what decisions to make with attacks on the internal network. The function of these Intrusion detection systems is that these systems collect information from several different sources in computer systems and networks and compare this information with pre-existing patterns written by the system as to whether there are attacks or weaknesses within the network (Inam Ullah, 2014).

Intrusion detection system is classified into two types of intrusion detection: host system and network. Host-Based Intrusion Detection System is a tool used on a network node or a computer connected to the network. The CID scans inbound and outbound traffic to a specific host for signs of malicious activity or threats and generates alarms for specific malware or intrusions found. In large companies and enterprises for the security of internal networks, these host systems are used to send reports to the monitoring site, where analysis and solution, and counteraction of these problems take place. A network intrusion detection system is a device that connects to a network like a network protocol analyzer, or “sniffer,” as it is commonly called.

### 2.3.1. Principle of operation of Intrusion Detection Systems

A network intrusion detection system is not just about capturing a threat and checking data for malware or intrusion threats. The network intrusion detection system monitors the entire network traffic and sends an alarm to the monitoring node for further actions when an intrusion is detected.

Deployment of multiple network intrusion detection systems in the enterprise at critical network nodes (Eugene Albin, 1995, p 12).

One of the main steps in detecting SID attacks is non-anomaly. This method is because the attack on a computer system will usually differ markedly from the regular operation of a computer system. A cybercriminal will exhibit a behavior pattern that will not resemble the behavior pattern of an ordinary, average network user. The knowledge base of computer system security is also used to timely identify threats to network security. It contains all the known experiments with the detection of illegal use of a computer network, as well as a set of most of the known methods of intrusion into a computer network.

The Intrusion detection systems stores these methods in its knowledge base, and when it invades the network, it detects threats by searching the knowledge base. Intrusion detection systems can detect two critical errors, false-positive errors, and false-negative errors. A false-negative error is a compulsive behavior defined by intrusion detection systems as normal user behavior. In contrast, the false-positive error is legitimate user behavior being considered Intrusion detection systems as compulsive behavior. (E. Biermann, 2001).

### 2.3.2. Detection Methodology

Imagine an analogy with a general " burglar alarm " to describe the concept of intrusion detection and external threat detection. Imagine an analogy with a general "burglar alarm"<sup>1</sup>. It is a computer system or network that detects possible security policy violations and raises the alarm to notify the appropriate authorities. This system is called SSO, short for 'Site Security Over.' Some of the same problems, "false-positives" and bypassing burglar alarms, are common to both types of intrusion detection systems. (Axelsson. 1998, p.43) Unfortunately, one system cannot deal with absolutely every intrusion threat. For example, even the most sophisticated attacker will bypass alarms since the system operates under a much simpler security policy. All user activity is checked by monitoring any user activity that can be interpreted as suspicious. If the computer system detects every

---

<sup>1</sup> Burglar alarm/intrusion alarm" is similar to an intrusion detection system.



legitimate intrusion attempt accurately, the problem would be solved much faster and more efficiently. Intrusion and threat detection methods fall into three main categories:

- Detection based on signatures (SD)
- Anomaly based detection (AD)
- Stateful Protocol Analysis (SPA)

These can further be divided and compared according to Table 1 below.

**Table 1: Pros and cons of intrusion detection methodologies.**

<b>Signature-based (knowledge-based)</b>	<b>Anomaly-based (behavior-based)</b>	<b>Stateful protocol analysis (specification-based)</b>
<p data-bbox="183 952 207 985">+</p> <ul style="list-style-type: none"> <li>● Simplest and effective method to detect known attacks.</li> <li>● Detail contextual analysis.</li> </ul>	<p data-bbox="609 952 633 985">+</p> <ul style="list-style-type: none"> <li>● Effective to detect new and unforeseen vulnerabilities.</li> <li>● Less dependent on OS.</li> <li>● Facilitate detections of privilege abuse.</li> </ul>	<p data-bbox="1050 952 1074 985">+</p> <ul style="list-style-type: none"> <li>● Know and trace the protocol states.</li> <li>● Distinguish unexpected sequences of commands.</li> </ul>
<p data-bbox="183 1355 207 1388">-</p> <ul style="list-style-type: none"> <li>● Ineffective to detect unknown attacks, evasion attacks, and variants of known attacks.</li> <li>● Little understanding to states and protocols.</li> <li>● Hard to keep signatures/patterns up to date.</li> </ul>	<p data-bbox="609 1355 633 1388">-</p> <ul style="list-style-type: none"> <li>● Weak profiles accuracy due to observed events being constantly changed.</li> <li>● Unavailable during rebuilding of behavior profiles.</li> <li>● Difficult to trigger alerts in right time.</li> </ul>	<p data-bbox="1050 1355 1074 1388">-</p> <ul style="list-style-type: none"> <li>● Resource consuming to protocol state tracing and examination.</li> <li>● Unable to inspect attacks looking like benign protocol behaviors.</li> <li>● Might incompatible to dedicated OSs or APs.</li> </ul>

<ul style="list-style-type: none"> <li>• Time consuming to maintain the knowledge.</li> </ul>		
---	--	--

Table 1 shows the advantages and disadvantages of intrusion detection methodologies. (Axelsson, 2000).

### 2.3.3. Intrusion detection system for the Large Companies

For many large and small companies, online workflow control is an integral part of their business. Computers and servers' control national infrastructure components such as the power grid. The integrity and availability of all these systems must be protected from a variety of threats that can potentially disrupt the stable operation of the company. Amateur hackers, competing corporations, non-state actors, and even foreign governments can carry out sophisticated attacks on computer systems. (Ahmed Patel, 2010). This means that information, databases, and communications security have become critical to large companies' security and economic well-being in general. It follows that to detect confidentiality violations, it is necessary to ensure security by implementing effective intrusion detection and prevention systems. In the following sections, 2.4.1.a.—2.4.1.c, offers a review of the most popular and effective intrusion detection systems.

#### 2.4.2.a. Snort Intrusion detection system

*Snort* plays one of the most important network security roles in the market for intrusion detection systems. This system is an affordable and lightweight network intrusion detection tool that can be deployed to monitor medium TCP / IP networks and detect a wide range of suspicious network traffic, network intrusions, and outright attacks in time. (Martin Roesch, 1999). He can provide the network department of the company with enough necessary information to make the necessary decisions promptly to eliminate the network threat in the event of suspicious activity. *Snort* also exists to fix flaws in network security when new potential intrusions are noticed. *Snort* is a system for small to medium-sized networks with a small number of users. *Snort* is used when it would be

impractical to use expensive commercial Intrusion detection systems sensors. *Snort* is a relatively inexpensive intrusion defense system.

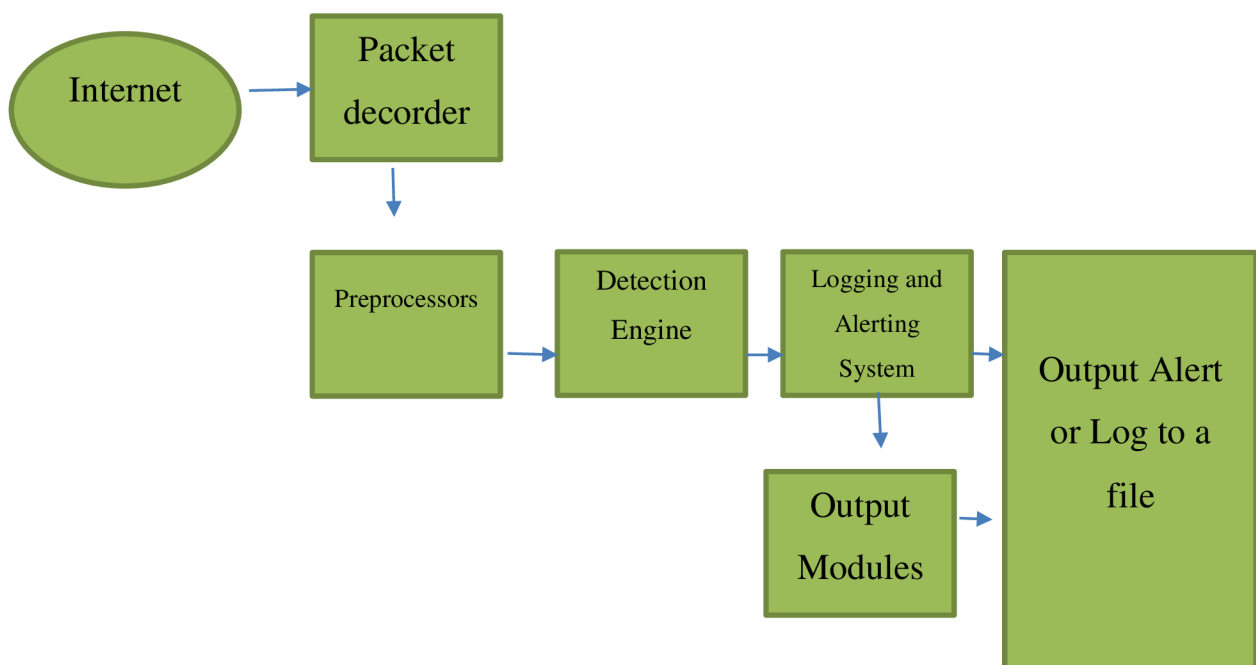
Compared to other systems, but the issue of security is paramount. *Snort* is an open-source network intrusion detection system and prevention system. This system analyzes traffic and data flow in networks in real-time, monitoring and analyzing the protocol and timely detecting other types of attacks. *Snort* rules can be written in any language, the structure of *SNORT* is convenient and easy to read, and rules can also be customized and adapted for users. (Wonhyung Park, 2018). Due to the extensive buffer, *SNORT* can compare the threat with previous templates during an attack, which will allow systematically taking measures to prevent an attack. The system analyzes the threat codes, and if the threat coincides with the previous templates, the solution is easy. *Snort* analyzes the traffic in real-time and finds the key to solving the problem if the attack is new. Additionally, after solving the problem and preventing the threat, *Snort* writes this package of solutions to its database to counter similar threats in the future.

*Snort* is essentially a combination of several components. All components work together to find a specific attack and then take the appropriate action required for that particular attack. (Vivek Kumar Singh, 2018). The main components of *Snort* include:

1. Batch decoder
2. Preprocessors
3. Detection mechanism
4. Registration and notification system
5. Output modules

It consists of the following major components shown in figure 1.

**Figure 1: *Snort* Intrusion Detection System components.**



Source: (Eugene Albin, 2011).

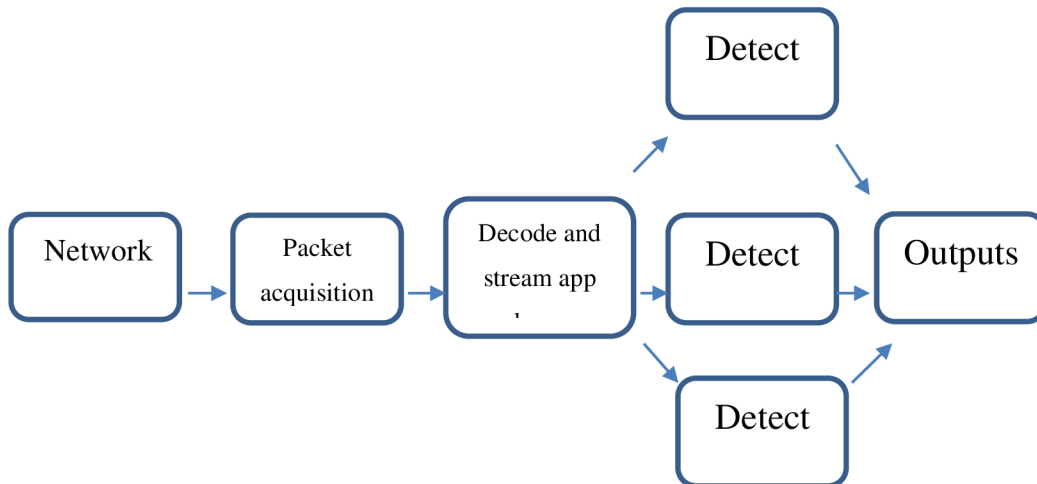
Figure 1 shows the main components involved in the *Snort* intrusion detection process. It is initiated by the packet decoder, which collects packets from the network and sends them to the preprocessor for the required layout modifications. The detection engine detects any anomaly based on the defined *Snort* rules, generates alerts, and logs messages to users. (Vivek Kumar Singh, 2018).

#### 2.4.2.b. *Suricata* Intrusion detection system

*Suricata* is a high-performance Network Intrusion detection system, IPS and Network Security Monitoring engine. It is open source and owned by a community-run non-profit foundation, the Open Information Security Foundation (OISF). *Suricata* was developed by the Open Information Security Foundation. By allowing multiple threads to be contained in a single discovery engine, a multi-threaded discovery engine can make intelligent decisions about splitting processing and coordinating signature detection between these threads within a single detection engine. Multi-threaded processing can take advantage of this prediction. According to the Nielsen internet bandwidth law, there is also a 50% increase in network bandwidth each year (Nielsen, 2010).

The performance of our intrusion detection systems should increase as our demand for network bandwidth is also increasing. *Suricata* developers decided to contact multi-threaded processing requires this (OISF, 2011a). Considering that the most resource-intensive work performed intrusion detection engine - detection, *Suricata* developers decided to use threads for detection. Figure 3 shows an example of creating three discovery streams. *Suricata* can receive network traffic from a network card or previously recorded network traffic from a file stored in PCAP format. Figure 2 shows an example of creating three discovery streams.

**Figure 2: *Suricata* Intrusion Detection System components.**



Source: Eugene Albin, 2011.

A *Suricata* can receive network traffic from a network card or previously recorded network traffic from a file stored in PCAP format. The traffic goes through decoding. The module is first decoded according to its protocol, and then the streams are reassembled before being distributed among the signature detection modules (Albin, Eugene, 2011).

#### 2.4.2.c. *Bro* (Zeek) Intrusion Detection System

*Bro* - This is a network intrusion detection system, also known as Zeek. It was initially written by Vern Paxson of Lawrence Berkeley National Laboratory and International Institute of Computer Science. *Bro* is an open-source UNIX (a family of portable, multitasking, and multi-user operating systems)-based Network Intrusion Detection System (NIDS) that monitors network traffic looking for suspicious activity. (Miguel A. Calvo Moya, 2008). Real-time notification is one of the best things about *Bro*. One of the significant disadvantages of past threat and intrusion detection is the lack of real-time intrusion control and the long delay before an attack is detected. If an attack is detected, it will be much easier to track down the attacker by tracking the site traffic. It also allows users to minimize damage, prevent further break-ins and maintain a record of all network activities (Vern Paxson, 1999).

The way *Bro* works is that *Bro* detects intrusions by first analyzing network traffic to extract application-level resonances and then running event-driven analyzers that compare activity against pre-defined patterns that are considered problematic. (Miguel A. Calvo Moya, 2008). *Bro* was initially developed as a research platform for intrusion detection and traffic analysis and has since earned a reputation for being a good intrusion detection system with its protocol and ingress analysis functionality that monitors servers' security status and stability in real time. This is a very useful criterion for implementing an intrusion detection system in a large company.

Another difference between *Bro* and his intrusion detection counterpart is that *Bro* also works like an IDS by adding a network-based detection / analysis plugin. It's worth noting that, originally, *Bro* was designed as an academic toolbox, so usability was rather poor prior to version 2.0. However,

starting with version 2.0, *Bro* switched to another job and hired dedicated software engineers to optimize the system and improve quality and usability. (Hendra Gunadi, 2017).

**Figure 3: *Bro* Intrusion Detection system Components**



Source: Vivek Kumar, 2014

Figure 3 shows the main components involved in the process of *Bro*'s work. It initiates capturing and filtering packets from the network and sending the remaining packets to the event engine. The event engine performs various integrity checks by checking the checksum of IP headers and handles the parsing of specific protocols such as DNP3. The generated events are sent to the policy layer, which analyzes packets to detect anomalies and generates alerts and actions based on scripts/rules. (Vivek Kumar, 2014).

### 3. Practical part

This section of thesis provides an explanation of the methodologies used to ascertain the best IDS for the case sample: *Kaztransoil*. The section is divided into several parts and offers a logical progression of ideas that led to the analysis and results.

#### 3.1. Special market research

The purpose of the practical part of the research is to determine the necessary criteria for the safe operation of the company's departments and to compare the technical characteristics and functional components of the three information security systems. Data analysis using two methods: *Multi-criteria decision analysis* and *scoring method* based on case study -- *Kaztransoil*. This company is a critical infrastructure business in the Republic of Kazakhstan that requires a robust intrusion

detection system to maintain continuity of operations. *Kaztransoil* is an oil drilling company that exports petroleum fuels globally from Kazakhstan.

### 3.2. Methodology

In the first part of my research, a focus group discussion will be conducted to identify and select the criteria and technological configurations of the three intrusion detection systems necessary for further comparison. 7 employees of the IT department of *Kaztransoil* will participate in the focus group discussion. These employees work closely with the information security of all departments of *Kaztransoil*. Their opinion will be considered expert and will allow me to competently identify the necessary criteria and technological configurations of three intrusion detection systems for further comparison of these criteria. This method was chosen because it is easy to implement and also in the course of a lively discussion between representatives of the company's information security, it will be possible to make the most correct and necessary criteria. The focus group discussion will be done via skype.

In the second part of my research, I will empirically analyze the parameters of intrusion detection systems, which will be derived from the focus group discussions required for optimal performance of departments. And after collecting the necessary data, a scoring analysis will be carried out to understand the necessary configurations and characteristics of threat detection systems for the stable operation of the company's divisions. The circle of respondents will include 20 people from 4 departments of *Kaztransoil* - 5 employees of the energy department, 5 employees of the dispatch department, 5 employees of the information technology department and 5 employees of the procurement department. The *scoring method* will enable the correct calculate the results, taking into account the percentage of need for all investigated configurations.

The third part of the thesis will be based on a comparison of the three information security systems by examining technical characteristics and configurations. The analysis of decision making according to the criteria will result in a comparison of the intrusion detection software that *Kaztransoil* can utilize to protect it's business. This can further be applied to other critical infrastructure businesses in Kazakhstan.



The analysis dealt with three alternative threat detection systems. Each of these systems has its own characteristics, which may differ fundamentally from the characteristics of another company. One threat detection system may spend a certain amount of time on operations, while another may spend less time on processes, although it may use more CPU. All criteria must be considered and how they will communicate with each other. All three threat detection systems are generally suitable for a large company, but my analysis should show which of these three systems is the most optimal and suitable for a large company using *Kaztransoil* as an example. For the third part of my research, *Multi-Criteria Decision Analysis*, or MCDA, was chosen.

*Multi-Criteria Decision Analysis* is a method excellent for solving problems when choosing between several relatively similar but conflicting alternatives. This analysis method contains all the essential details of a useful tool that will help me make objective and fair decisions. I can focus on which truth is useful, logical, and relatively easy to use it. For the most part, multi-criteria decision analysis is required to:

- Divide the solution into smaller and more understandable parts.
- Analysis of each individual part and parameters.
- Integration of parts for a meaningful solution.

When used for group decision making, multi-criteria decision analysis helps groups to discuss the possibility of deciding (the problem that needs to be solved) so that they can take into account the values that everyone considers important. It also gives people a unique opportunity to consider and discuss difficult trade-offs between alternatives. Basically, it helps people think, rethink, query, tune, make decisions, rethink something else, test, tweak, and finally make decisions. (G.A. Mendoza, 2006)

### **3.3. Focus Group Discussion**

The circle of participants in the focus group discussion consisted of 7 employees of the IT department of the oil company *Kaztransoil* in the city of Nur-Sultan in the Republic of Kazakhstan. The discussion took place through discussion in a joint conversation on Skype. Inclusion criteria: the

interviewee should be closely related to information security in the company. Age and gender don't matter. The purpose of the discussion was to identify the main criteria and technological configurations for the selection and implementation of an intrusion detection system in a large company. The focus group meetings lasted about 40 minutes, of which 30 minutes were spent in group discussions. 10 minutes the study procedures were described. The participants agreed to participate in the discussion but wished to remain anonymous for security reasons.

### 3.3.1. Organizing Focus Group Material and Defining a Unit of Analysis

For the convenience of data processing, video recordings of focus groups were carried out, and then converted into a written text format by their full transcription into English. Questions and comments group facilitators were included to test their neutrality. No verbal behavior of the participants and no sounds or pauses was deciphered. (F.Moretti, 2011).

### 3.3.2. Focus-Group Questions

Several questions were developed for the focus group. The main goal of the focus group discussion is the most necessary technological parameters and characteristics of intrusion detection systems for introducing these systems into a large company. The questions were divided into 3 parts. The first part is the technological characteristics of intrusion detection systems that are responsible for the performance and usefulness of intrusion detection systems data to the resources of the systems of a large company. The second part was responsible for the usability of this intrusion detection system. For the third part, secondary characteristics such as price, country of production, year of production, and so on were responsible.

The factors influencing the choice of intrusion detection systems were divided into 3 levels of importance. The respondents noted that the most important factors are technological configurations and characteristics. Because this is the main goal of implementing these systems in a large company. Without the effectiveness of these intrusion detection systems, their implementation would be pointless.

The most important criteria in the opinion of the respondents were described. First is **the usefulness of the time-period**. *"For information security in a large company, the usefulness of the information security systems involved is important. During a certain period of time, there may be a different number of attacks and threats, and in turn, each intrusion detection system may have a different usefulness over a certain period of time."* the employee wished to remain anonymous. Also, **power (the number of cores)** plays an equally important role. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system.

The respondents also mentioned **the speed of information processing**. *"For information security in a large company, not only the power, but also the speed of the security system is important. Every minute, a huge amount of information passes through the ports of the company's servers. Intrusion detection systems need to quickly respond and fight threats and attacks using an intrusion detection system."* -- the employee wished to remain anonymous.

In each company and in each separate department, different system platforms of personal computers can be used. *"If, for example, the intrusion detection system does not support Linux, but supports HP, and in some department only Linux is used, then this will cause IT departments and the company as a whole a lot of trouble. It may be decided to use two intrusion detection systems, which will also lead to a waste of funds from the company's budget."* - The employee wished to remain anonymous.

Therefore, **cross-platform support** is also important. Also, respondents note **resource usage**, as it is also important to pay attention to the importance of economical use of intrusion detection system for RAM and server resources. From the secondary criteria and from the convenience for the company, the respondents noted **the price and the interface**.

The price is not always important to the company, since almost every company will spare no expense to ensure the company's security, but it will still be analysed in further analysis. As for the interface, respondents noted that mostly only IT department employees deal with intrusion detection systems. And basically, professional employees of the IT department know how to handle any of them and the convenience for them does not matter, it is another matter if an unprepared employee is faced with these systems. Therefore, the interface will also be analysed in further analysis.

### 3.4. EMPIRICAL ANALYSIS

#### 3.4.1. Research Approach

To determine the required configurations and requirements for intrusion detection systems in a large company, I took a quantitative approach. The quantitative approach makes it possible to establish a connection between the purpose of the study and the collection of data about the empire from a certain circle of people surveyed. (March 1925). The choice of a quantitative approach is associated with the need to attract a larger number of interviewed company employees to determine the necessary requirements for threat detection systems for stable operation in their structures.

#### 3.4.2. Target population

To collect empirical data, it was decided to interview four departments of *Kaztransoil*. Such as supply department, dispatch department, energy department and information technology department. These departments are closely related to information and databases. The data servers of the departments store a lot of classified information and more. And this information is carefully guarded, and it is important that network security personnel can not only quickly and efficiently eliminate threats and attacks, but also can detect them in time. *Kaztransoil* was chosen because it is a large company with many employees and new information security technologies.

Additionally, to authorize this survey, 4 letters were sent to the heads of each of the aforementioned departments. A total of 20 employees were interviewed, 5 for each separate department out of 4. The interview was conducted in the form of a prepared questionnaire for each of the employees.

#### 3.4.3. Questionnaire Design

At the heart of any survey is the questionnaire. The results of the survey are critically dependent on the correctly drawn-up questionnaire. In developing the questionnaire, various approaches and methods were explored to design the questionnaire's structure in social research. Additionally, when designing the questionnaire, the work of John A. Krosnik (2010) was relied on to minimize errors in

responses. Thus the questionnaire was developed by best practices highlighted by Krosnik concerning focus group questionnaires frequently used in qualitative work.

The completed questionnaire was consistent and straightforward and did not include such variables as gender and age since it does not matter; only the profession and position of the respondent are necessary for the questionnaire. The questionnaire consists of two parts. The questions will have both open and closed questions and will be measured by rating scales. The first part consists of questions 1-3; primary and secondary questions serve as descriptive clarifications. These questions include name, position, profession, and department in which the employee works. Position and Department are essential in analyzing results because it is necessary to understand what types of data a given employee is dealing with and the extent to which threat detection systems are, used in their work structure. The questions in this part are open-ended since there is a calculation of the individual answers of each respondent.

Then there are questions 4-7 about the importance of introducing threat detection systems into the company and potential threats. Next, questions 8-14 provided variables. It will be necessary to determine the importance of the performance characteristics of the threat detection systems, technical configurations, and criteria for the performance of the IDSs. To determine by what criteria to compare threat detection systems.

#### 3.4.4. Collecting data

The closed-ended questions should determine which technical characteristics should play a critical role in choosing the best and optimal intrusion detection system. Respondents are given 7 characteristics and technical configurations of intrusion detection systems. Their task with a rating from 1-5 to determine the degree of importance of this configuration for the effective work of their profession and their department. In the Likert scale (1932), 5 points are most often used; Osgood, Suci and Tannenbaum's semantic differential (1957) uses 7 points; and Thurston (1928). For my questionnaire, I chose the Likert rating scale (1932). Where 1 is irrelevant and 5 is extremely important. During the study, 25 copies of questionnaires were made in the form of a paper questionnaire, where 5 in case of damage to one of the copies. These questionnaires were distributed to 20 employees from 4 different departments of the company. The results are listed in Table 2.

In table 2, we can see the ordered answers of each of the respondents, we are not interested in names, as well as gender and age. For a clear understanding of their field of activity, it is necessary to know their department and occupation, namely the position held in the company. Posts should be tightly connected with databases and information because it is on the databases, as we know from the Literary Part, that attacks are made in many cases.

**Table 2: Closed-ended interview questions and answers**

Position	Department	Usefulness of period of time	Interface	Power (Number of Cores)	The speed of processing	Price	Cross-platform support	The Use of Recourse
Head of Energy Department	the energy department	5	1	5	5	1	4	5
Human resource manager	the energy department	4	2	5	5	1	4	5
Administrator	the energy department	5	1	5	5	1	5	4
Workflow manager	the energy department	5	3	5	5	3	5	5

Manager	the energy department	4	1	4	5	1	5	4
Head of Dispatch control Department	the dispatch control department	4	1	4	5	1	4	5
Human resource manager	the dispatch control department	5	2	5	5	1	5	4
chief dispatcher	the dispatch control department	4	2	4	5	2	4	4
dispatcher	the dispatch control department	4	1	4	4	1	4	5
manager	the dispatch control department	5	4	4	5	2	4	4
Database administrator	the information technology	5	1	5	5	2	5	5

	department							
Computer network administrator	the information technology department	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>
Security administrator	the information technology department	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>
Software Analyst	the information technology department	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>	<b>2</b>	<b>5</b>	<b>5</b>
Software architect	the information technology department	<b>5</b>	<b>1</b>	<b>5</b>	<b>5</b>	<b>2</b>	<b>5</b>	<b>5</b>
Head of procurement Department	the procurement department	<b>3</b>	<b>2</b>	<b>4</b>	<b>4</b>	<b>1</b>	<b>4</b>	<b>5</b>



supplier	the procurement department	4	3	3	4	2	4	5
Administrator	the procurement department	5	2	4	5	1	5	5
HR Manager	the procurement department	5	2	3	4	1	4	5
accountant	the procurement department	5	2	3	5	2	5	5

Table 2. It is worth taking a closer look at each of the characteristics I have proposed.

1. **Usefulness of the time period** - For information security in a large company, the usefulness of the information security systems involved is important. There may be a different number of attacks and threats detected over a period, in turn, each Intrusion detection system may have a different usefulness over a period of time, how important it is for the company to be assessed by the respondents (score according to scale 1-5).
2. **Interface.** At this point, respondents assess how important it is for the Intrusion detection system to have a convenient and simple interface (score according to scale 1-5).

3. **Power** (number of cores) - The number of cores used by the Intrusion detection system increases the power and efficiency of the Intrusion detection system, the question is how important it is for the company (score according to scale 1-5).
4. **Speed of processing** - For information security in a large company, not only the power is important, but also the speed of the security system. A huge amount of information passes through the ports of the company's servers every minute. And the question is how important it is to respond quickly and handle threats and attacks with an Intrusion detection system (score according to scale 1-5).
5. **Price** - respondents are also asked to answer whether price is important in choosing Intrusion detection system (score according to scale 1-5).
6. **Cross-platform support.** - This paragraph is devoted to how important it is for a company to support the Intrusion detection system for various platforms such as Linux, HP, Apple, et cetera (score according to scale 1-5).
7. **Resource Usage** - This section focuses on the importance of economical use of Intrusion detection system for RAM and server resources. (1-5).

### 3.5. The Weighted Scoring Method

The weighted appraisal method exists to prioritize the analysis of multiple conflicting criteria based on empirical assessments. This method was chosen to extract the highest-priority technical configurations and characteristics for comparison in more detail in the second part of the practical work. Using this method enabled the researcher to highlight the highest priority functions and characteristics of threat detection systems.

#### 3.5.1. The Weight percentage

No two criteria are of equal importance, which proves the usefulness of the weighted model. Before making calculations, assigning weight values to each criterion is necessary, which means that a

‘weight’ is the percentage of priority of a particular value. To understand what percentage of weight is assigned to which criteria have, the practical part was informed by the writings of Nicholas Morpus (2021). In these, he assessed the weight percentages for the software. The weight estimates in the software are weighted as follows:

- Usefulness and ease of use (40%)
- Support (20%)
- Price (20%)
- Features (20%)

As you can see, we rate the ease of use at 40%, while the other four categories are at 20%, which gives ease of use more room to influence the overall rating. (Morpus, 2021). In my case, usefulness includes criteria such as the ‘Usefulness of Period of Time,’ ‘Power‘ (Number of Cores), the ‘Speed of Processing,’ the ‘Use of Recourse,’ and ease of use or ‘Cross-platform support and Interface.’ This means that these criteria will have equal weight, and only the price of the instruction detection systems has a lower percentage of weight. The final weight estimate for each criterion will be 15 percent, while the price is 10 percent. The weight of the scoring method is organized from left to right in Table 3, where each factor is divided evenly to account for the true value of each criteria according the corresponding IDS. For instance, “speed of processing” and interface are weighed equally but scored according to a scale of 1-5 depending on the responses in the focus group. See Table 3 for a breakdown of the percentages relative to the criteria.

**Table 3: Weight determination for the weighed scoring method**

	The weight	15%	15%	15%	15%	10%	15%	15%
Position	Department	Usefulness of period of time	Interface	Power (Number of	The speed of processing	Price	Cross-platform support	The Use of Recourse

				Cores)				
Head of Energy Department	the energy department	5	1	5	5	1	4	5
Human resource manager	the energy department	4	2	5	5	1	4	5
Administrator	the energy department	5	1	5	5	1	5	4
Workflow manager	the energy department	5	3	5	5	3	5	5
Manager	the energy department	4	1	4	5	1	5	4
Head of Dispatch control Department	the dispatch control department	4	1	4	5	1	4	5
Human resource manager	the dispatch control department	5	2	5	5	1	5	4
chief dispatcher	the dispatch control department	4	2	4	5	2	4	4

dispatcher	the dispatch control department	4	1	4	4	1	4	5
manager	the dispatch control department	5	4	4	5	2	4	4
Database administrato r	the informatio n technology department	5	1	5	5	2	5	5
Computer network administrato r	the informatio n technology department	5	1	5	5	1	5	5
Security administrato r	the informatio n technology department	5	1	5	5	1	5	5
Software Analyst	the informatio n technology	5	1	5	5	2	5	5

	department							
Software architect	the information technology department	5	1	5	5	2	5	5
Head of procurement Department	the procurement department	3	2	4	4	1	4	5
supplier	the procurement department	4	3	3	4	2	4	5
Administrator	the procurement department	5	2	4	5	1	5	5
HR Manager	the procurement department	5	2	3	4	1	4	5
accountant	the procurement department	5	2	3	5	2	5	5

### 3.5.2. Calculations analysis

Now that all the variables and weights have been entered into the table, it is possible to calculate and find the total scores for each parameter. To do this, the researcher multiplied each rating by its weight and then added them together and got the overall ratings for each criterion, e.g., see table 4.

**Table 4: The Weighted Scoring Methods Calculations**

	The weight	15%	15%	15%	15%	10%	15%	15%
Position	Department	Usefulness of period of time	Interface	Power (Number of Cores)	The speed of processing	Price	Cross-platform support	The Use of Recourse
Head of Energy Department	the energy department	5*0,15= 0,75	1*0,15= 0,15	5*0,15= 0,75	5*0,15= 0,75	1*0,1= 0,1	4*0,15= 0,6	5*0,15= 0,75
Human resource manager	the energy department	4*0,15= 0,6	2*0,15= 0,3	5*0,15= 0,75	5*0,15= 0,75	1*0,1= 0,1	4*0,15= 0,6	5*0,15= 0,75
Administrator	the energy department	5*0,15= 0,75	1*0,15= 0,15	5*0,15= 0,75	5*0,15= 0,75	1*0,1= 0,1	5*0,15= 0,75	4*0,15= 0,6
Workflow	the	5*0,15=	3*0,15=	5*0,15=	5*0,15=	3*0,1=	5*0,15=	5*0,15=

manager	energy department	<b>0,75</b>	<b>0,45</b>	<b>0,75</b>	<b>0,75</b>	<b>0,3</b>	<b>0,75</b>	<b>0,75</b>
Manager	the energy department	<b>4*0,15=0,6</b>	<b>1*0,15=0,15</b>	<b>4*0,15=0,6</b>	<b>5*0,15=0,75</b>	<b>1*0,1=0,1</b>	<b>5*0,15=0,75</b>	<b>4*0,15=0,6</b>
Head of Dispatch control Department	the dispatch control department	<b>4*0,15=0,6</b>	<b>1*0,15=0,15</b>	<b>4*0,15=0,6</b>	<b>5*0,15=0,75</b>	<b>1*0,1=0,1</b>	<b>4*0,15=0,6</b>	<b>5*0,15=0,75</b>
Human resource manager	the dispatch control department	<b>5*0,15=0,75</b>	<b>2*0,15=0,30</b>	<b>5*0,15=0,75</b>	<b>5*0,15=0,75</b>	<b>1*0,1=0,1</b>	<b>5*0,15=0,75</b>	<b>4*0,15=0,6</b>
chief dispatcher	the dispatch control department	<b>4*0,15=0,6</b>	<b>2*0,15=0,30</b>	<b>4*0,15=0,6</b>	<b>5*0,15=0,75</b>	<b>2*0,1=0,2</b>	<b>4*0,15=0,6</b>	<b>4*0,15=0,6</b>
dispatcher	the dispatch control department	<b>4*0,15=0,6</b>	<b>1*0,15=0,15</b>	<b>4*0,15=0,6</b>	<b>4*0,15=0,6</b>	<b>1*0,1=0,1</b>	<b>4*0,15=0,6</b>	<b>5*0,15=0,75</b>



manager	the dispatch control departm ent	$5*0,15=$ <b>0,75</b>	$4*0,15=$ <b>0,6</b>	$4*0,15=$ <b>0,6</b>	$5*0,15=$ <b>0,75</b>	$2*0,1=$ <b>0,2</b>	$4*0,15=$ <b>0,6</b>	$4*0,15=$ <b>0,6</b>
Database administr ator	the informat ion technolo gy departm ent	$5*0,15=$ <b>0,75</b>	$1*0,15=$ <b>0,15</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>	$2*0,1=$ <b>0,2</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>
Computer network administr ator	the informat ion technolo gy departm ent	$5*0,15=$ <b>0,75</b>	$1*0,15=$ <b>0,15</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>	$1*0,1=$ <b>0,1</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>
Security administr ator	the informat ion technolo gy departm ent	$5*0,15=$ <b>0,75</b>	$1*0,15=$ <b>0,15</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>	$1*0,1=$ <b>0,1</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>
Software Analyst	the informat ion	$5*0,15=$ <b>0,75</b>	$1*0,15=$ <b>0,15</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>	$2*0,1=$ <b>0,2</b>	$5*0,15=$ <b>0,75</b>	$5*0,15=$ <b>0,75</b>

	technology department							
Software architect	the information technology department	5*0,15= 0,75	1*0,15= 0,15	5*0,15= 0,75	5*0,15= 0,75	2*0,1= 0,2	5*0,15= 0,75	5*0,15= 0,75
Head of procurement Department	the procurement department	3*0,15= 0,3	2*0,15= 0,3	4*0,15= 0,6	4*0,15= 0,6	1*0,1= 0,1	4*0,15= 0,6	5*0,15= 0,75
supplier	the procurement department	4*0,15= 0,6	3*0,15= 0,45	3*0,15= 0,45	4*0,15= 0,6	2*0,1= 0,2	4*0,15= 0,6	5*0,15= 0,75
Administrator	the procurement department	5*0,15= 0,75	2*0,15= 0,3	4*0,15= 0,6	5*0,15= 0,75	1*0,1= 0,1	5*0,15= 0,75	5*0,15= 0,75
HR	the procure	5*0,15=	2*0,15=	3*0,15=	4*0,15=	1*0,1=	4*0,15=	5*0,15=

Manager	ment departm ent	<b>0,75</b>	<b>0,3</b>	<b>0,45</b>	<b>0,6</b>	<b>0,1</b>	<b>0,6</b>	<b>0,75</b>
Accountant	the procure ment departm ent	<b>5*0,15= 0,75</b>	<b>2*0,15= 0,3</b>	<b>3*0,15= 0,45</b>	<b>5*0,15= 0,75</b>	<b>2*0,1= 0,2</b>	<b>5*0,15= 0,75</b>	<b>5*0,15= 0,75</b>
	Score:	<b>13,65</b>	<b>4,95</b>	<b>13,05</b>	<b>14,4</b>	<b>2,7</b>	<b>13,65</b>	<b>14,25</b>

### 3.5.3. Discussion

After completing the weighted score calculation, the following results were found:

1. *The speed of processing- 14,4 %*
2. *The Use of Recourse- 14,25 %*
3. *The usefulness of period of time- 13,65 %*
4. *Cross-platform support- 13,65 %*
5. *Power (Number of Cores)- 13,05 %*
6. *Interface- 4,95 %*
7. *Price – 2,7 %*

As shown above, the technological configurations and functionality have a significantly higher priority for users of threat detection systems. The first 5 positions in the ranking are very close to each other in terms of values; these are conflicting criteria. In turn, the interface and the price are categorically lagging behind the other compared criteria. This means that these points are irrelevant for the company's employees. This is explained by the fact that the interface is unnecessary because

the threat detection systems are tightly managed and maintained by IT staff who know how to use almost any threat detection system. The same goes for the price because resources for information security are allocated from the company's budget. The company is large, and therefore, the company spares no resources for the stable and secure operation of the servers. This means that further analysis will compare the first five criteria and configurations of threat detection systems in the market.

### 3.6. Analyzing Data for Multi-Criteria Decision Analysis

This section explains the criteria by which the decision-making process of MCDA based.

- ***Time of processing***

For information security in a large company, power and the speed of the security system are essential. A considerable amount of information passes through the ports of the company's servers every minute. In addition to reliability, the system must correctly filter much information without losing filtering quality. To further inform the research design of the practical part, the researcher relied on the results of a similar experiment done at the University of Informatics in Oslo, Norway. Due to the limitations of the project herein (IDS testing is costly and time-consuming), the results from this experiment serve as a secondary reference of data to support the analysis in this thesis.

The first experiment was to run *Snort*, *Bro*, and *Suricata* simultaneously so that they could analyse and filter the same amount of information being fed to server ports. They were launched simultaneously and were set to run for four days. The files ended up being 40 GB in size, and with this file, three IDSs were launched (*Jonas Tafto Rodfoss, 2011*).

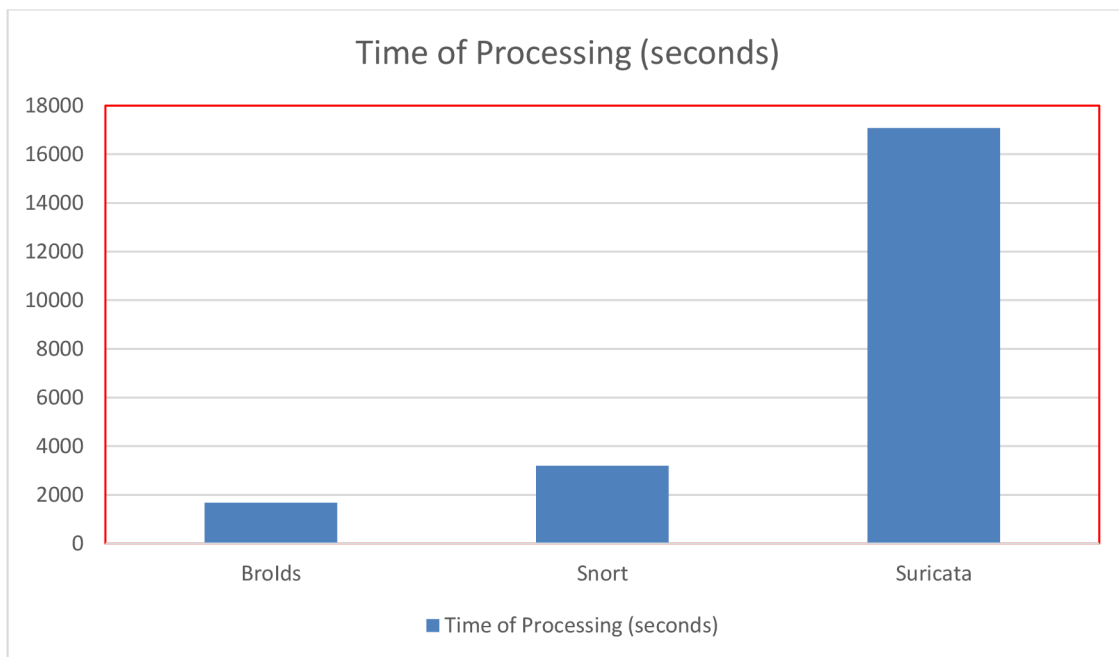
- *Bro* used **27 minutes 51 seconds= 1671 seconds.**

- *Snort* consumed **53 minutes 19 seconds = 3199 seconds.**

- *Suricata* used **4 hours 44 minutes 37 seconds.**

In Figure 4, the results are displayed in a chart that accounts for the time in seconds the IDSs took to analyze and filter the same amount of information fed via the server ports.

**Figure 4: Time of processing testing results in a chart**

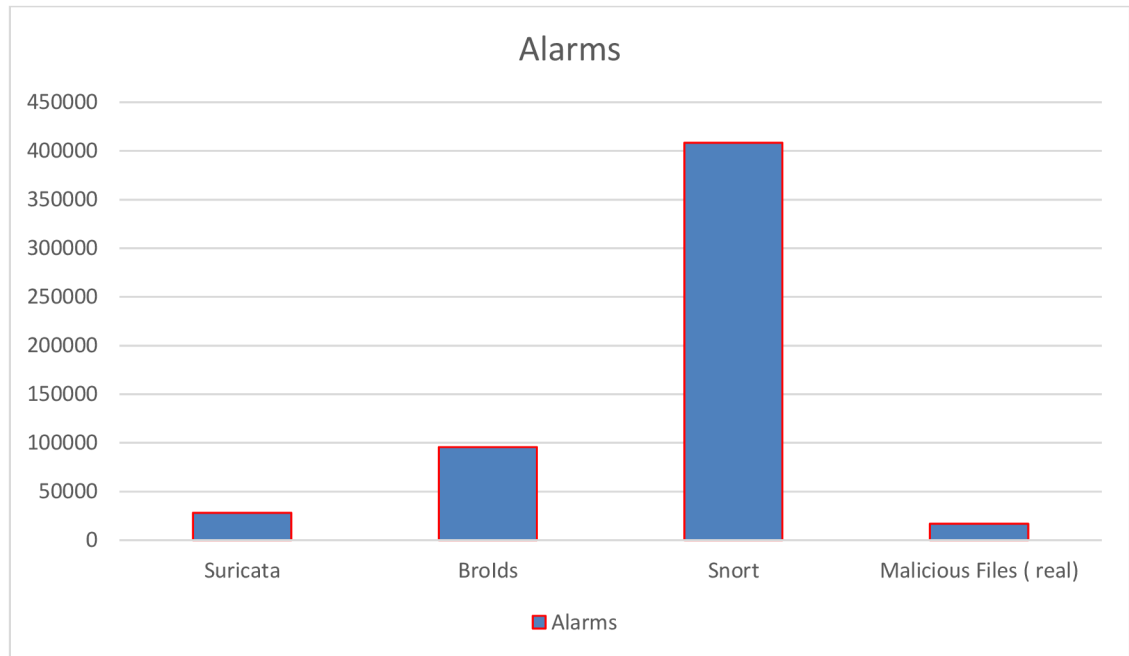


- ***Usefulness over period of time***

Processing 40 GB of files specially prepared for verification took a significant amount of time, overloading the intrusion detection function of the systems. As a result, several threats passed through the server security system and penetrated the company's servers. The following experiment aimed to determine how many useful alarms will be executed by information systems when processing 40 GB of the duplicate files simultaneously, given that there were approximately **17,000** malicious files.

- *Snort* produced as many as **408 390 alarms**.
- *Bro* produced **95 574 alarms**.
- *Suricata* **28 243 alarms**.

**Figure 5: The difference in the number of alarms for each of the intrusion detection systems**



In Figure 5, the difference in the number of alarms for each intrusion detection system is displayed.

- ***Number of Cores***

*Snort* and *Bro* use only 1 server core when the system is running, while the *Suricata* can use all available cores. For the convenience of calculations, I will replace 1 = 1 core, 2 or more = 2.

- ***Cross-platform support***

*Snort* and *Suricata* support all possible operating systems, while *Bro* supports most, but not all. I replaced '1' with 'yes' for the convenience of calculations, which supports all possible operating

systems. Similarly, '2' was replaced with the measurement 'no,' which does not support all possible operating systems.

- *The Use of Recourse*

One of the essential criteria influencing the choice of an IDS is the optimal load on the company's servers. Data security can be compromised if the servers cannot handle the load and the security system cannot operate. In such cases, leaks and theft of user data and company databases occur. The information system must be reliable and be able to distribute the load on the server ports.

**Table 5: The percentage of consumed processor resources**

<b>P/IDS</b>		<b><i>Snort</i></b>	<b><i>Suricata</i></b>	<b><i>BroIDS</i></b>
<b>Stable CPU usage state</b>		<b>46%</b>	<b>46,4%</b>	<b>44,4%</b>
<b>Usage CPU when testing</b>		<b>68%</b>	<b>58,2%</b>	<b>99%</b>
<b>Stable RAM usage state</b>		<b>71,6%</b>	<b>46,4%</b>	<b>69,9%</b>
<b>RAM using when testing</b>		<b>76,1%</b>	<b>55%</b>	<b>73%</b>

Table 5 shows the percentage of consumed processor resources for the necessary operations to detect internal and external attacks on the company's server.

### 3.7. Multi-Criteria Decision Analysis

Based on the data obtained, three stages of calculations will be performed:

**The first stage** calculates the data from Table 2 according to the *Multi-Criteria Decision Analysis* method. In other words, by obtaining the individual number of points for each CID of the system.

**The second stage** is the calculation by the *Multi-Criteria Decision Analysis* method, the data from table 6 are separate from table 2, since they require individual calculations due to the multitude of categories. (Factors evaluated in the analysis of operational processes).

The **third stage** involved calculations using MCDA to determine the most optimal and IDS for a *Kaztransoil*.

#### 3.7.1. The first stage

In the *Multi-Criteria Decision Analysis* formula, favorable criteria are those criteria under which are most cost-effective. In Table 6, a summary of the findings is given, considering the attributes of the IDS software: SNORT, SURICATA, and BROIDS.


**Table 6: The entered data for each of the criteria for further analysis**

Attribute of criteria	Time of Processing (sec)	Usefulness over a period of time (17000 p.m.f)	Number of Cores. (1-1, 2- >2)	Cross-platform support (1=yes, 2=no)
<i>SNORT</i>	3199	408390	1	1
<i>SURICATA</i>	17077	28243	2	1
<i>BROIDS</i>	1671	95574	1	2



**Figure 6: Formula of linear normalization for further calculations in Multi-Criteria Decision Analysis**

**Linear  
Normalization**



Beneficial	$\bar{X}_{ij} = \frac{X_{ij}}{X_j^{Max}}$
Non-beneficial	$\bar{X}_{ij} = \frac{X_j^{min}}{X_{ij}}$

Source: Shaurya Uppal, 2020

To determine which formula to use, you need to understand if our criteria are helpful or not. In the Multi-Criteria Decision Analysis formula, favorable criteria are those criteria under which the more there are, the more profitable for us.

The decision according to this formula means that with a useful calculation, the score will be equal to the value divided by the maximum value among the other criteria. If the formula is not useful, then the estimate will be equal to the minimum value divided by all other values in sequence.

**Table 7: Determination of the formula suitable for each of the criteria based on Linear Normalization**

	<b>Non-beneficial</b>	<b>Non-beneficial (17000)</b>	<b>Beneficial</b>	<b>Non-beneficial</b>
<b>Attribute of criteria</b>	<b>Time of Processing (sec)</b>	<b>Usefulness over a period of time (17000 p.m.f)</b>	<b>Multithreading (Number of Cores. (1-1, 2- &gt;2))</b>	<b>Cross-platform support ( 1-yes, 2-no)</b>
<i><b>SNORT</b></i>	<b>1671/3199</b>	<b>17000/408390</b>	<b>1/2</b>	<b>1/1</b>
<i><b>SURICATA</b></i>	<b>1671/17077</b>	<b>17000/28243</b>	<b>2/2</b>	<b>1/1</b>
<i><b>BROIDS</b></i>	<b>1671/1671</b>	<b>17000/95574</b>	<b>1/2</b>	<b>1/2</b>

Having determined the required formula, calculations begin for each of the criteria. In case of non-benefit, the minimum value is divided by the other criteria, while in case of benefit, each value is divided by the maximum value of all criteria according to the formula.

**Table 8:  
Multi-  
Criteria  
Decision  
Analysis  
Calculatio  
ns**

<b>Weightage</b>	<b>25%=0,25</b>	<b>25%=0,25</b>	<b>25%=0,25</b>	<b>25%=0,25</b>
<b>Attribute of criteria</b>	<b>Time of Processing (sec)</b>	<b>Usefulness over a period of time (17000 p. m.f)</b>	<b>Multithreading (Number of Cores. (1-1, 2- &gt;2)</b>	<b>Cross-platform support ( 1-yes, 2-no)</b>
<b><i>SNORT</i></b>	<b>0,52*0,25</b>	<b>0,04*0,25</b>	<b>0,5*0,25</b>	<b>1*0,25</b>
<b><i>SURICATA</i></b>	<b>0,0978*0,25</b>	<b>0,6*0,25</b>	<b>1*0,25</b>	<b>1*0,25</b>
<b><i>BROIDS</i></b>	<b>1*0,25</b>	<b>0,177*0,25</b>	<b>0,5*0,25</b>	<b>0,5*0,25</b>

Each of the criteria is equally weighted, as found in previous analyzes. Each of the criteria is given 25 percent weight. Each value from the previous calculation is multiplied by 25 percent using the formula to get the final result.

**Table 9: The final results of the calculations: Ranking/Score**

<b>Attribute of criteria</b>	<b>Time of Processing (sec)</b>	<b>Usefulness over a period of time (17000 p. m.f)</b>	<b>Multithreading (Number of Cores. (1-1, 2- &gt;2)</b>	<b>Cross-platform support ( 1-yes, 2-no)</b>	<b>Performance score</b>	<b>Rank</b>
<i>SNORT</i>	<b>0,13</b>	<b>0,01</b>	<b>0,125</b>	<b>0,25</b>	<b>0,515</b>	<b>3</b>
<i>SURICATA</i>	<b>0,024</b>	<b>0,14</b>	<b>0,25</b>	<b>0,25</b>	<b>0,664</b>	<b>1</b>
<i>BROIDS</i>	<b>0,25</b>	<b>0,04</b>	<b>0,125</b>	<b>0,125</b>	<b>0,54</b>	<b>2</b>

In table 9, after adding up the final results of the calculations, the ranks are set, which show which of these systems have a high priority for a large company, based on the performance characteristics, utility, the number of cores involved, and the support of server systems.

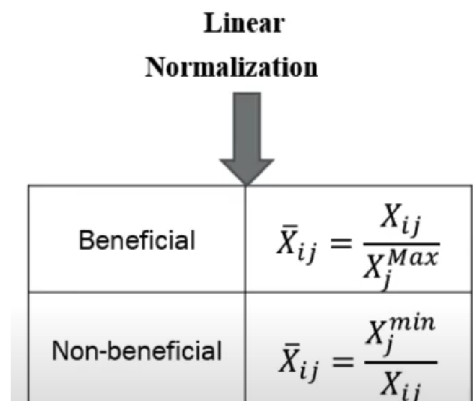
### 3.7.2. The second stage (The Use of Resources Calculations)

Table 10 shows the percentage of consumed processor resources for the necessary operations to detect internal and external attacks on the company's server. In this experiment, a test penetration, and an attack on the server through open ports were performed to obtain the desired parameters and results. The goal is to identify the vulnerability of systems and the percentage of spent RAM resources and processor load. With these initial data, I selected the IDSs according to their weighted score. With the *Multi-Criteria Decision Analysis*, it is evident that, because *Snort* and *Bro* use only one processor core, in the event of intensive attacks and increased server loads, the system has to spend more CPU power, which reflects negatively in the scoring. In turn, the most recent IDS in the list, *Suricata*, can use up to 4 processor cores, allowing users to use the full power of the servers and lighten the load on the CPU.

**Table 10: The percentage of RAM and CPU resource utilization for each intrusion detection system.**

P/IDS		<i>Snort</i>	<i>Suricata</i>	<i>BroIDS</i>
Stable usage state	CPU	46%	46,4%	44,4%
Usage when testing	CPU	68%	58,2%	99%
Stable usage state	RAM	71,6%	46,4%	69,9%
RAM when testing	using	76,1%	55%	73%

**Figure 7: Formula of linear normalization for further calculations in Multi-Criteria Decision Analysis**



Source: Shaurya Uppal, 2020

To determine which formula to use, you need to understand if our criteria are helpful or not. In the Multi-Criteria Decision Analysis formula, favorable criteria are those criteria under which the more there are, the more profitable for us.

The decision according to this formula means that with a beneficial calculation, the score will be equal to the value divided by the maximum value among the other criteria. If the formula is non-beneficial, then the estimate will be equal to the minimum value divided by all other values in sequence.

**Table 11. Determination of the formula suitable for each of the criteria based on Linear**

<b>L.Normalization</b>	<b>P/IDS</b>	<b><i>Snort</i></b>	<b><i>Suricata</i></b>	<b><i>BroIDS</i></b>
<b>Non-beneficial</b>	<b>Stable CPU usage state</b>	<b>44,4/46</b>	<b>44,4/46,4</b>	<b>44,4/44,4</b>
<b>Non-beneficial</b>	<b>Usage CPU when testing</b>	<b>58,2/68</b>	<b>58,2/58,2</b>	<b>58,2/99</b>
<b>Non-beneficial</b>	<b>Stable RAM usage state</b>	<b>46,4/71,6</b>	<b>46,4/46,4</b>	<b>46,4/69,9</b>
<b>Non-beneficial</b>	<b>RAM using when testing</b>	<b>55/76,1</b>	<b>55/55</b>	<b>55/73</b>

**Normalization**

At this stage, having chosen a non-beneficial formula, we divide the lowest value among all criteria for each individual criterion to obtain an assessment for each criterion.

**Table 12: Multi-Criteria Decision Analysis Calculations**

<b>Weightage</b>	<b>L.Normalization</b>	<b>P/IDS</b>	<b><i>Snort</i></b>	<b><i>Suricata</i></b>	<b><i>BroIDS</i></b>
<b>25%=0,25</b>	<b>Non-beneficial</b>	<b>Stable CPU usage state</b>	<b>0,96*0,25</b>	<b>0,95*0,25</b>	<b>1*0,25</b>
<b>25%=0,25</b>	<b>Non-beneficial</b>	<b>Usage CPU when testing</b>	<b>0,85*0,25</b>	<b>1*0,25</b>	<b>0,58*0,25</b>
<b>25%=0,25</b>	<b>Non-beneficial</b>	<b>Stable RAM usage state</b>	<b>0,64*0,25</b>	<b>1*0,25</b>	<b>0,97*0,25</b>
<b>25%=0,25</b>	<b>Non-beneficial</b>	<b>RAM using when testing</b>	<b>0,72*0,25</b>	<b>1*0,25</b>	<b>0,75*0,25</b>

The weighting of each of these criteria is identical because we have decided from previous analyzes that these criteria are equally important for the implementation of intrusion detection systems. Each is assigned 25 percent and is multiplied by each individual criterion.

**Table 13: The final results of the calculations, the ranks**

<b>P/IDS</b>	<b><i>Snort</i></b>	<b><i>Suricata</i></b>	<b><i>BroIDS</i></b>
<b>Stable CPU usage state</b>	<b>0,24</b>	<b>0,2375</b>	<b>0,25</b>
<b>Usage CPU when testing</b>	<b>0,2125</b>	<b>0,25</b>	<b>0,145</b>
<b>Stable RAM usage state</b>	<b>0,16</b>	<b>0,25</b>	<b>0,2425</b>
<b>RAM using when testing</b>	<b>0,18</b>	<b>0,25</b>	<b>0,1875</b>
<b>Performance score</b>	<b>0,7925</b>	<b>0,9875</b>	<b>0,825</b>
<b>Rank</b>	<b>3</b>	<b>1</b>	<b>2</b>



In table 13, after adding up the results of the calculations, the ranks are set, which show which of these systems are of higher priority for a large company based on the characteristics of resources and server load.

### 3.7.3. The third stage

The values from the previous two stages enabled the researcher to compare them based on the MCDA principle and derive the overall scores for each intrusion detection system. Using the estimates obtained, the scoring of the most optimal intrusion detection system for implementation in the information security of a *Kaztransoil* are displayed in Tables 14, 15, and 16.

**Table 14: Scores on two separate analyses**

<b>IDS</b>	<b>Performance Score 1</b>	<b>Performance score 2</b>
<i>Snort</i>	<b>0,515</b>	<b>0,7925</b>
<i>Suricata</i>	<b>0,664</b>	<b>0,9875</b>
<i>BroIds</i>	<b>0,54</b>	<b>0,825</b>

In the table 14, we can see the scores obtained for two analyzes, which will be compared separately to obtain an overall score because of the last general analysis.

**Table 15: Multi-Criteria Decision Analysis Calculations**

Weightage	50%=0,5	50%=0,5
-----------	---------	---------

	Beneficial	Beneficial
IDS	Performance Score 1	Performance score 2
<i>Snort</i>	0,515/0,664*0,5	0,7925/0,9875*0,5
<i>Suricata</i>	0,664/0,664*0,5	0,9875/0,9875*0,5
<i>BroIds</i>	0,54/0,664*0,5	0,825/0,9875*0,5

Having determined the formula I need, and this is a benefit. The second round of calculations takes place according to the MCDA linear normalization formula. With 50 percent weight for each test.

**Table 16: The final results of the calculations, the ranks**

IDS	Performance Score 1	Performance score 2	Score for two analyzes	Rank
<i>Snort</i>	0,387	0,401	0,788	3
<i>Suricata</i>	0,5	0,5	1	1
<i>BroIds</i>	0,406	0,417	0,823	2

In summation, the analysis results showed the following scores:

*Suricata* - 1

*Bro* - 0.823

*Snort* - 0.788

When adding up all the scores obtained, it is noticeable that *Suricata* has the best result among the three intrusion detection systems.

#### **4. Conclusion**

In conclusion, the analysis showed that *Suricata* was the most cost-effective and comprehensive choice after comparing all the criteria for *Kaztransoil*. This conclusion was derived after the mathematical calculation using the *Multi-Criteria Decision Analysis* method, whereby interviews informed the scores of professionals from the case sample: *Kaztransoil*.

These points indicate that all the technical configurations and characteristics are most suitable for implementation in a large company. Because each of the criteria was added mathematically using numbers. All these three intrusion detection systems are different, some of the systems are newer, and the others are already well-tested. With this study, the same method can be applied to other critical infrastructure businesses in Kazakhstan in selecting an optimal IDS tailored to individual needs and criteria.

Information security in the wireless segment is highly pervasive in the critical infrastructure business community in Kazakhstan, where concepts like information protection, threat prevention, threat prediction, and threat analysis are in high demand relative to the available IDS in developed countries. Although *Suricata* is the clear choice for *Kaztransoil*, the use of MCDA can be applied generally to other cases, and indeed this thesis concludes with the recommendation for further research concerning Intrusion Detection software and their applicability/availability in developing parts of the globe.

The next logical step in following this line of research would be to compile a selection of critical infrastructure businesses in Kazakhstan and expand the opportunity for interviews at conferences and trade shows where cyber-security solutions are presented and shared. This should simultaneously include desk research to compile a list of the most globally available IDS software whereby a comprehensive analysis and scoring of these systems can be achieved. Such research opportunities are presently underreaching. They warrant further investigation both for academic purposes and to

inform critical infrastructure businesses in developing countries about the existing IDS solutions and their ranking in terms of the criteria given in this thesis.

## 5. References

1. **Shumatov, E.G.** *Galym Gali Abdullin and New Kazakh Patriotism*. Nur-Sultan : autor neznámý, 2018.
2. **E.V., Mordasova.** *Information Security and Protection of information*.
3. *The Audit Commission review*. **B. Fitzsimons, L. Wilton, T. Lamont, L. McCulloch and J. Boyce.** London : autor neznámý, 2002.
4. *Global Wi-Fi Survey*. **Wakefield.** 2010.
5. **N.M., Gabdyzhamalov.** *CURRENT STATE AND PROSPECTS FOR THE DEVELOPMENT OF INFORMATION*. Astana : Kazakhstan University of Law, 2010.
6. **V.N, Yaseneva.** *Information Security*. Nizhny Novgorod : NNGU, 2017.
7. **Karygiannis, Tom.** *Wireless Network Security*. Gaithersburg : National Institute of Standards and Technology, 2002.

8. *Where's the Security in WiFi? An Argument for Industry Awareness.* **Sagers, Dr. Glen.** Hawaii : Hawaii International Conference on System Sciences, 2015.
9. **Brain, Marshall.** *How WiFi Works.* USA : HowStuffWorks, Inc., 2004.
10. *THE FUTURE DIRECTIONS IN EVOLVING WI-FI:.* **Cantav, Şeymanur.** místo neznámé : International Journal of Next-Generation Networks, 2014.
11. *Wifi Hotspot: Advantages and Disadvantages of Wifi Hotspots.* **Bornstein, Michelle.** místo neznámé : Lulu Press, Inc., 2015.
12. **Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith.** *Passive Wi-Fi: Bringing Low Power to.* Santa Clara, CA, USA : University of Washington, 2016.
13. **P.V.Gayatri.** *Developing an Intelligent e-Restaurant with a Menu Recommender for Customer-centric Service using Wi-Fi technology. .* : International Journal of Computer Applications, 2014.
14. **Tom Karygiannis, Les Owens.** . : National Institute of Standards and Technology, 2002.
15. *Wireless Network Security: Vulnerabilities, Threats and Countermeasures.* **Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim.** . : International Journal of Multimedia and Ubiquitous Engineering, 2008.
16. *Ransomware: Evolution, Mitigation and Prevention.* **Ronny Richardson, Max M. North.** Kennesaw Stat : Kennesaw State University, 2017.
17. *Ransomware: A Growing Menace.* **Gavin O’Gorman, Geoff McDonald.** . : Symantec, 2012.
18. *Intrusion Detection Systems.* **Bace, Rebecca.** . : NIST Special Publication on Intrusion Detection System, 2001.
19. **Albin, Eugene.** *A COMPARATIVE ANALYSIS OF THE SNORT AND THE SURICATA.* MONTEREY, CALIFORNIA : NAVAL POSTGRADUATE SCHOOL , 2011.

20. **E. Biermanna, E. Cloete, L. M. Venter.** *A comparison of Intrusion Detection systems.* . : Computers & Security, 2001.
21. **Axelsson, Stefan.** *Research in Intrusion-Detection Systems.*. Göteborg, Sweden : Department of Computer Engineering Chalmers University of Technology, 1998.
22. **Ahmed Patel, Qais Qassim, Christopher Wills.** *A survey of intrusion detection and prevention systems.* . : Information Management & Computer Security, 2010.
23. **Park, Wonhyung.** *Enhancing of Security Ethics Model base on Scenario in Future Autonomous Vehicle Accident.* Tokyo : 접수일(2018년 12월 4일), 게재확정일(2018년 12월 26일), 2018.
24. **Vivek Kumar Singh, Haythem Ebrahim, Manimaran Govindarasu.** *Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment.* . : Department of Electrical and Computer Engineering, Iowa State University, Ames, 2018.
25. **Paxson, Vern.** *Bro: a system for detecting network intruders in real-time real-time.* . : Computer Networks, 1999.
26. **Moya, Miguel A. Calvo.** *ANALYSIS AND EVALUATION OF THE IDS.* . : PROYECTO DE FIN DE CARRERA, 2008.
27. **Gunadi, Hendra.** *Bro Covert Channel Detection (BroCCaDe) Framework: Scope and Background.* . : Murdoch University IT NSRG Technical Report 20171117A, 2017.
28. **Moretti, Francesca.** *A standardized approach to qualitative content analysis of focus group discussions from different countries.* . : Patient Education and Counseling, 2011.

## 6. Appendix

Figure 8: An example of a questionnaire, an employee wished to remain anonymous.

**You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.**

1. What is your full name? (you can remain anonymous).

*Anonymous*

2. What is your current position at Kaztransoil?

*Security administrator*

3. The department in which you work?

*The information technology department*

4. Have you encountered attacks on your department's networks?

*Several times in 3 months we meet with attacks.*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*Yes. I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.





## 7. Appendix II: Interview chart

**You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.**

1. What is your full name? (you can remain anonymous).

*Anonymous*

2. What is your current position at Kaztransoil?

*Head of Energy Department*

3. The department in which you work?

*Energy Department*

4. Have you encountered attacks on your department's networks?

*Several times.*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Security of our department's networks under the responsibility of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

Not much.

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 3*

2. What is your current position at Kaztransoil?

*Human resource manager*

3. The department in which you work?

*The energy department*

4. Have you encountered attacks on your department's networks?

*Never*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*Yes. I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

**You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.**

1. What is your full name? (you can remain anonymous).

*Anonymous 4*

2. What is your current position at Kaztransoil?

*Administrator*

3. The department in which you work?

*The energy department*

4. Have you encountered attacks on your department's networks?

*Never*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous* 5

2. What is your current position at Kaztransoil?

*Workflow manager*

3. The department in which you work?

*The energy department*

4. Have you encountered attacks on your department's networks?

*Several Times*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous J*

2. What is your current position at Kaztransoil?

*Manager*

3. The department in which you work?

*The energy department*

4. Have you encountered attacks on your department's networks?

*Never*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

**You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.**

1. What is your full name? (you can remain anonymous).

*Anonymous 6*

2. What is your current position at Kaztransoil?

Head of Dispatch control Department

3. The department in which you work?

The dispatch control department

4. Have you encountered attacks on your department's networks?

*Several Times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous*

2. What is your current position at Kaztransoil?

*Human resource manager*

3. The department in which you work?

*The dispatch control department*

4. Have you encountered attacks on your department's networks?

*Several Times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.



You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous*

2. What is your current position at Kaztransoil?

Chief dispatcher

3. The department in which you work?

The dispatch control department

4. Have you encountered attacks on your department's networks?

*Several Times*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous*

2. What is your current position at Kaztransoil?

*Dispatcher*

3. The department in which you work?

*The dispatch control department*

4. Have you encountered attacks on your department's networks?

*Several Times*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 9*

2. What is your current position at Kaztransoil?

*Manager*

3. The department in which you work?

*The dispatch control department*

4. Have you encountered attacks on your department's networks?

*Several Times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Network security under the control of the IT department.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- **very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 10*

2. What is your current position at Kaztransoil?

Database administrator

3. The department in which you work?

The information technology department

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

6. How aware are you of possible attacks and threats on the company's network?

Our department knows how to deal with almost any known attack.

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 11*

2. What is your current position at Kaztransoil?

Computer network administrator

3. The department in which you work?

The information technology department

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

6. How aware are you of possible attacks and threats on the company's network?

Our department knows how to deal with almost any known attack.

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 12*

2. What is your current position at Kaztransoil?

*Software Analyst*

3. The department in which you work?

*The information technology department*

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

**You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.**

1. What is your full name? (you can remain anonymous).

*Anonymous 13*

2. What is your current position at Kaztransoil?

*Software architect*

3. The department in which you work?

*The information technology department*

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 14*

2. What is your current position at Kaztransoil?

Head of procurement Department

3. The department in which you work?

The procurement department

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

Our department knows how to deal with almost any known attack.

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent **3- moderately important** 4- very important 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.



You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 15*

2. What is your current position at Kaztransoil?

*Supplier*

3. The department in which you work?

*The procurement department*

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*I'm familiar with IDS*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness

over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent **3- moderately important** 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important,

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent **3- moderately important** 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 16*

2. What is your current position at Kaztransoil?

Administrator

3. The department in which you work?

The procurement department

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

Our department knows how to deal with almost any known attack.

7. Are you familiar with Intrusion Detection Systems?

Not much

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 17*

2. What is your current position at Kaztransoil?

*HR Manager*

3. The department in which you work?

*The procurement department*

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

6. How aware are you of possible attacks and threats on the company's network?

*Our department knows how to deal with almost any known attack.*

7. Are you familiar with Intrusion Detection Systems?

*Not much*

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent **3- moderately important** 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important **4- very important** 5- extremely important.

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

**1-absolutely not important** 2- important but to a small extent 3- moderately important 4- very important 5- extremely important.

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important.

You are presented with a questionnaire, the results of which will be used in research work in order to determine the best intrusion detection system for a large company.

1. What is your full name? (you can remain anonymous).

*Anonymous 19*

2. What is your current position at Kaztransoil?

Accountant

3. The department in which you work?

The procurement department

4. Have you encountered attacks on your department's networks?

*Several times at month*

5. How important is the security of networks in the wireless segment of your department to you? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

6. How aware are you of possible attacks and threats on the company's network?

Our department knows how to deal with almost any known attack.

7. Are you familiar with Intrusion Detection Systems?

Not much

8. There can be a different number of attacks and threats over a period of time, and in turn, each intrusion detection system can have a different usefulness over a period of time. How important is the usefulness of the information security systems involved? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

9. The number of cores used by the intrusion detection system increases the power and efficiency of the intrusion detection system. Assess how important this parameter is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent **3- moderately important** 4- very important 5- extremely important

10. Every minute a huge amount of information passes through the ports of the company's servers. Intrusion detection systems must respond quickly and combat threats and attacks with intrusion detection systems. Rate how important the speed of the security system is for your department. (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

11. How important is cross-platform intrusion detection system in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

12. How important is the importance of economical use of intrusion detection system to RAM and server resources in your department? (Highlight or underline your chosen answer)

1-absolutely not important 2- important but to a small extent 3- moderately important 4- very important **5- extremely important.**

13. How important is the price of Intrusion Detection Systems in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important

14. How important is the interface of Intrusion Detection System in your department? (Highlight or underline your chosen answer)

1-absolutely not important **2- important but to a small extent** 3- moderately important 4- very important 5- extremely important