APPLICATION OF NATO MODELS FOR BUILDING INFORMATION INFRASTRUCTURE IN CRISIS SITUATIONS

Violeta VASILEVA, PhD
Future Innovation Labs, Sofia, Bulgaria
Associate Professor Veselina ALEKSANDROVA GAGAMOVA, PhD
Rakovski National Defence College, Sofia, Bulgaria
DOI: 10.55535/RMT.2024.4.15

The effective functioning of the national security system during disasters, accidents and other crisis situations related to cyber security and cyber defence requires the realization of opportunities for inter-institutional interaction of all elements of the system. This paper presents certain opportunities as part of the methodology to apply NATO models to develop the system design of information infrastructure with capabilities to achieve the required levels of operational interoperability to respond to cyber threats to national security. For the architectural configuration, the NATO Technical Reference Model (NTRM) is applied and the NATO Common Operating Environment Component Model (NCOECM) is used for defining the information infrastructure components of the system design. By implementing the proposed methodology, a model of architectural configuration of an information infrastructure of a Security Operations Centre component has been developed – the Security Information Event Management (SIEM) Server. A specification of the technical and software configuration of the SIEM server is developed.

Keywords: NATO models; methodology; cybersecurity and cyber-defence; system design; interoperability and resilience;

INTRODUCTION

Informational infrastructure comprises a unity of its components, the relations among them, the principles and rules that govern their design and development. Security Information Event Management (SIEM) server as a component of cybersecurity informational systems should be architecturally configured by implementing the proposed NATO models. For that purpose, a model of an information infrastructure component (SIEM server) has been developed with a specification of its technical and software configurations by using the two main NATO references models: 1. NATO Technical Reference Model (NTRM) and 2. NATO Common Operating Environment Component Model (NCOEM) [Allied Data Publication 34 (ADatP-34)].

Architectural development requires modelling, which helps us understand the connection between the requirements, on the one hand, and the architectural concept, on the other hand. The requirements must be presented in a chart format according to NATO C3 Technical Architecture Implementation Handbook [ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002]. The NC3TA-IHB identifies in Annex A the templates that need to be filled out by project managers and architects, but does not provide a methodology how to do this. It is up to the project managers and architects to choose appropriate methodologies that fit their needs. There is a need for a methodology to fill out the NC3TA templates from Annex A. A proposal for such methodology is presented by the authors. As an example of the application of such a methodology, the paper presents the development of the architectural configuration of SIEM server.

MODELS FOR ARCHITECTURAL CONFIGURATION OF THE COMPONENTS OF THE INFORMATION INFRASTRUCTURE OF SYSTEMS IN CRISES MANAGEMENT ENVIRONMENT

For achieving the resilience of Information Systems in Cyber Conflict Environment it is necessary that the development of cybersecurity systems for organizations should be interoperable. Therefore, the application of NATO models would assist the development of organizations' cybersecurity systems.

One of the main models of system compatibility is the NATO Technical Reference Model (NTRM). It is a model for describing the information environment,

defining applications data and information infrastructure components data. It also defines the service areas (capabilities that are grouped by function) as well as their interfaces. The structure of the Technical Reference Model considers the separation of data from applications as well as applications from software configuration. The model is designed to separate applications and the external environment from the platform. It allows for the application compatibility and the independence from external devices (i.e., Keybords, Mouse, Webcam, USB Drive, External Hard Drive, Joystick, Game Controller etc.). For this purpose, the model defines the Application Program Interfaces (APIs) and the External Environment Interfaces (EEI).

The NTRM model includes five layers – three categories of objects (entities) and two interfaces, as follows:

- Application Software Entity;
- Application Program Interface/API;
- Application Platform Entity;
- External Environment Interface/EEI;
- External Environment Entity.

The application software consists of user and supporting software applications (software) or, as it is generally popular, user and application software.

Application Programming Interfaces (APIs) are applications that implement the connection between the service and the platform, i.e., applications between the application software and the application environment.

The application environment platform contains a system of services that physically materialize the information processes, i.e., system services and physical environment services (data exchange).

External Environment Interfaces (EEIs) provide the user with access to data and applications. Moreover, they provide connections between the application and the external environment. The concept of Internal Interfaces complements the description of APIs and EEIs.

The External Environment Entity includes external services that interact with those of the physical environment of the application software. These services are classified into the general categories of user services (mouse, display), information exchange services, and communication services (Local Area Network/LAN, Wide Area Network/WAN).

According to NTRM, the Application Platform Entity includes the following 12 Application Platform Service Areas (Allied Data Publication 34/ADatP-34):

- User Interface Services.

- Data Management Services.
- Data Interchange Services. These services provide support for the interchange of data between applications on the same or on heterogeneous platforms.
- Graphics Services. These services provide functions required for creating and manipulating graphics.
- Communication Services. These services provide distributed applications support for data access and applications interoperability in heterogeneous or homogeneous networked environments.
- Operating System Services.
- Internationalisation Services. Within the context of the NTRM, internationalisation provides a set of characteristics and data representation services.
- System Management Services.
- Security Services.
- Distributed Computing Services. These services provide specialised support for applications that may be physically or logically dispersed among computer systems in a network.
- Software Engineering Services.

Common Command and Control (C2) Applications Services. These services provide the ability to view data (i.e., share) in a common way across the network. Common C2 Applications Services promote interoperability among diverse functional mission area domains.

DEFINING THE ORGANIZATION OF THE COMPONENTS OF THE INFORMATION INFRASTRUCTURE OF THE CYBERSECURITY SYSTEM

For the effective functioning of the Computer Security Incident Response Team (CSIRT), it is necessary to provide the following components of the information infrastructure of the cybersecurity system in organizations:

- technological equipment with the relevant sensors for monitoring the communication and information infrastructure;
- intrusion detection and prevention systems – IDS/IPS/IDPS; (Intrusion Detection and Prevention Systems/IDPS is used to integrate IDS and IPS technologies);

- systems for processing and analysis of computer incidents – Security Information Event Management (SIEM) to support the actions of the team in reading a large number of registered events from cyber defence sensors;
- video surveillance systems, Next Generation Firewalls;
- trained and highly qualified personnel in the field of cyber defence;
- software for cyber forensics;
- a web server with cyber awareness information service.

The services to be provided by the SOC[1] can be divided into three main categories:

- response services (reactive services) provided in response to incidents – the main purpose of these services is to limit the damage caused by incidents;
- preventive incident response services (proactive services) – these services include detecting and reducing the possibility of a potential incident or event related to the security of the information system or network being protected;
- security improvement services – these services help to improve the quality of internal security. They are provided by experts in the field so that effective joint activities can be carried out within the organization so as to indirectly prevent the occurrence of incidents.

It is extremely important to react quickly and effectively when security breaches occur. One of the advantages of the incident response capability is that it maintains a systematic incident response (i.e., successive incident handling) so that appropriate action can be taken. Incident response helps staff minimize the loss or theft of information and disruption of services caused by accidents.

Security Information Event Management System

The use of the Security Information Event Management (SIEM) system for processing and analysing computer incidents is proposed as an incident response system. SIEM solutions provide a comprehensive view of the network in real time and help teams be more active in combating security threats (*"What Is SIEM?"*, n.d.). The advantage of SIEM solutions is that they combine security event management (SEM), which performs data analysis for events and real-time log files to ensure event correlation, incident response threat monitoring, with Security Information Management (SIM), which retrieves and analyses audit data and generates a report.

[1] Computer Security Incident Response Team (CSIRT) or Security Operations Centre (SOC), CERT/CC (Computer Emergency Response Team/Coordination Center, IRT (Incident Response Team), CIRT (Computer Incident Response Team), SERT (Security Emergency Response Team), CIRC (Computer Incident Response Team).

SIEM software identifies data and sorts it into categories such as malicious activity, failed and successful logins, and other potentially malicious activity.

When the software identifies an activity that may pose a threat to the organization, alerts are generated that indicate a potential security issue. These alerts can be set as low or high priority using a set of predefined rules. For example, if a user account generates 20 failed login attempts within 20 minutes, this may be marked as a suspicious activity but set with a lower priority, as the user is more likely to have forgotten their login information. However, if the account has 120 unsuccessful login attempts within 5 minutes, it is more likely to be under attack and marked as a high severity incident *("What is SIEM? SIEM Defined, Explained, and Explored"*, Forcepoint.com, 2023).

SIEM solutions provide a powerful method for threat detection, real-time reporting and long-term analysis of audit records and security events.

Because SIEM solutions can collect audit records of events from multiple applications and devices, they allow IT security experts to identify, review, and respond more quickly to potential security breaches. Identifying the threat in the early stages ensures a mitigating effect.

Accident Response Systems – Detection and Prevention of Intrusion Attempts/IDS/IPS/IDPS

Intrusion detection is the process of monitoring events occurring in a computer system or network and analysing signs of possible incidents that are breaches or imminent threats of breaches of computer security policies, acceptable use policies, or standard security practices. Intrusion Detection System (IDS) is software that automates the process of detecting network intrusion attempts. Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also try to stop possible incidents. The term Intrusion Detection and Prevention Systems (IDPS) is used to integrate IDS and IPS technologies.

Many IDPS can identify intelligence, which may mean that an attack is imminent or that a particular system or system feature is of particular interest to attackers. Another application of IDPS is to gain a better understanding of the threats that are detected, using artificial intelligence technologies and analysing the frequency and characteristics of attacks. The aim is to be able to define appropriate security measures. Some IDPS may change their security profile when a new threat is detected.

IPS technology differs from IDS technology in the fact that IPS technology can respond to an open threat by trying to prevent its success. IPS systems have sensors operating in training or simulation mode (Petters, n.d.).

Along with these systems, the components of the information infrastructure of the cybersecurity system in organizations include video surveillance systems, next-generation firewalls and others.

The traditional firewall provides access control, i.e., check the status of network traffic. Next-generation firewall (NGFW) can block modern threats such as malware and application-level attacks.

It is necessary to conclude that the breaches and attacks nowadays impose the need to develop the ability to detect, investigate and mitigate the consequences of computer accidents. This is a reason to define the following option for the organization of the components of the information infrastructure of the cybersecurity system in organizations in cyber conflict environment. Two areas are considered: providing services and monitoring security events to prevent accidents.

The information infrastructure of the cybersecurity system in organizations includes the following component servers and workstations as an option: Security Information Event Management System (SIEM) for incident handling and analysis, Security Server; WAP (Web Application Proxy); DNS (Domain Name Server); Database Server for database; Active Directory (AD) – Domain Controller (DC) with Active Directory; e-mail server – Exchange Server; Logs Server for recording events; IDS/IPS (IDPS); NVR (Network Video Recorder) server for video surveillance; PBX (Private Branch Exchange – telephone system), web server with WordPress installation) etc., as well as workstations of security administrators, remote users. They are presented in *figure 1*.

In the architectural configuration of the components of the information infrastructure of the cybersecurity system in organizations for the term "*component*" the terms *functional configuration*, *platform* and *configuration* are also used.

The various components (platforms) of the information infrastructure of the cybersecurity system are considered as functional configurations. Each of them has a distribution of its elements into five layers: network services; kernel services; infrastructure services; common support application services and application services.

In this sequence, the functional configurations of the platforms (components) are defined, as shown in *figure 1*, as well as their system design. According to the concept of architectural configuration of the components of the information infrastructure, for each of the components the following descriptions or configurations are developed, which represent a different aspect – functional, technical and software configuration. For each of the three configurations a graphic and tabular design is being developed (*"Functional Configuration (FC) Template"* – NSV-12, *"Technical*

Configuration (TC) Template" – NTV-3, *"Software Configuration (SC) Template"* – NTV-4), according to the templates[2] [(ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002, pp. 49-67, Annex A] of the NTRM Concept.

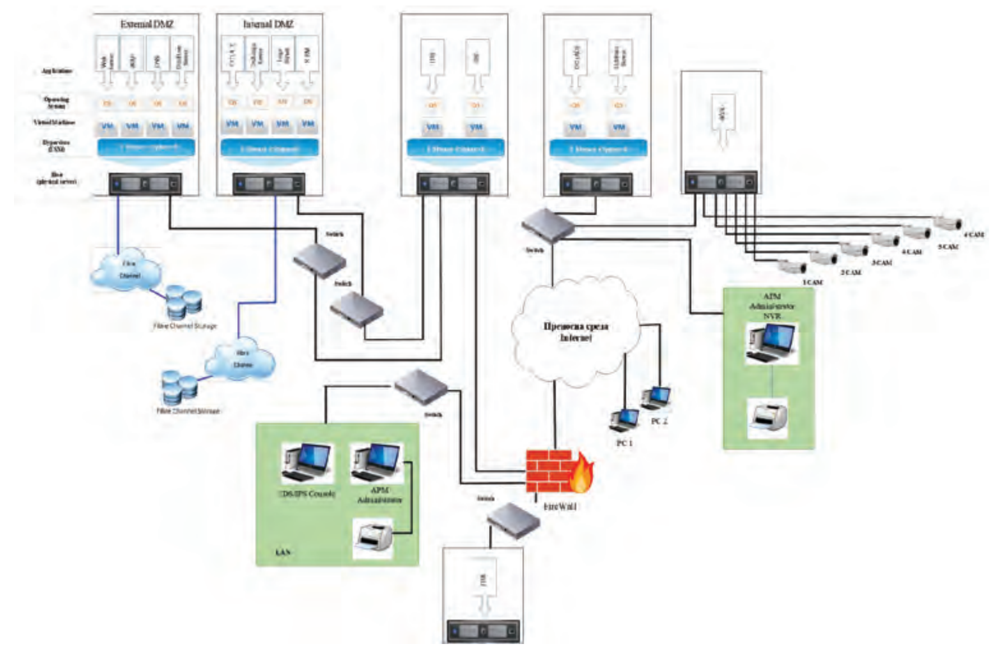

Figure 1: CIRT system information infrastructure components (authors' compilation)

ARCHITECTURAL CONFIGURATION OF A SERVER FOR PROCESSING AND ANALYSIS OF COMPUTER INCIDENTS – SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SERVER

Functional configuration of the server for processing and analysis of computer incidents – Security Information Event Management (SIEM) is shown in graphical form, *figure 2*, and tabular view, *table 1*, which represents the *"Functional Configuration Template"* NSV-12, according to the architectural configuration concept. Functional configuration is built through the five layers of services previously listed: application services; common support application services; infrastructure services; kernel services; network services.

Elements of the following functional components are located in each of these layers: Management components; Network components; Application components; Basic components; Security components.

[2] Annex A – NC3TA Compliance Templates includes NATO System View Template 12 (NSV-12) Functional Configurations, NATO Technical View Template 3 (NTV-3) Technical Configurations, NATO Technical View Template 4 (NTV-4) Software Configurations.

At the level of functional configuration, the SIEM architecture has been developed. It is presented in more detail with the technical and software configuration.

A technical configuration is a transition from a technical view to software configurations that define specific segments and their component and software products. The Internal and External Interoperability Profiles (IIPs and EIPs) are indicated here too.

The software configuration presents the software for executing the technical configuration. The components and standards used in the technical configuration are transformed into products and segments.

Functional Configuration of SIEM

In tabular form, template NSV-12, *"Functional configuration template"*, is used, which presents the functional services and interfaces *(Table 1)*.

Table 1: NSV-12 functional configuration (FC) template of the security information and event management server (SIEM) (authors' compilation)

NSV-12	FUNCTIONAL CONFIGURATION (FC) TEMPLATE		
Project title	CIRT INFORMATION SYSTEM		
Project POC	Name	Address	Tel/Fax/ Email
FC title	Functional Components of Security Information and Event Management SIEM		
FC Type *Note: Choose existing type, otherwise, create new child FC under one of the main categories, or create a new category*	SIEM SERVER Analysis, profiling, automation, and summarizing potential threats. Incident investigation, threat intelligence.		
FC Services at:	Foundation Services	Network Services	

Note: Describe the application services in functional terms	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Traffic Balancing Network stack	Configuration Control / Remote installation; Operation systems; Windowing software; Applications; Devices. Databases	Vulnerability scanning User information Asset information Threat intelligence	Data collection Correlation Normalization Data aggregation	Analysis applications Reporting applications Real-time monitoring applications Server applications
Functional Interface *Note: Describe the functional interface with other FCs in terms of required interoperability services (e. g.: email, authentication) and the required quality and quantity attributes (e.g.: no. of messages, security credentials) using the NSV1 (a-d), NSV3 and NTVI* templates	SSH[3] interface port 22 SMTP[4] interface port 25 RDATE[5] interface port 37 Port Mapper interface port 111 HTTPS[6] interface port 443 Syslog interface port 514				

[3] Secure Shell (SSH) is a cryptographic network protocol. See, for instance, https://www.ssh.com/, retrieved on 5 January 2024.

[4] Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used in sending a dreceiving e-mail, https://www.smtp.com/, retrieved on 5 January 2024.

[5] RDATE is a get and possibly set the system date and time from a remote host for Unix OS e-mail, http://manpages.ubuntu.com/manpages/bionic/man8/rdate.8.html, retrieved on 5 January 2024.

[6] Hypertext Transfer Protocol Secure (HTTPS), https://www.ssl.com/faqs/what-is-https/, retrieved on 5 January 2024.

Technical Configuration of SIEM

The main purpose of the technical configuration is to determine the technological and technical standards that must be applied in the design and construction of the system. Technical configuration is a technical transformation of the functional configuration. It means that the application services that are described in the functional configuration are transformed into components with their basic standards. The internal and external interoperability profiles are also indicated here, which are developed both graphically *(figure 2, figure 3)* and tabular *(table 2)* in NTV-3 *"Technical Configuration (TC) Template"*.

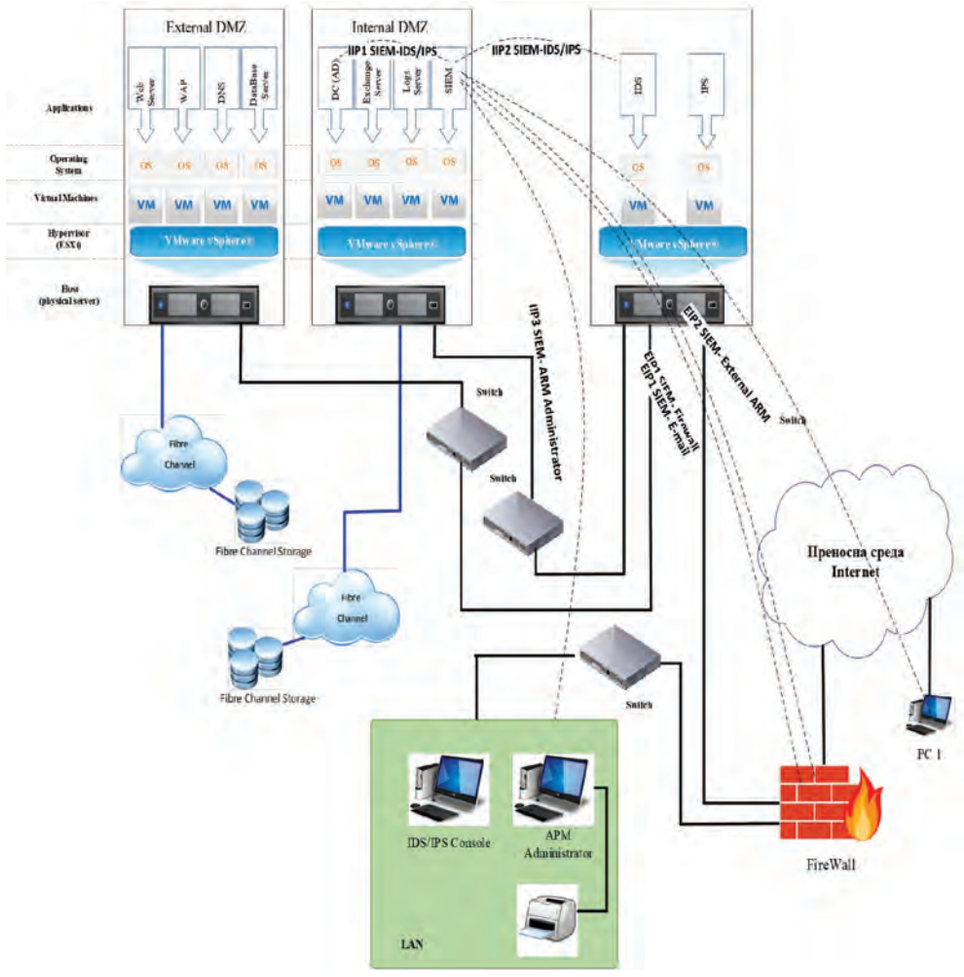

Figure 2: Technical configuration with interoperability profiles between the components of the information environment (authors' compilation)

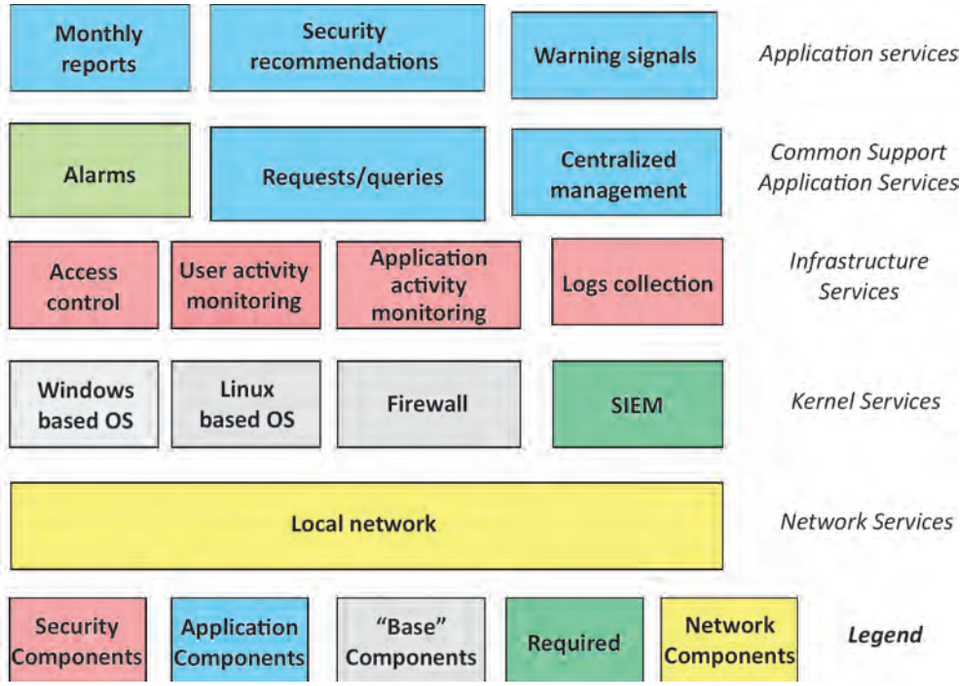

Figure 3: Graphic representation of the technical configuration of the SIEM server according to NCOECM (authors' compilation)

In technical configurations, internal interoperability profiles are defined within relevant protocols and standards. To allow flexibility in order to replace obsolete products with new ones, it is advisable to choose open standards and choose products that use such standards. The technical configuration is presented in *table 2*.

Table 2: NTV-3 technical configuration of SIEM server (authors' compilation)

NTV-3	TECHNICAL CONFIGURATION (TC) TEMPLATE (to be filled at Procurement Phase for Target Architecture)				
TC Components and Standards at: *Note: attach for each required component a detailed description*	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Local network	Windows based OS Linux based OS Firewall SIEM	Access control Identity management User activity monitoring Behaviour analysis Application activity monitoring Logs collection	Alarms Requests / queries Centralized management	Monthly reports Security recommendations Warning signals

Internal Interoperability Profiles (IIP) between TC and: *Note: Attach for each IIP a detailed description*	IIP1 – Active Directory Server – Domain Controller IIP2 – Server *"IDS/IPS"* IIP3 – Workstation for monitoring and administration of Windows OS
Interoperability Profile between TC and: *Note: Attach for each E1P a detailed description* EIP-Number and Basic Functionality: *Note: Use numbering as follows EIP<TCnr>-<TCnr>*	EIP1 – Firewall EIP2 – Workstation – A remote workstation for administering the Linux operating system (OS) EIP3 – Email Server

Internal Interoperability Profiles (IIP) are as follow:

- Profile IIP1 – Data exchange with a server active directory (Kerberos, LDAP[7], File Replication, Global Catalog, DNS)
- Profile IIP2 – Data exchange with a server IDS/IPS
- Profile IIP3 – Data exchange with the Windows OS workstation

Software Configuration of SIEM

As it has been already mentioned, the Software Configuration is a software implementation of the technical configuration. The software configuration consists of the real products that are used, which describe the software solution of the technical configuration. The software configuration represents the software for executing the technical configuration, which means that the components and standards used in the technical configuration are transformed into products and segments. The software configuration of SIEM is graphically presented in *figure 4*, and, in tabular form, in *table 3*.

[7] Lightweight Directory Access Protocol (LDAP) for interacting with directory servers and used for authentication and storing in formation about users, groups, and applications, https://ldap.com/, retrieved on 7 January 2024.

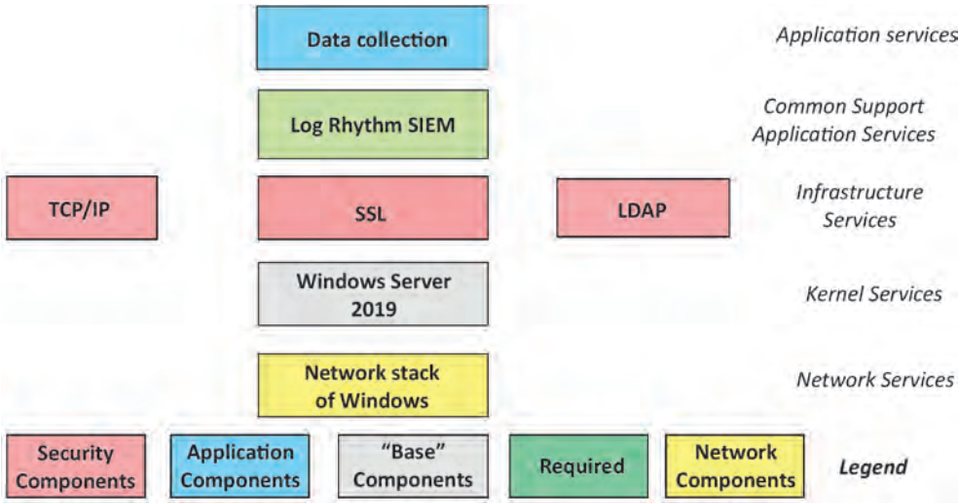

Figure 4: Graphical representation of SIEM software configuration according to NCOECM (authors' compilation)

Within the information environment, software packages, which are located horizontally in the graphical representation of the software configuration, are presented in separate units, also known as *segments*. The segments are similar in functionality to modules and can be easily added to any hardware platform. Segmentation gives the user the opportunity to choose from packaged and tested software components that are considered necessary in a particular situation. SIEM software configuration is developed in *table 3*.

Table 3: NTV-4 SIEM software configuration template (authors' compilation)

NTV-4	SOFTWARE CONFIGURATION (SC) TEMPLATE *(to be filled in the Procurement Phase for Target Architecture)*				
SC products in: *Note: Indicate software version number and standard(s) which are covered by the software package*	*Network Services Layer*	*Kernel Services Layer*	*Infrastructure Services Layer*	*Common Support Application Layer*	*Specific Mission Application Layer*
	Network stack of Windows	Windows Server 2019	TCP/IP[8], SSL[9], LDAP	Log Rhythm SIEM[10]	Data collection

[8] TCP/IP -Transmission Control Protocol/Internet Protocol.
[9] SSL – Secure Sockets Layer.
[10] Log Rhythm: SIEM Platform&Security Operations Center

Segments:	*Segment 1*	*Segment 2*	*Segment 3*	*Segment 4*	*Segment 5*
Note: Describe the products that constitute the different segments	Network stack of Windows	Windows Server 2019	TCP/IP, SSL, LDAP Log Rhythm	Data collection	
Interfaces	Internal	Internal	External	External	External
Interfaces *Note: Describe interfaces in terms of APIs embedded in products or as separate products; Mention the standards supported and possible parameter settings*	IIP1– UDP[11] port 88 for Kerberos[12] authentication IIP1 – TCP port 3268 and 3269 for the Global Catalog IIP1 – TCP and UDP port 53 for DNS[13] IIP1 – TCP 139 and UDP port 138 for file replication IIP1 – UDP port 88 for Kerberos authentication IIP1 – TCP port 3268 and 3269 for the Global Catalog IIP1 – TCP and UDP port 53 for DNS exchange IIP1 – TCP 139 and UDP port 138 for file replication IIP1 – TCP port 514 to collect logs EIP1 – Interface for exchanging information with Firewall EIP2 – TCP port 514 to collect logs EIP3 – TCP port 80 for web applications EIP3 – TCP port 443 for web applications EIP3 – TCP port 22 to exchange messages				

CONCLUSIONS

To develop the architecture of an organization's computer incident response centre, a proposal is offered to use NATO models to architecturally configure the components of the information infrastructure of cybersecurity systems.

It can be concluded that the authors have presented a methodology for application of NATO models for building information infrastructure in crisis conditions that includes architecture configuration and system design of its components in a specific way – by using NATO models. Various tools have been used, such as figures, tables and textual explanation. This presentation of the information infrastructure is not very popular among developers' teams, especially in the field of Resilient Information Systems design. We hope that the topic would be interesting because defining the information infrastructure and its software configuration could

[11] UDP – User Datagram Protocol.

[12] Kerberos is a network authentication protocol developed by the Massachusetts Institute of Technology. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, retrieved on 7 January 2024.

[13] DNS – Domain Name Server.

successfully be used to improve the design of such systems in order to meet the challenges of crisis conditions environment.

ACKNOWLEDGEMENTS

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030, and was adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

BIBLIOGRAPHY:

1. Allied Data Publication 34 (ADatP-34) (n.d.). *NATO C3 Technical Architecture, Volume 2 Architectural Descriptions and Models* (Version 6.0). ISSC NATO Open Systems Working Group. Retrieved from NC3TA-Vol 2- v6.xml.
2. Demirov P., S. E. (2019). Informatsiya tai information natasreda, kato obekt za zashtita v cyber prostranstvoto. *Sborniktrudove NK, ISSN 1314-1937.* NVU "V. Levski".
3. ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268. (2002). *NATO C3 Technical Architecture Implementation Handbook (NC3TA-IHB* (Vol. Version 1).
4. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, retrieved on 7 January 2024.
5. Lightweight Directory Access Protocol (LDAP), https://ldap.com/, retrieved on 7 January 2024.
6. Petters, J. (n.d.). Varonis.com, https://www.varonis.com/blog/ids-vs-ips, retrieved on 9 August 2024.
7. Secure Shell (SSH), https://www.ssh.com/, retrieved on 5 January 2024.
8. Simple Mail Transfer Protocol (SMTP), https://www.smtp.com/, retrieved on 7 January 2022.
9. *"What is SIEM? SIEM Defined, Explained, and Explored".* (https://www.forcepoint.com/cyber-edu/siem, retrieved on 19 August 2024.
10. *"What Is SIEM?"*. (n.d.). Splunk.com, https://www.splunk.com/en_us/data-insider/what-is-siem.html#overview, retrieved on 7 January 2024.
11. Vasileva, V. (2020). Information Sharing Processes in Public Sector Cybersecurity Structures. *9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education,* pp. 136-147. Sofia: Publishing Complex – UNWE, http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2019.pdf, retrieved on 5 August 2024.