Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks

Tamara Radivilova
V.V.Popovskyy dept. Infocommuniction Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
tamara.radivilova@gmail.com

Kirichenko Lyudmyla
Dept. of Applied Mathematics
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
lyudmyla.kirichenko@nure.ua

Oleksandr Lemeshko, Dmytro Ageyev, Maksym Tawalbeh
V.V.Popovskyy dept. Infocommuniction Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandr.lemeshko@nure.ua, dmytro.aheiev@nure.ua, tavalbeh@icloud.com

Andrii Ilkov
Department of Combat Application of Radio Engineering Weapons
Ivan Kozhedub Kharkiv National Air Force University
Kharkiv, Ukraine
andreyilkov428@gmail.com

2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T) | 978-1-7281-9177-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/PICST51311.2020.9467973

***Abstract*— Information security is an important challenge due to the increasing number of attacks and intrusions. In this paper, approaches and systems for monitoring traffic and events, intrusion detection systems, deep packet inspection tools, and network packet sniffing systems are analyzed. It is shown that for intrusion detection and analysis of illegal actions in the network are used all the many systems and approaches described. A comparative analysis of incident, vulnerability and asset management systems was conducted. Based on this analysis, it is possible to develop recommendations for the use of each system depending on the requirements of the organization.**

Keywords*— vulnerability, attack, deep packet inspection, machine learning, user and entity behavior analytics, intrusion detection, threat, security information and event management

I. Introduction

The pandemic has caused an increase in remote connections within organizations, increasingly sophisticated methods from the kill chain and careful hiding of one's presence, all leading to increased information security risks [1,2]. Changing threat vectors towards complex multi-vector attacks and increasing complexity of security solutions lead to the rapid development of security information and event management (SIEM) systems. The systems enable real-time monitoring of information systems, analysis of security events occurring in nodes of a computer network [3-8]. The data collected and analyzed by such systems can help detect information security incidents or anomalies that stay unnoticed by specialized security tools [8-11].

To ensure and maintain information security, a variety of methods are used to prevent, monitor and eliminate unauthorized access. Information security actions are also aimed at protecting against damage, distortion, blocking or copying of information. An important and fundamental point is that all tasks should be solved simultaneously, because only then a full and reliable protection is provided. Many systems are used to detect intrusions and analyze illegal actions in the network: intrusion detection systems (IDS), deep packet inspection (DPI), network packet capture systems, firewalls, anti-virus protection tools, cryptographic protection tools, etc [12-14]. Specialists and scientists from different countries developed approaches to defeat information security threats.

In [14], the authors addressed the DPI delay problem and proposed the Fast Packet Inspection (FPI) model, which while preserving End-to-end encryption E2EE ensures data integrity and malware detection. In [15] the authors proposed an intrusion detection system that is based on the use of various machine classifiers MLlib (machine learning library) based on spark MLlib and the use of deep learning approaches such as Conv-AE convolutional autocoder. The author of manuscript [16] propose an several consecutive characters to represent by character intervals, that reduce the number of concatenating transfer edges and improve the efficiency of deep packet inspection. The authors of [17] have developed and presented a formalization of the relation of threads and packets, a mathematical description of the DPI system architecture calculation model, precisely the packet analysis time depending on the number of processors, and a physical DPI architecture model based on the Wentzel-Ovcharov model. In paper [18] the authors propose a comprehensive intrusion detection and attack identification method based on the synergy of machine learning behavior analysis, signature analysis with deep packet analysis, entropy protocol analysis. In the manuscript [19] the authors describe the monitoring and packet capturing system that was implemented on the campus wireless LAN network to analyze and identify packet loss and flooding attacks using random early detection (RED) algorithm. In article [20], the authors analyze modern packet capturing technologies and frameworks, analyzing their advantages and disadvantages when used to analyze and process network data from the perspective of packet capture speed, resources used and application flow. The authors of manuscript [21] use Python libraries and Data Science techniques on a real network to improve the packet capture process and graphical analysis techniques. In the paper [22] the authors use Deep Packet Inspection in combination with Deep Flow Inspection to

This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

978-1-7281-9177-5/20/$31.00 ©2020 IEEE

identify different types of man-in-the-middle attacks by detecting network traffic and filtering packets of incoming network traffic using DPI and DFI Method Libraries and DFI Feature Library. The authors of paper [23] propose an approach to intrusion detection based on emission data analysis using machine learning techniques, which combines DPI (deep packet inspection) and DFI (deep flow inspection). Thus, there is no doubt about the actuality of the work.

The purpose of this paper is to analyze intrusion monitoring and detection systems and provide recommendations on how to use these systems to improve information security.

II. Information Security Event Monitoring Systems.

Information security event monitoring is the process of checking all security events received from various sources. Event sources can include operating system logs, antivirus systems, network equipment, infrastructure security analysis scanners, and other sources of an organization's infrastructure. Event monitoring systems can be divided into the following categories: SIEMs are systems for managing events received from various sources, allowing real-time analysis of events [11]. User Behavior Analytics (UBA) are systems that collect and analyze user actions to search for possible insider threats and attacks. User and Entity Behavior Analytics (UEBA) are systems that collect and analyze user actions to find anomalies in the behavior of employees and various systems [24].

Event monitoring systems can be divided into the following categories: SIEMs are systems for managing events received from various sources, allowing real-time analysis of events. UBAs are systems that collect and analyze user actions to search for possible insider threats and attacks. UEBAs are systems that collect and analyze user actions to find anomalies in the behavior of employees and various systems [25]. In this paper, as specialized security solutions are considered intrusion detection systems (IDS), deep packet inspection (DPI) and network packet capturing systems. That is, attack search and detection systems that aim to increase the level of protection of an organization's infrastructure [13, 26, 27].

Open Source Intrusion Detection System (IDS) Suricata, which is used to monitor network activity and security and is a network IDS and IPS tool [5, 12, 24, 25]. Suricata supports Deep Packet Inspection (DPI) Zeek (Bro), a traffic analysis and network intrusion detection system. Zeek 3.0.0 contains modules for traffic analysis, analysis and parsing of application-level network protocols, modules for logging (archive) of network activity, modules for integration with third-party information systems and real-time data exchange. Moloch's Large Scale Packet Capture System is a fast and simple web application for navigating through collections of PCAP files that contain packet fields and is capable of parsing and indexing billions of network sessions. It can also be used for real-time traffic capture and as a network forensic tool for incident investigations.

The Next generation firewall (NGFW) and SIEM systems are used to implement network activity monitoring, which also have disadvantages when used. In each of the variants there is a performance issue. In NGFW and UTM, the IDS module is often simply disabled due to high load. In addition, when discussing attack detection tools, it is often signature analysis that is meant, and modern attackers, as we defined above, already know how to bypass such measures.

SIEM only works with logs sent to it by a limited number of sources (which are also susceptible to being shut down by perpetrators). Also, the number of malicious content installers who use chains of calls to legitimate host utilities and executing code is constantly increasing, and automatic detection tools do not have time to build a chain to install a dangerous object into the system. SIEM processes a significant number of events per second (EPS) from non-network sources and often has to compromise some correlation rules or multiply the cost of hardware resources [3, 6-8]. Also, attackers hide their activities on the system by redirecting network logs to temporary files. It is also impossible to detect all communication channels with command and control servers, even with Threat Intelligence. To detect malware it is necessary to use algorithms to detect hidden DNS-, SMTP-, HTTP- and ICMP-tunnels used by attackers to hide their activity from protection means, to steal data. In addition to searching for such hidden tunnels, the network security system must be able to create and use its own similarity detection algorithms along with statistical methods.

In the described systems there is no possibility to profile activity in the system, to solve this problem UEBA systems of analysis of user behavior and entities are used. UEBA contains entity profiling and analysis services, which are applications, storage systems, network traffic, devices, servers and data, and allow to solve problems not only of internal leaks of confidential data, but also of external attacks aimed at the system. Threat Intelligence Platform is an emerging class of technology that enables real-time aggregation, correlation and analysis of threat information from multiple sources [1, 4, 10, 27]. By importing threat data from multiple sources and formats, correlating it, and then exporting it to a particular organization's existing security systems, Threat Intelligence Platform automates proactive threat management and mitigates its negative impact.

Data from the platform must flow back into systems and security products used by the organization, such as SIEM systems, firewalls, intrusion detection systems, and others.

The problems described above show that to detect malicious actions, we need tools that meet today's requirements for threat detection (or a combination of detection methods), deep traffic analysis, and data storage for investigation. The above-mentioned existing approaches are combined in what is known as Next Generation Security Monitoring. Next Generation Security Monitoring collects, processes, manages and analyzes network logs, system and transactional, intelligence and event data in real time at very high speed. The system continuously monitors security controls and the corporate environment and instantly captures incidents for investigation and response [1, 2]. In terms of architecture, there are two basic models of service delivery:

- CRE model. The protection equipment is located at the customer's site. The operator fully manages and accompanies the operation of this equipment. This model is the most popular today.

- Cloud model. Equipment is located at the operator's site, and a customer is provided with a traditional communication channel, cleaned from viruses, spam and other security threats. This model is the most promising, due to easy and quick connection of a client.

Figure 1 shows a scheme of interaction between the main components of Next Generation Security Monitoring.

As can be seen from the figure 1, the Next Generation Security Monitoring system includes the main data streams from services, Threat Intelligence SIEM interaction and detecting behavioral anomalies system and monitors and audits data and processes.

Table 1 provides a comparison of information assurance systems from leading vendors.

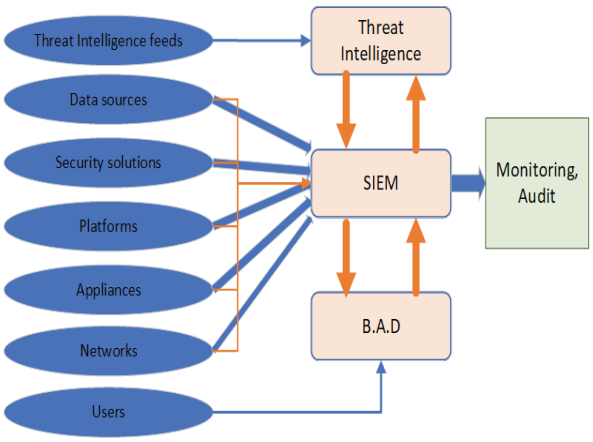

Fig. 1. Scheme of Next-Generation Security Monitoring components

TABLE I. MANAGEMENT OF INCIDENT, VULNERABILITY AND ASSET IN INFORMATION ASSURANCE SYSTEMS FROM LEADING VENDORS

Assessment Criteria/Vendor	Micro Focus (HP) ArcSight	IBM Qradar	McAfee ESM	RSA NetWitness	Splunk
Escalate an incident	By the level and path	Manually	Manually or with automatic alerting	Manually or with automatic alerting	manually or with automatic alerting on SOAR or through the modular notification mechanism
Integration with Service Desk systems	API, email	API, email, SNMP	API, email	Syslog	API, email, SNMP
Identify false positives	manually	manually	manually	manually	manually or with pre-determined correlation rule
Autoregistration of vulnerabilities	yes	yes	yes	no	yes
Setting or importing asset information	yes, with correlation rules, CMDB integration	from security scanners, CSV files, API	Active Directory, CSV files, API, from security scanners	no	AD, CMDB, SCOM, Cisco ISE, Symatec Endpoint Protection and etc.
Limit channel consumption	yes	yes	Receiving load control	sequential	yes and SSL compression and non-SSL
Authentification	Local, Radius, LDAP, Active Directory	Local, Radius, Tacacs, Active Directory, LDAP	Local, RADIUS, CAC, Active Directory, LDAP	Active Directory	Active Directory, LDAP, SAML, RADIUS
Network traffic data collection	Netflow/J-flow/IPFIX	SPAN, Netflow, sFlow, jFlow, etc.	Nitro IPS/IDS, NetFlow, sFlow, etc.	SPAN, Netflow, sFlow, jFlow, etc, full capture packets	NetFlow, jFlow, sFlow, IPFIX, HTTP, MySQL, IMAP, POP3, XMPP, Splunk App For Steam
UBA&UEBA	ArcSight UBA	User Behavior Analytics for QRadar	no	no	Splunk Extreme Search, Splunk UBA
Machine learning	ArcSight UBA	QRadar Advisor With Watson	yes, with Investigator	no	Splunk UBA, Splunk ML Toolkit, Splunk Extreme Search

III. CONCLUSION

This paper analyzes approaches and systems for monitoring traffic and events, intrusion detection systems, deep packet inspection tools, and systems for capturing network packets. It is shown that for intrusion detection and analysis of illegal actions in the network are used all the many systems described, as well as deep packets inspection, sniffer, packet captures, firewalls, user and entity behavior analytics, anti-virus protection tools, trusted boot tools, intrusion detection tools, cryptographic protection tools, etc.

A comparative analysis of incident management, vulnerability and asset systems from leading vendors has been conducted. Based on this analysis it is possible to develop recommendations for the use of each system depending on the requirements of the organization. In future work, it is planned to analyze and simulate the operation of these systems in different security environments.

REFERENCES

[1] I. Dobrynin, T. Radivilova, N. Maltseva and D. Ageyev, "Use of Approaches to the Methodology of Factor Analysis of Information

Risks for the Quantitative Assessment of Information Risks Based on the Formation of Cause-And-Effect Links," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 229-232. doi: 10.1109/INFOCOMMST.2018.8632022,

[2] N. Poluektova, T. Klebanova and L. Guryanova, "Risk Assessment of Corporate Infocommunication Systems Projects Using Bayesian Networks," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2018, pp. 31-34, doi: 10.1109/INFOCOMMST.2018.8632150.

[3] O. Mulesa, V. Snytyuk, I. Myronyuk, "Forming the clusters of labour migrants by the degree of risk of hiv infection," *Eastern-European Journal of Enterprise Technologies*, vol. 3(4), pp. 50-55, 2016. doi: 10.15587/1729-4061.2016.71203.

[4] J. Matuszewski, "Evaluation of jamming efficiency for the protection of a single ground object," *2017 Radioelectronic Systems Conference*, vol. 10715, Poland, 2018, pp. 107150B. doi: https://doi.org/10.1117/12.2316629.

[5] O. Barabash, O. Laptiev, O. Kovtun, O. Leshchenko, K. Dukhnovska and A. Biehun, "The Method dynavic TF-IDF," *International Journal of Emerging Trends in Engineering Research (IJETER),* vol. 8(9), pp 5713-5718, 2020.

[6] A. Semenov, "Mathematical simulation of the chaotic oscillator based on a field-effect transistor structure with negative resistance," *2016 IEEE 36th International Conference on Electronics and Nanotechnology (ELNANO)*, 2016, pp. 52-56. doi: 10.1109/ELNANO.2016.7493008.

[7] O. Lemeshko and O. Yeremenko, "Enhanced method of fast re-routing with load balancing in software-defined networks," *Journal of Electrical Engineering,* vol. 68(6), pp. 444-454, 2017. https://doi.org/10.1515/jee-2017-0079

[8] F. Geche, A. Batyuk, O. Mulesa and V. Voloshchuk, "About Kernel Structure Construction of the Generalized Neural Functions," *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, 2018, pp. 151-156, doi: 10.1109/DSMP.2018.8478485.

[9] O. Yeremenko, O. Lemeshko and A. Persikov, "Secure routing in reliable networks: proactive and reactive approach," In: Shakhovska, N., Stepashko, V. (eds.) *AISC*, vol. 689, pp. 631–655. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-70581-1_44

[10] L. Kirichenko, A.S. A. Alghawli and T. Radivilova, "Generalized Approach to Analysis of Multifractal Properties from Short Time Series," *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 11(5), 2020, pp.183-198. doi: 10.14569/IJACSA.2020.0110527

[11] A. Bessalov, L. Kovalchuk, V. Sokolov, P. Skladannyi and T. Radivilova, "Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves," *Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2020)*, Kyiv, Ukraine, vol.2746, pp.1-13, 2020.

[12] V. Savchenko, O. Ilin, N. Hnidenko, O. Tkachenko, O. Laptiev and S. Lehominova, "Detection of Slow DDoS Attacks based on User's Behavior Forecasting," *Intern. Journal of Emerging Trends in Engineering Research (IJETER),* vol.8(5), pp.2019-2025, 2020.

[13] O. Laptiev, I. Polovinkin, S. Vitalii, O. Stefurak, O. Barabash and O. Zelikovska, "The method of improving the signal detection quality by accounting for interference," *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 2020, pp. 172-175, doi: 10.1109/ATIT50783.2020.9349298.

[14] S.-Y. Kim, S.-W. Yun, E.-Y.Lee, S.-H. Bae and I.-G. Lee, "Fast Packet Inspection for End-To-End Encryption," *Electronics,* vol. 9(11), pp.1937, 2020.

[15] M.A. Khan and J. Kim, Toward Developing Efficient Conv-AE-Based Intrusion Detection System Using Heterogeneous Dataset," *Electronics,* vol. 9(11), pp.1771, 2020. https://doi.org/10.3390/electronics9111771

[16] R. Sun, L. Shi, C. Yin and J. Wang, "An improved method in deep packet inspection based on regular expression," *Journal of Supercomputing,* vol. 75, pp. 3317–3333, 2019. https://doi.org/10.1007/s11227-018-2517-0

[17] B. Goldstein and V. Fitsov, "The Mathematical Model for Calculating Physical Entity of DPI Analyser," In: Vishnevskiy V.M., Samouylov K.E., Kozyrev D.V. (eds) *Distributed Computer and Communication Networks: Control, Computation, Communications. DCCN 2020.* Communications in Computer and Information Science, vol. 1337, pp 382-393. Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-66242-4_30

[18] T. Radivilova, L. Kirichenko, A. S. Alghawli, A. Ilkov, M. Tawalbeh and P. Zinchenko, "The complex method of intrusion detection based on anomaly detection and misuse detection," *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2020, pp. 133-137, doi: 10.1109/DESSERT50317.2020.9125051.

[19] B. Siregar, M. S. Manik, R. Rahmat, U. Andayani and F. Fahmi, "Implementation of network monitoring and packets capturing using random early detection (RED) method," *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 2017, pp. 42-47, doi: 10.1109/COMNETSAT.2017.8263571.

[20] J. Li, C. Wu, J. Ye, J. Ding, Q. Fu and J. Huang, "The Comparison and Verification of Some Efficient Packet Capture and Processing Technologies," *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech),* 2019, pp. 967-973, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00177.

[21] F. Aryeh, B. Alese and O. Olasehinde, "Graphical analysis of captured network packets for detection of suspicious network nodes," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* , 2020, pp. 1-5.

[22] A. Ghosh and A. Senthilrajan, "An Approach for Detecting Man-In-The-Middle Attack Using DPI and DFI,". In: Pandian A., Palanisamy R., Ntalianis K. (eds) *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2019).* Lecture Notes on Data Engineering and Communications Technologies, vol. 49, pp.563-574. Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-43192-1_64

[23] Y.T. Guo, Y. Gao, Y. Wang, M.Y. Qin, Y.J. Pu, Z. Wang, D.D. Liu, X.J. Chen, T.F. Gao, T.T. Lv, Z.C. Fu, "DPI & DFI: A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection," *Procedia Engineering*, vol.174, pp. 1309-1314, 2017. https://doi.org/10.1016/j.proeng.2017.01.276.

[24] L. Kirichenko, P. Zinchenko and T. Radivilova, "Classification of Time Realizations Using Machine Learning Recognition of Recurrence Plots," In: Babichev S., Lytvynenko V., Wójcik W., Vyshemyrskaya S. (eds) *Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2020.* Advances in Intelligent Systems and Computing, vol 1246. Springer, Cham, pp. 687-696, 2021. https://doi.org/10.1007/978-3-030-54215-3_44.

[25] T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh, V. Bulakh and P. Zinchenko, "Intrusion Detection Based on Machine Learning Using Fractal Properties of Traffic Realizations," *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2019, pp. 218-221. doi: 10.1109/ATIT49449.2019.9030452.

[26] T. Radivilova, L. Kirichenko and A. S. Alghawli, "Entropy Analysis Method for Attacks Detection," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 443-446. doi: 10.1109/PICST47496.2019.9061451.

[27] T. Radivilova, L. Kirichenko, D. Ageiev and V. Bulakh, "Classification methods of machine learning to detect DDOS attacks," *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Metz, France, 2019, pp. 207-210. doi: 10.1109/IDAACS.2019.8924406