Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare

Sergiy Gnatyuk[1], Rat Berdibayev[2], Andriy Fesenko[3], Olha Kyryliuk[4], and Anatoly Bessalov[5]

[1] *National Aviation University, 1 Liubomyr Huzar ave., Kyiv, 03058, Ukraine*
[2] *Almaty University of Power Engineering and Telecommunication, 126/1 Baytursynuli str., Almaty, 050013, Kazakhstan*
[3] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01033, Ukraine*
[4] *Volodymyr Vynnychenko Central Ukrainian State Pedagogical University, 1 Shevchenka str., Kropyvnytskyi, 25000, Ukraine*
[5] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudravska str., Kyiv, 04053, Ukraine*

Abstract

Today Security Information and Event Management (SIEM) systems are used to prevent information loss in computer systems and networks. There are many approaches to SIEM realization. This paper is devoted to the analysis of existing SIEM and their characteristics in accordance with international standards and specifications, as well as a comparative description of their capabilities and differences, advantages and disadvantages. These results will be used in research project realization devoted to open source SIEM development and implementation in critical infrastructure to improve the cybersecurity level in the context of information warfare and cyber threats realization.

Keywords

SIEM, firewall, IDS, cyber attack, cyber monitoring, security management, risk management, information warfare.

1. Introduction

Today, the number of cyber threats is increasing, this is due to the development of new technologies and an insufficiently good level of testing of the developed software and physical software, as well as the lack of maintenance and support for outdated software and server software. Because of this, there are various vulnerabilities in protocols, software, as well as the architecture of electronic equipment, which affects the security of information on the entire global Internet network, both local and public [1,2].

Therefore, to correct these security flaws, systems for real-time event monitoring and incident management, well-known as SIEM (security information and event management), were created in order to prevent the future consequences of the exploitation of vulnerabilities by undesirable persons, as well as to minimize damage to the end user. In the current article, we will consider the existing SIEM systems, consider their structure, and also conduct a comparative analysis of their capabilities and differences, advantages and disadvantages, and compliance with international standards and specifications. Consider the main security and incident management systems further [3].

2. Main Characteristics of SIEM

For certification, all SIEM systems must comply with the international group of information security standards: ISO / IEC 27000 PCI-DSS, HIPAA, NIST 800-171, DoD, RMF, GDPR.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: s.gnatyuk@nau.edu.ua (S. Gnatyuk); r.berdybaev@aues.kz (R. Berdibayev); aafesenko88@gmail.com (A. Fesenko); kyryluk@ukr.net (O. Kyryliuk); a.bessalov@kubg.edu.ua (A. Bessalov)
ORCID: 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-8341-9645 (R. Berdibayev); 0000-0001-5154-5324 (A. Fesenko); 0000-0002-9764-8756 (O. Kyryliuk); 0000-0002-6967-5001 (A. Bessalov)

To solve problems related to security and fixing events of a SIEM system, consider the main functionality of SIEM systems:

- *Data aggregation:* data log management; data is collected from various sources.
- *Correlation:* finding common attributes, linking events to meaningful clusters.
- *Alert:* automated analysis of correlated events and generation of notifications (alarms) about current problems (e-mail, GSM-gateway, applications on the phone).
- *Display facilities:* displays graphs to help identify work anomalies using prepared patterns.
- *Compatibility:* using add-ons to automate data collection, create reports to adapt aggregated data to existing information security management and audit processes.
- *Data storage:* the use of long-term data storage in historical order to correlate data over time and for further computer forensics and investigation of network incidents.
- *Expert analysis:* the ability to search through a variety of journals on various nodes, including for software and technical expertise.

3. Analysis of Modern SIEM Systems

Based on these characteristics, we have analyzed up-to-date SIEM systems and compare their capabilities. It was the main objective of this research study.

3.1. IBM QRadar Security Intelligence Platform

IBM QRadar Security Intelligence Platform [4] consists of a number of integrated systems for event collection, monitoring, security analysis and incident investigation:

1. Log Manager.
2. SIEM.
3. Flow Processor.
4. Vulnerability Manager.
5. Risk Manager.
6. Network Insights.
7. Watson Advisor for Cyber Security.
8. Packet Capture and Incidents Forensics.

QRadar allows you to collect and process information about information security events from security audit logs, analyze network statistics (NetFlow, etc.), independently analyze network traffic and transmitted information, build a network topology and emulate changes in configuration files of network equipment, identify vulnerabilities and unsafe settings systems, completely capture traffic and recreate a chain of communications between network nodes.

Benefits of the IBM QRadar Security Intelligence Platform (Fig. 1):

- A unified platform for the systematic creation of SOC: collection and analysis of information security events, detection of abnormal network activity, scanning of vulnerabilities and identification of unsafe configurations, integration with artificial intelligence IBM Watson, network forensics and transition to incident response processes in IBM Resilient.
- Flexible architecture of QRadar Platform, which allows you to redefine the role and functions of platform modules and does not limit client companies to rigid frameworks of a once-selected scheme.
- A large number of free applications, content and integration modules.

Figure 1: IBM QRadar Security Intelligence Administrator GUI

3.2. logRhythm

LogRhythm [5], as a platform, offers an intelligent security solution that uses artificial intelligence to analyze logs and traffic on Windows and Linux systems (Fig. 2).

System advantages:

- has an expandable data storage;
- suitable for systems where there is no structured data, no centralized visibility or automation;
- suitable for small and medium-sized organizations;
- allows you to filter out useless information or other logs and narrow the analysis down to the network level;
- Compatible with a wide range of logs and devices, and seamlessly integrates with Varonis to enhance threat and incident response capabilities.

Figure 2: LogRhythm Administrator GUI

3.3. HPE ArcSight

Hewlett Packard Enterprise (HPE) ArcSight is the most widespread SIEM system in the East-European market [6].

HPE ArcSight is targeted at midsize to large enterprises and service providers (Fig. 3).

The HPE ArcSight platform can be deployed as a device, software, or virtual instance. HPE ArcSight supports a scalable n-tier architecture with HPE ArcSight Management Center.

HPE ArcSight benefits:

- Arcsight ESM provides a complete set of SIEM capabilities that can be used to support a large-scale SOC, including a complete incident investigation and management workflow, and a dedicated deployment management console.
- HPE User Behavior Analytics identifies anomalies based on user behavior analysis and complements traditional correlation, which is the core function of arcsight.
- DNS Malware Analytics analyzes DNS traffic and provides complete visibility of the IT infrastructure, which helps to identify network vulnerabilities even before attackers take advantage of them.
- Arcsight Threat Central contains an online threat knowledge base and allows you to share information on how to detect and eliminate them.

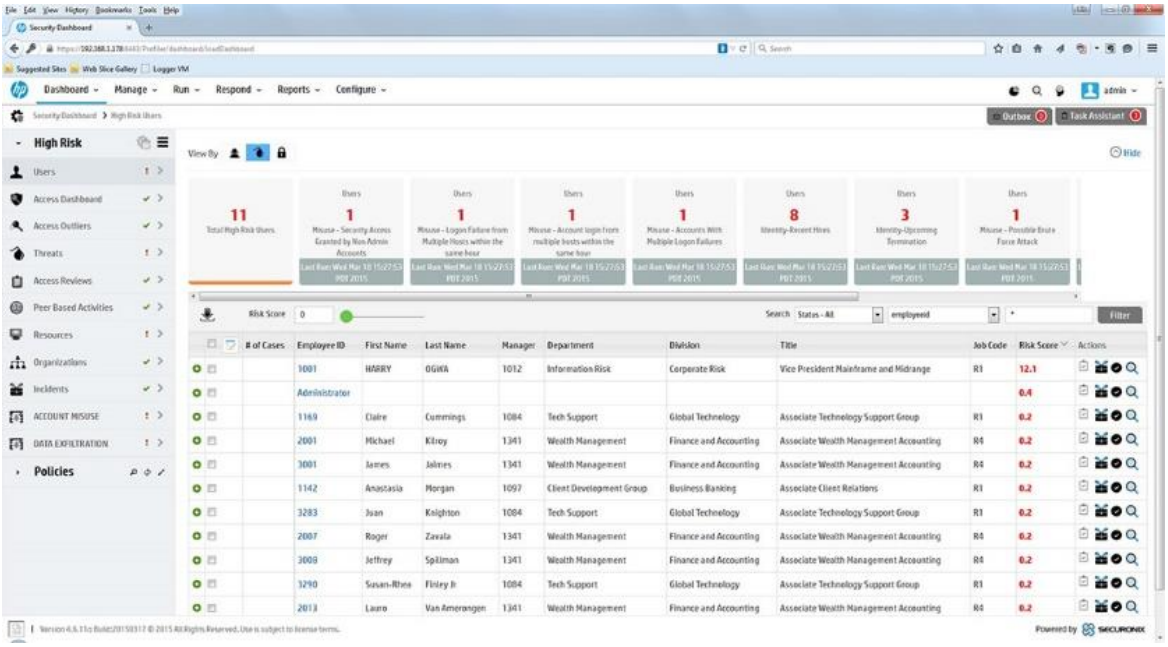

Figure 3: Analytics of user and entity behavior in HPE ArcSight

3.4. Splunk

Splunk is a tool that leverages the power of artificial intelligence and machine learning to deliver actionable, effective, and predictive insights (Fig. 4).

Splunk [5,7] is suitable for all types of organizations for both on-premises and SaaS deployments. Key benefits:

- Fast threat detection.
- Identification and assessment of risks.
- Management of alerts.
- Ordering events.
- Fast and efficient response.
- Works with data from any machine, both on-premises and in the cloud infrastructure.

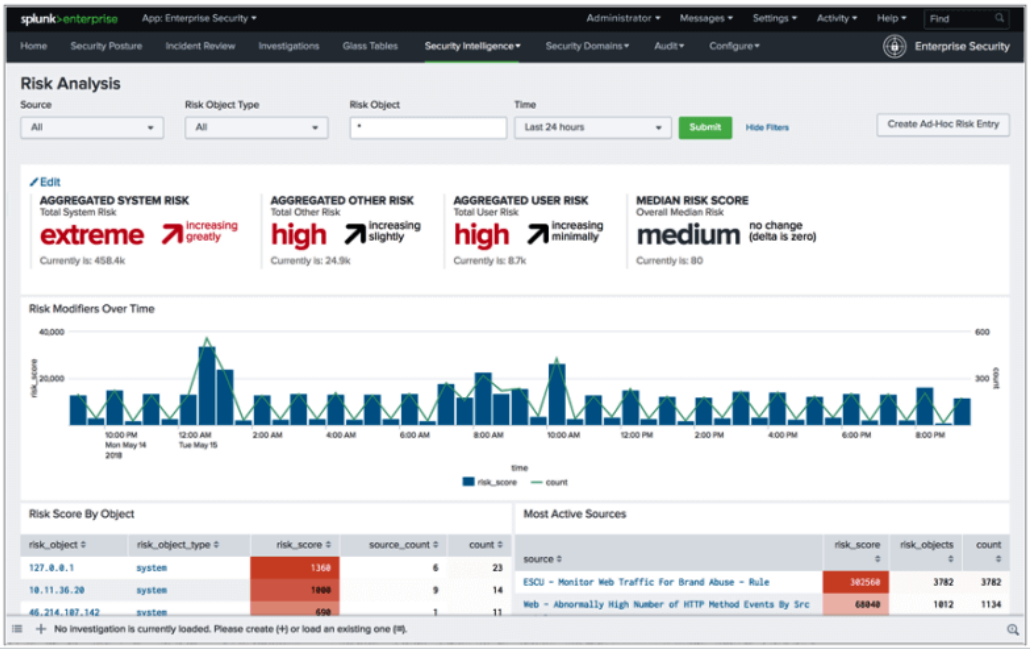

Figure 4: Splunk admin GUI

3.5. McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) [5] is delivered as physical and virtual devices and software. The three main components that make up SIEM are ESM, Event Receiver and Enterprise Log Manager, which can be deployed together as a single instance or separately for distributed or large-scale environments (Figure 5).

McAfee Enterprise Security Manager benefits:

- Enterprise Security Manager has good coverage of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) devices.
- McAfee Data Exchange Layer (DXL) from Intel Security provides non-API integration with third-party technologies. This approach makes it possible to use ESM as a SIEM platform.
- McAfee Global Threat Intelligence extends Enterprise Security Manager's SIEM system by adding a source of continuously updated threat intelligence, enabling rapid detection of events involving communications with suspicious or malicious IP addresses.

Figure 5: McAfee Enterprise Security Manager Administrator GUI

3.6. Alien Vault USM

Alient Vault USM is a comprehensive information security management platform that centralizes and simplifies threat detection, incident response, and compliance management in cloud and on-premises environments (Fig. 6).

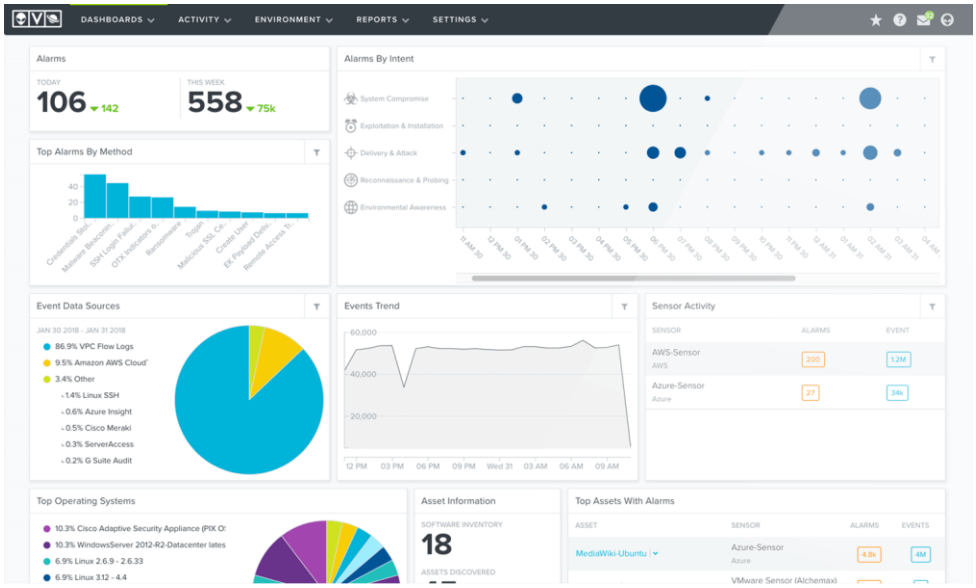

Figure 6: AlienVault interface

Key features of AlienApps [6]:

- Extract and analyze security data from third-party applications.
- Visualize external data in graphical USM Anywhere information dashboards with many functions.
- Manage third-party security solutions based on threat intelligence analyzed in USM Anywhere.
- Leverage progressive security features as new AlienApps modules are added to USM Anywhere.

3.7. FortiSIEM

FortiSIEM is a comprehensive, scalable security, performance, and compliance management tool for all infrastructure components, capable of working with both the cloud and the Internet of Things (IoT) [15–18]. The FortiSIEM solution [5] is aimed at reducing the complexity of detecting threats while increasing the effectiveness of the security system and exchanging information with the product, including about discovered vulnerabilities (Fig. 7.).

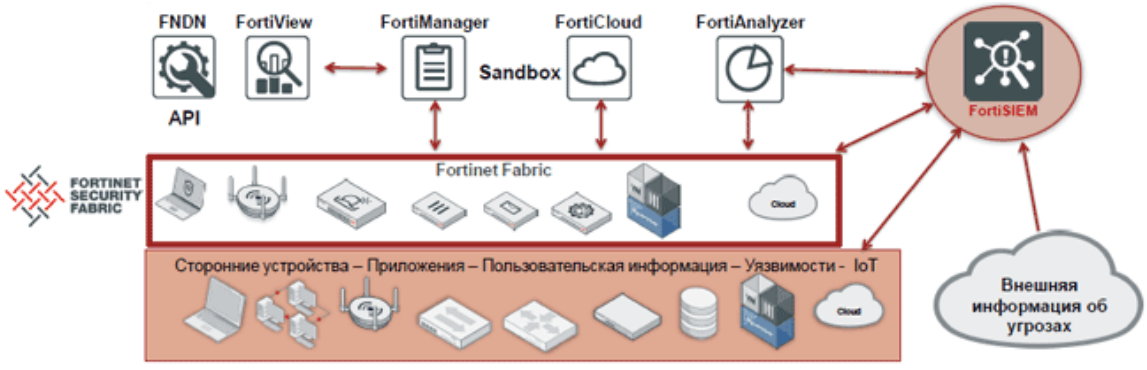

Figure 7: FortiSIEM in the Fortinet Security Fabric concept

Key features of FortiSIEM (Fig. 8):

- Scalable and flexible log collection.
- Incident notification and management.
- Providing the user with fully functional custom dashboards.
- Integration of external threat data.
- Providing a scalable analysis function.
- Set baselines and identify statistical anomalies in endpoint /server/user behavior.
- Integration of external technologies.

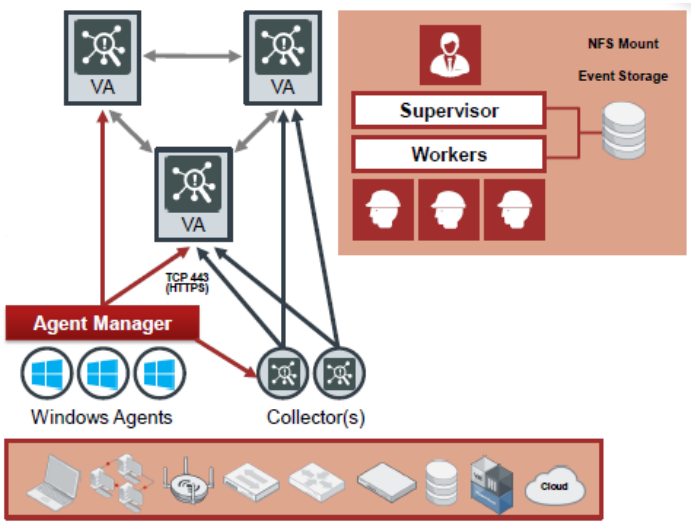

Figure 8: FortiSIEM architecture

3.8. Ixia ThreatARMOR

Key features (Fig. 9):

- Ensuring full bandwidth.
- Eliminate threats by blocking all traffic from known malicious sites and untrusted countries.
- Elimination of the possibility of false positives - visual confirmation of malicious actions for all blocked sites.
- Improved processing efficiency by reducing the number of safety alerts.
- Threat Intelligence updates every 5 minutes using Cloud Update Subscription (ATI).
- Quick identification of compromised internal systems.
- Blocking the connection with the captured ip-addresses.
- Dual power redundancy and built-in bypass capability for maximum reliability.
- Easy 30-minute setup with no further adjustments or maintenance, and centralized management from the cloud.
- Increases the return on investment and performance of the network security infrastructure [7].

Figure 9: FortiSIEM architecture

3.9. MozDef (Mozilla Defense Platform)

The Mozilla SIEM system MozDef [7] is used to automate security incident handling. The system is designed from scratch for maximum performance, scalability and fault tolerance, with a microservice architecture - each service runs in a Docker container (Fig. 10).

Benefits:

- Does not use agents - works with standard JSON logs.
- Easily scalable due to microservice architecture.
- Supports cloud service data sources including AWS CLOUDTRAIL and GUARDDUTY.

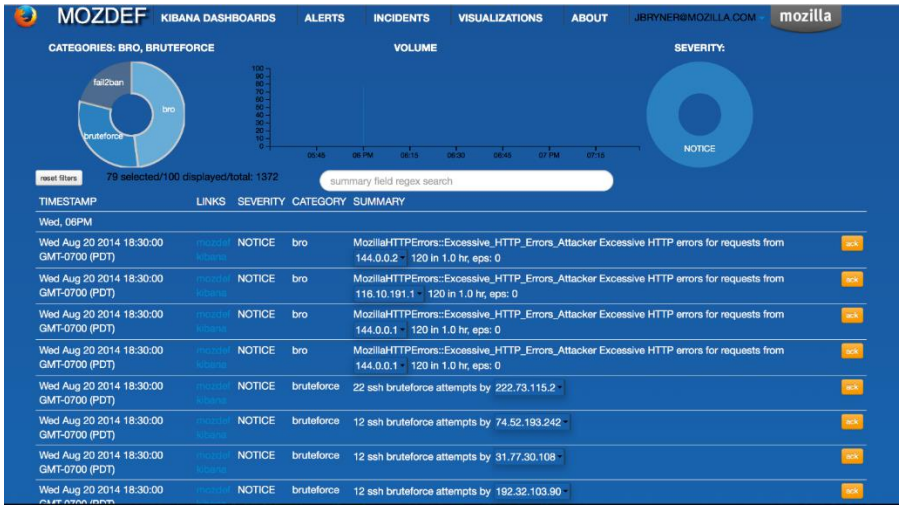

Figure 10: Mozdef interface

3.10. Wazuh

System advantages (Fig. 11):

- Based and compatible with the popular SIEM OSSEC.
- Supports various installation options: DOCKER, PUPPET, CHEF, ANSIBLE.
- Supports monitoring of cloud services including AWS and AZURE.
- Includes a comprehensive set of rules to detect many types of attacks and allows them to be compared in accordance with PCI DSS V3.1 and CIS.
- Integrates with the SPLUNK log storage and analysis system, event visualization and API support [8].

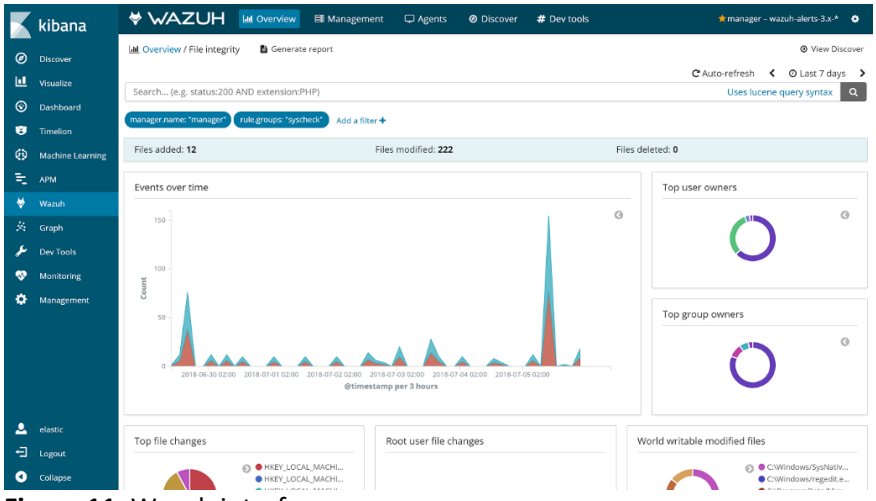

Figure 11: Wazuh interface

3.11. Prelude OSS

Prelude OSS (Fig. 12) solution is a flexible modular SIEM system that supports many log formats, integration with third-party tools such as OSSEC, Snort and Suricata network detection system. Advantages [8,9]:

- A time-tested system in development since 1998.
- Supports many different log formats.
- Normalizes data to IMDEF format, making it easy to transfer data to other security systems.

Figure 12: Prelude OSS interface

3.12. Sagan

System advantages (Fig. 13):

- Fully compatible with SNORT database, rules, and user interface.
- Multi-threaded architecture provides high performance [8].

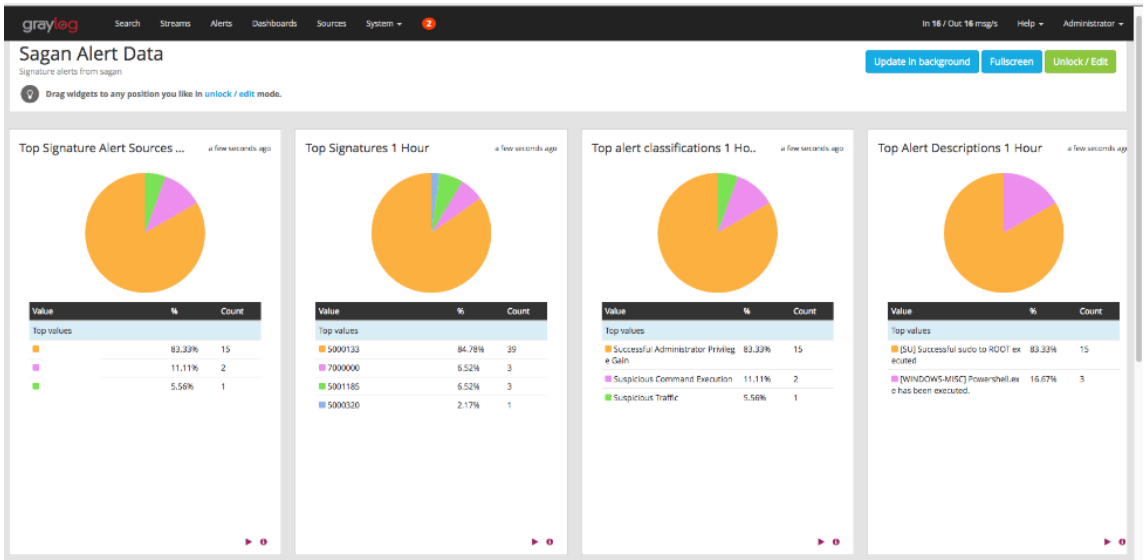

Figure 13: Sagan interface

3.13. Maxpatrol

The advantages of this system (Fig. 14):

- Modularity of the product providing high scalability and performance.
- Deep integration of the SIEM system with the MAXPATROL security analysis tool.
- Correlation rules are resistant to changes in its infrastructure.
- Vendor's willingness to connect any source of logs.
- An event normalization system that allows you to search for events using various structured data.
- Customer customization support—the ability to create your own event filters, correlation rules, collection profiles.
- The ability to distribute incidents among employees, track the status of investigations and conduct work processes within the SIEM system.

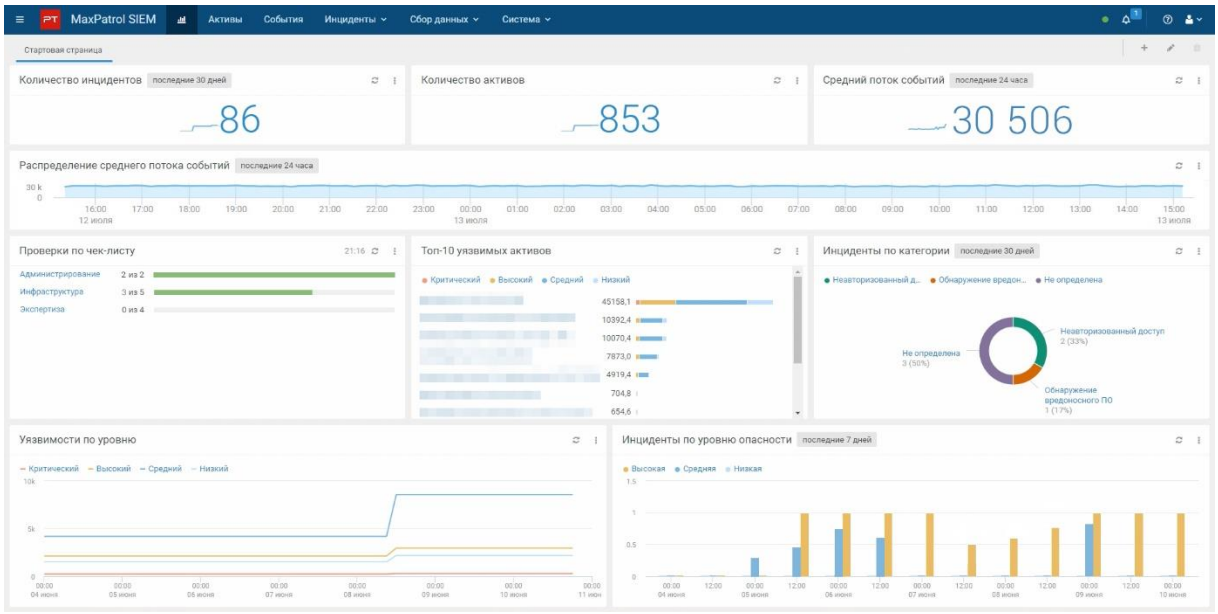

Figure 14: Maxpatrol interface

3.14. SOLARWINDS

SolarWinds (Fig. 15) has great capabilities for managing logs and reporting, responding to incidents in real time [5,10].

Main features of the system:

- Fast detection of suspicious actions and threats.
- Continuous monitoring of the security status.
- Determining the time of the event.
- Compliance with DSS, HIPAA, SOX, PCI, STIG, DISA and other regulations.
- Solarwinds' solution is suitable for small and large businesses. It has both on-premises and cloud Deployment options and runs on Windows and Linux.

Figure 15: Solarwinds interface

3.15. ANAGEENGINE

EventLog Analyzer ManateEngine is a SIEM solution that focuses on analyzing various logs and extracting various performance and security information from them (Fig. 16).

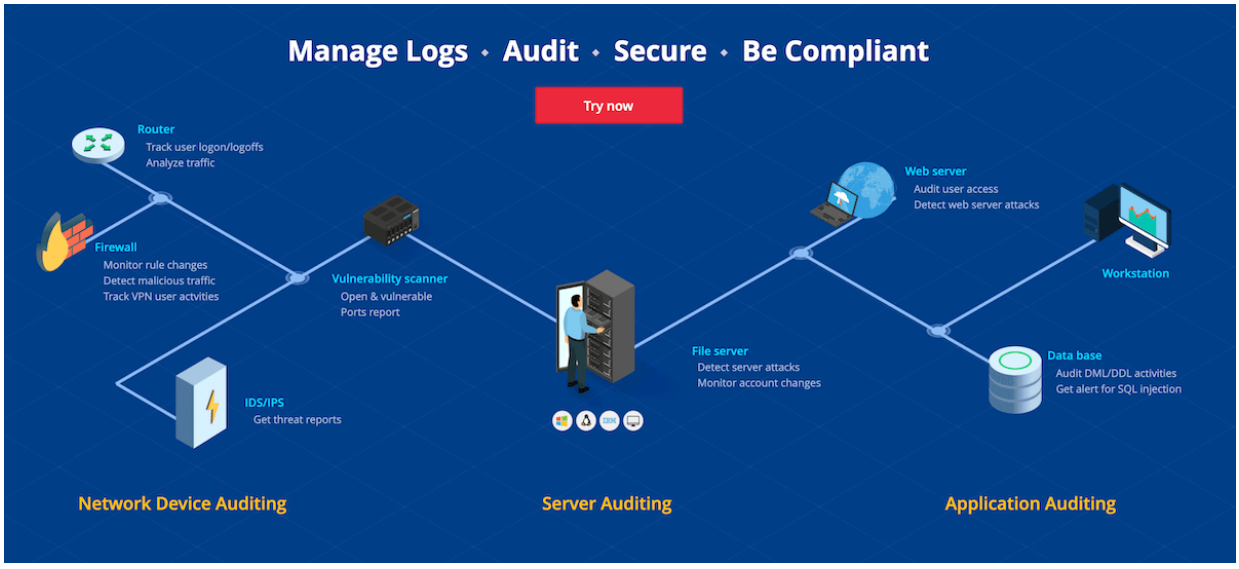

Figure 16: ANAGEENGINE interface

Target areas include key sites and applications such as web servers, DHCP servers, databases, print servers, mail services, etc.

In addition, the ManageEngine analyzer, which runs on Windows and Linux systems, is useful for bringing systems into compliance with data protection standards such as PCI, HIPPA, DSS, ISO 27001, etc. [9,11].

3.16. EventTracker

Key features of the SIEM EventTracker platform (Fig. 17):

1. Real-time alert and incident response. EventTracker generates rule-based alerts with dashboard updates and fix recommendations.
2. Search and forensic analysis. Logs are indexed in Elastic Search using an extensible shared indexing model.
3. Making report. The reporting module includes over 1,500 predefined security and compliance reports. Full support is included for PCI-DSS, HIPAA, ISO 27001, NIST 800-171, DoD, RMF, GDPR and more.
4. Behavior analysis and correlation. EventTracker quickly detects and tracks changes in systems and user behavior. Real-time processing and correlation gives a complete picture of what's new and different.
5. Threat analysis. EventTracker integrates with valuable threat data streams from ecosystem partners and open source vendors to provide fast and accurate threat detection to your network [5,12].

3.17. Micro Focus ArcSight

Micro Focus ArcSight is a cybersecurity product that provides big data security analytics and intelligence software for information security and event management (SIEM) and account management.

Real-time threat detection and response supported by efficient, intelligent open source SIEM (security information and event management) software. Micro Focus ArcSight is a cybersecurity product that provides *big data* security *analytics* and intelligence software for *information security and event management* (SIEM) and account management [6,13].

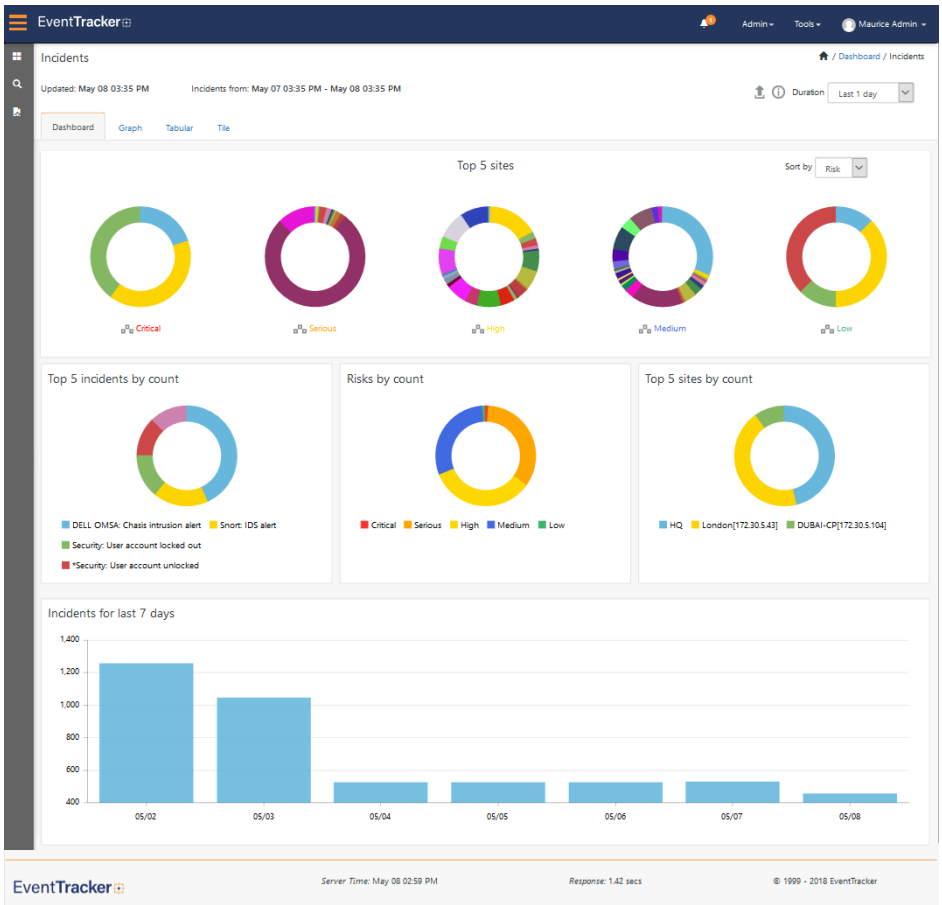

Figure 17: EventTracker interface

3.18. Trustwave SIEM Enterprise

Trustwave benefits:

- Users of other Trustwave security products will benefit from improved bi-directional integration with technologies in their portfolio that support automatic response capabilities, such as isolating compromised endpoints or blocking user accounts;
- Trustwave SIEM Enterprise (Fig. 18) has one of the simplest architectures, which reduces the load on clients during deployment and subsequent expansion [10].

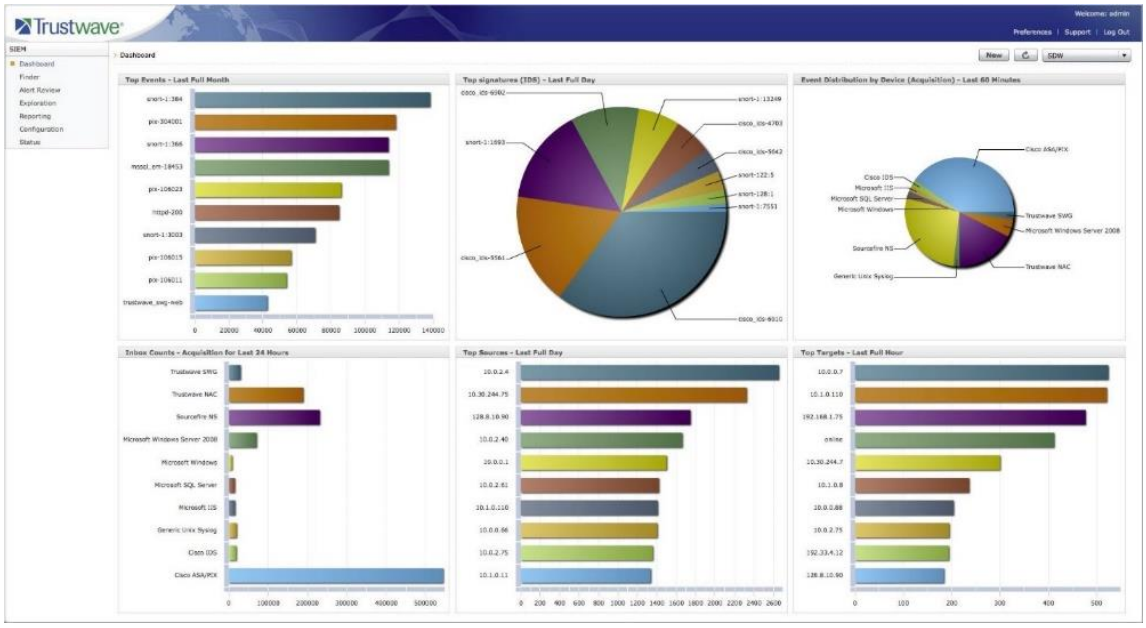

Figure 18: Graphical Administrator Interface Trustwave SIEM Enterprise

3.19. BlackStratus SIEM Storm

The BlackStratus SIEMStorm device provides flexible threat visualization and mitigation tools across distributed networks. SIEMStorm integrates with existing network and security equipment, providing the following advanced features [10,14]:

1. Extended architecture. Blackstratus Siemstorm provides full failover and tiered redundancy to meet complex regulatory requirements, business continuity and risk management.
2. Real-time visualization of the attack. Identify zero-day attacks using complex metrics based on rules, vulnerabilities, statistical and historical correlations.
3. Correlation of vulnerability. Integrate data from CVE-compliant intrusion detection systems, eliminate false positives and free your team to focus on real threats
4. Transparency. Gain unprecedented visibility across distributed networks to correlate activity in separate network environments, identify hidden threats, suspicious trends, and other potentially harmful behavior
5. Making report. Blackstratus Siemstorm provides easy reporting for iso, pci, hipaa, sox and other compliance standards

3.20. RSA NetWitness Suite (EMC)

RSA NetWitness Suite provides threat visibility using data from security events and other log sources, full packet capture, NetFlow, and endpoints (via RSA NetWitness Endpoint).

RSA NetWitness is focused on real-time monitoring, analysis, and alerting in addition to proactive threat support and incident response and forensic investigation [5,14].

Benefits of RSA NetWitness Suite:

- The rsa netwitness platform brings together threat detection and event monitoring analytics, investigation and analysis of threats in network traffic, endpoints and other sources of security events and logs.
- Modular deployment options allow customers to choose to monitor network traffic and monitor and analyze events and logs as needed.
- RSA LIVE provides a simple and automated approach to ensure uninterrupted delivery of threat intelligence, content and other updates.

4. Comparative Analysis of SIEM Systems

Fig. 19 demonstrates results of the detailed analysis of SIEM systems for the following characteristics:

1. Audit and verification for compliance with standards.
2. Complete system / log processing system.
3. Assessment of the security of the resources of the controlled system.
4. Checking the compliance of the IS management system with existing requirements and standards.
5. Information security risk management [17–19].
6. Collection and storage of incoming security events.
7. Processing and analysis of registered security events [22–24].
8. Detection of attacks and violations of security policies in real time.
9. Identification and analysis of security incidents.
10. The ability to investigate incidents.
11. Search for vulnerabilities.
12. Formation of reports.
13. Support for working with clouds [15–18].
14. Support for working with Big Data platforms [25].
15. Possibilities of integration with new systems.
16. Advanced search and data visualization capabilities.
17. User friendly interface.
18. Supported operating systems.
19. The main sources of logs.
20. System cost.

5. Conclusion

In this paper, we reviewed existing modern SIEM systems, their functionality, the basic principle of their operation, and also conducted a comparative analysis of each of them, their capabilities and differences, advantages and disadvantages of use. An analysis was also carried out for compliance with international specifications and standardizations in this sphere.

Based on the analysis, we can declare that the FortiSIEM system is the most optimal. Systems IBM QRadar, LOGRHYTHM, according to the selection criteria, also gain a large number of points, but are expensive and not available for many companies. Also, developers should pay their attention on the open source solutions specified in Table 1 and 2.

In the future these results will be used in research project realization devoted to open source SIEM development and implementation in critical infrastructure to improve the cybersecurity level in the context of information warfare and cyber threats realization.

Table 1

Multicriteria analysis of SIEM systems (part 1)

System name	Audit and Compliance	Complete System (PS) / Log Processing System (SOL)	Assessment of the security of the resources at the controlled system	Verification of compliance of the IS management system with existing requirements and standards	Information security risk management	Collecting and storing incoming security events	Processing and analysis of registered security events	Detect attacks and security policy violations in real time	Identification and analysis of security incidents	Incident investigation capability
IBM QRadar	+	PS	+	+	+	+	+	+	+	+
LOGRHYTHM	+	PS	+	+	+	+	+	+	+	+
HPEArcSight	+	PS	+	+	+	+	+	+	+	+
Splunk	+	PS	+	+	+	+	+	+	+	+
McAfee (ESM)	+	PS	+	+	+	+	+	+	+	+
AlienVault USM	+	PS	+	+	+	+	+	+	+	+
Alien Vault OS SIM	–	PS	+	+	+	+	+	+	+	±
FoniSIEM	+	PS	+	+	+	+	+	+	+	+
Ixia ThreatARMOR	+	PS	+	+	+	+	+	+	+	+
MozDef	+	PS	–	+	–	+	+	+	+	+
Wazuh	+	PS	not indicated	+	–	+	+	+	+	+
Prelude OSS	+	PS	not indicated	+	+	+	+	+	+	+
Prelude SIEM	+	PS	not indicated	+	+	+	+	+	+	+
Sasan	–	SOL	–	–	–	+	+	+	+	+
Maxpatrol	+	PS	+	+	+	+	+	+	+	+
SolarWinds	+	PS	+	+	+	+	+	+	+	+
ManateEnaine	+	SOL	–	+	–	+	+	+	+	+
EventTracker	+	PS	–	+	–	+	+	+	+	+
Micro Focus ArcSight	+	PS	+	+	+	+	+	+	+	+
Trustwave SIEM Enterprise	+	PS	–	+	+	+	+	–	+	+
BlackStratus SIEMStonn	+	PS	–	+	–	+	+	+	+	+
SearchInfonn SIEM	+	PS	+	+	+	+	+	+	+	+
RuSIEM	+	PS	+	+	+	+	+	+	+	+

Table 2
Multicriteria analysis of SIEM systems (part 2)

System name	Search for vulnerabilities	Report generation	Cloud support	Support for working with Big Data platforms	Possibilities of integration with new systems tomorrow	Advanced search and data visualization	User friendly interface	Supported operating systems	Main sources of logs	System cost
IBM QRadar	+	+	+	+	+	+	+	linux	Lots of	$ 63000 +
LOGRHYTHM	+	+	+	+	+	+	+	linux/windows	Lots of	$ 28000 +
HPEArcSight	+	+	+	+	+	+	+	linux	Lots of	500 thousand rubles +
Splunk	+	+	+	+	+	+	+	Unix/Windows	Lots of	Free 500 mb S 5.000 for 1 GB day
McAfee (ESM)	+	+	+	+	+	+	+	Windows	Lots of	$ 261000 +
AlienVault USM	+	+	+	+	+	+	+	Linux/Windows	Lots of	$ 1075/mo.
Alien Vault OS SIM	+	+	–	–	–	+	+	Linux/Windows	Lots of	free
FoniSIEM	+	+	+	+	+	+	+	Linux/Windows	Lots of	$ 900 +
Ixia ThreatARMOR	+	+	–	–	+	+	+	Unix/Windows/ other	Lots of	£ 3158/year
MozDef	–	+	+	+	+	+	+	Centos 7	Json	free
Wazuh	+	+	+	+	+	+	+	Linux	Windows/ Linux logs	free
Prelude OSS	+	+	–	–	–	+	+	Linux	Lots of	free
Prelude SIEM	+	+	–	–	–	+	+	Linux	Lots of	9
Sasan	–	+	–	–	–	+	–	Linux	Lots of	free
Maxpatrol	+	+	+	+	+	+	+	–	Lots of	RUB 1,840,000 +
SolarWinds	+	+	+	+	+	+	+	Linux/Windows agents	Lots of	2.055 € +
ManateEnaine	+	+	–	–	–	+	+	Windows	Windows/ Linux logs	$ 1000 +
EventTracker	+	+	+	+	–	+	+	Windows	Windows/ Linux logs	$8995
Micro Focus ArcSight	+	+	+	+	+	+	+	Linux	Lots of	500 thousand rubles +
Trustwave SIEM Enterprise	+	+	+	+	–	+	+	Centos 7	Lots of	$1000/year
BlackStratus SIEMStonn	+	+	–	–	–	+	+	–	not indicated	–
SearchInfonn SIEM	+	+	+	+	+	+	+	Linux/Windows	Lots of	Negotiable
RuSIEM	+	+	–	–	+	+	+	Ubuntu 16	Lots of	Paid/no fee

6. Acknowledgement

This work is carried out within the framework of research grant №AP06851243 “Methods, models and tools for security events and incidents management for detecting and preventing cyber attacks on critical infrastructures of digital economics” (2020–2022), funded by the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

7. References

[1] V. Buriachok, V. Sokolov, P. Skladannyi, Security rating metrics for distributed wireless systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 222–233, 2019.

[2] Kipchuk, F., et al. Investigation of Availability of Wireless Access Points based on Embedded Systems. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019. https://doi.org/10.1109/picst47496.2019.9061551

[3] I. Bogachuk, V. Sokolov, V. Buriachok, Monitoring subsystem for wireless systems based on miniature spectrum analyzers, in: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, 2018. https://doi.org/10.1109/infocommst.2018.8632151.

[4] Ariel Query Language Guide, IBM QRadar 7.3.3 (2013 and 2019). Available on: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_aql.pdf

[5] Vielberth M. and Pernul G. “A Security Information and Event Management Pattern”. 12th Latin American Conference on Pattern Languages of Programs (SugarLoafPLoP 2018), 2018, p. 27.

[6] Agrawal K., Makwana H. “A Study on Critical Capabilities for Security Information and Event Management”. International Journal of Science and Research (IJSR). Vol. 4 Issue 7, July 2015 Rock, pp. 1893-1896.

[7] Henrik Karlzén, “An Analysis of Security Information and Event Management Systems”. University of Gothenburg, Göteborg, Sweden, January 2009. Available on: http://publications.lib.chalmers.se/records/fulltext/89572.pdf

[8] SIEM Analytics: http://www.siem.su/compare_SIEM_systems.php

[9] J. Lee, Y. Kim, J. Kim and I. Kim, “Toward the SIEM architecture for cloud-based security services,” 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV 2017, pp. 398-399, DOI: 10.1109 / CNS.2017.8228696.

[10] I. Bachane, Y. I. K. Adsi and H. C. Adsi, “Real time monitoring of security events for forensic purposes in Cloud environments using SIEM,” 2016 Third International Conference on Systems of Collaboration (SysCo), 2016, pp. 1-3, DOI: 10.1109/SYSCO.2016.7831327.

[11] B. Al Sabbagh and S. Kowalski, “A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM),” 2016 European Intelligence and Security Informatics Conference (EISIC), 2016, pp. 192-195, DOI: 10.1109/EISIC.2016.049.

[12] A. Serckumecka, I. Medeiros and A. Bessani, “Low-Cost Serverless SIEM in the Cloud,” 2019 38th Symposium on Reliable Distributed Systems (SRDS), 2019, pp. 381-3811, DOI: 10.1109/SRDS47363.2019.00057.

[13] M. Nabil, S. Soukainat, A. Lakbabi and O. Ghizlane, “SIEM selection criteria for an efficient contextual security,” 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017, pp. 1-6, DOI: 10.1109/ISNCC.2017.8072035.

[14] R.-V. Mahmoud, E. Kidmose, A. Turkmen, O. Pilawka, J.M. Pedersen, “DefAtt - Architecture of Virtual Cyber Labs for Research and Education”, 2021 International Conference on Cyber Situational Awareness Data Analytics and Assessment (CyberSA), pp. 1-7, 2021.

[15] Yu. Danik, R. Hryschuk, S. Gnatyuk, “Synergistic effects of information and cybernetic interaction in civil aviation”, Aviation, Vol. 20, №3, pp. 137-144, 2016.

[16] Berdibayev R., Gnatyuk S., Yevchenko Yu., Kishchenko V. “A concept of the architecture and creation for SIEM system in critical infrastructure”, Studies in Systems, Decision and Control, Vol. 346, 2021, pp. 221-242.
[17] Gnatyuk S., Berdibayev R., Avkurova Z., Verkhovets O., Bauyrzhan M. “Studies on cloud-based cyber incidents detection and identification in critical infrastructure”, CEUR Workshop Proceedings, 2021, Vol. 2923, pp. 68-80.
[18] J. Lee, Y. S. Kim, J. H. Kim and I. K. Kim, “Toward the SIEM architecture for cloud-based security services,” 2017 IEEE Conference on Communications and Network Security (CNS), 2017, pp. 398-399, DOI: 10.1109/CNS.2017.8228696.
[19] Faure, E., Shcherba, A., Vasiliu, Y., Fesenko, A. Cryptographic key exchange method for data factorial coding (2020) CEUR Workshop Proceedings, 2654, pp. 643-653.
[20] Astapenya V., Buriachok V., Sokolov V., Skladannyi P. and Ageyev D. “Last mile technique for wireless delivery system using an accelerating lens”, Proceedings of 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, pp. 811-814, 2021. DOI:10.1109/PICST51311.2020.946788
[21] V. Kuzmin, M. Zaliskyi, R. Odarchenko, Yu. Petrova, “New Approach to Switching Points Optimization for Segmented Regression during Mathematical Model Building”, CEUR Workshop Proceedings, 2022, Vol. 3077, pp. 106-122.
[22] I. Ostroumov and N. Kuzmenko, “Configuration Analysis of European Navigational Aids Network,” 2021 Integrated Communications Navigation and Surveillance Conference (ICNS), 2021, pp. 1-9, DOI: 10.1109/ICNS52807.2021.9441576.
[23] O. Solomentsev, M. Zaliskyi, O. Shcherbyna, O. Kozhokhina, “Sequential Procedure of Changepoint Analysis During Operational Data Processing”, Microwave Theory and Techniques in Wireless Communications, 2020, pp 168-171, DOI: 10.1109/MTTW51045.2020.9245068.
[24] I. Ostroumov, N. Kuzmenko “Compatibility analysis of multi signal processing in APNT with current navigation infrastructure,” in Telecommunications and Radio Engineering, vol. 77, issue 3, 2018, pp. 211-223.
[25] I. Zhukov, N. Pechurin, L. Kondratova et al, Increasing the accuracy of the information load annual growth evaluation on the internet of things, CEUR Workshop Proceedings, vol. 2588, 2019, art. 158907.