DOI: https://doi.org/10.26642/ten-2024-1(93)-170-175
UDC 004.4+004.77

**A.A. Yefimenko, Ph.D., Assoc. prof., Head of Dept.**
**M.V. Honcharov**
*Zhytomyr Polytechnic State University*

# The Study of the Possibilities of Using SOC Based on Free and Open Source Software

*The article considers a specific combination of Security Operations Center solutions that use free open source software as an alternative to Security Operations Center based on expensive proprietary ones. The study identifies each of the components of such a Security Operations Center, describes their place and interaction in the process of detecting, analyzing and mitigating the consequences of cyber attacks. The competitiveness of such an Security Operations Center is analyzed, its advantages, disadvantages and development prospects are determined.*

*The research analyzes a specific combination of free open-source tools, detailing each component's role and interaction in detecting, analyzing, and mitigating cyber threats. The proposed free open-source Security Operations Center comprises a Security Information and Event Management system (Elastic Stack), Security Orchestration, Automation and Response platform (TheHive and Cortex), Intrusion Prevention/Intrusion Detection System (Snort), Endpoint Detection and Response/Extended Detection and Response (Wazuh), threat intelligence platform (MISP), vulnerability scanner (OpenVAS), malware analysis tool (YARA), honeypot solution (Honeyd), and detection testing framework (Atomic Red Team).*

*The study illustrates use cases demonstrating the Security Operations Center's response to ransomware infections, vulnerability exploits, and honeypot triggers, highlighting the synergistic interplay between components. Advantages of the free open-source Security Operations Center include cost-effectiveness, customizability, agility, reliability, community support, and resilience. Drawbacks encompass complexity, integration challenges, limited documentation, lack of vendor support, potential security risks, and restricted features compared to enterprise solutions.*

*The research concludes that while deploying and managing free open-source tools can be complex, the advantages of a free open-source Security Operations Center outweigh the disadvantages, making it a viable option for organizations with specific security needs, especially those with budgetary constraints.*

***Keyword*** *SOC (Security Operations Center); FOSS (Free Open-source Software); IS (Information Security); threat detection; incident response; threat intelligence.*

**Introduction.** The COVID-19 pandemic and the ongoing war in Ukraine have disrupted the operations of many companies, forcing them to face new and evolving cybersecurity threats. As a result, the need for reliable and effective security measures has never been greater. One way to strengthen protection against cyber threats is to implement a Security Operations Center (SOC). While traditional SOCs based on proprietary enterprise-level solutions have been the norm for many years, a new trend has emerged: SOCs based on free and open source software (hereinafter referred to as FOSS).

**An overview of the modern FOSS SOC solutions market.** The market of FOSS tools for cybersecurity has been growing rapidly in recent years. According to a report by MarketsandMarkets, the open source security market is expected to grow from $1.5 billion in 2020 to $3.5 billion in 2025, at a CAGR of 18.3%. This growth can be attributed to the increasing adoption of open source software by companies due to its cost-effectiveness and flexibility.

As for specific tools, there are several popular FOSS options in the cybersecurity market. For example, the popular SIEM tool, ELK Stack, has become widely used due to its flexibility and scalability. Another popular FOSS tool is the Suricata intrusion detection system, which has gained popularity for its ability to detect and prevent network intrusions.

Other popular FOSS tools in the cybersecurity market include EDR/XDR solutions such as OSSEC and Wazuh, SOAR platforms such as TheHive and Cortex, and vulnerability scanners such as OpenVAS and Nikto. These tools have gained popularity due to their ability to provide powerful cybersecurity solutions at a lower cost than their proprietary counterparts.

Many cybersecurity blogs and publications have noted the growth of the open source software market and the benefits of using open source software in cybersecurity. For example, CSO Online published an article in 2021 entitled "Why Open Source Software is the Future of Cybersecurity," which emphasizes the cost savings and customization opportunities provided by open source software.

Overall, the open source software market for cybersecurity tools is expanding rapidly and is expected to continue to grow in the coming years. As more and more companies look for cost-effective and flexible solutions to their cybersecurity needs, FOSS options are likely to become an increasingly popular choice.

**Research methods.** To achieve the set goals, the analytical and the applied methods were chosen. Firstly, relevance of SOC running on FOSS and its modern applications were identified. Secondly, using the analysis the solutions for SOC based on FOSS were identified, and possible combination of such solutions were composed into a SOC model. In addition, conclusions were drawn to determine whether such a SOC model would be competitive with an SOC running on enterprise solutions.

**Composition of FOSS solutions into a functioning SOC**

Based on the resource from CISA, Free Cybersecurity Services and Tools [1], the following combination of FOSS solutions was selected to study the possibility of building a functioning and effective SOC based on them:

1. SIEM system - ELK Stack [2].
2. SOAR - TheHive in combination with Cortex [3].
3. IPS/IDS system - Snort [4].
4. EDR/XDR - Wazuh [5].
5. Threat intelligence - MISP [6].
6. Vulnerability scanner - OpenVAS [7].
7. Malware analysis - YARA [8].
8. Honeypot solution - Honeyd [9].
9. Detection testing - Atomic Red Team [10].

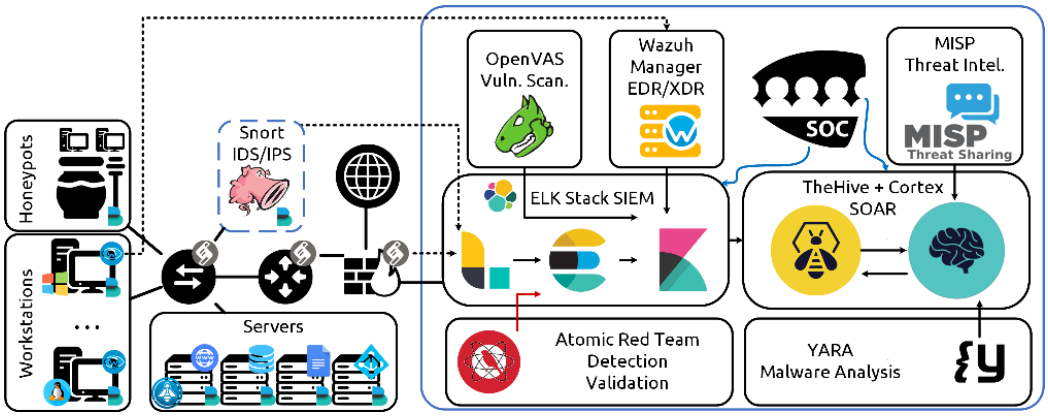


*Fig . 1. Schematic diagram of an SOC based on the above solutions*

In such a SOC, the components interact as follows:

- The SIEM (ELK Stack) receives log data from the Wazuh and filebeat agents installed on the endpoints. It also receives alerts from Snort, Wazuh, and Honeydeal.
- SOAR (TheHive + Cortex) receives alerts from the SIEM and automatically triggers incident response playbooks using Cortex.
- IPS/IDS (Snort) monitors network traffic and sends alerts to the SIEM if it detects suspicious or malicious activity.
- EDR/XDR (Wazuh) secures endpoints and continuously monitors and reports any suspicious activity to the SIEM.
- Threat Intelligence (MISP) provides context to security events and enriches alerts generated by the SIEM.
- Vulnerability scanner (OpenVAS) scans the network and endpoints for vulnerabilities and reports the results to the SIEM.
- Honeypot (Honey) is used to detect and catch intruders by emulating vulnerable systems and services.
- Malware Analysis (YARA) is used to analyze suspicious files detected by Wazuh agents and Open-VAS scanning.
- Detection Validation (Atomic Red Team) provides continuous testing of the SOC's detection capabilities to ensure that it effectively counteracts new threats.

SOAR based on TheHive + Cortex perfectly integrates with all of these solutions and can be used to automate the processes of the following SOC solutions:

- YARA: Automate YARA scans of incoming files or samples. For example, when a new file is sent to TheHive, Cortex can automatically run YARA rules against it to determine if it matches any known malware or threat indicators.
- OpenVAS: Automate vulnerability scanning and reporting with OpenVAS. For example, Cortex can be used to run scans on specific targets or groups of targets, and TheHive will then generate alerts and tickets for any vulnerabilities found.

- Atomic Red Team: Automate the testing of identified vulnerabilities using the Atomic Red Team testing framework. For example, Cortex can be used to run specific tests on an endpoint or group of endpoints, and TheHive can be used to generate alerts and tickets for any present vulnerabilities found.
- MISP: Automating the exchange and correlation of data about indicators of compromise. For example, Cortex can be used to query the MISP for threat indicators related to an ongoing investigation, and TheHive will then correlate those indicators with other events or alerts in the system.

**Overview of possible use cases**

When creating the model of such a SOC, potential scenarios of attacks on the company's infrastructure were considered and the response and interaction of SOC components in the process of detecting, analyzing and mitigating the consequences of such attacks were envisaged.

- Use case 1: Workstation infected with ransomware.

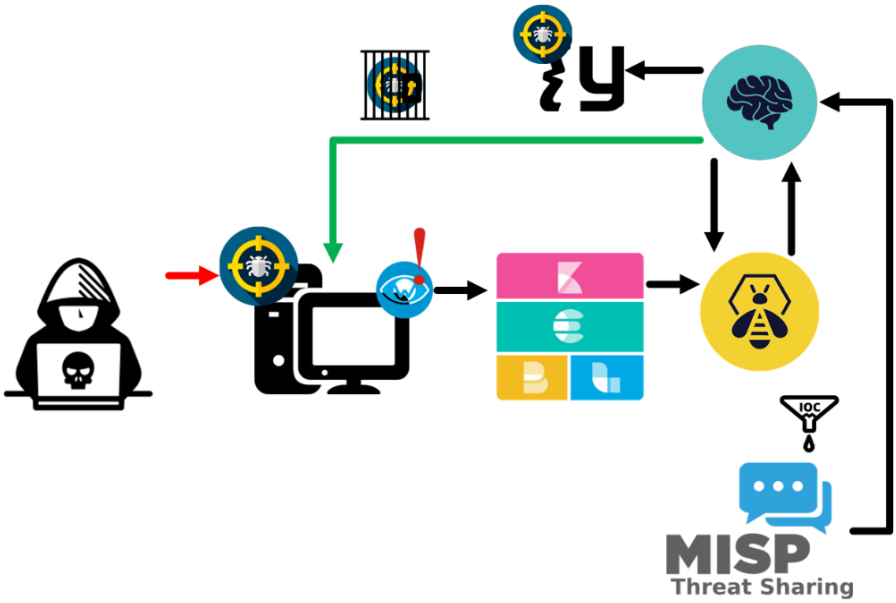


*Fig . 2. Visualization of use case 1*

Response: The Wazuh agent installed on the workstation will trigger an alert and send it to the ELK stack for analysis. The SOC analyst will investigate the alert and determine that the workstation has been infected with ransomware. Using the MISP threat intelligence platform, they will determine the type of ransomware and any associated indicators of compromise. TheHive will then run the Cortex playbook, which will quarantine the infected workstation and begin analyzing the malware with YARA.

Use case 2: Vulnerability scan reveals critical vulnerability on web server.

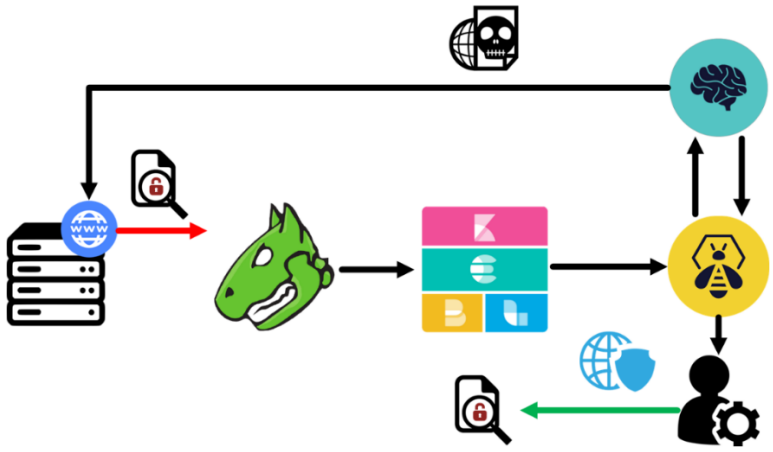

*Fig . 3. Visualization of use case 2*

Response: The OpenVAS vulnerability scanner will detect the vulnerability and send an alert to the SOC via the ELK stack. The SOC analyst will use TheHive to assign a responsible system administrator and oversee the patching process. Also, using TheHive, a Cortex playbook will be launched to try to exploit the vulnerability and check its impact on the system. The exploitation attempt can also be used to test the effectiveness of the IPS/IDS system.

- Use case 3: The attacker triggered the honeypot.

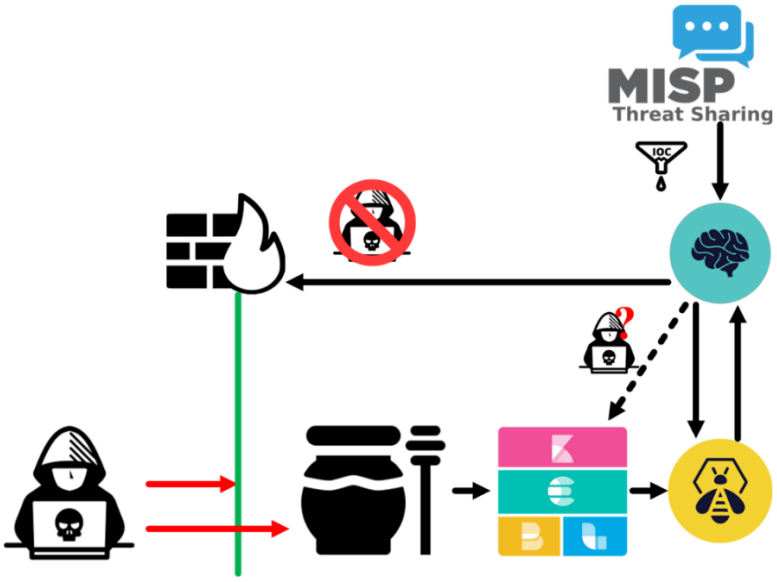


*Fig . 4. Visualization of use case 3*

- Response: Honeyd detects the attacker's activity and sends an alert to the ELK stack. The SOC analyst, using TheHive, will run a Cortex playbook that automatically blocks the attacker's IP address on the firewall. Cortex, using the MISP threat intelligence platform, will automatically detect related IoCs and search for similar attacks in the ELK stack. As part of the response, YARA can also be used to analyze malware if it is detected on a compromised honeypot.

**Advantages and disadvantages of running FOSS SOC.**

Advantages:

1. Cost-effective: FOSS SOC is cost-effective as it eliminates the need for expensive licenses, maintenance, and upgrade fees associated with enterprise solutions. Organizations can save a significant amount of money on licensing fees and can reallocate the funds to other areas of the business.
2. Customization: FOSS SOC allows for more customization as organizations can tailor the solution to their specific needs. They can modify the source code to add or remove functionality, integrate with other tools, or develop their own plugins or modules.
3. Agility: FOSS SOC is more agile and flexible than enterprise solutions. It can adapt quickly to changing environments and requirements. New features and functionalities can be added or modified easily as they are developed by the community or in-house developers.
4. Reliability: FOSS SOC is developed and maintained by a large community of developers and users who actively participate in testing and debugging the software. This leads to a more reliable and stable solution.
5. Support: FOSS SOC has a strong community support network that provides help and assistance to users. Support is often available through online forums, user groups, and developer communities.
6. Resiliency: FOSS SOC has a distributed model, with many different developers and users contributing to its development. This makes it more resilient to attacks and vulnerabilities, as there are many different eyes on the codebase.

Disadvantages:

1. Complexity: FOSS SOC can be complex to set up and configure, requiring specialized knowledge and skills. It may require additional training and resources to properly implement and maintain.
2. Integration: FOSS SOC may require additional resources and effort to integrate with other security tools and technologies. It may also require customization to meet specific business needs.
3. Documentation: FOSS SOC may lack proper documentation and support, making it difficult for new users to implement and maintain.
4. Lack of vendor support: FOSS SOC may lack vendor support, which can lead to longer resolution times for issues and problems.

5. Security: FOSS SOC may be less secure than enterprise solutions due to a lack of proprietary security measures and fewer resources available for security testing and hardening.
6. Limited features: FOSS SOC may have limited features compared to enterprise solutions, as it may not have the same level of investment in research and development.

In process of comparing FOSS and enterprise SOC calculation of estimated monthly expanses on running every solution:

*Table 1.*

*Monthly expanses of running FOSS versus enterprise SOC solution*

| **Solution** | **FOSS SOC Software Name** | **FOSS Expanses per Month** | **Enterprise SOC Software Name** | **Enterprise Expanses per Month** |
|---|---|---|---|---|
| SIEM | ELK Stack | Free | Splunk | $1,500-$2,000+ |
| SOAR | TheHive, Cortex | Free | Chronicle | $3,000-$6,000+ |
| IPS/IDS | Snort | Free | Cisco Firepower | $1,000-$2,500+ |
| EDR/XDR | Wazuh | Free | Microsoft Defender for Endpoints | $1,000-$2,000+ |
| Threat Intelligence | MISP | Free | Microsoft Threat Intelligence | $5,000-$10,000+ |
| Vulnerability Scan | OpenVAS | Free | Rapid7 Nexpose | $1,500-$3,000+ |
| Honeypot | Honeyd | Free | TrapX | $10,000-$20,000+ |
| Malware Analysis | YARA | Free | AnyRun | $500-$1,500+ |

**Conclusion.** In conclusion, running an SOC on FOSS is a viable alternative for organizations that want to establish a SOC without incurring significant financial investments. The FOSS SOC market is growing rapidly, and many FOSS tools are becoming increasingly popular due to their effectiveness and flexibility. However, FOSS tools can be complex to deploy and manage, which can lead to additional costs associated with training personnel. Overall, the advantages of running an SOC on FOSS outweigh the disadvantages, making it a suitable option for organizations with specific security needs.

**References:**


1. CISA (2023), *Free Cybersecurity Services and Tools*, [Online], available at: https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
2. Elastic, *The ELK Stack: From the Creators of Elasticsearch*, [Online], available at: https://www.elastic.co/what-is/elk-stack
3. *TheHive Project*, [Online], available at: https://thehive-project.org/
4. Snort, *Network Intrusion Detection & Prevention System*, [Online], available at: https://www.snort.org/
5. Wazuh (2023), *The Open Source Security Platform*, [Online], available at: https://wazuh.com/
6. MISP, *Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing*, [Online], available at: https://www.misp-project.org/
7. OpenVAS, [Online], available at: https://openvas.org/
8. GitHub, «The pattern matching swiss knife», *VirusTotal/yara*, [Online], available at: https://github.com/virustotal/yara
9. «Developments of the Honeyd Virtual Honeypot», [Online], available at: https://www.honeyd.org/
10. Atomic Red Team, *Canary R. Explore Atomic Red Team*, [Online], available at: https://atomicredteam.io/



**Yefimenko Andrii** – Ph.D., Assoc.prof., Head of Dept., Zhytomyr Polytechnic State University.
https://orcid.org/0000-0003-2128-4797
Scientific interests:
– protection of information in computer networks and cloud security.

**Honcharov Mykhailo**
https://orcid.org/0009-0004-4643-4098

**Єфіменко А.А., Гончаров М.В.**

**Дослідження можливостей використання SOC на основі безкоштовного та відкритого програмного забезпечення**

У статті розглядається особлива комбінація рішень операційного центру безпеки, що використовують безкоштовне програмне забезпечення з відкритим вихідним кодом, як альтернатива таким центрам на базі високовартісного пропрієтарного ПЗ. У дослідженні визначено компоненти такого операційного центру безпеки, описано їх місце та взаємодію в процесі виявлення, аналізу та пом'якшення наслідків кібератак. Також проаналізовано конкурентоспроможність та визначено переваги, недоліки та перспективи розвитку запропонованого рішення.

У дослідженні проаналізовано конкретну комбінацію безкоштовних інструментів з відкритим вихідним кодом, детально описано роль та взаємодію кожного компонента у виявленні, аналізі та пом'якшенні наслідків кіберзагроз. Запропонований безкоштовний операційний центр безпеки з відкритим вихідним кодом складається з системи управління інформацією та подіями безпеки (Elastic Stack), платформи оркестрування, автоматизації та реагування безпеки (TheHive і Cortex), системи запобігання вторгненням/виявлення вторгнень (Snort), системи виявлення та реагування на вторгнення на кінцеві точки/розширеного виявлення та реагування на вторгнення (Wazuh), платформи розвідки загроз (MISP), сканера вразливостей (OpenVAS), інструменту для аналізу шкідливого програмного забезпечення (YARA), рішень Honey, а також системи для перевірки на наявність шкідливого програмного забезпечення (Atomic Red Team).

У дослідженні проілюстровано приклади використання, що демонструють реакцію операційного центру безпеки на інфікування вірусами-здирниками, використання вразливостей і спрацьовування honeypot, з акцентом на синергетичну взаємодію між компонентами. Переваги безкоштовного операційного центру безпеки з відкритим вихідним кодом включають економічну ефективність, можливість налаштування, гнучкість, надійність, відмовостійкість та підтримку з боку фахової спільноти. Серед недоліків центру визначено загальну складність, проблеми з інтеграцією, недостатність документації, відсутність підтримки з боку постачальників, потенційні ризики для безпеки та обмежені можливості порівняно з корпоративними рішеннями.

У дослідженні зроблено висновок, що хоча розгортання та управління безкоштовними інструментами з відкритим вихідним кодом може бути складним, переваги безкоштовного операційного центру безпеки з відкритим вихідним кодом переважають недоліки, що робить його життєздатним варіантом для організацій з особливими потребами в безпеці, особливо для тих, які мають бюджетні обмеження.

**Ключові слова:** операційний центр безпеки безкоштовне програмне забезпечення з відкритим кодом; ІБ (інформаційна безпека); виявлення загроз; реагування на інциденти; розвідка загроз.

Стаття надійшла до редакції 26.04.2024.