LAB 11 – Risk Analysis and Management

By :- Faraz Ahmed

1. Memo

To: CEO David Murray, CEO
From: Faraz Ahmed, Security Engineer
Date: November 13th, 2024
Subject: Assessment of SIEM Solution for UBNetDef Wiki Network Security

The purpose of this report is to access whether implementing a SolarWinds Security Information and Event Management (SIEM) is a justified solution for the UBNetDef Wiki Network or not. This report also includes a technical assessment of Personally Identifiable Information (PII) which is currently getting collected within the UBNetDef Wiki Network and evaluates whether SolarWinds is capable enough for our data or we need a cost-effective alternative option such as Wazuh which would provide robust defence for UBNetDef Wiki's security and operational needs in its functionality. Personally Identifiable Information (PII) basically investigates all collected data within the network and evaluates the current risk analysis and then proposes a perfect alternative SIEM solution if SolarWinds is not good enough.

Table of Contents

2. Executive Summary

UBNetDef SysSec finds that the proposed implementation for a SolarWinds SIEM on the UBNetDef Wiki Network is not justified. So, by evaluating the Personally Identifiable Information (PII) data handling on UBNetDef Wiki's Network reveals that it gathers certain types of PII which certain many levels of business and organizational risks and also have some sensitive PII fields which are being stored which is a crucial security concern. The CIO's risk evaluation identifies all potential threats but it does not have sufficient information about risk associated with Specific PII vulnerabilities and its changes of being exploited by an attacker. While the we know that SolarWinds better at managing risks and efficient in managing it, but the cost and infrastructure may exceed projected benefits and budget of UBNetDef Wiki so it will be difficult for organization is handle SolarWinds into their network.

UBNetDef SysSec finds that Wazuh is a cost-effective and robust alternative to SolarWinds. Wazuh offers a comprehensive monitoring, threat detection and response capabilities which comes under our goals of achieving a reliable and scalable solution with comparatively less overall cost than SolarWinds. It also offers effective vulnerability management, incident alerting, and threat response tools necessary to meet UBNetDef Wiki's security goals. So, any additional hardware for hosting Wazuh which may be necessary can cost approximately $300 and installation by two Security Engineers can take upto 7-8 hours based on UBNetDef's current system and infrastructure.

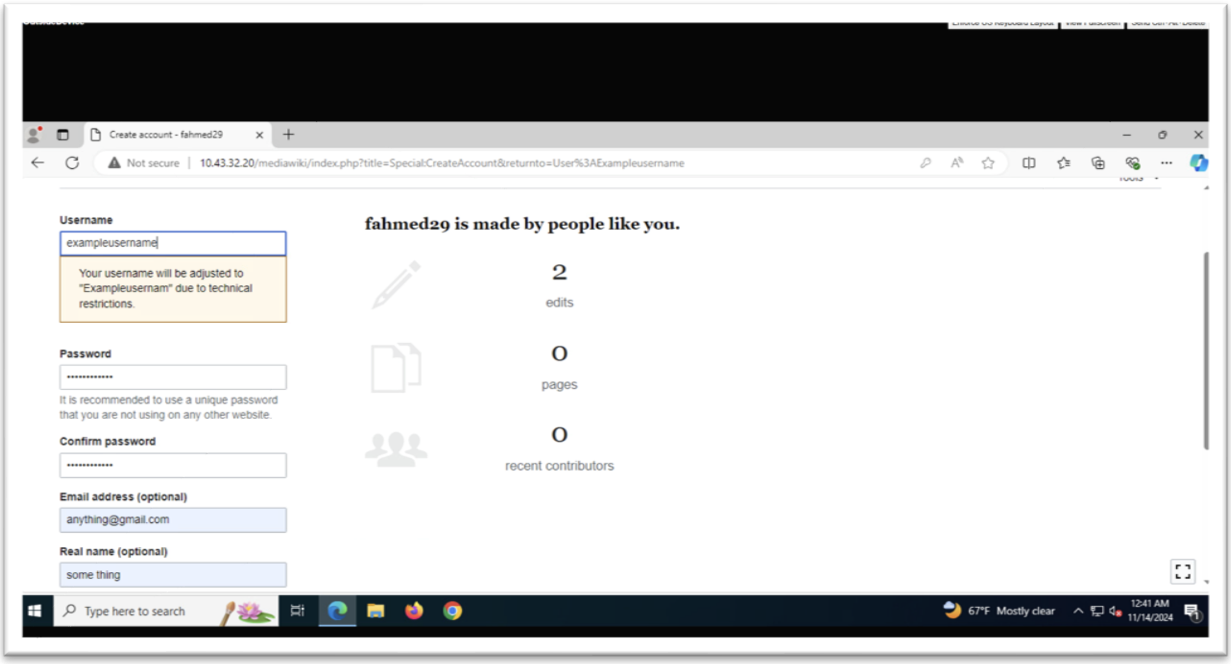
3. Technical Findings

➢ Section I: PII Security Assessment

- **PII:** PII is any information about an individual which is stored and maintained by an organization, which includes any information that can be used to distinguish or track that particular individual's basic identity such as name, date and place of birth, parents name and physical address. It also contains other information that is linked to an individual like medical, educational, employment or financial information.
  Example:- Personal phone number, IP address, Personal email address, Religion affiliated or sexual orientation.
- **SPII:** SPII is any sensitive and personal information which if compromised, could result in substantial harm, embarrassment and inconvenience to an individual.
  Example:- Social security number, passport numbers, driver's license number, bank account number, credit or debit card number and biometric data.

  Basic and key difference between PII and SPII is the sensitivity of the data of an individual. So, if PII data is stolen or damaged by an attacker it may or may not affect the individual but if SPII data is stolen or damaged then it can definitely affect individual emotionally and mentally.

- Now we login to MediaWiki in OutsideDevice to check what kind of sensitive data or PII does it takes from the user and store into the system. So we enter "http://<UbuntuWebServer IP>/mediawiki?useskin=vector" in the URL and when we see the homepage in MediaWiki, we create a new account. Then we enter the new details as shown in figure 1 below.



Create account - fahmed29

Not secure | 10.43.32.20/mediawiki/index.php?title=Special:CreateAccount&returnto=User%3AExampleusername

Username

exampleusername

Your username will be adjusted to "Exampleusernam" due to technical restrictions.

Password

••••••••••••

It is recommended to use a unique password that you are not using on any other website.

Confirm password

••••••••••••

Email address (optional)

anything@gmail.com

Real name (optional)

some thing

fahmed29 is made by people like you.

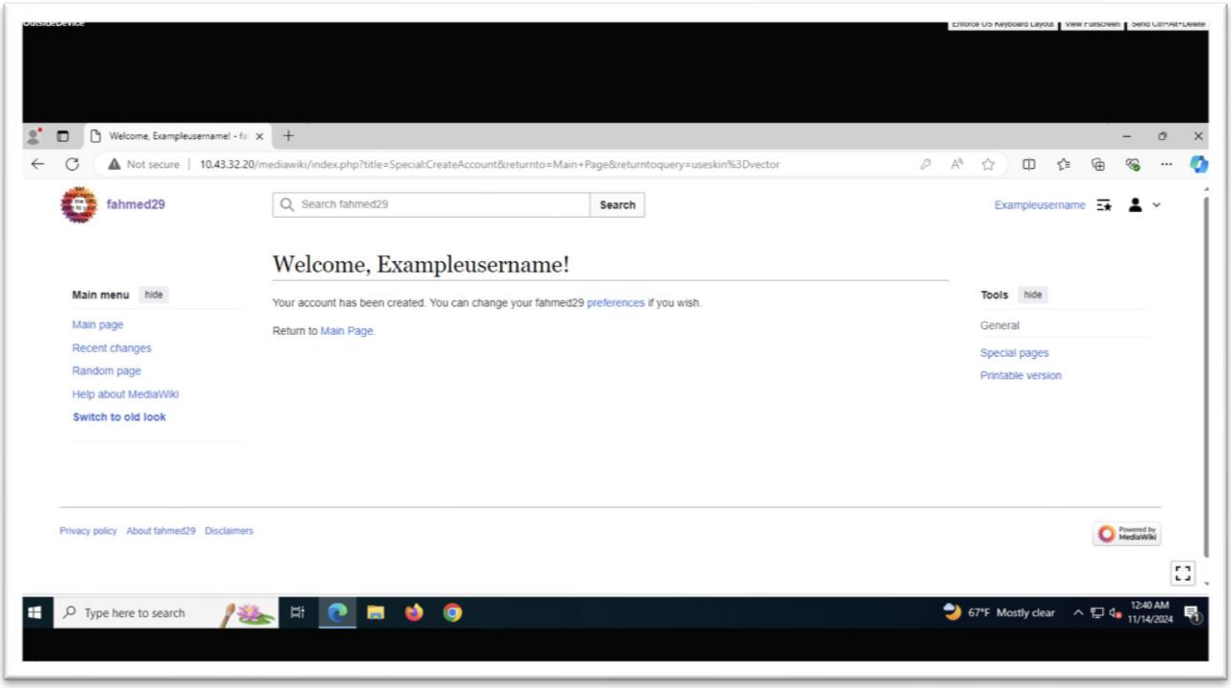
2 edits

0 pages

0 recent contributors

Figure 1: Screenshot of registration process for creating new user by entering information as prompted.

- After entering fake details and creating a test account, we can see that we are logged in with our new test account as shown in Figure 2 which confirms that our new test account is created.



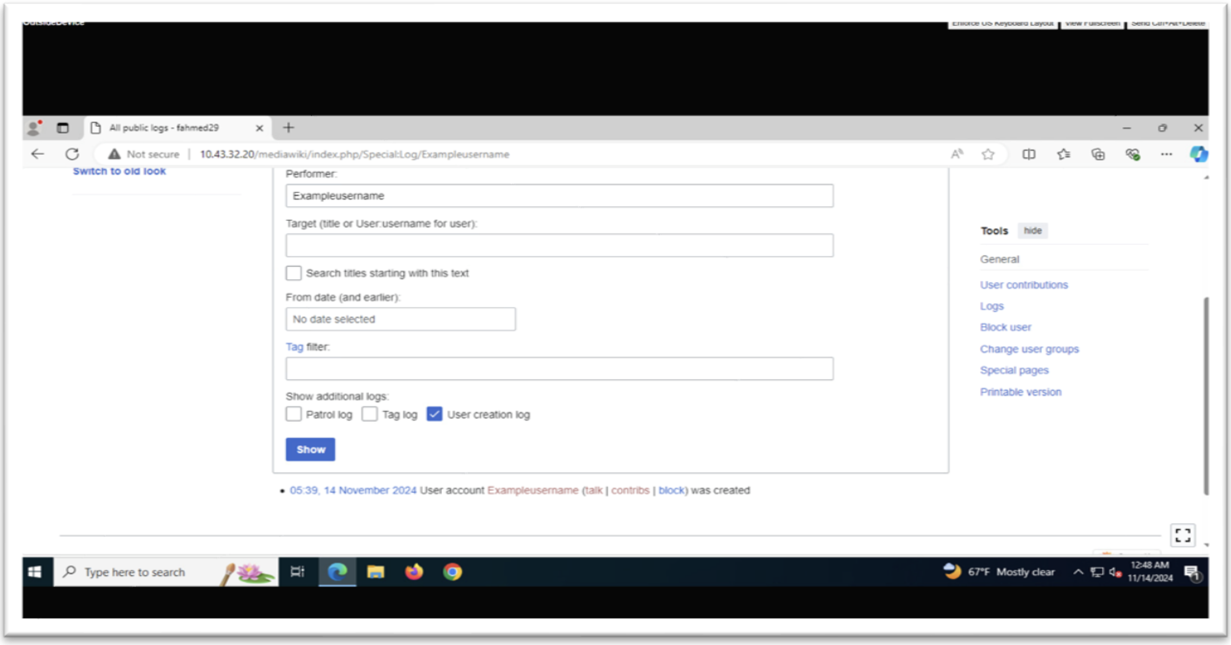
Welcome, Exampleusername!

Your account has been created. You can change your fahmed29 preferences if you wish.

Return to Main Page.

Figure 2: Screenshot of main page of newly created user in MediaWiki.

- So, now we log in through our admin credentials to the admin account and check what all PII or sensitive detail we can access from the frontend of the MediaWiki. Now from Figure 3, we can see the from Admin control we can only observe account's username and last activity date and time (as highlighted below). These data are not that crucial for the normal user and will not make any difference if known by anyone. So, there is no threat to PII data in MediaWiki.



Performer: Exampleusername

Target (title or User:username for user):

□ Search titles starting with this text

From date (and earlier): No date selected

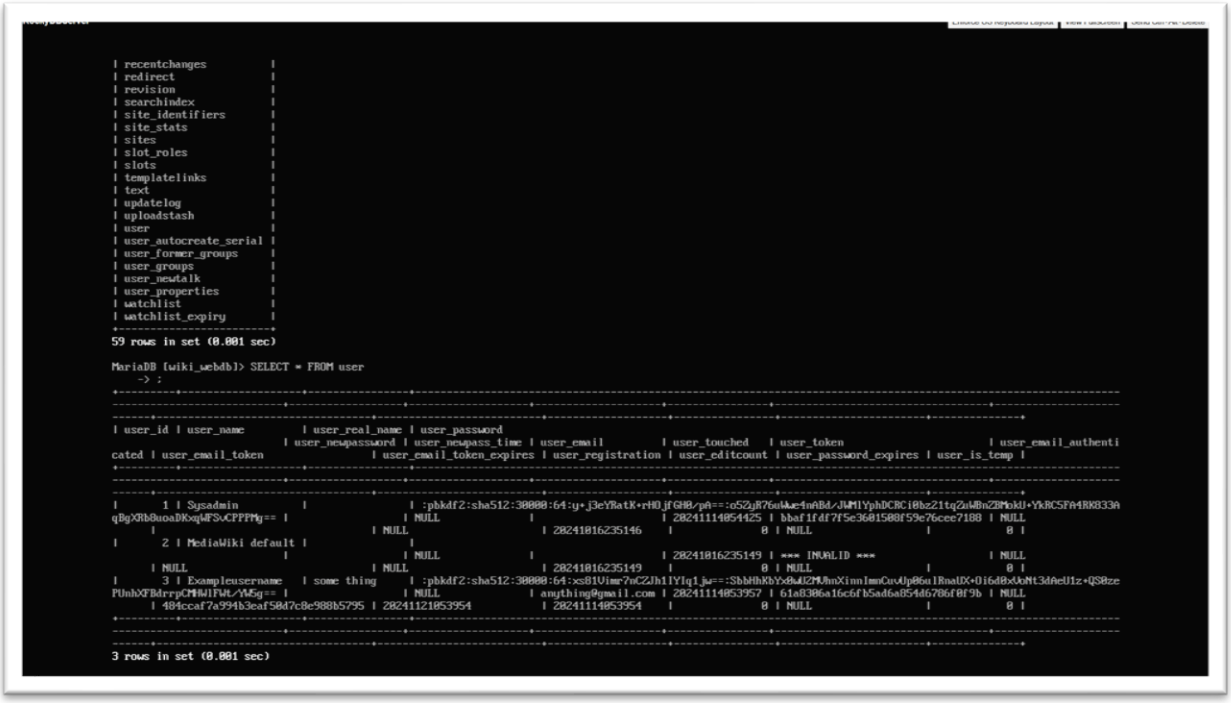
Tag filter:

Show additional logs:
□ Patrol log □ Tag log ☑ User creation log

- 05:39, 14 November 2024 User account Exampleusername (talk | contribs | block) was created

Figure 3: Screenshot of activity or PII seen through frontend of MediaWiki.

- After that we will check if backend of MediaWiki is also safe or not. For that we will using RockyDBServer and open MariaDB services using “sudo mysql -u root -p” then look through all the database in it using “SHOW DATABASES;” then pick the database which we think contains all the sensitive data. Then we “USE that database and type SHOW TABLES;” which shows table shown in Figure 4. After that we enter “SELECT * FROM user;” which will give details of all users registered in that MediaWiki webpage. From Figure 4 we can note that all the details which the user entered to create the new account can be seen which can consist of his/her SPII or sensitive personal data. We can note that the table shows enter username with password, full name and email which can be used by the attacker for bad means. So, backend of MediaWiki is has this major PII vulnerability.



```
| recentchanges          |
| redirect               |
| revision               |
| searchindex            |
| site_identifiers       |
| site_stats             |
| sites                  |
| slot_roles             |
| slots                  |
| templatelinks          |
| text                   |
| updatelog              |
| uploadstash            |
| user                   |
| user_autocreate_serial |
| user_former_groups     |
| user_groups            |
| user_newtalk           |
| user_properties        |
| watchlist              |
| watchlist_expiry       |
+------------------------+
59 rows in set (0.001 sec)

MariaDB [wiki_webdb]> SELECT * FROM user
    -> ;
+---------+-------------------+----------------+------------------------------------------------------------------------------------------------------------
------------------------------+-------------------+-------------------+------------------+-------------------+----------------------------------+-------------------
------+----------------------------------+---------------------------+-------------------+----------------+----------------------+--------------+
| user_id | user_name         | user_real_name | user_password
                              | user_newpassword | user_newpass_time | user_email         | user_touched   | user_token                       | user_email_authenti
cated | user_email_token                 | user_email_token_expires | user_registration | user_editcount | user_password_expires | user_is_temp |
+---------+-------------------+----------------+------------------------------------------------------------------------------------------------------------
------------------------------+-------------------+-------------------+------------------+-------------------+----------------------------------+-------------------
------+----------------------------------+---------------------------+-------------------+----------------+----------------------+--------------+
|       1 | Sysadmin          |                | :pbkdf2:sha512:30000:64:y+j3eYRatK+rHOjfGH0/pA==:o5ZyR76uWwe4nABd/JWM1YphDCRCi0bz21tqZuWBnZBMokU+YkRC5FA4RK833A
qBgXRb8uoaDKxqWFSvCPPPMg== |                | NULL             |                   |                    | 20241114054425 | bbaf1fdf7f5e3601508f59e76cee7188 | NULL
      |                                  | NULL                     | 20241016235146    |              0 | NULL                 |            0 |
|       2 | MediaWiki default |                |
                              |                | NULL             |                   |                    | 20241016235149 | *** INVALID ***                  | NULL
      | NULL                             | NULL                     | 20241016235149    |              0 | NULL                 |            0 |
|       3 | Exampleusername   | some thing     | :pbkdf2:sha512:30000:64:xs81Vimr7nCZJh1IYIq1jw==:SbbHhKbYx0wU2MVhnXinnImnCuvUp06ulRnaUX+Oi6d0xVoNt3dAeU1z+QS0ze
PUnhXFBdrrpCMHW1FWt/YW5g== |                | NULL             |                   | anything@gmail.com | 20241114053957 | 61a8306a16c6fb5ad6a854d6786f0f9b | NULL
      | 484ccaf7a994b3eaf50d7c8e988b5795 | 20241121053954           | 20241114053954    |              0 | NULL                 |            0 |
+---------+-------------------+----------------+------------------------------------------------------------------------------------------------------------
------------------------------+-------------------+-------------------+------------------+-------------------+----------------------------------+-------------------
------+----------------------------------+---------------------------+-------------------+----------------+----------------------+--------------+
3 rows in set (0.001 sec)
```

Figure 4: Screenshot of MediaWiki backend on RockyDBServer to see some of the SPII stored.

- So, as we can note that there is SPII vulnerability in the system which can be exploited by the attacker and is needed to be mitigated by the organization. So, the presence of SPII can increase the risk factors of overall system and can make the system vulnerable for attackers to exploit it.
- Attacks can attack the backend of MediaWiki to get some passwords and emails of some users as maybe some users use some passwords for other account and the attacks will grab that username and password and using brute force method to get into their other accounts. So, the username, password and email can help attack not only access MediaWiki account of the user, but also maybe get into other application’s account using same credentials. It is still very likely to happen as if attacker got admin access, he/she can take over any amount of data in the database and modify it according to him/her.
- Using these credentials, threat actors can access and manipulate any data in MediaWiki web page as he/she has access of each and every account even has admin control which he can use to change credentials so that users can’t gain access to their lost account again after losing it and thus can do whatever he/she wants.

Section II: Wazuh as an Alternative SIEM Solution

- UBNetDef SysSec finds that Security Information and Event Manager (SIEM) Wazuh is a suitable alternative to the SolarWinds SIEM proposed for the UBNetDef Wiki. Wazuh is a reliable open-source Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platform. It is basically designed to provide real-time risk monitoring, log analysis and alerting about any vulnerabilities across network systems making it a robust and well suitable low-cost SIEM alternative for organizations seeking equally strong security system without buying high costs SIEM products like SolarWinds.
- Some of the features of Wazuh which can fulfil the goals of SIEM are :-

i. Log Collection and Analysis- Wazuh also offers organized log collection and analysing it in real-time across overall network endpoints. This function is similar to SolarWinds and helps UBNetDef to properly monitor and analysis all activities on network.

ii. Threat Detection and Incident Response- Wazuh runs the active scans throughout the systems and detect threats and automatically responses it which is one of the core and crucial function of SolarWinds.

iii. Vulnerability Detection- Wazuh can detect vulnerabilities in a system and this will help to prevent exploitation of that weakness in the system.

- Wazuh can also mitigate technical risk by :-

i. Enhanced Detection of threats- Wazuh has an organized logging and maintaining any unauthorized intrusion and detect it to mitigate which increases detection accuracy and reducing the likelihood of an undetected breach.

ii. Reduced Vulnerabilities- Wazuh's ability to monitor all the activities taking place in the current network in real time. It monitors all configuration changes, access logs and any unpatched vulnerabilities to decreases threats in that network system.

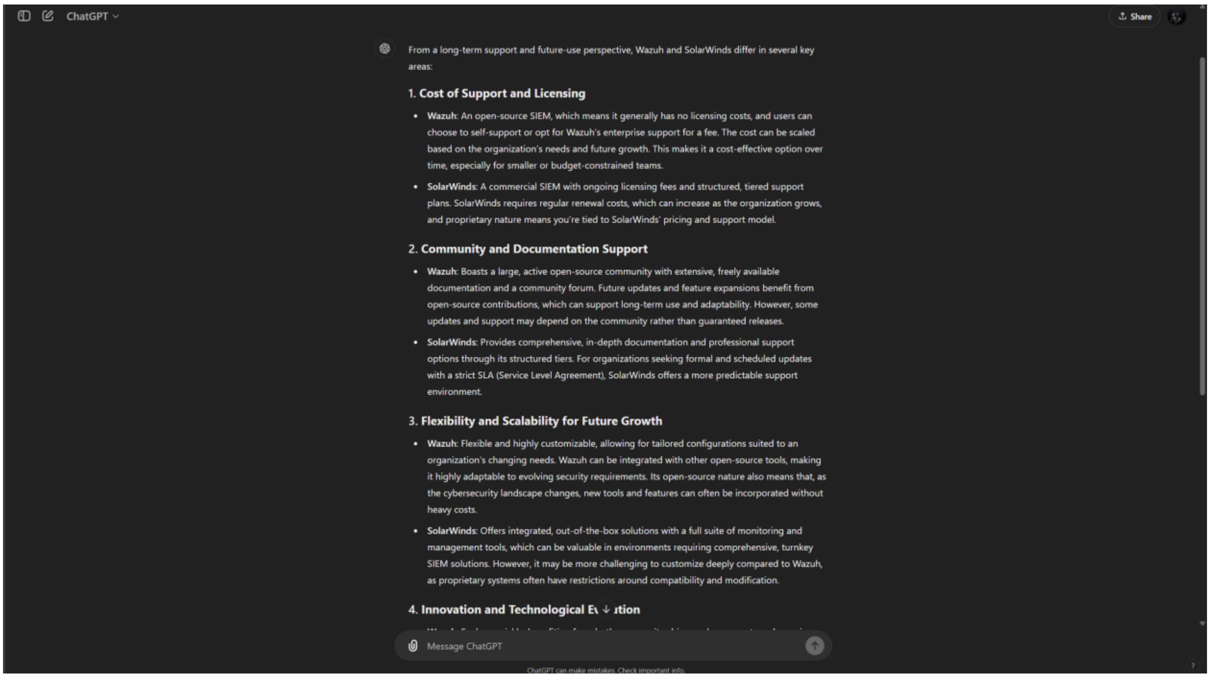
iii. Automated Response System- Wazuh has an automated system to detect and responded immediately to stop that threat then and there. This restricts the threat and stops it from spreading malware and attacking it to any sensitive areas in the network.

- Difference between Wazuh and SolarWinds from the perspective of support over time- Wazuh and SolarWinds both support future growth perspective but SolarWinds has an edge over Wazuh due to being a commercial enterprise product. SolarWinds offers a structured, dedicated and organised support as a part of its licensing agreement with the organization. This also includes access to always available customer support team, regular software updates and security patches and also proper logging and monitoring of every single activity. Customer support is always crucial that can prioritize quick and efficient analysing and responding which can reduce the impact of threat in the system. SolarWinds also have a larger team which can be great in larger infrastructure and scalable systems of larger organizations. Whereas Wazuh is a less budget, open-source solution which provides flexibility and scalability without expensive licensing costs, which is beneficial for organizations with less budget. However, it doesn't have much support and assistance so it is most of community-driven and contributions and organization can contact support through forums, online resources and online support plan subscription. While this all can be ok for organizations with skilled internal IT teams, but it may introduce delays in critical and crucial situations. So, for long-term growth, SolarWinds provides a stable, predictable support environment ideal for scaling with a consistent external support team. Whereas Wazuh has limited support team and resources for organization with limited budget.

4. References

- Wazuh - Open Source XDR. Open Source SIEM.
- Security Event Manager - View Event Logs Remotely | SolarWinds
- Differences Between PII, Sensitive PII, and PHI – Municipal Websites Central Help Center
- Understanding Wazuh: The Free, Open Source Security Platform for XDR & SIEM | by Sigmund Brandstaetter CISSP, CCSP, CISM, OSCP, CEH | Medium
- SolarWinds Attack & Details You Need To Know About It | Simplilearn

-



From a long-term support and future-use perspective, Wazuh and SolarWinds differ in several key areas:

1. **Cost of Support and Licensing**

- **Wazuh**: An open-source SIEM, which means it generally has no licensing costs, and users can choose to self-support or opt for Wazuh's enterprise support for a fee. The cost can be scaled based on the organization's needs and future growth. This makes it a cost-effective option over time, especially for smaller or budget-constrained teams.
- **SolarWinds**: A commercial SIEM with ongoing licensing fees and structured, tiered support plans. SolarWinds requires regular renewal costs, which can increase as the organization grows, and proprietary nature means you're tied to SolarWinds' pricing and support model.

2. **Community and Documentation Support**

- **Wazuh**: Boasts a large, active open-source community with extensive, freely available documentation and a community forum. Future updates and feature expansions benefit from open-source contributions, which can support long-term use and adaptability. However, some updates and support may depend on the community rather than guaranteed releases.
- **SolarWinds**: Provides comprehensive, in-depth documentation and professional support options through its structured tiers. For organizations seeking formal and scheduled updates with a strict SLA (Service Level Agreement), SolarWinds offers a more predictable support environment.

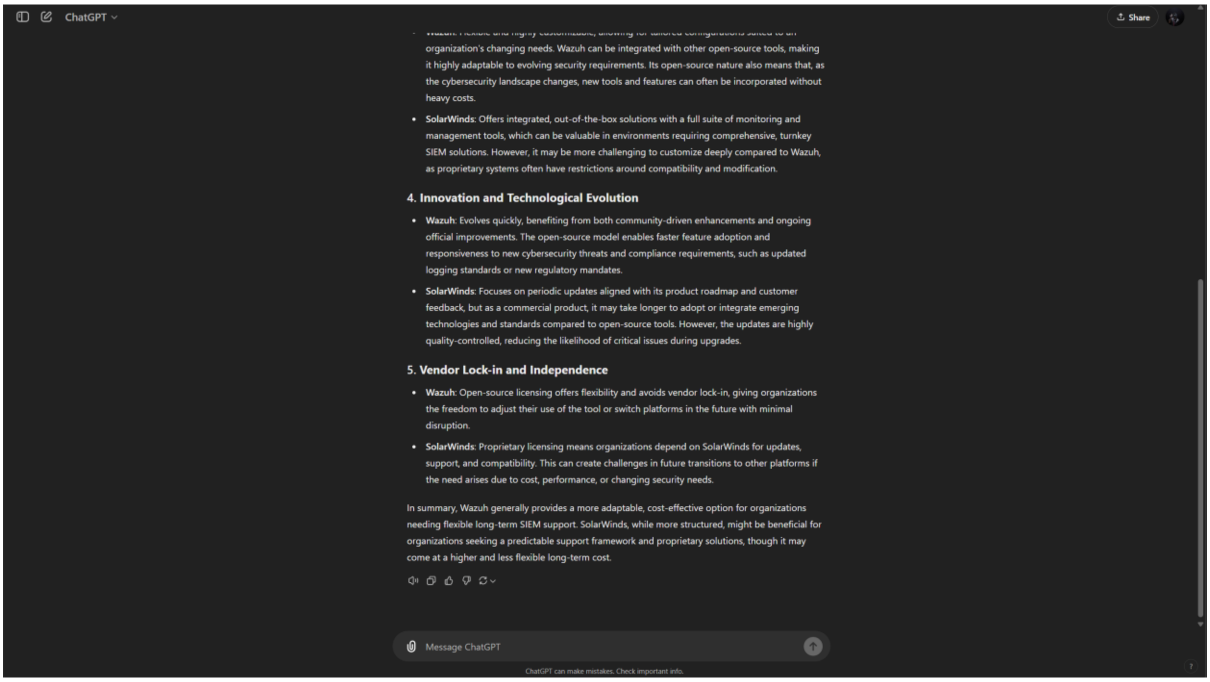
3. **Flexibility and Scalability for Future Growth**

- **Wazuh**: Flexible and highly customizable, allowing for tailored configurations suited to an organization's changing needs. Wazuh can be integrated with other open-source tools, making it highly adaptable to evolving security requirements. Its open-source nature also means that, as the cybersecurity landscape changes, new tools and features can often be incorporated without heavy costs.
- **SolarWinds**: Offers integrated, out-of-the-box solutions with a full suite of monitoring and management tools, which can be valuable in environments requiring comprehensive, turnkey SIEM solutions. However, it may be more challenging to customize deeply compared to Wazuh, as proprietary systems often have restrictions around compatibility and modification.

4. **Innovation and Technological E↓ution**

ChatGPT can make mistakes. Check important info.

-



- **Wazuh**: Flexible and highly customizable, allowing for tailored configurations suited to an organization's changing needs. Wazuh can be integrated with other open-source tools, making it highly adaptable to evolving security requirements. Its open-source nature also means that, as the cybersecurity landscape changes, new tools and features can often be incorporated without heavy costs.
- **SolarWinds**: Offers integrated, out-of-the-box solutions with a full suite of monitoring and management tools, which can be valuable in environments requiring comprehensive, turnkey SIEM solutions. However, it may be more challenging to customize deeply compared to Wazuh, as proprietary systems often have restrictions around compatibility and modification.

4. **Innovation and Technological Evolution**

- **Wazuh**: Evolves quickly, benefiting from both community-driven enhancements and ongoing official improvements. The open-source model enables faster feature adoption and responsiveness to new cybersecurity threats and compliance requirements, such as updated logging standards or new regulatory mandates.
- **SolarWinds**: Focuses on periodic updates aligned with its product roadmap and customer feedback, but as a commercial product, it may take longer to adopt or integrate emerging technologies and standards compared to open-source tools. However, the updates are highly quality-controlled, reducing the likelihood of critical issues during upgrades.

5. **Vendor Lock-in and Independence**

- **Wazuh**: Open-source licensing offers flexibility and avoids vendor lock-in, giving organizations the freedom to adjust their use of the tool or switch platforms in the future with minimal disruption.
- **SolarWinds**: Proprietary licensing means organizations depend on SolarWinds for updates, support, and compatibility. This can create challenges in future transitions to other platforms if the need arises due to cost, performance, or changing security needs.

In summary, Wazuh generally provides a more adaptable, cost-effective option for organizations needing flexible long-term SIEM support. SolarWinds, while more structured, might be beneficial for organizations seeking a predictable support framework and proprietary solutions, though it may come at a higher and less flexible long-term cost.

ChatGPT can make mistakes. Check important info.

Thanks for taking your time and reading the whole report properly to stop any further vulnerabilities and monitor PIIs and SPIIs properly in the UBNetDef's network system.

Best Regards,

Faraz Ahmed

Security Engineer

UBNetDef.