Summary post

**Collaborative Learning Discussion 2**

In week 3 of this forum, provide a summary of the discussion for formative feedback via the [**discussion forum**](https://www.my-course.co.uk/mod/hsuforum/view.php?id=568829).

Instruction: Agree or otherwise, with reasons, with the contributions and reviews made by other students on the topic under discussion, enhancing your original post. This should be 300 words (excluding references). This summary post accounts for 10% of your final module score.

This summary post is also a required component of your e-portfolio and provides evidence of your personal growth. You can submit the e-portfolio for this module at the end of week 12 for feedback

**The benefits of a SOC/SIEM in network security**

Writer : [**Liana Havryliuk**](https://www.my-course.co.uk/user/view.php?id=17103&course=7514)

Last 4 days ago

There are two fundamental technologies that can help support a business from a network operational perspective. They focus on a business using an implementing a SOC (Security Operations Centre) and SIEM (Security Incident Event Management) tied with internal and external Threat Intelligence. These two technologies combined will allow a business to effectively manage and assess network traffic but also take a proactive view understanding what threats a business is exposed to.

A SOC allows for centralization of network traffic through a SIEM which allows businesses to set use cases to look for anomalies that may have a negative impact. Use cases are set to allow the collection and correlation of data, for a SIEM to be effective you must be able to interrogate, provide analysis, and incident response effectively to alerts that are being raised. However, technology alone cannot help defend. There must also be a team that allows for certain levels of response depending on the severity of a particular alert.

Threat Intelligence is an outward-looking perspective that allows businesses to gain a better view of what their external threat landscape looks like as well as what their risk exposure is. A good example here can be seen with footprint intelligence that allows businesses to understand if they have been breached if accounts have been compromised if data has been exfiltrated from a business or senior executives have been put at risk. Coupled with having the ability to have a consistent view of data that may have been published on the deep or dark web.

[**34 days ago**](https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=290148#p1014732)

*Peer – Response Ali*

The article clearly outlines some of the key benefits of deploying SOC/SIEM in network security. By having a dedicated SOC/SIEM in network security system, businesses are able to continuously monitor the traffic flowing across their networks. This way, they have a better visibility of the threats to which their networks could be exposed to. The article however fails to show the differences between SIEM and SOC systems. SIEM is primarily used to collect aggregate log information. SOC on the other hand is a combination of people, processes, and technologies picked from the analysis done on SIEM. The two complement each other with SIEM doing the analysis work and SOC responding to any alerts (Akinrolabu, Agrafiotis, & Erola, 2018). It is also worth noting that SOC/SIEM systems have developed a highly advanced complex analysis method based on Artificial Intelligence (AI) and Machine Learning (ML). This helps to determine the aspects of the data that need further investigation and those that require immediate attention(González-Granadillo, González-Zarzosa, & Diaz, 2021).

I support the views expressed in the article. The application of SOC/SIEM security in business is quite beneficial mainly because it is cost effective, has a better collaboration, and offers continuous monitoring of the networks. SOC/SIEM also reduces the amount of time taken by the traditional systems to identify various threats and act on them (Mohanur Jagadeesan, 2020; Dietz, Vielberth, & Pernul, 2020). Consequently, the extent of the possible damage that could be incurred is also reduced.

**Wireguard VPN and cloud firewalls**

  writer : [**Jonathan Ashmore**](https://www.my-course.co.uk/user/view.php?id=16729&course=7514)

Last 9 days ago

Virtual Private Networks (VPNs) and firewalls are two separate components of networking. Both are responsible for securing the user’s network, privacy, and data. This discussion looks two emerging technologies: Wireguard VPN and cloud firewalls.

Wireguard is recent development in VPN technology developed by Jason Donenfeld in 2016. It is deployed on the layer 3 of the ISO model (Abdulazeez et al., 2020), and according to Hoxcha is fast, easy to use, modern VPN utilising the latest cryptography. Wireguard has many advantages such as high performance, user-friendliness; minimal attack surface, advanced cryptography, and well coded (2021). Delving deeper, Wireguard can be deployed as a secure shell (SSH), and by exchanging simple public keys. It uses modern cryptography such as Curve25519 and CHAcha20; and is compiled from roughly 5000 lines of code which is significantly less than the older OpenVPN’s massive codebase (Dronenfeld, 2021). Unlike other proprietary VPN software like Express VPN’s Lightway protocol, Wireguard is fully open source and available on GitHub (Donenfeld et al, 2021).

 A firewall in the simplistic sense is a type of computer software or hardware deigned to protect computer networks and systems from dangerous software and threat actors. Since the 1980’s, firewalls have matured into various types ranging from being installed on commercial routers to cloud firewalls (Dosal, 2019).As an increasing number of organisations are moving their data servers and I.T infrastructure to the cloud, service cloud providers are offering is Firewall as a Service (FWaaS) (Cloudfare, 2021). There are benefits to using a FWaaS: easily scalable and maintained, integrates with cloud infrastructure; no physical choke points, multiple deployments are protected, and malicious traffic is blocked. Another advantage of FWaaS is cost. Khakpour and Liu assert that a small US organisation could save up to 38% in firewall deployments if they use a FWaaS (2012).

In conclusion, Wireguard is attracting much attention for its speed and deployability with the added benefit of being fully open source. Firewalls as a Service are customisable: you only pay for what you use model, scalable, and selectable types depending on the threat.

*Peer – Response Ali*

   You centered your discussion on cloud firewalls and wire guard VPN. You highlighted several benefits of wire guard VPN, including minimal attack surface, user-friendliness, high performance, and advanced cryptography. Another advantage you did not mention is that it is easy to detect vulnerabilities in Wire Guard (Lipp et al., 2019).  I agree with these benefits. However, there are some weaknesses of the wire guard VPN. For example, Abdulazeez et al. (2020) argued that the automation of wire guards could make VPN providers log user data. Dowling and Paterson (2018) argued that a network admin could block the wire guard VPN because it works when it is on user datagram protocol (UDP) only. Although these disadvantages can hinder the effectiveness of wire guard VPN, Abdulazeez et al. (2020) argued that it could be better than other VPN protocols, including generic routing encapsulation (GRE) and internet protocol security (IP sec). Therefore, I support your argument regarding the effectiveness of wire guard VPN.

You also focused on cloud firewalls, emphasizing Firewall as a Service (FWaaS) benefits. However, I think it is important to address some weaknesses of FWaaS. Firewalls have several vulnerabilities. For example, Alsaqour et al. (2021) argued that personal firewalls are vulnerable to hacking due to static IP addresses and open connections. According to Alsaqour et al. (2021), firewalls cannot be used as standalone security measures because of misused security patches, insider attacks, and lack of deep packet inspection. Other vulnerabilities include configuration mistakes and DDoS Attacks (Kumar, 2016). Anwar et al. (2021) argued that the high exposure of firewalls to external attacks renders them ineffective in cloud environments. However, they can be used after taking special security measures. In conclusion, your discussion post is educative and was well-researched.