This discussion aims to briefly explain the key points of two cyber security technologies: SIEM (Security information and event management) and NGFW (Next-Generation Firewall).

**SIEM** combines “security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware” (FireEye, n.d). The principal operation collects, analyses, reports, and correlates data from multiple sources inside the organisation to identify deviations and potential real-time threats while storing them for future analysis and feedback. It is a holistic and centralised approach to cyber security in real-time incident response and forensic research.

Advanced SIEM solutions integrate AI and machine learning, enhancing efficiency and reducing the workload of security teams (SOC), albeit they demand significant setting and maintenance effort to harness its benefits.

Despite the merits mentioned above, SIEM is not suitable for every organisation. It demands a notable investment in finance, technology (i.e., IDS1, IPS2) and human resources (SOC team). It suffices to say that there is no universal solution that best matches every environment. An initial analysis should set the priorities regarding the assets, threats, legislation, and technological background before choosing the appropriate product.

Α **Next-generation firewall** is the cutting-edge technology in firewalls, as it develops previous firewalls’ features and enhances them with additional “anti-malware” services. In this way, an NGFW is capable of deep packet inspection (content evaluation) and application analysis, features that transform it into a decision machine rather than a mere network filter. NGFW monitors the traffic across the OSI layers and can detect and prevent possible threats up to the application’s layer. Furthermore, there is an additional capability to correlate specific security rules with users or groups, a feature that was not presented in the previous generations (Neupane et al., 2018)

In spite of the undeniable benefits that NGFW embodies, there are shortcomings and limitations. Above all, it still relies on the rules-parameters settings and the appropriate user handling.

Additional limitations come from the performance purview. How much latency is acceptable during the inspection? (i.e., How much time is needed to decrypt an SSL packet to inspect the content?)

A firewall has been and still is a profound tool in every network. NGFW is expected to add value, but it should not be considered infallible even if it has become more intelligent.

1 Intrusion Detection Systems (IDS) 2 Intrusion Prevention Systems (IPS)

**References**

FireEye. (N.D) What is SIEM and how does it work? Available from: https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html [Accessed: 26 February 2021].

Luk, K. (2011) ‘Choosing your Next-Generation Firewall’, *NetworkWorld Asia*, 8(1), pp. 38–39. Available from: http://0-search.ebscohost.com.serlib0.essex.ac.uk/login.aspx?direct=true&db=bsu&AN=101434347&site=eds-live [Accessed: 1 March 2021].

Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E. & Zunino, R. (2019) ‘The Applicability of a SIEM Solution: Requirements and Evaluation’, *Proceedings - 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2019*, pp. 132–137. doi: 10.1109/WETICE.2019.00036.

Neupane, K., Haddad, R. & Chen, L. (2018) ‘Next Generation Firewall for Network Security: A Survey’, SoutheastCon 2018, St. Petersburg, Florida, USA, 2018, pp. 1-6, doi: 10.1109/SECON.2018.8478973.

Podzins, O. & Romanovs, A. (2019) ‘Why SIEM is Irreplaceable in a Secure IT Environment?’, in *2019 Open Conference of Electrical, Electronic and Information Sciences, eStream 2019 - Proceedings*, pp. 1–5. doi: 10.1109/eStream.2019.8732173.