Discussion Forum – 2 Peer Response

Post by **Demian Berisford-Maynard**

102 days ago

Peer response

Hi Gokul.

I really get excited whenever I hear about Fortinet and Juniper. Thank you for explaining the Application Filtering technology.

I have a question about Vulnerability Management tools. Which tools would you say are very useful, and which ones would you say are really bad or inadequate?

Kind regards
Demian

51 words

1.

Reply to **Demian Berisford-Maynard** from **Gokul Kurunthasalam**

102 days ago

Peer Response

Hi Demian,

I appreciate your post and inquiries. The Vulnerability Management tool is a prioritised vulnerability management solution that includes numerous security-enhancing features such as comprehensive vulnerability assessment, built-in patching, system configuration management, CIS compliance, web server hardening, high-risk software auditing, and port auditing. Vulnerability Manager Plus is a lightweight agent-based solution that integrates effortlessly into any business of any size or manner of operation.

According to Gartner's chart 2021, Qualys, Rapid7, and Tenable Nessus scanners are the market leaders in vulnerability management products. Personally, I have experienced these tools as well as in Trend Micro, and all these VMs has fantastic features. I am unsure about the insufficiency of other vendor tools because I have not had exposure to them.

References:

"https://www.gartner.com/reviews/market/vulnerability-assessment" published on 2021.

126 words

2.

Post by **Iason Rigas**

101 days ago

Peer Response

Hi Gokul,

Thank you for your very interesting post. I would like to share a few thoughts on vulnerability management tools, which without doubt are very useful weapon in the arsenal of every IT department. As with everything else, it is not only about the tool itself but also about how to use it properly in the right context and the right environment. It is interesting how some companies (especially small ones) deploy VM tools only to get frustrated a few hours later by the huge amount of feedback they are getting and which sometimes they lack the expertise to analyse properly. To interpret the results correctly one needs to understand well the environment as well as the business context. Experts need to interpret the results to determine what is a false positive and what is a genuine vulnerability that needs to be addressed (Irwin,2020). This can be a source of frustration especially if the number of false positives is not manageable.

A second interesting effect is complacency. The fact that no vulnerabilities are detected by the tool doesn’t necessarily mean that there is no attack surface. Often an attack surface exists because of poor design or poor implementations. An example could be a network which is secure in terms of software vulnerabilities and in which such a tool brings up no findings but in which user management is poor and credentials are not kept secure. In such contexts the management might be surprised by a breach, wondering how it could be possible that after deploying such expensive solutions an attack was still possible. Last but not least VM tools will not offer any protection from zero days and from anything which is not part of their database or detection mechanism

References

Luke Irwin, 2020, *The pros and cons of vulnerability scanning*, *https://www.itgovernance.co.uk/blog/the-pros-and-cons-of-vulnerability-scanning*.

3.

Post by **Moseli Ts'oeunyane**

101 days ago

Peer Response

Hi Gokul,

Thank you for the clear and precise illustration of the technologies. My points here will add onto what you have already outlined. Next Generation Firewalls are a must for any organization for securing the perimeter. Entry into the environment is one of the most catastrophic incidents and deploying the best of the latest NGFW is of utmost importance. To top what you already mentioned, these firewalls also provide Intrusion Prevention Systems(IDS), sandboxing for malware prevention and containment whilst also getting the most up to date threats from various intelligent feeds(Checkpoint, 2022) hence even ensuring detection and prevention there-off of the most recent and zero-day threats

Vulnerability management is an essential component of cyber hygiene, ensuring that the absolute basics are catered for. Perhaps another aspect to include in the discussion is that of authenticated and unauthenticated scans, with authenticated scans providing even further flaws that can be exploited once the threat actor has gained foothold into the environment. Another way to look at is it is that you get to minimize risks against insider threats as well, since rogue employees may just attempt to exploit such vulnerabilities.

References:

1. Checkpoint (2022) Next Generation Firewall (NGFW) Available from: **https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/** [Accessed 29n April 2022]