Gokul Kurunthasalam

Summary Post
NGFWs – IPS, IDS and WildFire®

Two security technologies were mentioned in the initial post: NGFWs and vulnerability management tools. Appreciate Moseli Ts'oeunyane's reaction to the post that Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) play a critical role in the security module of next-generation firewalls (NGFWs). And you have correctly identified these firewall features. I'll also include another essential new feature from Palo Alto Networks - WildFire (Patented by Palo Alto Networks)

The malware can then be detected and blocked using the WildFire Analysis Environment. When a firewall identifies an unknown sample, it immediately submits it to WildFire for analysis to determine whether the sample is benign, grayware, phishing, or malicious. WildFire then develops signatures to identify freshly identified malware and instantly makes the most recent signatures available globally for retrieval. It examines incoming samples to these signatures and blocks malware initially discovered by a single firewall.

Vulnerability Management – SIEM and SOAR

Appreciate your feedback, Iason Rigas and Demian Berisford-Maynard, regarding vulnerability management technologies and their shortcomings. I want to take this occasion to discuss the VM tools Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR). Foreman (2010) stated that vulnerability is a weakness in the software or hardware that allows the use of the product beyond its design intent with an adverse effect on the software, system or data. Gartner (2019a) defines the essential capabilities of a SIEM system as extensive log and event management, log analysis and correlation, incident management, and reporting. SIEM is a term that refers to two distinct areas: security information management (SIM) and security event management (SEM)

Nowadays, SIEM solutions can be enhanced with a SOAR component. Gartner (2019b) defines the SOAR as a digital workflow structure that enables enterprises to aggregate security operations team-monitored inputs and design incident analysis and response methods. A SOAR system will manage the whole lifecycle of a security event, starting with detection and qualification, progressing through triage, enrichment, escalation, and containment, and concluding with remediation.

References:

WildFire® by Palo Alto Networks (2022) https://docs.paloaltonetworks.com/wildfire [Accessed 1st May 2022]

"Security Engineering: A Guide to Building Dependable Distributed Systems" by Anderson, R. (2008) 3rd ed. Wiley Publishing Inc.

González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759

"University Computer Network Vulnerability Management using Nmap and Nexpose" Published in International Journal of Advanced Trends in Computer Science and Engineering Volume 10, No.6 (ISSN 2278-3091) by Kismat Chhillar and Saurabh Shrivastava; Bundelkhand University, India; Published Date: December 06, 2021.

Collaborative Discussion 2 - Summary Post - Gokul K.pdf