Point of View

Vulnerability Orchestration Automation Remediation (VOAR)

"No More Manual Errors"

by **Manish Negi**

In the enterprise, infrastructure vulnerabilities are a daily occurrence. Often undetected by traditional security solutions and standard controls, these venerabilities can make it far easier for cyber criminals, malware, or rogue users to breach the standard walls of defense of the corporate IT function and compromise your IT infrastructure.

In today's environment where cybercrime is evolving extremely fast, traditional endpoint security solutions are no longer enough to protect an enterprise from all threats. These solutions also fall short of providing complete visibility which is required across the enterprise.

To address these issues, LTIMindtree has created VOAR (Vulnerability Orchestration Automation Remediation). This service helps enterprises to overcome manual challenges and take steps to proactively report the vulnerability, with the ability to track all vulnerabilities from a single dashboard.

VOAR uses intelligence-driven tools to tailor searches and reports that help enterprises to understand and address weaknesses within their environment. The main objective of VOAR is to automate the identification, followed by categorization, validation, and taking the required remediation action while meeting the SLAs with less human intervention.

Cloud-Native Service Management and FInding the Right Partner

Automate Context Addition

Security orchestration can automate enrichment and context addition for vulnerabilities before handing off control to the analysts for manual remediation. This maintains a balance between automated and manual processes by ensuring that analyst time is not spent in executing repetitive tasks, but in making critical decisions and drawing inferences.

Rapidly Take Initiatives

The longer the vulnerability monitoring and management process is, the greater are the opportunities for attackers to breach an underlying network and do significant damage. If enterprises are slow in closing gaps, there are increased opportunities for cybercriminals to elicit greater damage. Having some level of automation enables organizations to rapidly take initiatives to close vulnerability gaps with little human interaction.

More automation generally correlates to organizations being able to move more quickly and efficiently with their existing resources. This helps in closing gaps comprehensively and at a faster pace. This reduces the time for attackers to take advantage of the vulnerabilities that are not yet remediated. Not only does automation enable organizations to better protect themselves, but it also streamlines and enhances their overall workflow. VOAR can intake vulnerability notifications from third party sources and integrate vulnerability data logic which can be accessed through dashboards and reports.

End to End Automation

Automatically assign system owners to specific vulnerabilities. These vulnerabilities can be prioritized based on a variety of sources. These sources could include the vulnerability scanner and any other internal/external variables that are only known to your organization.

Conclusion

A proper vulnerability orchestration automation and remediation solution forms the backbone of a comprehensive security program. Most organizations exhibit lack of governance on the remediation process due to manual efforts. Many organizations lack in maintenance of patches and fixing false positives within agreed SLAs. Such issues require the help of an automation solution to address these challenges.

On an average, 53% of businesses in the world have experienced some type of cyberattack in the past 12 months, costing over $11.7 million in known damages per organization. In many instances, even though the patch is available, due to manual efforts, there is a possibility of the team forgetting to update the patches. This can prove to be extremely expensive for organizations, as many data breaches happen due to incorrect or missing updates of critical software patches.

Even before people began working from home, enterprise level ransomware was up 12% in 2019 with total damage estimated to be close to $11.5 billion. According to information from a data protection company, ransomware treats are expected to cost the global economy six trillion dollars by 2021. Organizations, hence require quick visibility and response on their vulnerabilities to mitigate risks early. Against this context, LTIMindtree's VOAR service can empower organizations with the required intelligence to proactively identify vulnerabilities and take steps to remove them with reduced human intervention.

About the Author

Manish Negi
Senior Security Architect, LTIMindtree

Manish is a cyber security professional with diverse experience in security consulting, He has worked extensively in managing corporate infrastructure security for global clients across domains, including defense, banking and insurance, retail, and healthcare. At LTIMindtree, Manish is responsible for identifying customers' technical and business requirements to identify and suggest infrastructure security solutions as per industry standards.