Datasheet

ACTIVE VULNERABILITY MANAGEMENT

We assess the enterprise IT environment in two approaches, External & Internal vulnerability management. This approach will identify application, network, web related vulnerabilities on the servers exposed to the Internet. With a vulnerability scanner, we will periodically scan the Customer's Internet Facing IPs with defined scanning parameters. At the end of each month, the ActiveBytes team will validate the findings from the vulnerability scanner and create a report for valid findings to share with the corresponding client team that is responsible for fixing the vulnerability issues. Our team will keep track of all the identified issues, their status and remind the respective team if no action is taken. The expected behavior is to not identify the same previous scanned vulnerability. This will ensure that the enterprise security posture is continuously improved.

Some steps from our vulnerability management service

- Scoping, Infrastructure analysis and vulnerability assessment program design
- Implementation of technical prerequisites for the vulnerability assessment program like test equipment & automation of evaluation
- Implementation of vulnerability assessment processes
- Reporting, Remediation and follow-ups

Active Vulnerability Management (External)

Our Approach

- Vulnerability scanning of customers internet facing assets
- Monthly report publishing
- Remediation stage
- Tracking the status

We scan the public IP VLANS every month and after finding false positives, the report with valid findings is shared with the client enterprise team. Also, we extend our support in coordinating the remediation with the IT team. Finally in order to ensure that the same risk is solved, we track the reported vulnerability issue and make sure it's closed.

After the identification of vulnerabilities, it is verified whether these are not false-positive, and vulnerabilities are assessed in unity also in relation to other vulnerabilities. When assessing vulnerabilities, exploitation of the vulnerabilities is not part of the process.

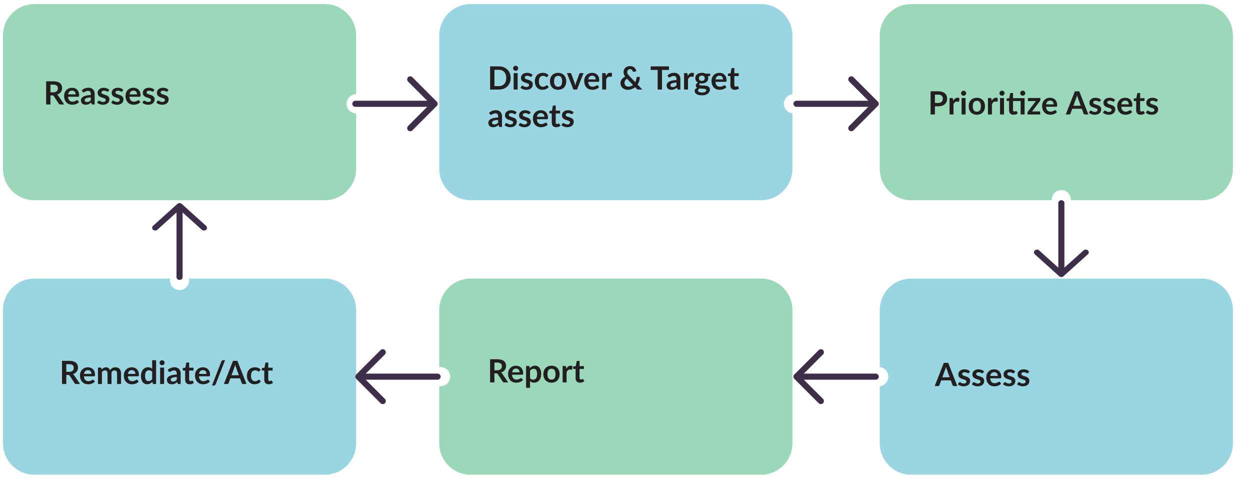
Active Vulnerability Management (Internal)

ActiveBytes team uses active vulnerability management solutions for the effective identification and management of internal vulnerabilities. We have well defined methods to understand the severity of the vulnerability.

- Vulnerability Age
- CVSSv3 Impact Score
- Exploit Code Maturity
- Product Coverage
- Threat Sources
- Threat Intensity
- Exposure of the vulnerability

By considering multiple factors, the effective severity of the vulnerability is determined and shall be raised to the client team for action like security patching. The timeline of the actions for different classifications of vulnerabilities will be agreed upon with the customer and the matrix shall be used by our security team.

Our Approach



From the integrated internal systems and network, we will look for vulnerabilities like default passwords, neglected software patches, security misconfigurations etc. and report with recommendations. This will help the team to know the organization's threat landscape and reduce attack surface and mitigate risk. We will have coordinated, cross functional team to work, utilizing tools and resources to gain greater insights for remediation.

Benefits

- Mature enterprise security posture
- Reduce overall risk through timely remediation
- Flexible & customized as per enterprise context
- Gain operational effectiveness by aligning teams with project goals
- Enhanced visibility with efficient racking & Reporting
- Achieve regulatory requirements by meeting compliance standards
- Maintain customer trust & Business reputation by securing data

Contact us

✉ contact@active-bytes.com ☎ +971 50 513 3973

www.active-bytes.com