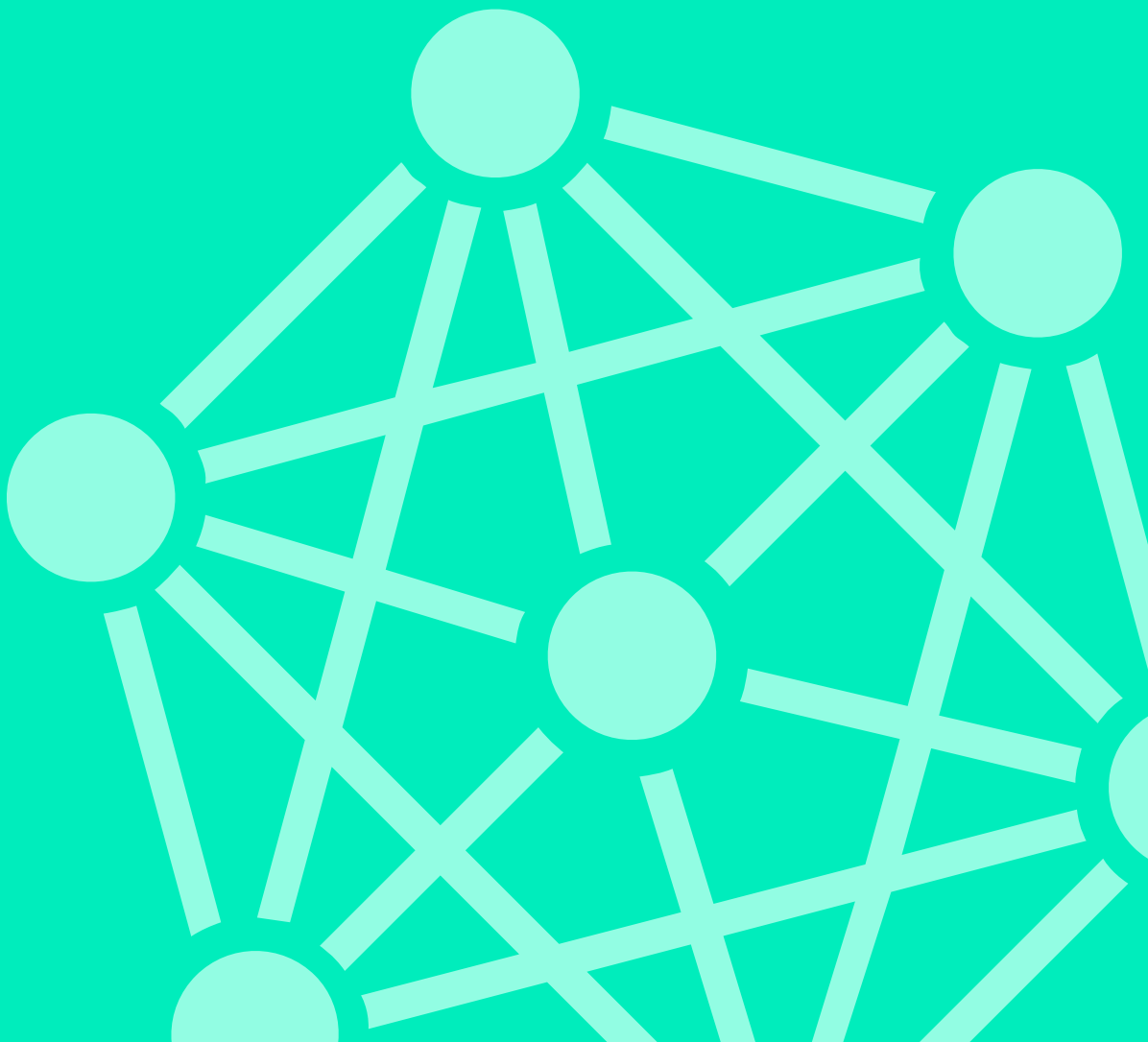
Logsign

Logsign Security Orchestration, Automation and Response (SOAR) Use Case:

Vulnerability Management



Vulnerability Management

Customer Challenge

Discovery of vulnerabilities in an organization's IT infrastructure is a strategically beneficial exercise. Vulnerability management involves proactive as well as reactive security measures. If there exists a vulnerability and your SOC team has not mitigated it, attackers may exploit this vulnerability and disrupt your business operations in n number of ways. Ignoring the presence of vulnerabilities in IT systems is equivalent to keeping the door open for thieves.

How to manage vulnerabilities with Logsign SOAR

Logsign SOAR helps your SOC team in achieving a delicate balance between automated and manual processes for vulnerability management. It assists your team in:

1. Adding manual information about vulnerabilities;
2. Using contextual information about assets and vulnerabilities;
3. Enriching alerts with endpoint information and CVE data;
4. Adding information about vulnerabilities to an incident;
5. Calculating the risk and impact of an incident; and
6. Allowing the SOC team to remain in control of mitigation measures and patch management.

Business Process Analysis

It may take a security analyst for up to 50 minutes to undertake the manual process. However, with the help of automation, Logsign SOAR cuts down this time to 1-2 minutes.

Benefits

Logsign SOAR automates parts of your vulnerability management process with control and decision-making power resting with your team. Automation helps in minimizing response time to alerts, and as a result, your organization keeps on addressing vulnerabilities before attackers exploit them.