Vulnerability Management

Vulnerability Management

Solvay is adopting a Vulnerability Management Process using a Vulnerability Management Lifecycle

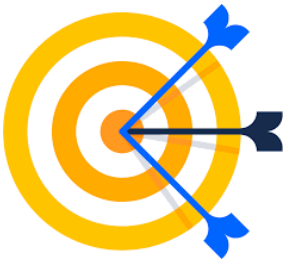
and including:

- Governance structure
- Design processes
- Defined roles and responsibilities
- Appropriate tools

This will help Solvay to identify, quantify and prioritize remediation of vulnerabilities, as well as track remediation progress.

Our Mission?

- Detect vulnerabilities across Solvay's environment
- Provide asset operating teams reports with remediations that need to be applied
- Prioritize the remediation actions based on risk reduction
- Provide additional feedback and support when needed
- Create dashboards for both security managers and operating teams with overview of the Solvey assets vulnerability status



What is a vulnerability?

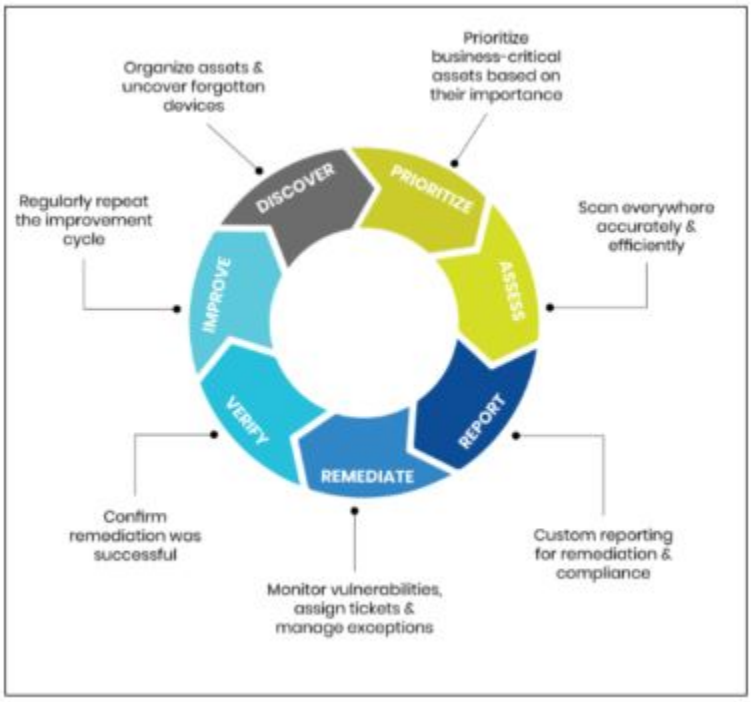
A vulnerability is a cybersecurity weakness that a bad actor could exploit to gain unauthorized access to your enterprise network and compromise resources. The vulnerability could be present in unpatched or out-of-date software, or occur due to missing or weak authentication credentials. System misconfigurations, poor data encryption, malicious insider threats, injection flaws and zero-day vulnerabilities are some other, common types.

If an attacker successfully exploits a vulnerability, they can damage your organization in many ways. Here are a few examples:

- Run malicious code on your systems, such as ransomware
- Install dangerous malware
- Steal sensitive data
- Conduct corporate espionage

What is Vulnerability Management?

- Vulnerability management as a “process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization.
- Focused assessments on the adequacy and implementation of technical, operational, and management security controls



What is the Vulnerability Management Cycle?

Discover assets	Prepare an asset inventory for monitoring.
Prioritize enterprise assets	Prioritize assets based on the potential impact of a vulnerability’s exploitation (identify business-critical assets).
Find and assess vulnerabilities	Identify vulnerabilities using vulnerability scanner software (CrowdStrike, Qualys, etc.)
Prioritize and report vulnerabilities	Prioritize identified vulnerabilities based on potential impact and risk, prepare a detailed report
Address vulnerabilities	Address vulnerabilities based on priority (apply security patches, upgrade software, etc.)
Verify remediation	Assess where remediation actions were successful
Continuous improvement	Maintain the cycle of excellence through feedback and continuous improvement

What is the scope of Vulnerability Assessment?

blocked URL

- Workstations and Servers (O/S, Middleware, Tools)
- Business Applications
- Network devices
- IoT, Industrial Control Systems

How to Contact VOC (Vulnerability Operations Center)?

Email to:

oti-security-vulnerabilities@solvay.com

---

blocked URL

- **SOC Team**
- **Contact Vulnerability Operations Center**