INTRODUCTION TO VULNERABILITY MANAGEMENT

Enterprise technologies are complex systems that require several components to work together across a distributed network. Each component can have its own security vulnerabilities that expose the entire system to security threats. These components can be:

- Hardware or software
- Developed in-house or procured externally
- Deployed in-house or accessed as internet- and cloud-based services

It's virtually impossible to address vulnerabilities in all such components that customers don't develop or control, especially when many vulnerabilities are unknown, leading to zero-day exploits.

At

the same time, failing to secure sensitive business information and assets against vulnerabilities within the technology components that power your business can prove costly. Research suggests that hackers perform a cyber-attack every 39 seconds—that's 2,244 times a day!

Finding the right incident response plan can be challenging and often, too late to prevent the loss especially considering the time it takes to discover a breach in the first place. In 2019, security breaches went unnoticed for an average of 206 days.

This is where vulnerability management comes in. Let's take a look.

What is vulnerability management?

Vulnerability management is the outcome of a vulnerability assessment initiative. It's defined as the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" vulnerabilities within a technology system. The scope of vulnerability management extends the domain of computer security, encompassing:

- Business operations
- External partnerships
- Workforce training
- Legal and environmental limitations facing a business organization

A breach can emerge from security gaps that exist in several unforeseen sources other than the technology itself:

- **Weak business process.** Sensitive information exposed to external partners or inadequate security protocols adopted against new security threats.
- **Inadequate legal cover.** Failing to oblige partners, employees, and customers to follow security best practices.
- **Inadequate access controls.** Allowing access to sensitive information and assets.
- **Human errors.** Failure to educate and train employees on following security best practices, allowing broad access to sensitive business information, codebase and servers.
- **Physical and environmental issues.** Power outages and natural disasters can affect access to data stored off-site.

In the real-world, these challenges can be avoidable and the best security strategies often focus on reducing the risk and impact of a security breach in the first place. The starting point would be to manage vulnerabilities that exist within the business and the technologies that it uses. These vulnerabilities can be known or unknown. An effective vulnerability management program is designed to encompass all possible vulnerabilities and their impact to the business.

What is a vulnerability management program?

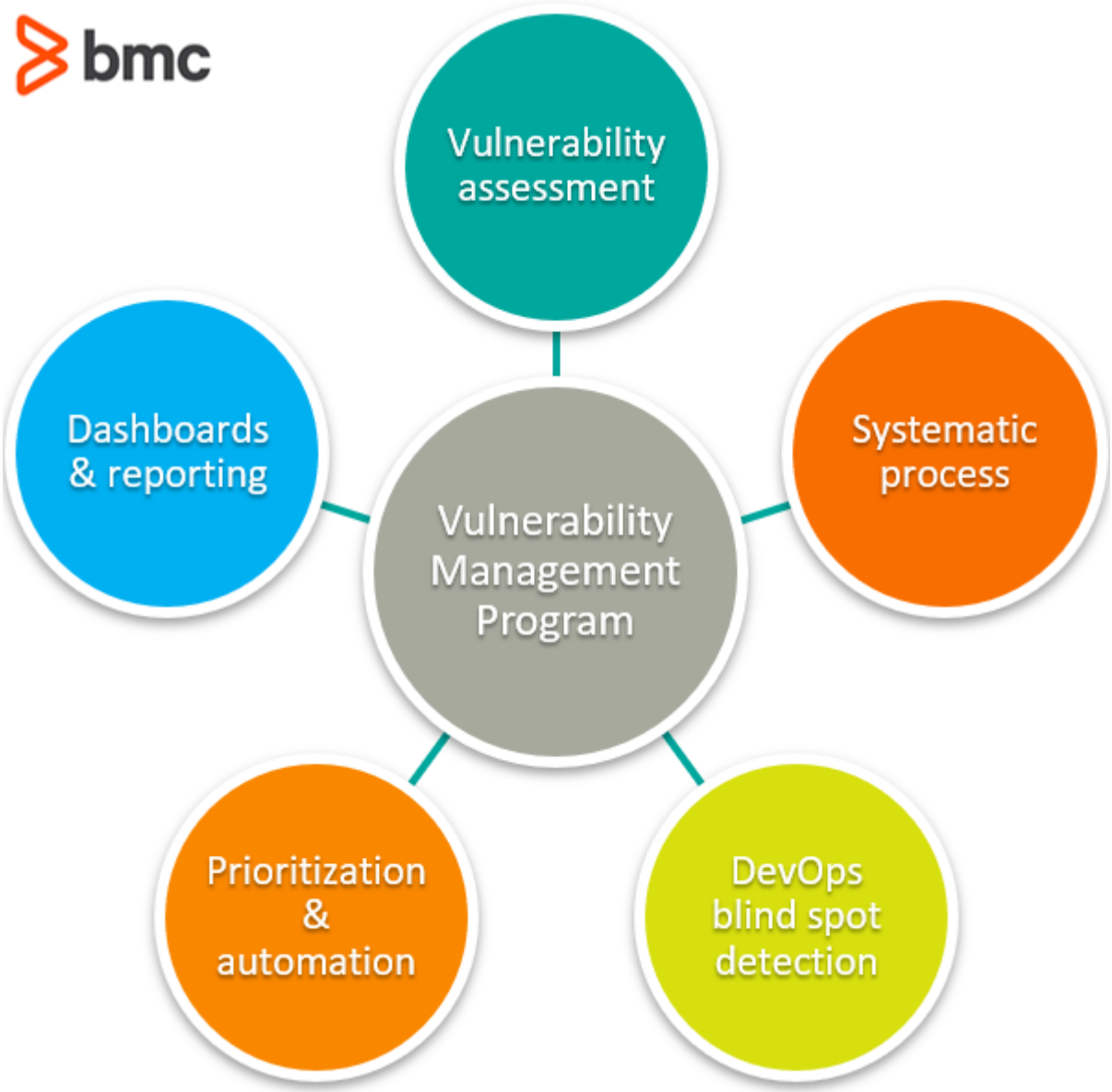
A vulnerability management program is designed uniquely for each organization, taking into consideration:

- Security threats the organization faces
- Technologies used
- Legal and geographic limitations
- Customer and market requirements

- Additional factors

COMPONENTS OF A VULNERABILITY MANAGEMENT PROGRAM

Typically, the following components are shared across all successful Vulnerability Management programs in the modern era of technology:



Vulnerability assessment

Vulnerability management builds on the knowledge acquired with vulnerability assessment to adopt effective measures in treating the risk and impact.

However, vulnerabilities evolve continuously in response to changing threat landscape, procurement of new technologies, and updates, as well as changes in business process. A necessary provision to re-evaluate vulnerabilities and the associated risks remains an important part of the ongoing vulnerability management program.

Systematic process

Establish a formal process to conduct vulnerability assessment and treatment as an ongoing activity. This process will include tracking and documentation of:

- Policies
- Technologies
- Business operations
- The efforts involved in mitigating new vulnerability risks

Vulnerability management relies heavily on advanced technology solutions capable of identifying vulnerabilities and communicating optimal and timely actions for SecOps response teams.

Blind spot detection for DevOps

As the adage goes: "You can't manage what you can't measure". Continuous monitoring is integral to vulnerability management, especially in DevOps environments where rapid changes in infrastructure configurations can expose vulnerability risks. If the new systems are not scanned, vulnerabilities can exist as blind spots—just waiting for hackers to compromise.

Automated discovery capabilities can help manage this security gap by identifying known vulnerabilities and prompting the installation of security patches before the infrastructure is used in the security sensitive SDLC pipeline.

Prioritization & automation

Once you've identified the vulnerabilities, share the information with appropriate SecOps team members, IT Ops, or business units using the vulnerable technologies. These members may prioritize vulnerability treatment based on organizational and business policies, as well as preferences within teams and departments. For instance, some teams may not want to spend time investigating and disabling services that are not needed for certain periodic intervals. However, the service may continue to expose the business to security risks while it is not monitored.

A vulnerability management program should be designed to automate remediation processes and minimize the security risks using advanced technologies. The manual approach to vulnerability management can no longer suffice in modern enterprise IT environments.

Fixing a vulnerability can require prolonged efforts that must be repeated and is still prone to human errors. An effective Vulnerability Management system preserves and reuses the decisions involved in treating new vulnerabilities as they arise. Additionally, vulnerabilities should be fixed as soon as a patch is available, but within predefined policies of prioritization, patch deployment bandwidth limitations and others.

Dashboards & reporting

Vulnerability management solutions access logs from a vast network and monitor the infrastructure continuously. SecOps teams can easily get overwhelmed with the amount of information that's available to make decisions on managing vulnerabilities, which are often required in real-time. An intuitive, easy to use and comprehensive dashboard and reporting mechanism is therefore a key component of a Vulnerability management solution.

The main challenge for SecOps and IT Ops is to make the right information about ongoing vulnerability assessment available, followed up with a fast and effective remediation process. This gap is closed only when the right insights are promptly available to appropriate decision-makers.

Additional resources

For more information, browse the BMC Security & Compliance Blog or read the following articles:

- An Introduction to Vulnerability Reports
- SecOps for Dummies
- SecOps in Action, and how you can benefit from it
- Too Many Vulnerabilities and Too Little Time? Why Automation is an Imperative
- What is Security Threat Modeling?
- What is CVE? Common Vulnerabilities and Exposures Explained