Vulnerability Management Best Practices

Reading

55m

✓ Status | Incomplete

Introduction

In this course, you have seen what a vulnerability is, what a vulnerability assessment is, and how these are an integral part of the Risk Management Process. Now, you will zoom in on the Vulnerability Management Process and best practices for managing the vulnerabilities that might exist and crop up in our own organization.

Following the best practices and an appropriate process when conducting the vulnerability assessment will ensure that you have thorough and appropriate results that support your organization's needs. A crucial outcome of the Vulnerability Management Process is a vulnerability assessment report, which helps an organization focus their risk management efforts in the right direction.

Overview

Before you dig deep into best practices, make sure you have a general overview. The short video below will introduce you to critical parts of vulnerability assessments, active and passive scanning, authenticated versus unauthenticated scanning, and how vulnerability assessments fit into the overall security of the organization, including security incident response.

1. Watch the short video on Vulnerability Assessment Best Practices
2. Take some notes for yourself about the overall process and the various components that go into making up an effective Vulnerability Assessment Process.

Reading

Now that you have a high level overview of the overall process, it's time to examine industry best practices for conducting a vulnerability assessment.

Vulnerability management can be divided into a four phase process, as can be seen in this diagram:

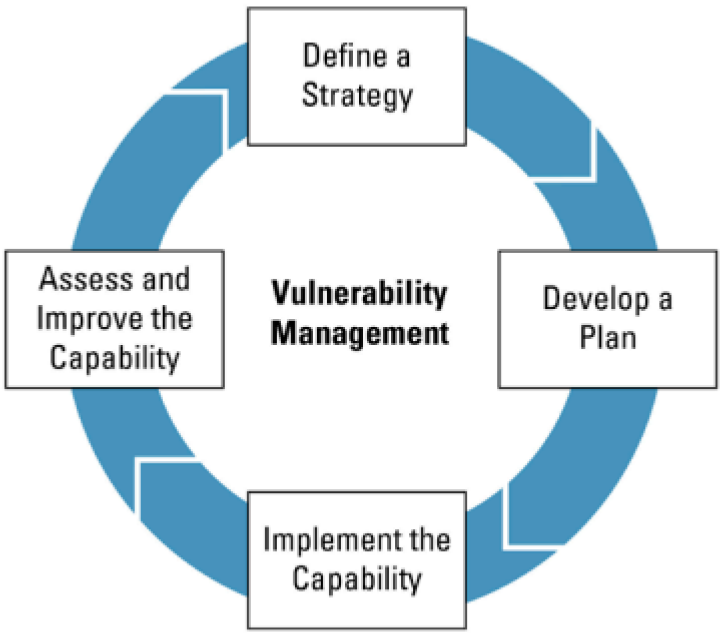

Figure 1: The Vulnerability Management Process

(image source: CISA)

> ⚠ Don't let the word "assess" fool you.
>
> In this process, the actual vulnerability assessment doesn't fall in the fourth stage (Assess and Improve the Capability) despite its title.

The overall process is specifically focused on the defining and planning, implementation, and post-evaluation of the vulnerability assessments themselves. The implementation phase, which is stage three, Implement the Capability, is where the vulnerability assessment will actually take place.

Four Phases of a Vulnerability Management Process

Phase 1: Define a Strategy

Involve all levels of the organization, especially the upper levels, so decisions can be made and supported about what focus, scope, and methods of testing fit within the capabilities and requirements of the organization and support its goals.

Phase 2: Develop a Plan

Plan the approach; decide on requirements, tools, information needs, both to support the test and from it, and how to deal with updating the plan as needed.

Phase 3: Implement the Capability

Take the plan and put it into action; inform and include stakeholders; make sure all requirements are met and in place; perform the test; collect the results; measure, categorize, and prioritize the results; research and measure costs and results of exploitation, including business effect and exposure; and come up with recommended mitigations, what all is affected, and what is required to implement remediations.

Phase 4: Assess and Improve the Capability

Analyze and evaluate the completeness and effectiveness of the program and decide on ways to improve it going forward.

Challenges of the Process

If you stop and think about this process, this is not a short-term endeavor. It is going to take a team from across all levels of the organization, with dedicated time to plan, implement, and evaluate all of this. There is also a cost attached to it.

In addition, this is a process that is not completed just once, or once in a while, but repeatedly, as a regular monitoring of the organization's vulnerability status and Risk Management Process.

Best Practices

> ? Given the scope of this process, what do you think might be some key best practices to ensure this is a valuable part of a company's processes?
>
> *Jot down some of your own ideas, then read on to compare.*

- **Keep the business in focus:** tie the entire process, right from the initial concept and buy-in stages through the final evaluation of the overall project, to the business, its goals, needs, and capabilities.
- **Don't leave anyone out:** ensure all required stakeholders, internal and external, and from all levels of the organization, are involved and reported to appropriately.
- **Plan, plan, plan:** plan as much as possible, for all possibilities. Don't forget a process for updating the plan.
- **Understand before acting:** evaluate needs, capabilities, and options, for the business, the test, and the outcomes, before making decisions on methods, timings, and approaches.
- **Reports are key:** research, and report as thoroughly as possible on the results *and* the process, to ensure improvements can be decided on and implemented appropriately going forward.
- **Keep policies in mind:** company policy is a crucial part of the security and privacy controls, as well as the vulnerability monitoring and assessing process of an organization.

Further Reading

Deep dive into the process and good practice for planning and completing a Vulnerability Management Process.

> As you read, consider how and where the vulnerability assessment report fits into the process, and the impact a well-written (or poorly-written) report can have on an organization.

CISA, CRR Supplemental Resource Guide, Volume 4: Vulnerability Management

Key Takeaways

In this reading you have seen:

- How vulnerability assessments are part of a larger ongoing process that monitors the vulnerability status of an organization
- How the entire organization, especially upper levels, is an integral and critical part of the process of monitoring and managing the security and privacy controls and vulnerabilities therein within an organization
- Some of the best practices for managing, completing, and maintaining monitoring and remediation efforts with regards to an organization's security and privacy controls

Conclusion

It is important to understand that as a security professional, you do not act independently on an organization's assets, and security and privacy controls. In fact, it is critical to work *with* the organization to aid in the support and security of the organization's goals, within the organization's capabilities. This requires consultation, support,and buy-in from all levels of the organization in order to be able to do the job effectively.

References

CRR Supplemental Resource Guide, Volume 4: Vulnerability Management

✓ Mark Completed

← Previous
Vulnerabilities and the Risk Management Process

Next
Vulnerability Management Process Knowledge Check →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D4

Thu Jul 25

› Lectures (1)

⌄ Work (8)

6 hrs

- </> Case Study: Vulnerability Assessment Scan
- ⚡ Discussion: Vulnerability Assessment Scan Case Study
- ? Vulnerability Assessments Knowledge Check
- Vulnerabilities and the Risk Management Process
- Vulnerability Management Best Practices
- ? Vulnerability Management Process Knowledge Check
- Vulnerability Assessment Report Templates
- ⚡ Report Templates Review

W05D4 Schedule »

Powered by Lighthouse Labs.