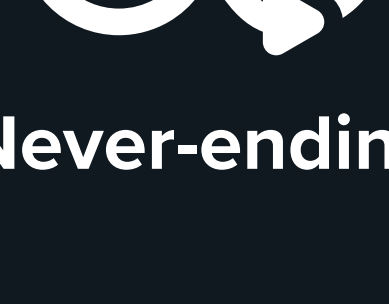


Vulnerability Management Program

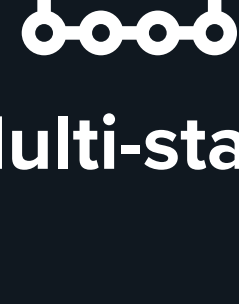
BEST PRACTICES

1

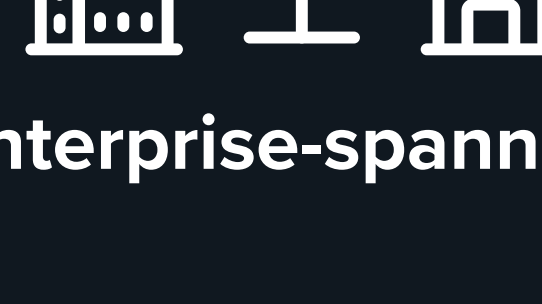
Vulnerability Management is...



Never-ending



Multi-stage



Enterprise-spanning

2

A Successful Vulnerability Management Program requires:



Ownership



Accountability



Budget



Visibility

3



Create a Threat and Vulnerability Management Quarterback Role

The quarterback **KNOWS WHO IS ABLE TO REMEDIATE** vulnerabilities for each application and system.

The quarterback and remediation owner **WORK COLLABORATIVELY** to evaluate vulnerabilities.

4

Document Your Vulnerability Management Program with:



Policies



Standards



Procedures

5



Automated Vulnerability Scanning



Manual Pentesting

SCAN everything in your environment, including **CLOUD INFRASTRUCTURE**

Use **AUTHENTICATED MODE** to scan high-value resources

Use penetration testing to find **WHAT SCANNERS MISS**

6

Where to Start with Penetration Testing?



Prioritize Your Perimeter.

First penetration test? Start with an external network penetration test.

But, don't forget about securing and testing your internal network.

Avoid a highly-protected exterior paired with an unprotected interior. A system without sensitive information can be used to attack sensitive systems.

7

Know Your Vulnerability Footprint

A vulnerability footprint is all the technologies that might expose vulnerabilities.

8

Understand Your Vulnerability Landscape



Known CVEs

Common Vulnerabilities and Exposures

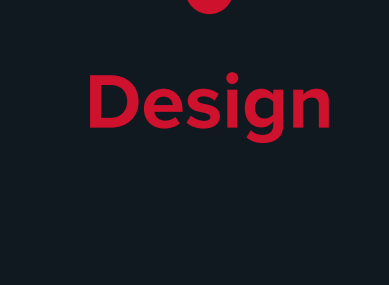


Known CCEs

Common Configuration and Enumeration



Architecture



Design

9

Integrate All Sources of Vulnerability Data into One System



10

Make the Information Consumable and Actionable



NETSPI NOTE:

Extremely large files of vulnerabilities are unmanageable.

11

Develop a Risk-Based Approach, Commensurate with Your Program's Maturity Level and Appetite for Business Risk

Less Mature Programs:

- Start by fixing the easy-to-remediate vulnerabilities with known exploits.

Advanced Programs:

- Extend your program to risk-based prioritization.
- Set timelines and thresholds for remediation by severity.

CRITICAL
7 days

HIGH
2 weeks

MEDIUM
1 month

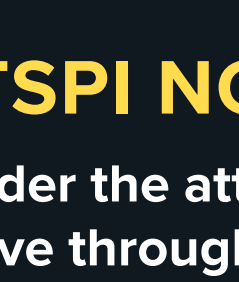
LOW
Patch-Driven Updates

12

Consider Whether a Vulnerability Threatens an Important System or a System with Access to an Important System



Cloud infrastructure with VPN access to the corporate network



Application or database in production



Internet-facing websites

13

Assign Vulnerabilities to and Work Closely with Application and System Remediation Owners



Work with the people who have the skills and knowledge to remediate the vulnerabilities.

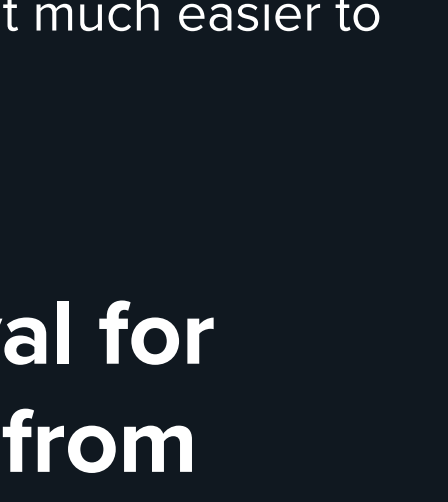


NETSPI NOTE:

The technology remediation owner is often a different person from the application owner as listed in the system of record.

14

Track Remediation



If you can integrate your vulnerability management system with your ticketing system, such as JIRA, automated trouble ticketing will make it much easier to assign and track remediation.

15

Get Approval for Exceptions from Business Leadership

- Exceptions occur when a vulnerability can't be remediated in a timely manner.
- Convert technical risk into business risk, so the CxO understands what could happen if this vulnerability is exploited.



NETSPI NOTE:

Exceptions can be delayed but **CANNOT** be put off forever.

16

Scan and Penetration Test Regularly to:



17

Track Metrics and Report to Senior Management, such as:

How many critical vulnerabilities are in our internet-facing systems?

How many of these critical vulnerabilities have known exploits?

How long it takes us to patch known vulnerabilities on average?

18

Consistently Look for Ways to Improve Your Vulnerability Management Program

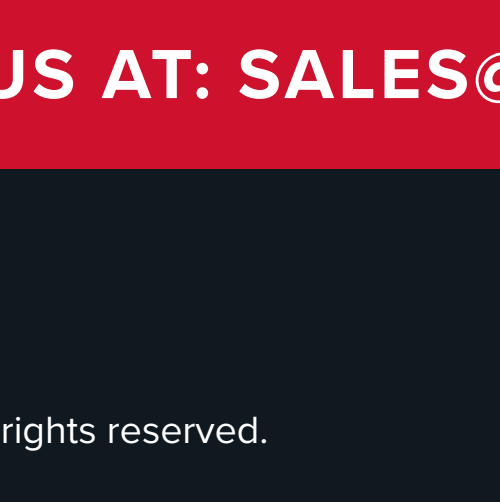


NETSPI NOTE:

The more you can automate the better, because spreadsheets, emails and SharePoint don't work for vulnerability management for a large company. Automation enables visibility and continuous improvement.

19

Commit to an Ongoing Vulnerability Management Program



Threat and vulnerability management is a program (not a project) — it never ends.

We're Experts in Penetration Testing and Vulnerability Management



Speak with a Vulnerability Management Expert Today!

CONTACT US AT: SALES@NETSPI.COM, NETSPI.COM OR 612.465.8880

Ver 01 - 03/2020
© 2020 NetSPI LLC. All rights reserved.

