Vulnerability Management

Campus Network Design & Operations Workshop

Overall Goals

- People often think that cybersecurity is about tools – firewalls, intrusion detection systems, etc.
- Tools are important, but cybersecurity is really about risk management
- You can’t be 100% safe
- Risk management is about having the policy and processes to both identify risks and then how you will expend resources to address them

Policy and Process

- These involve more than IT staff
- You need a collaborative approach with all stakeholders to have a shared understanding of risks and how they are addressed
- IT manages the systems, but often doesn't own the data

Example: At a university, the Registrar often controls student data – they collect it and are empowered to decide how it can and cannot be used

- Leadership needs to be involved

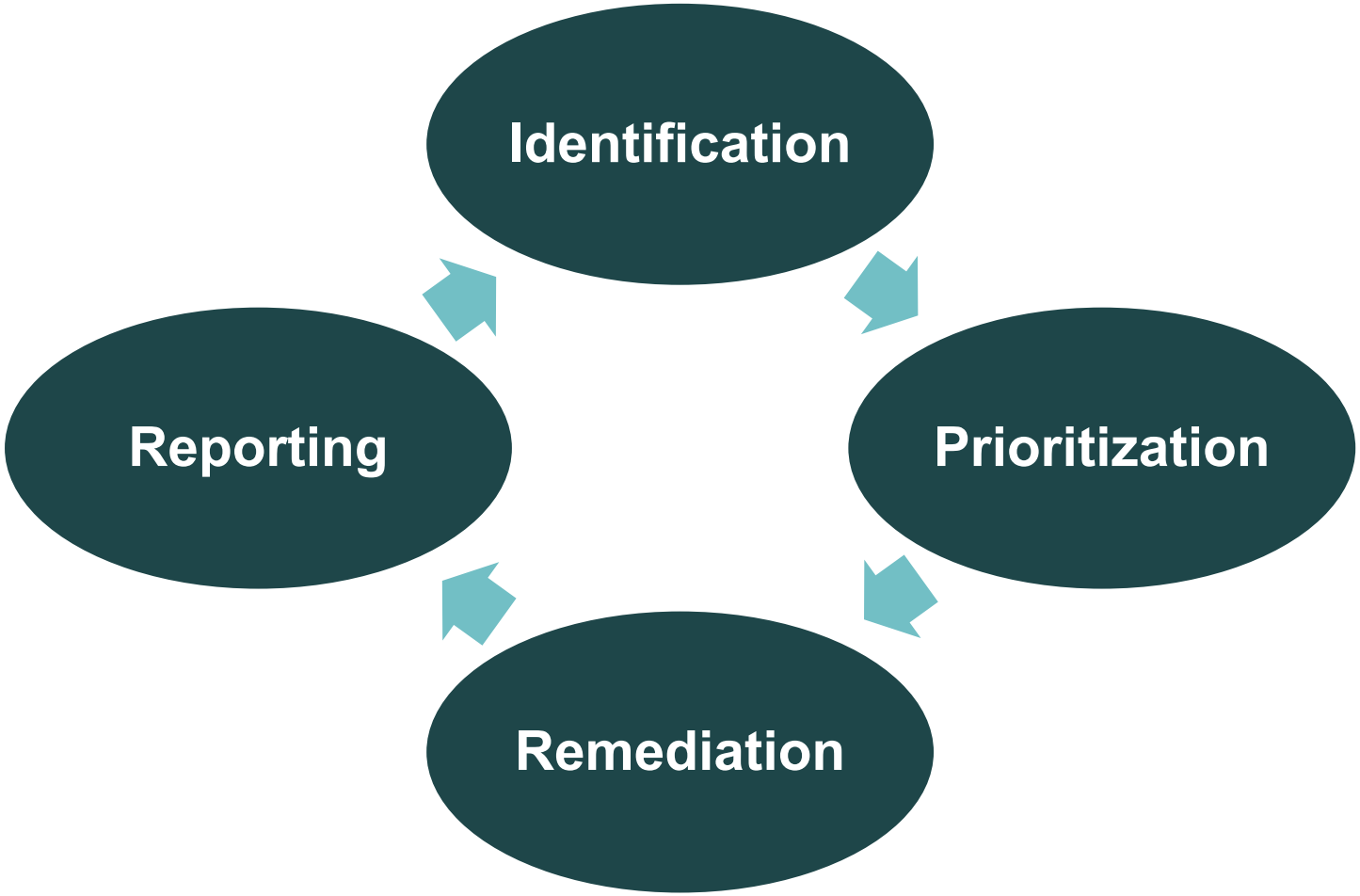
What is a Vulnerability?

- A vulnerability is a weakness in an information system that can be exploited by an attacker

- When we talk about Vulnerability Management, the primary vulnerability being addressed is an exploitable software flaw – either because a system wasn't patched or it was a 'zero-day' (a vulnerability that was disclosed before a patch was made available)

What is Vulnerability Management?

A continuous process designed to proactively identify, classify, remediate, and mitigate vulnerabilities in an IT infrastructure.



Why Vulnerability Management?

- To reduce the risk and ensure confidentiality, availability, and integrity of the systems the university uses to accomplish its business
- To protect the data entrusted to the university and comply with external regulations
  - Some of the external regulations that apply: FERPA, HIPAA, GLBA
  - Other institutionally important data: Research, and PII
- To protect the university's reputation

Key Components

- Asset Inventory
- Vulnerability Identification
- Patch Management
- Policies and process to tie it all together

Identification - Asset Inventory

- What does inventory have to do with vulnerabilities?

- You have to know what you're protecting:
  - What and where (physical and network) your systems are
  - What data is being processed and who are the owners
  - Who understands the system and who can address the vulnerabilities

Identification - Asset Inventory

- What is the relative criticality of the systems and data?
- Identify your critical systems
  - *Examples:*
  - If you have Active Directory, who runs your domain controllers? Where are they?
  - For student data, what server hold the database and what endpoints do processing?

Identification – Vulnerability Scanners

- Vulnerability Scanners are used to identify vulnerable (unpatched) systems on your network
- Some vendors are extending their vulnerability scanner into External Attack Surface Management
  - Attack surface is what services can be seen from the internet
  - This goes beyond software patching and helps determine misconfigurations
    - *Example*: an IP security camera connected to the wrong network, and the feed is available to the world

Approaches to Vulnerability Scanning

Two main approaches to vulnerability scanning

1) Agents installed on systems

2) Sensor devices deployed on your network

Agent Based Scanning

Strategy: install a software agent on systems to collect data

- Pros
  - Often more complete detection results as the agent has full visibility into the system
  - Handles devices (like laptops) that move around the network
- Cons:
  - Needs existing tooling to deploy
  - Only works on systems that an agent can be installed

Network Based Scanning

Strategy: install network sensors to remotely query systems

- Pros
  - Can scan systems that don’t support agents (example: IOT)
  - Can identify systems you didn’t know where there

Network Based Scanning

- Cons:
  - Sensors need full connectivity to all systems; configuration needs to be kept updated as network changes
  - Doesn’t deal with systems that move around the network
  - More tuning needed to avoid breaking fragile equipment
  - Much less complete detections unless credentials are used

Network Based Scanning

Some network-based scanners support loading credentials: the sensor will remotely log into the system to scan it.

This provides the same level of visibility as a solution with agents, but with the drawback of having to manage and secure the credentials.

What To Look For

The key value a vulnerability scanner provides is **visibility** into the vulnerabilities on your systems.

- As much detail as possible – either agents (with support for the systems you run) or network scans with credentials
- IPv6 support – its not practical to scan your whole space looking for devices, so you'll want to be able to feed in addresses to scan
- Support – vulnerability scanning is an inexact science. You'll have false positives, false negatives, and scans that break devices

What To Look For

- Granular scanning configuration to support exceptions
  - Some hosts can break with an aggressive scan
  - You have some other mitigation in place for a particular vulnerability or host and don't want it to keep being flagged

- Detailed reporting: existing vulnerabilities, fixed vulnerabilities, and ones that were fixed that reappeared, systems no longer reporting data. You want all the data!

What To Look For

- Nice to haves
  - Process to help prioritize vulnerabilities
  - Attack Surface scanning
  - Web application scanning
  - Identification of devices on the network

Vulnerability Scanner Options

- Some of the big commercial players in this space are Tenable and Qualsys, but there are many others

- Open source/free solutions are limited
  - The real value in a vulnerability scanner is the continually updated feed of vulnerabilities they can identify
  - *Example*: OpenVAS is an open source vulnerability scanner but the free feed has very limited coverage

Free Vulnerability Scanner Options

- You can piece together visibility based on data you may already be collecting
  - Your patch management system may give you reports on what is installed
  - EDR solutions often have a vulnerability report
- US Education entities are considered critical infrastructure, and CISA provides a free vulnerability scanning service https://www.cisa.gov/cyber-hygiene-services

Free Vulnerability Scanner Options

- Open Source tools can provide attack surface information
- *Some Examples*:
  - Shodan is a search engine for internet visible devices and services
    - You can get a basic Shodan subscription for free if you have an academic email address: https://help.shodan.io/the-basics/academic-upgrade
  - nmap is a surprisingly useful tool for basic attack surface scanning

Vulnerability Scanning Gotchas

- Network scans without credentials is an inexact process
  - The scan is essentially is doing some of what a hacker or pen tester would do to probe the environment
  - There is a risk of misidentifying services
    - Both false positives and false negatives
    - *Example*: Hunting for end of life windows systems, the tool may misidentify a Windows Server 2012 (which are end of life) systems as running Windows Server 2016 (which are still supported)

Vulnerability Scanning Gotchas

- Network scanning carries the risk of causing an outage
  - Some hosts can hang or malfunction when undergoing an external vulnerability scan
    - This usually only happens with embedded or IOT type devices
  - *Example*: Network attached printers will often start spewing out paper when port 9100 is scanned
  - Scanners can be configured to sweep subnets for devices – which means they'll very rapidly make connections to dozens of ports for every IP in the subnet (whether it is in use or not). This could overwhelm a firewall or NAT appliance between the scanner and the device

Vulnerability Scanning Gotchas

- Cloud/Hosted Services
  - Don’t run vulnerability scans against infrastructure you don’t have permission for!
  - The best practice is to have contractual agreements that the provider is properly handling cybersecurity, including having a vulnerability management program

- Align your scanning interval with your remediation and reporting intervals

Vulnerability Prioritization

Your goal is to have a realistic risk based prioritization of vulnerabilities

Vulnerability Prioritization

- How to evaluate the severity of a vulnerability
  - ‘Common Vulnerability Scoring System’ (CVSS). Standard rating from 1-10, 10 being the most severe. Widely used, but understand it is measuring impact not risk
  - Commercial vulnerability scanning solutions often have a proprietary system to try to better evaluate risk than CVSS
  - CISA publishes a catalog of ‘Known Exploited Vulnerabilities’ that they have seen in the wild. Anything on this list should be considered high priority. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Vulnerability Prioritization

- Other factors that influence priority
  - Importance of the system and data
    - *Example*: An Active Directory Domain Controller is higher priority than the average staff members desktop
  - Other mitigations in place
    - *Example*: A system on a private network is lower risk than one exposed to the internet
- Vulnerabilities due to misconfiguration will inherently vary based on the situation

Policy and Process

As we discussed at the very beginning, cybersecurity is really about policy and processes. As you've seen many factors go into vulnerability prioritization, so you need to define your priorities as part of your vulnerability management process.

You need to define your process as part of an overall Vulnerability Management policy.

Vulnerability Management Policy

- Who is responsible for vulnerability identification
  - *Examples*: Security group or Central IT team
- Who is responsible for remediation
  - *Examples*: Central IT group or the individual unit system administrator
- Consequences for not following the policy
  - *Example*: Device will be disconnected from the network until issue is addressed

Vulnerability Management Policy

- Timeline for addressing vulnerabilities based on the prioritization
  - *Example*:
    - A known exploited vulnerability exposed to the world must be addressed immediately, if its only exposed to internal campus network, it must be done in 7 days
    - CVSS critical vulnerabilities must be addressed within 30 days
    - CVSS high and medium vulnerabilities must be addressed within 90 days
    - Other vulnerabilities must be addressed as time allows
- Have a process for requiring patches to happen faster if there is an immediate threat.

Vulnerability Management Policy

- Exception process when the timeline can't be met
- Exception process should require
  - The reason the system isn't being patched
  - What is going to be done to protect the system instead of patching (compensating controls). This could be network isolation, increased monitoring, or accepting the risk.
  - When will the exception be re-reviewed?
  - Who gets to decide to grant the exception? (hint – it shouldn't be the system administrator)

Socializing the Policy

- It's critical to have backing of administration
- Communicate the policy to the campus community
  - Establish a common understanding of goals and expectations
  - System owners may be reluctant to implement
    - Be willing to talk and answer questions with concerned stakeholders
  - Patching is a fundamental part of running a system
    - The vulnerability management processes help make this easier

Remediation - Patch Management

Staying up to date on patching is one of the most important things you can do, yet is also is one the hardest.

But how can this be? It sounds easy right? Just run updates all the time. How is this hard?

Why Patching Doesn't Happen

- Reluctance to patch
  - Staff are overworked and don't have time
  - Nobody is confident enough to make changes to the system
  - Concern that the patch will break something
  - The downtime needed is unacceptable – either patching takes a long time, or new patches get issued too frequently

Why Patching Doesn't Happen

- You'll find that you can't patch
  - Support contract lapsed
  - System has gone end of life
  - Vendor takes a long time to issue patches
  - Vendor doesn't treat security seriously

Patching Solutions

Many of these problems IT can't solve alone. You need to have partnership with the other stakeholders of the process.

- Shared understanding of the importance of patch management
- Identify who is responsible for patching systems
- Plan for software end of life well in advance
- Have patch testing process and scheduled downtime to address service availability concerns
- Have agreed on policies or standards for patch management
- Choose vendors that care about cybersecurity

Patch Management Tips

- Patches can be disruptive (i.e. reboot the system), communicate timelines to end users and customers
  - Some vendors have cadences for updates – example Microsoft OS security patches come out on the 2nd Tuesday of the month
  - Have scheduled downtime for servers
  - When a patch requires it, reboot immediately after install (waiting can leave the system in an insecure or unstable state)

Patch Management Tips

- Best practice is to test before deploying to critical systems
  - Research online if anyone else is having problems
  - Know how to roll back patches if there is a problem
  - Consider a process of rolling out patches in phases

Phased Patch Rollout Example

- Have a group of test systems that get the patches immediately
  - Development systems and systems used by IT are good choices
- A week later, deploy to the bulk of your systems
- After two weeks, deploy to the most fragile systems

- This way you identify issues early and are not dealing with everything at once
- Make sure you're still hitting on the agreed upon timelines in your policy

Patch Management Tools

Its not feasible to patch a large number of systems by hand. You want a tool that will schedule patch download and installation across all your systems.

Examples of commercial tools: Microsoft InTune, Patch My PC, JAMF, RedHat Satellite

Examples of free tools: WSUS, Group Policy controls, ansible/powershell scripts

Patch Management Tools

- You need to get data out of your patch management tool
  - What new patches are available
  - What systems have and which ones are missing a patch
  - Systems that have failed installing a patch
  - Systems that have stopped checking in
  - Free solutions are often lacking on the reporting side so you'll have to roll your own
- Tools tend to be operating system specific; you may need more than one

Reporting

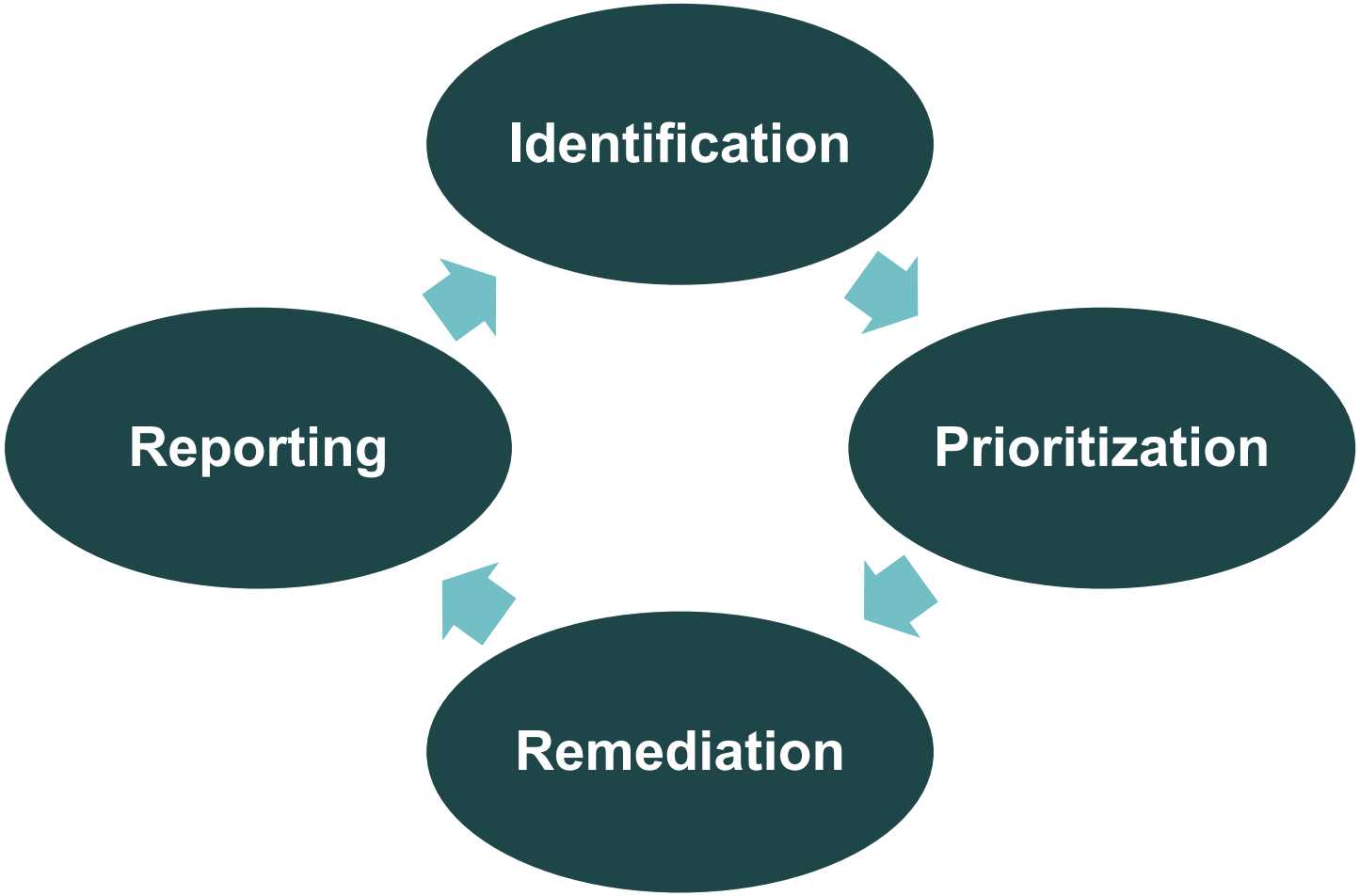
We already covered that your vulnerability scanning and patch management solutions need robust reporting capabilities.

The reporting phase of the vulnerability management cycle is where you use this data assess the state.

- You need metrics to determine if progress is being made – are the vulnerabilities being addressed (via patching or an exception)?
- You can’t enforce your policy without data

Vulnerability Management Cycle

New vulnerabilities are discovered daily. This cycle is continuous, and asynchronous - systems will be at different phases of remediation based on the prioritization



Summary

- Vulnerability management needs to involve more than IT
- Write a policy for your vulnerability management program, including timelines and who is responsible for which decisions and tasks. Have an exception process defined.
- Have a good inventory your systems/networks. Prioritize inventory of critical systems and ones with high value data
- Use a vulnerability scanning tool and be aware of its limitations
- Use a patch management tool to remediate vulnerabilities in line with your policy

Links

- CISA Cyber Hygiene Vulnerability Scanning Service (US only)- https://www.cisa.gov/cyber-hygiene-services
- CISA KEV Catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA maintains a big list of free or open source security resources: https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
- CVSS Information - https://www.first.org/cvss/
- Microsoft Windows Server Update Services - https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Links

- ShadowServer Foundation Reports – https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
- Shodan Free Academic License - https://help.shodan.io/the-basics/academic-upgrade

Questions/Discussion?