Vulnerability Management

University of Northern Colorado

Matt Langford
CHECO Spring 2019
2019/04/24

UNC

When I started

In the beginning

System owners are doing a reasonable job of taking care of their systems.

Most systems are getting updated regularly but no one is tracking it.

Vulnerability scanning is taking place and reports are being given to the system owners for resolution.

Issues

Assessing risk in the environment was a matter of opinion

Some owners are better at managing the systems than others.

Source of ownership was not being regularly updated and the definition of who owns the system is still under discussion.

Some systems and applications hadn't been updated in a long time. Some owners knew this, and others did not know they owned and were responsible for the system.

Some owners had a sense of the risk, but many were not aware, rarely was their management aware.

Vulnerability scan results are infrequently acted upon and are not being tracked.

No numbers available to provide a narrative regarding risk.

Vulnerability Management Program evolution

What was tried

- Better defining system owners
- Creating a committee (VMC)
- Better rating and identifying the servers
- Intrusive, insistent follow ups
- Copying managers
- Showing up in person
- Additional resources

Mixed results

Some of these items created partial victories but most failed because we hadn't made significant progress in gaining management support. The owners would bring forth edge cases or complain about an issue with the program. This would often derail any support and table the conversation for another day.

Vulnerability Management Program

Component Pieces

- Server authorization
- Systems updates
- Scanning for vulnerabilities
- Vulnerability inventory
- VMC (Vulnerability Management Committee)
- VMF (Vulnerability Management Form)
- RMI (Risk Management Inventory)
- Mitigating vulnerabilities
- Network Defense Team
- Firewall reviews
- Server de-authorization process

Tools

SCCM

System Center Configuration Manager is what we use to push packages out to our Windows workstations and servers.

Jamf

??? Apple Management Framework is what we use to push packages to our Apple workstation environment.

Ansible

Is what we use to schedule updates for our Linux servers.

Scanning

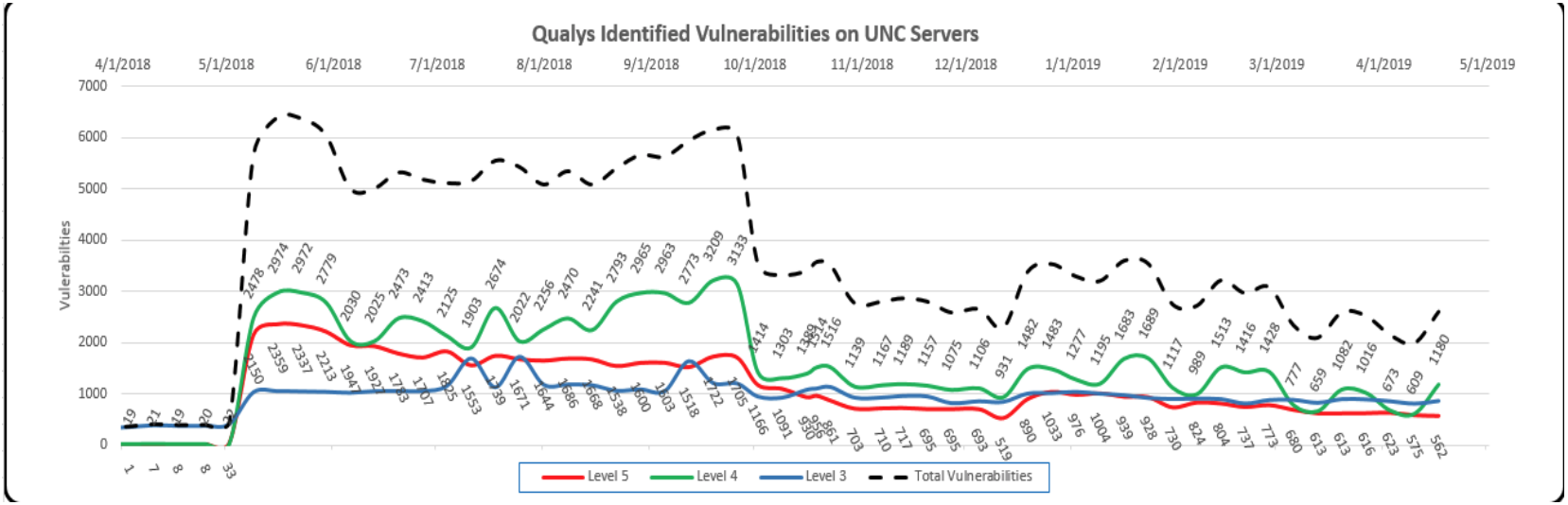
Qualys Scanner

Used for our server environment and our administrative machines. 512 systems for less than $7,500 including our PCI scan and verification.

Authenticated Scans (FTW)

Authenticated Windows, Linux and Data Base scans. False positives fall significantly and much fewer "potential" vulnerabililties.

Vulnerability Table



Winning strategies

Visibility

Get the information in front of the department heads (Directors) and other IM&T leadership. Build support with the management or at least a tolerance to spend resources on this work.

Patience

It is not going to be taken care of tomorrow. Take your time, build support, make friends, identify the people that can have the most impact.

Collaboration is key

Security does not typically have the staff, authority, or visibility into the environment to do it alone. We have had great success in dedicated working meetings.

Management of Risks

Other vulnerability management tools and techniques

- Administrative workstations (geek boxes)
- VPN
- Multi-factor authentication
- Network segmentation
- Conditional access rules (new)
- Permissions
- End Point Protection
  - Windows - SCEP, Defender, MSEPP, ???
  - Mac – SCEP now ESET
  - Linux – ESET
- O365 DLP (SharePoint, OneDrive, Email)
- UTM / NGF (FortiGate)
- Regular Firewall Reviews
- End user's awareness and education
- Separation of duties
- Policies, Procedures, Guidelines
- CIRT
- Backups and DR planning
- For CISOs set up a reoccurring search for last minute flights to Aruba

THANK YOU!

Matt Langford
CHECO Spring 2019
2019/04/24

UNC