QUALYS®

Vulnerability Management Programs & The Lessons Learned

Bill Olson, Director Vulnerability Management (SME)
Amol Sarwate, Director of Engineering

Intro and Agenda

- **Who I am**
- **17 Years In IT**
- **9 Years with a NJ consultancy**
- **8th Year with Qualys**
- **Last 18 months as the SME**
- **Listen, Learn, Collect Feedback**

Lessons Learned

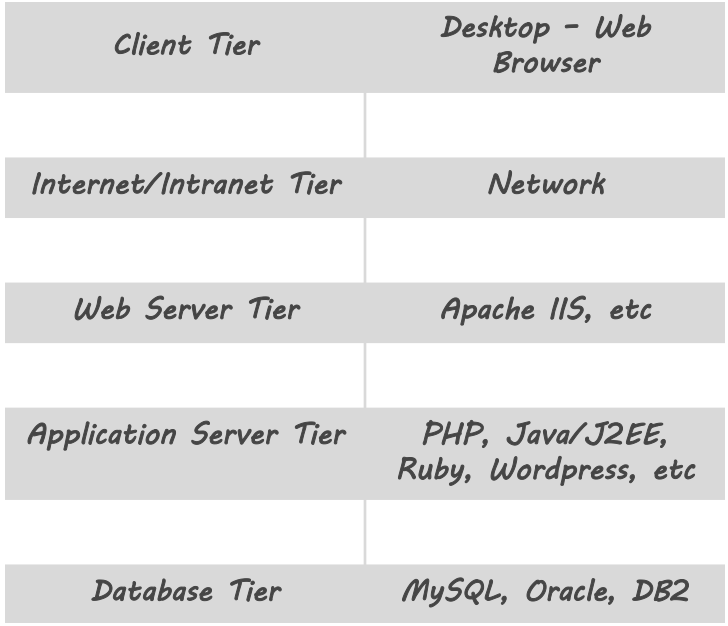
- **What does not work and why**
- **What does work**
- **War Stories**

Definitions

What is a vulnerability?

System and Applications not patched for known security flaws

- Hardware
- Operating System
- Application
- Database
- Network Equipment



Browser and Plugins

- Not up to date
- Not patched for known security flaw

Applications and Operating System not Configured for Secure Standards

- Never configured
- Configuration Changed

Web Applications and Web Services

- With known security issues
- Incorrectly Code
- Not patched for known security flaws

Why Should Anyone Care?

What is the difference between

Vulnerability Assessment & Vulnerability Management?

Vulnerability Assessment

- **Often simply only a scanning program**
- **Hard to measure success long-term**
  - Is it checking patch levels?
  - Is it lowering risk overall?
  - What processes are working?
  - Where is it not working in the organization?
  - Are you compliant?
- **Generally too much data as it lacks context**
- **Point in time only**

Vulnerability Management

- **Accountability**
- **Not just about vulnerability scanning**
  - A process to find, rate, remediate, track, progress
  - Should be about context, context and more context
- **Need to build a program that allows for the following**
  - Meeting compliance or regulator goals
  - Defined success factors
  - Measurable
  - Repeatable
  - Involved with other programs, patch management, ticketing, asset management, configuration management

Lesson #0
Vulnerability Management

Clients are scanning because they know they should be scanning, but there is a problem…

What is the goal of your VM program?

- Risk Management
- Threat Management
- Security Intelligence
- Security Patch Auditing

All of the above!

Lesson #1
What Makes VM Programs Fail

- **Bad Data**
  - (false positives, etc)
- **Data without relevancy or context**
  - What does this mean to the organization
  - What does this mean to the people reading the data (more on this shortly)
- **Data that is not timely**
  - Scanning more frequently is a good idea
  - Reporting with periodicity

Lesson #2
Why Patching Doesn't Happen

- **Can not find the owner**
  - Who owns the asset
  - Who owns the OS
  - Who owns the application
- **Can not be patched**
  - It will break something
  - Out of support
  - Can not afford the downtime
- **Something is broken**
  - People
  - Process
  - Technology

Lesson #3
What makes a program work

- People
- Process
- Security
- Politics

Vulnerability Management

People

- **What do they do?**
  - Ops
  - Security
  - Admins
- **What is important to them?**
  - Uptime
  - Looking good in their group
  - Looking good in the organization
- **Their Place in the organization**
  - Management / Team lead
  - Director
  - CIO
  - CISO
  - Board of Directors

Vulnerability Management Process

- **How often do you scan?**
  - Weekly
  - Daily
  - Monthly
- **How often do you report?**
  - Weekly
  - Monthly
  - Quarterly
- **What is it that is being measured?**
  - Open Vulnerabilities
  - Closed Vulnerabilities
  - Overdue Vulnerabilities
- **How do you prioritize patches?**
  - High risk
  - Low risk
- **When do you patch?**
  - Windows monthly
  - Unix quarterly
- **How do you classify assets?**
  - By Business Application
  - By Business Unit

Vulnerability Management
Security

- **Are all vulnerabilities equal?**
- **How many vulnerabilities do you have?**
- **What is the context of each vulnerability?**
  - How to do classify assets?
  - Do you rank each vulnerability

How do you measure the Security in the organization?

- SLAs
- Open
- Closed
- Risk

Are you audited on Security?

- PCI
- SOX
- HIPAA
- ISM
- ISO
- COBIT
- etc

Vulnerability Management

Politics

- **You are not on your own**
  - A partner with IT Operations
  - Audit
  - Management
- **Respect people**
  - Empathy
  - This is not punitive – is about helping and improving

Reporting

- Get your counts as perfect as possible
- If you write it down – it must be true
- People will have hurt feelings
- Do not report on things that are not fixable
- Create reports that tell a story

Lesson #4
Think Different

Many clients are focused on the wrong things

- Trying to fix all the vulnerabilities they have
- Focusing only vulnerabilities without context
- Looking to match patching tools
- Measuring the wrong things (how many open)
- Not integrating into other systems

Change the paradigm

- Admit you can not fix them all
- Look for areas of weakness
- Perform Root Cause Analysis each of theses lessons

Lesson #5
Think Different

The goal of a

Vulnerability Management Program should be to get to a place where you only focus on

Only The Exceptions

QUALYS®

CONTINUOUS SECURITY

bolson@qualys.com
asarwate@qualys.com
Twitter: @amolsarwate

Thank You