ISSA Portland

Thank you for Coming!

Gold Sponsors:

OPTIV

tenable network security

netskope

Silver Sponsor:

FireEye SECURITY REIMAGINED

Upcoming Events

DATE	MEETING TYPE	TOPIC	LOCATION
Thursday, Dec 17	Chapter Meeting & Holiday Social	Privileged Account Management Presented by: CyberArk	XPO Logistics & McMenamins Pool & Tavern
Thursday, Jan 21	ISSA Chapter Symposium	Cloud Security	Nike
Thursday, Jan 28	Conference	Data Connectors: Portland Tech-Security Conference	Marriott Downtown Waterfront
Fri-Sat, Jan 29-30	InfoSec Training	CISSP Review Course Presented by ISACA	UTASC Tanasbourne

Other Announcements

Oregon Center for Cyber-Security OCC-SEC) at MT. HOOD COMMUNITY COLLEGE

- 2 Year Associates Degrees:
  - CyberSecurity and Networking: Database Development
  - CyberSecurity and Networking
- CPCC Certificate Programs:
  - Business Cyber Vulnerability Analyst
  - Network and Firewall Security Technician
  - Secure Network Technician
- Palo Alto Networks Academy
- CompTIA Certification
- Digital Forensics – ACE Certified Examiner Certificates

Contact:
Wayne Machuca, PhD
Wayne.machuca@mhcc.edu
503-491-7631

Today's Presentation:
Vulnerability Management Programs & Lessons Learned

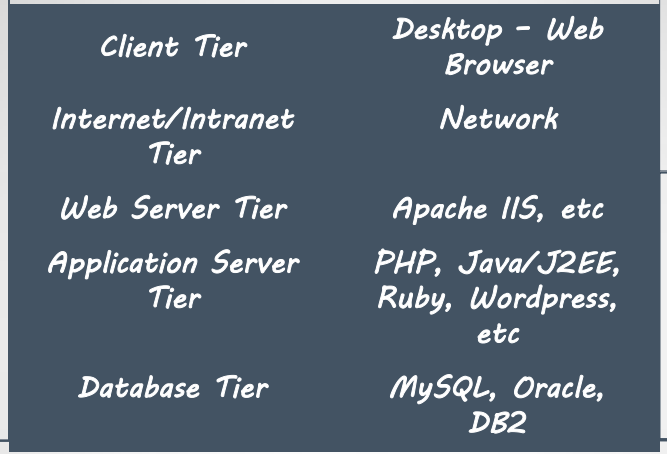
What goes on in the real world with Vulnerability Management programs and how you can construct a program that focuses on threat management, security intelligence, risk awareness and patch auditing.

Presented by: Bill Olson, Product Manager

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 OSs not Configured to Secure Standards

- Never configured
- Configuration Change

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

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 the data mean to the organization
- What does the data mean to the people reading the data (more on this later

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

Some is broken
- People
- Process
- Technology

Lesson #3
What makes Programs 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?

- Daily
- Weekly
- Monthly

How often do you report?

- Daily
- Weekly
- Monthly

What is being measured?

- Open Vulnerabilities
- Closed Vulnerabilities
- Overdue Vulnerabilities

How do you prioritize patches?

- High Risk
- High Severity
- Asset Criticality

When do you patch?

- By OS
- By Server
- By Workstation

How do you classify assets?

- By business Application
- By Business Unit

Vulnerability Management
Security

Are ALL vulnerabilities treated equally?

How many vulnerabilities do you have?

What is the context of each vulnerability?

- How do you classify assets?
- Do you manually rank vulnerability?**

How do you measure the Security in the organization?

- SLAs
- Open
- Closed
- Risk

Is your Security Audited?

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

Vulnerability Management
Politics

You are not alone
- Find a partner within IT Operations
- Audit
- Management

Respect People
- Empathy
- This should not be punitive
- It is about helping people
- It is about improving process

Reporting
- If you write it down it must be true
- Get your counts as perfect as possible
- Know people will have hurt feelings
- 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 **even more** Different

What is the goal of your program?

Some of the best programs are working towards one common goal

Focusing only on the

Exceptions

Discussion / Q & A

THANK YOU:
Bill Olson
bolson@tenable.com

Gold Sponsors:

Silver Sponsor: