How to construct a sustainable vulnerability management program

#whoami

-Howard Tsui

-Senior Threat and Vulnerability Management Engineer

-Financial industry in the United States

-Contact

- teaupdate12@gmail.com
- TSUIUST – twitter
- Howard Tsui – Linkedin

Talk Outline:

- Why do we need Vulnerability Management?
- What do we need?
- Vulnerability Management Lifecycle
- What won’t work?
- How to mature program?

Vulnerabilities- Are we vulnerable? Where?

1. OpenSSL 'Heartbleed
2. Shellshock
3. Stagefright
4. W32 conficker worm
5. MS17-010

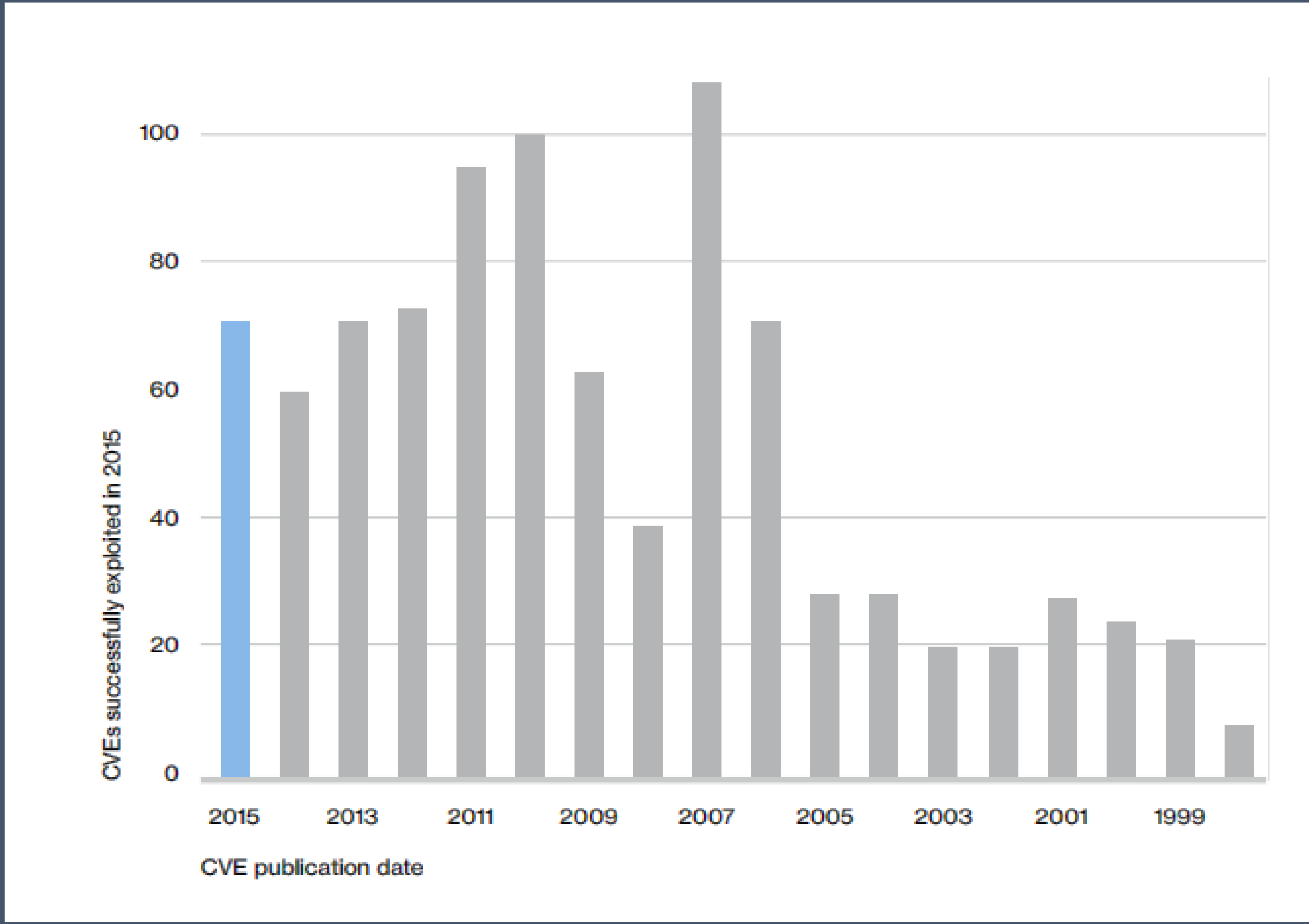
WPA2 Krack

External RDP port 3389

Apache 5

Windows 2003

Most of the breaches are not from 0 Days



Age of CVEs be exploited in 2015 sorted by publish date.

Citied Verizon 2016 DBRI

Why do we need Vulnerability Management?

- Vulnerability and threats

- Improve organizational security resiliency

- Compliance requirement

What do you need in Vulnerability Management?

Vulnerability scanner

Ticketing System

Asset Management (CMDB)

Be a people person

Vulnerability Management Lifecycle

Detect

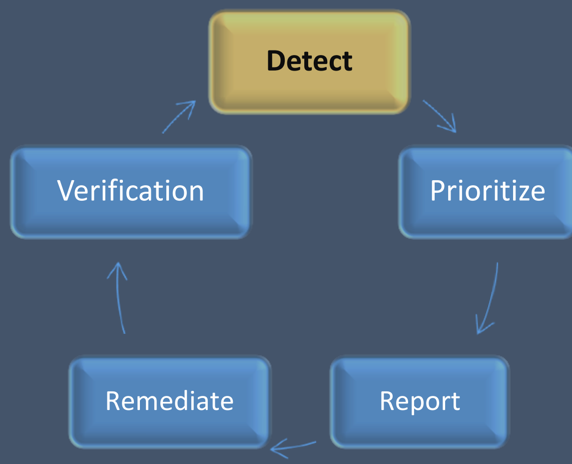
Prioritize

Report

Remediate

Verification

Detect – Vulnerability Scanning



Manual detection

Pro
- Accurate, less false positives
- Much more in depth

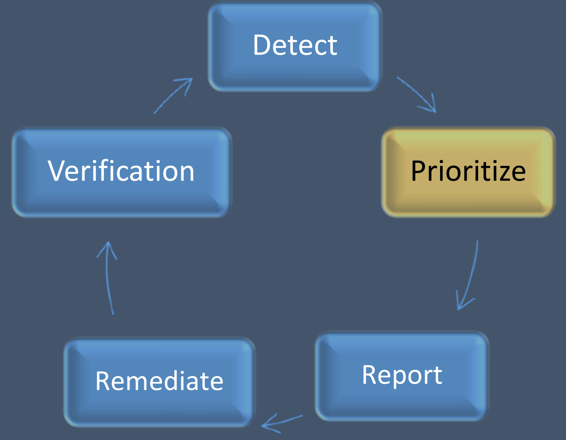
Con
- Time consuming
- Highly skilled

Automated detection

Pro
- Easy to use (Depends)
- Enterprise level scanning capability

Con
- False positive
- Expensive

Vulnerability Prioritization

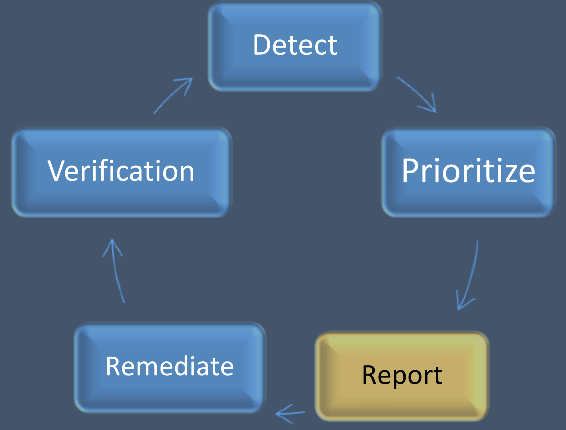


Always understand the vulnerability

- Prioritization
  - The money making software and server
  - Patch vulnerabilities that already have known exploits
  - Unsupported software
  - Look for the one solution that fix many vulnerabilities

- CVSS is a good start, but take them to the next level
  - Apply system scoring and criticality ratings. Etc, environmental factors

Report



- Target the audiences with the specific report type
  - There is no one report fits all
- Report automation and template
  - Integrate with current ticket and report process
- Always include SLA along with report
  - 14, 30, 60 days, etc.

What to include in the report or ticket?

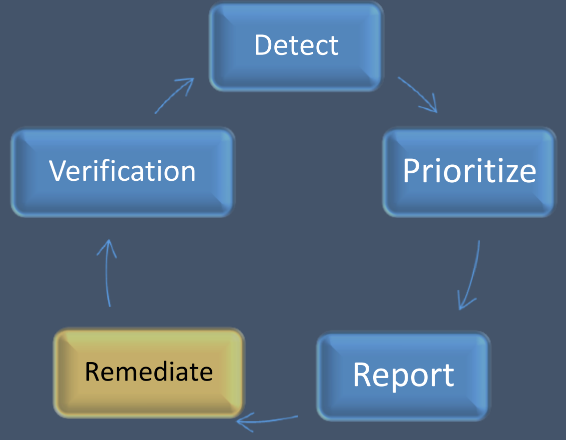
Dear Sysadmin:

<u>Title</u>: [Some kind of security identifier] [SLA] [vulnerability name]

<u>Body</u>: include <u>patch name</u> some where in the report
where was found, <u>IP, hostname, count. (excel is fine)</u>
Mention <u>SLA</u> again, nicely.

You don’t want this look

Remediation

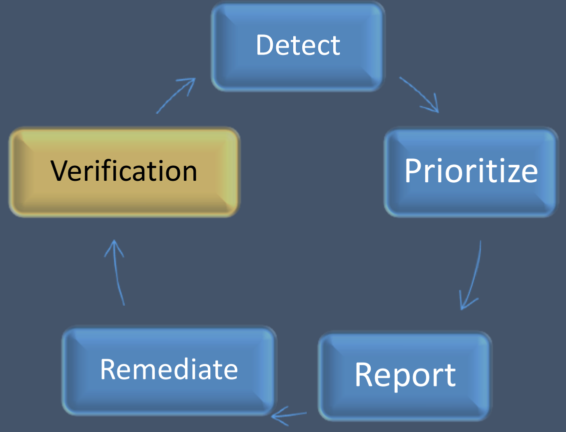


- If the current patching process works, **follow it**. Try not to reinvent new patch process, it will cause **confusion**

- Involve risk management depending on the outcome, initiate risk exception

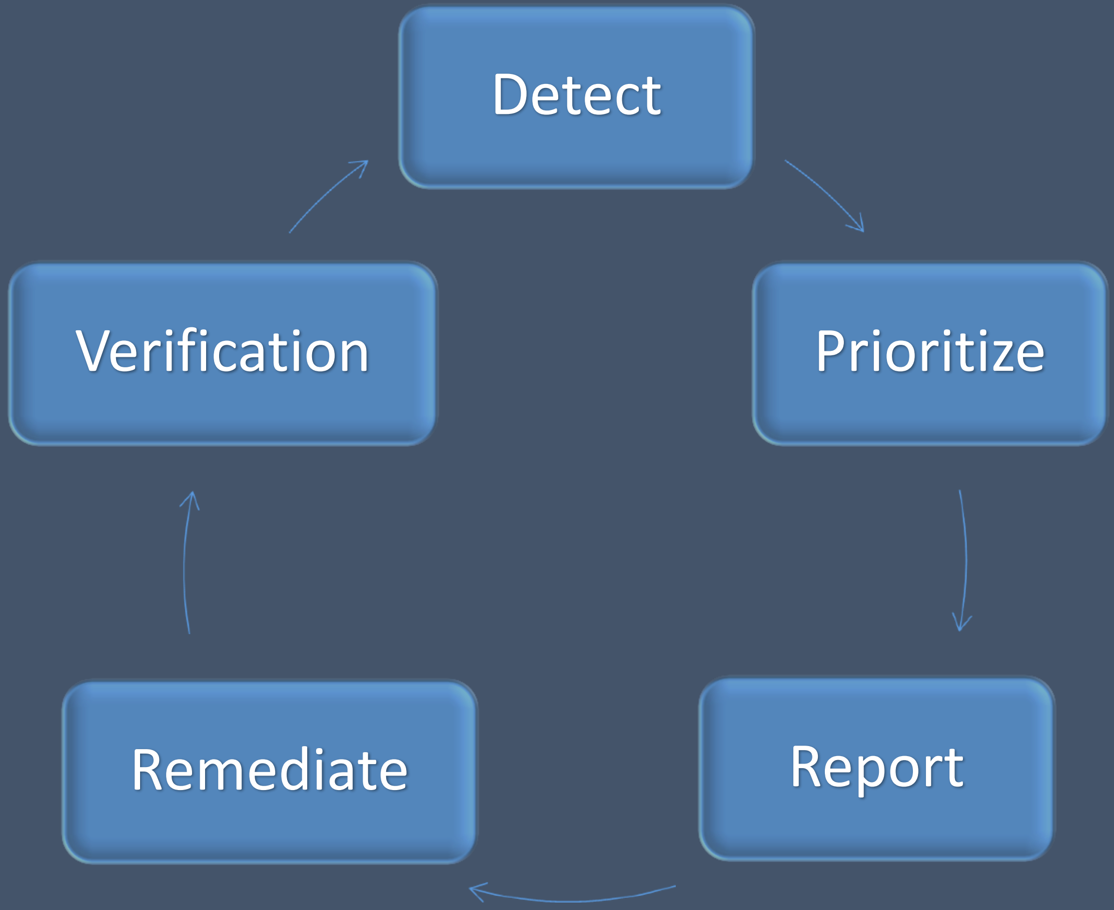
- Keep track of SLA and hold owners responsible. **Don't fall into the ticket black hole**

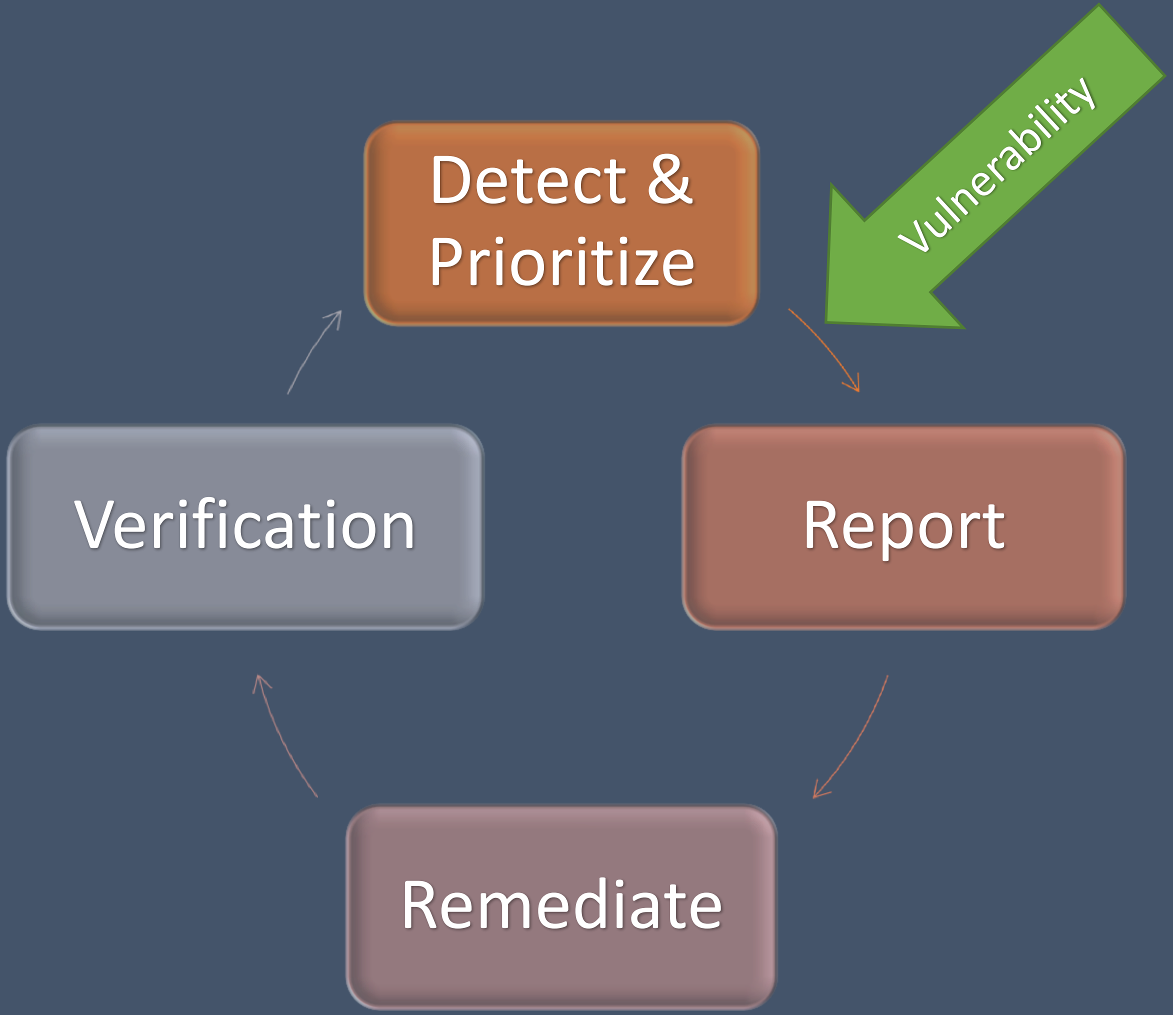
Verification



- Verify the same way you found it for accurate result
- Verify the remediation solution did not introduce more vulnerabilities
- Document the verification procedures and report in a central location… You will thank yourself later

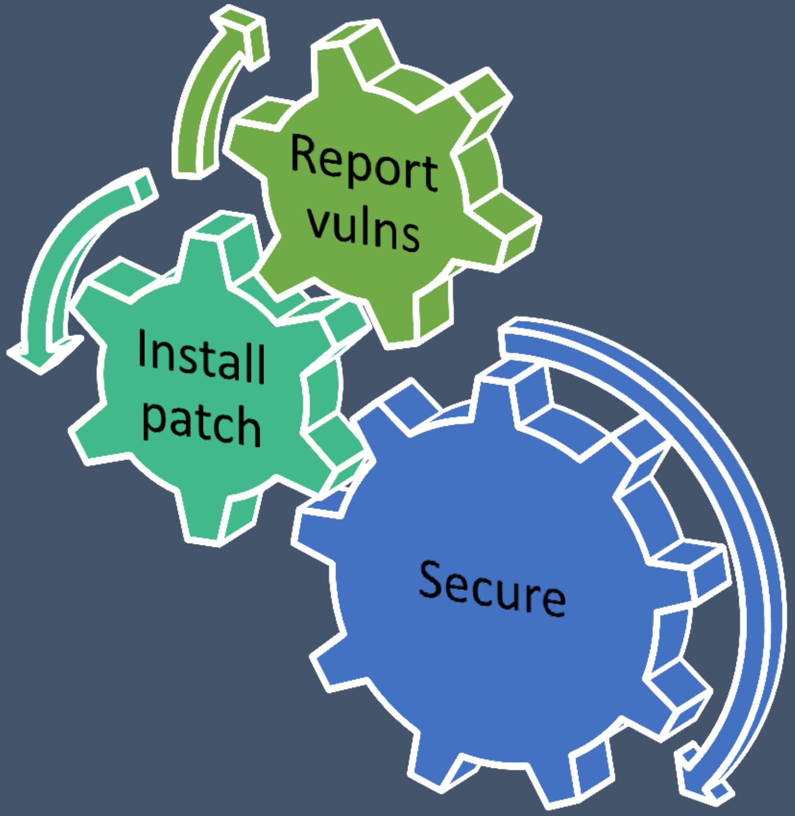
Mix & Match the Lifecycle





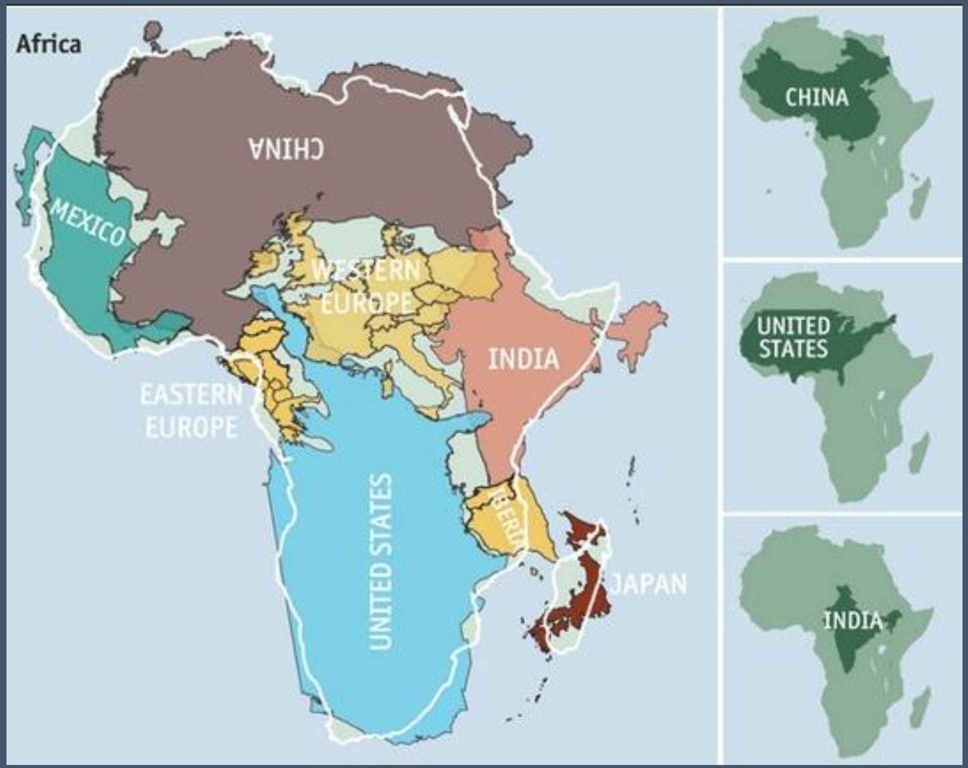
What won’t work

- Inaccurate vulnerability report or metrics
- No Cooperation with Risk Management
- Insufficient patch management program



What won’t work

Inaccurate vulnerability report or metrics

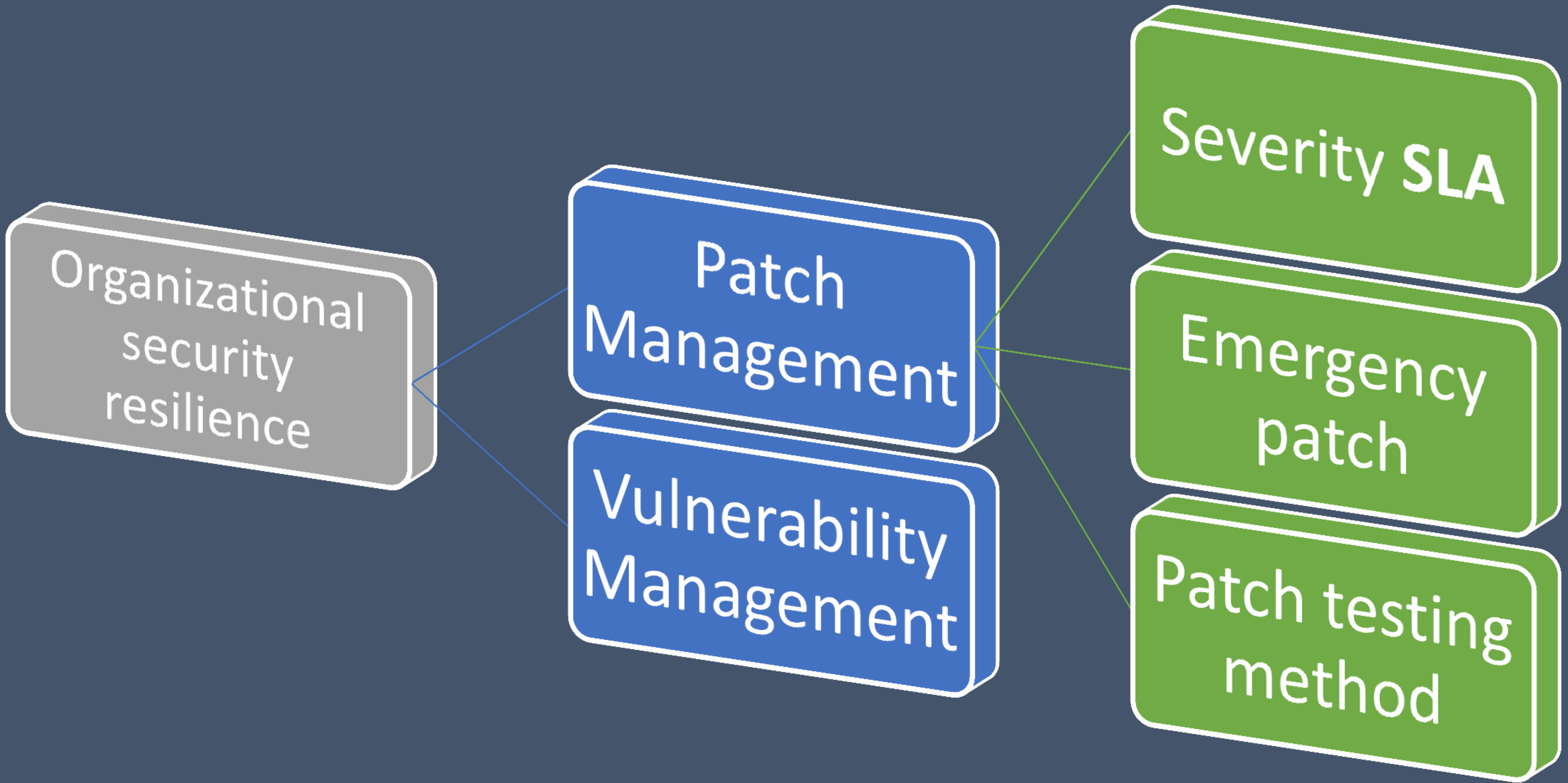


What won't work

Lack of team work with Risk Management

What won't work

Insufficient patch management program



I have everything, now what I can do?

- Security configuration management
- Incorporate threat intel feed for organization specific threat vulnerabilities
- Look for things that attacker likes to find that aren’t vulnerabilities
- Rely more on manual testing that can identify more complex vulnerabilities

To finish up, I want to leave you with this

The things we do to avoid vulnerability end up causing us more pain than vulnerability itself.

Q&A

Contact

teaupdate12@gmail.com

TSUIUST – twitter

Howard Tsui – Linkedin