Building an Effective Vulnerability Management Program

DAMIAN SOPHER
VULNERABILITY MANAGEMENT LEAD,
WESTINGHOUSE ELECTRIC COMPANY

Damian Sopher

VULNERABILITY MANAGEMENT LEAD WITH WESTINGHOUSE

14 YEARS IN INFORMATION TECHNOLOGY AND INFORMATION SECURITY

PARENT TO AN AMAZING 12YR OLD!

METALLICA FAN!

Vulnerability Management is…

"THE CYCLICAL PRACTICE OF IDENTIFYING, CLASSIFYING, REMEDIATING & MITIGATING VULNERABILITIES" - WIKIPEDIA

…in other words…

FIND IT.

PRIORITIZE IT.

REPORT IT.

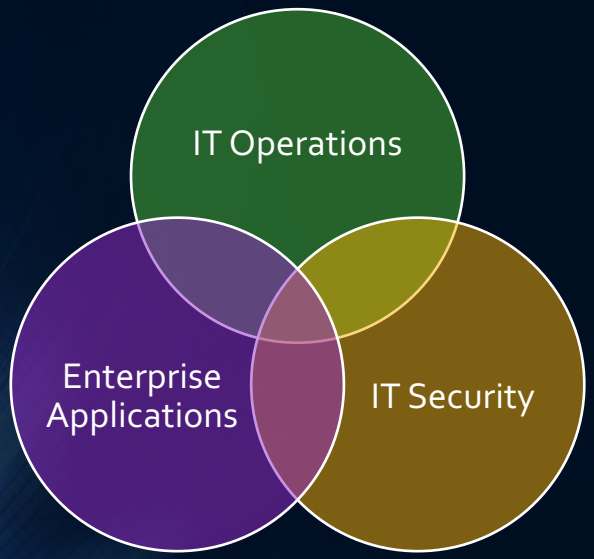
SQUASH IT.

REPEAT IT.

If you hear nothing else…

CENTERED AROUND COMMUNICATION

Core IT Relationships



KEY STAKEHOLDERS OF CHANGE IN THE IT ORGANIZATION

DEFINE EXPECTATIONS & GOALS

Vulnerability Management Lifecycle

Vulnerability Management Cycle: Discover

Discover

"WHAT VULNERABILITIES EXIST?"

"WHAT IS MY EXPOSURE?"

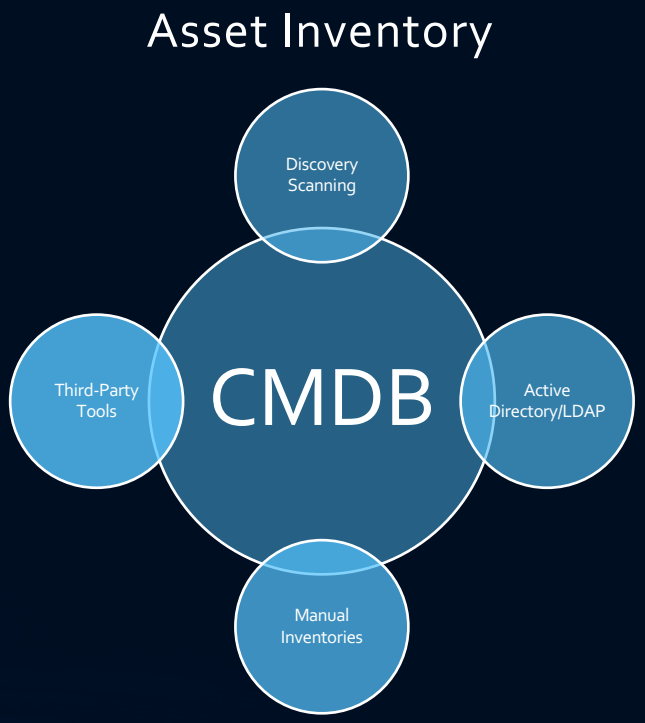
CONTINUOUS MONITORING

Discover

BUT WAIT… IS THIS EVERYTHING WE OWN?

NO REALLY… ARE YOU SURE?

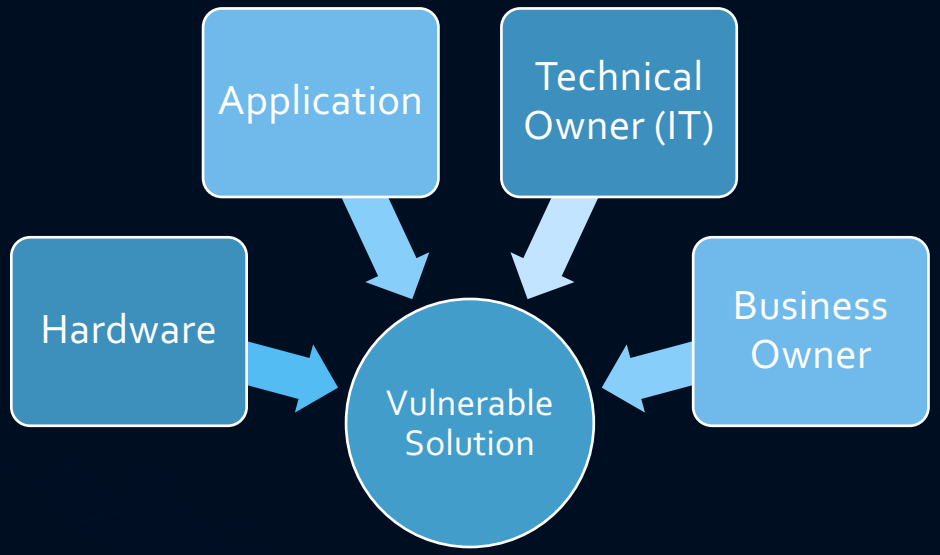
NOT JUST FOR HARDWARE, DON'T FORGET SOFTWARE



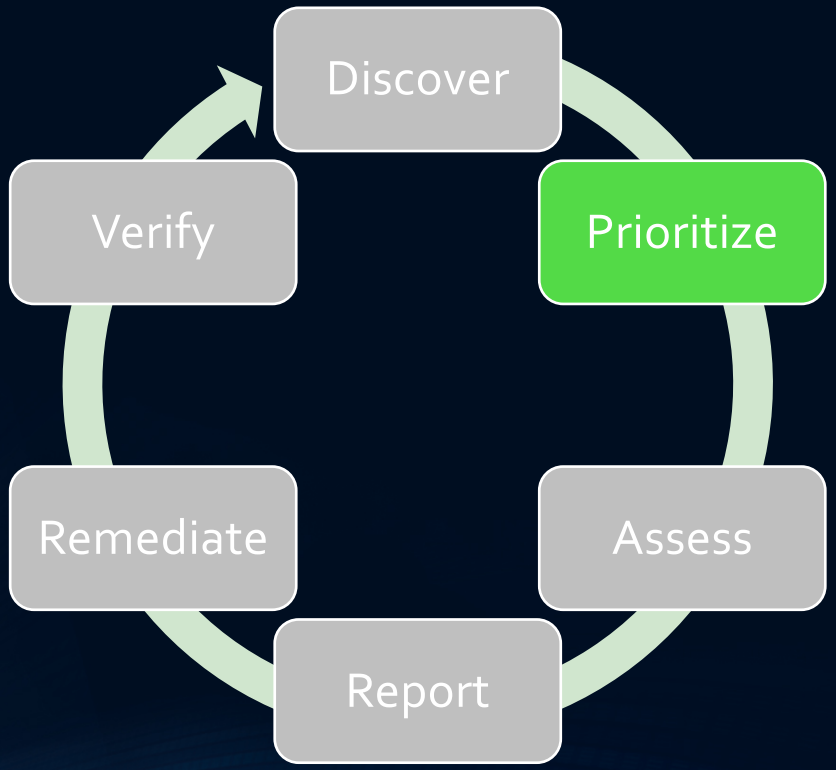
Discover

CONNECT KEY RELATIONSHIPS

DOCUMENT, DOCUMENT, DOCUMENT



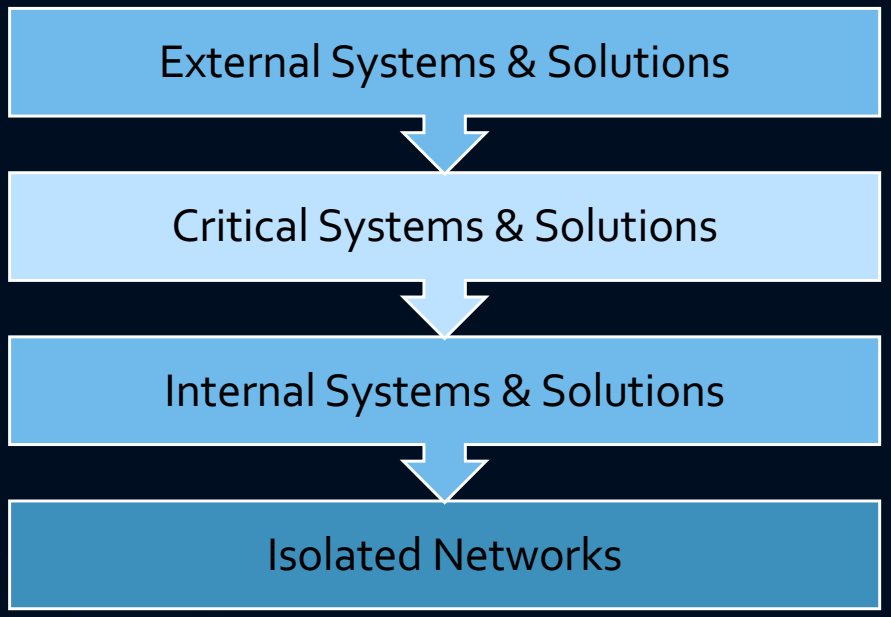
Vulnerability Management Cycle: Prioritize



Prioritize

WHAT SYSTEMS AND SOLUTIONS ARE THE MOST AT RISK

LOOK FROM THE OUTSIDE INWARD



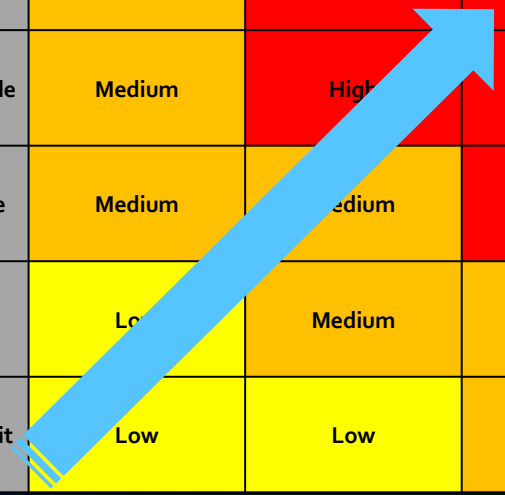
Prioritize

BREAK DOWN THE VULNERABILITY

ASSIGN A UNIVERSAL RISK SCORE

Vulnerability Risk Matrix

Severity / Difficulty	Moderate (1-3)	Severe (4-7)	Critical (8-10)
Novice Skill	Medium	High	High
Malware Kit or Metasploit Module Available	Medium	High	High
Exploit Available	Medium	Medium	High
Expert Skill	Low	Medium	Medium
No Known Exploit	Low	Low	Medium



Prioritize

TAKE THE RISK ASSIGNMENTS AND ASSIGN SLA

ALWAYS ESTABLISH EMERGENCY TIMELINES – I.E. AN ACTIVE ATTACK LEVERAGING AN EXPLOIT

Remediation Timeline

Vulnerability	Internet Facing	Critical Systems	Internal Only	Isolated Environments
Emergency	1 Day	5 Days	7 Days	7 Days
High	7 Days	14 Days	21 Days	35 Days
Medium	14 Days	21 Days	28 Days	42 Days
Low	21 Days	28 Days	35 Days	49 Days

Prioritize

IMPORTANT TO FOCUS ON AGED VULNERABILITIES

RISK CAN CHANGE OVERTIME AS NEW EXPLOITS ARE DEVELOPED

Vulnerability Age

Age by Severity	High	Medium	Low
0-29 Days	0	5	5
30-59 Days	10	3	25
60-90 Days	100	35	18
>90 Days	50	20	10

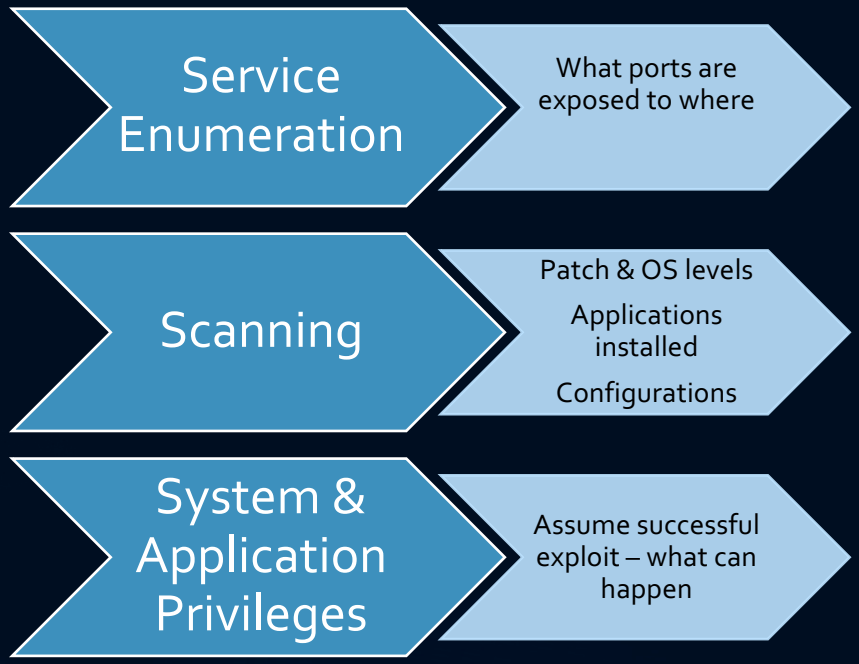
Vulnerability Management Cycle: Assess

Assess

REVIEW THE VULNERABILITY

IS THE SYSTEM OR APPLICATION IMPACTED?

ARE THERE MITIGATING CONTROLS?



Vulnerability Management Cycle: Report

Report

INFORM TECHNICAL TEAMS AND APPLICATION OWNERS

DEMONSTRATE RISK WHEN POSSIBLE

METRICS, METRICS, METRICS….

Key Metrics

TRENDS: OVERALL & KEY AREAS

VULNERABILITY AGE

EXTERNAL NETWORK PERIMETER

SYSTEMS WITH HIGH RISK

Vulnerability Management Cycle: Remediate

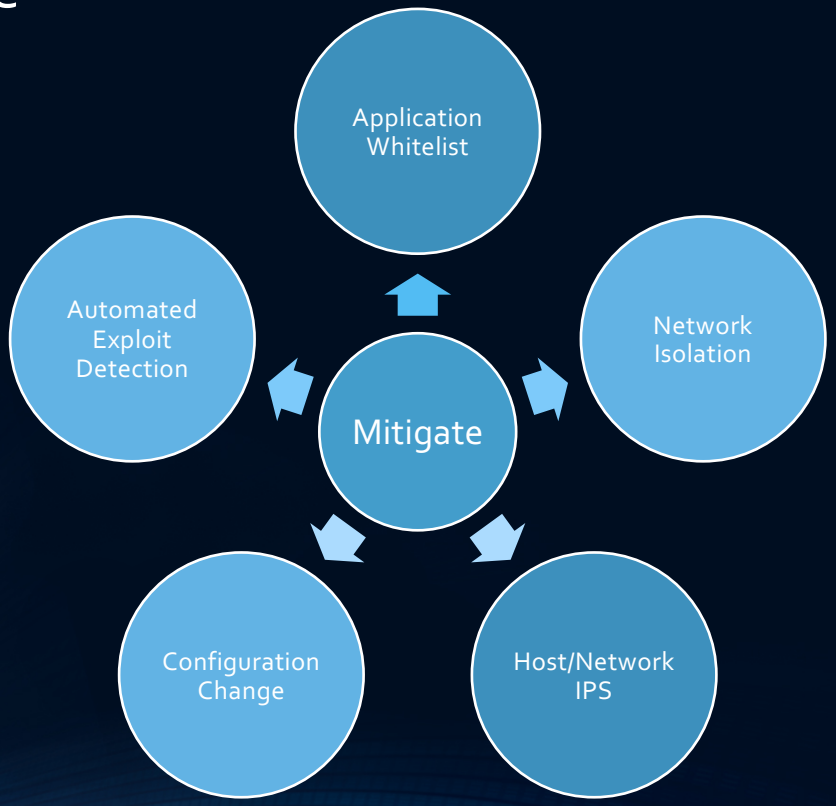
Remediate

PATCH: IS THERE AN UPDATE TO FIX THE ISSUE?

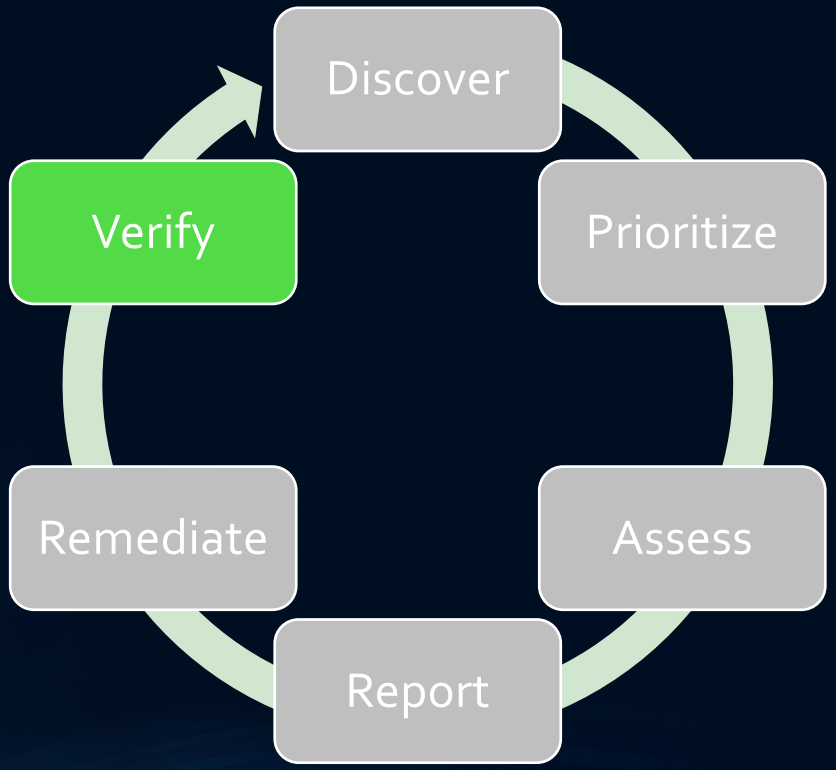
MITIGATE: CAN YOU CIRCUMVENT THE RISK?

DECOMMISSION: DO YOU NEED THE SYSTEM OR APPLICATION ANYMORE?

Remediate


Application Whitelist
Network Isolation
Host/Network IPS
Configuration Change
Automated Exploit Detection
Mitigate

Vulnerability Management Cycle: Verify



Verify

WAS THE REMEDIATION SUCCESSFUL?

WAS THERE ANY ISSUES DURING REMEDIATION?

TEST MITIGATIONS, VALIDATE ASSUMPTIONS

COMMUNICATE & REPORT

Now what?

Recap

- DISCOVER
  - Find new & existing vulnerabilities
  - Find new & existing systems & applications
- PRIORITIZE
  - Break down the risk
  - Ensure proper focus
- ASSESS
  - Verify risk to systems & applications
  - Determine necessary actions
- REPORT
  - Inform technical & application teams
  - Inform management
- REMEDIATE
  - Patch or mitigate vulnerability
  - Remove systems & applications
- VERIFY
  - Ensure remediation worked
  - Communicate success & issues

Last Minute Tips

BE A PART OF LIFECYCLE DISCUSSIONS

HELP DEFINE STANDARDS/BASELINES TO AVOID CONSISTENT INSECURE CONFIGURATIONS

PLAN TO RE-ASSESS YOUR PROGRAM ON AN ANNUAL BASIS. COMMUNICATE.

Thank you!

THANK YOU ALL FOR YOUR TIME!

MY INFO:

- Twitter: @Trask899
- Email: sopherd@outlook.com
- Website: Github.com/Trask899