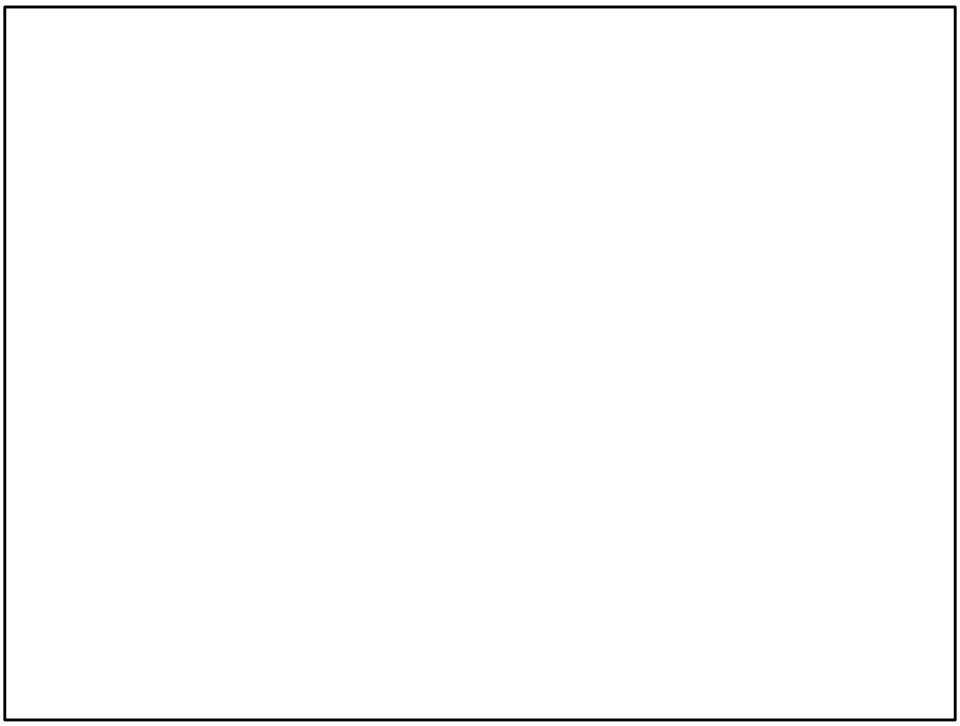

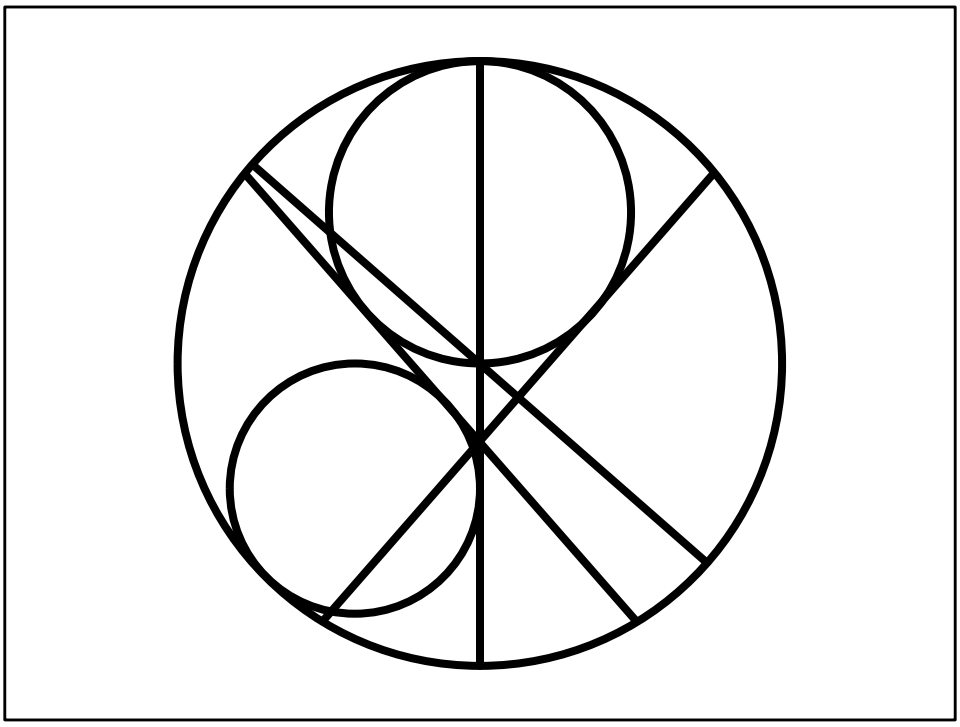

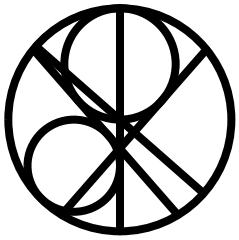

Building a Vulnerability Management Program

And growing it to Maturity

Who am I?

- Jacen Kohler
- UNT alumni, BS in in Computer Engineering
  - SrDesign Capstone: NASA IPv6 DHCP in Space
- Career:
  - Goldman Sachs: Summer Intern & FTE Cyber Security Analyst
  - Big4 Consulting: Sr Cyber Security Consultant
  - Critical Mfg: Vulnerability Management Program Lead
- Community:
  - Bsides DFW
  - Dallas Hackers Association
  - SouthWest CCDC Red Team

Overview

- What is Vulnerability Management
- Why you need a VM program
- Building support
- Design the program
- Implement the Program
- Mature the Program

What is Vulnerability Management

- Vulnerability: open to attack or damage
- VM: Continuous, proactive, and often automated process that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches
- What VM is NOT
  - Just the vulnerability scanner
  - Asset Management
  - Patch Program
  - Business Impact Analysis

https://www.merriam-webster.com/dictionary/vulnerability
https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management

Terms You'll Need to Know

- Common Vulnerability & Exposure (CVE)
- Common Vulnerability Scoring System (CVSS)
- Common Weakness Enumeration Specification (CWE)
- Common Platform Enumeration (CPE)
- Remediation
- Mitigation

https://cve.mitre.org/cve/
https://nvd.nist.gov/vuln-metrics/cvss
https://cwe.mitre.org/
https://cpe.mitre.org/about/

Why You Need a VM Program

- CISA Performance Goals
  - 1.E Mitigating Known Vulnerabilities
  - 2.W No Exploitable Services on the Internet
- NIST CSF
  - ID.RA-1: Asset vulnerabilities are identified and documented
  - PR.IP-12: A vulnerability management plan is developed and implemented
  - DE.CM-8: Vulnerability scans are performed
  - RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
  - ID.RA-6: Risk responses are identified and prioritized
  - RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources
- MITRE ATT&CK T1595.002

https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf
https://www.nist.gov/cyberframework/framework
https://attack.mitre.org/techniques/T1595/002/

Building Support

- Determine the program sponsor
- Identify your stakeholders
  - Who will be consuming your reports?
  - Who will be remediating your findings?
- Determine how a VM program could benefit them
- Secure funding

Design the Program

- Prerequisites
  - Asset Management
- Nice to haves
  - Threat Intel (Bring your own)

Design the Program

- Write the VM Policy
  - Remediation/Mitigation SLAs
  - Exception process
- Use Cases
- Service Catalog
- Requirements

Implement the Program

- Plan scan coverage based on network topology
- Network topology determines scan engine placement
- Deploy Agents to everything that can accept an agent
- Passive Scanners

Build Scans

- Agent vs Authenticated
- Device Type
- Network saturation
  - Scan after business hours?

Reporting

- Before and After patching
- By IT Team
- Leadership Reports

Metrics

- Broken SLAs
- Mean Time to Resolve
- Mean Time to Detect
- Break down by IT Team

Tooling Health

- Scan Coverage
- Authentication Success
- Missing Agents

Mature the Program

- Documentation
- Adjusted Risk Ratings
- Cloud integrations
- Websites/Apps
- IOT
- Configuration Management
- SAST/DAST/IAST
- Risk acceptance based on potential cost

Summary

- What is Vulnerability Management
- Why you need a VM program
- Building support
- Design the program
- Implement the Program
- Mature the Program

Resources

- Cyber Resiliency Review Supplemental Resource Guide Volume 4
- SANS SEC460: Enterprise and Cloud Threat and Vulnerability Assessment
- CISA Alerts & External Scan
- FBI's Domestic Security Alliance
- Vendor Research

https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf
https://www.sans.org/cyber-security-courses/enterprise-cloud-threat-vulnerability-assessment/
https://www.cisa.gov/news-events/cybersecurity-advisories
https://www.dsac.gov/

Questions?

- LinkedIn: LinkedIn.com/in/JacenRKohler
- Twitter: @JacenRKohler
- Mastodon: InfoSec.Exchange/@JacenRKohler
- GitHub.com/JacenRKohler/Presentations

https://www.linkedin.com/in/JacenRKohler/
https://twitter.com/JacenRKohler
https://infosec.exchange/@JacenRKohler
https://github.com/JacenRKohler/Presentations

Presented At:

- CISO SC / DFW SecCon 2 2023-March-28th

https://www.cisoxc.com/dfwseccon2-agenda

- test