Enterprise Vulnerability Management at Westat

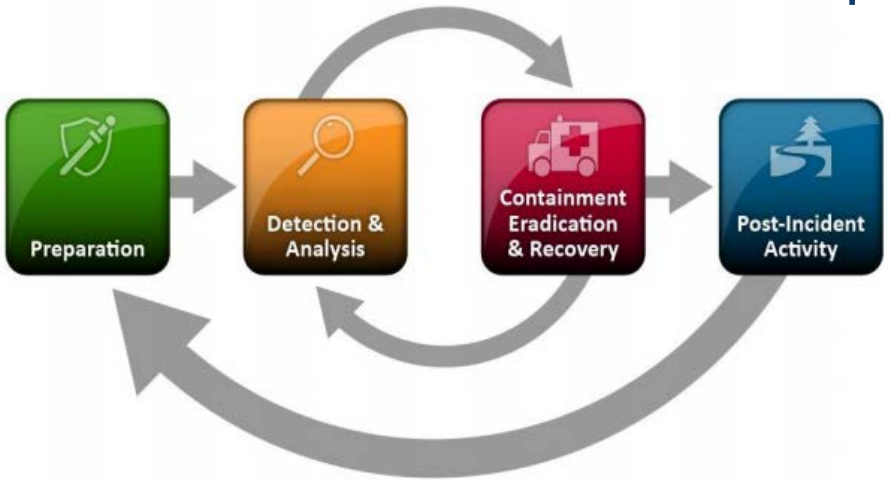
FedCASIC
March 2015
Dennis Pickett, CISSP
Westat

Introduction

- Who am I?
  - Dennis Pickett, Senior Manager of Information Security at Westat
- What will we be discussing?
  1. What is Vulnerability Management?
  2. Why is vulnerability management important?
  3. What activities are in a Vulnerability Management program?
  4. Westat's Vulnerability Management Program
  5. What do you do if a scan detects a possible breech?

What is Vulnerability Management?

- Cyclical process for identifying and remediating, or mitigating, vulnerabilities in the enterprise.
- It is critical for managing risks that could allow an attacker to compromise the confidentiality, integrity, and availability of an information system.
- Goal of preventing attackers from compromising information.
- Directly tied to Breech Detection and Incident Response.

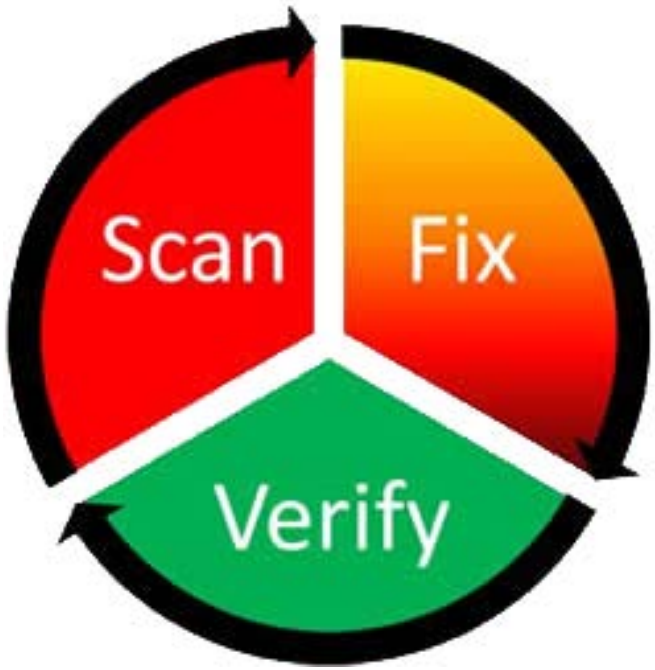


Why is vulnerability management important?

- Software and hardware is so vast and complex now that vulnerabilities are constantly being discovered, by both “good” and “bad” guys.
- Information technology (IT) is so dynamic that changes and updates are happening all the time. Often these can introduce new vulnerabilities.
- The threat landscape is increasingly concerning.
  - Attacks are more complex.
  - Attacks are more targeted.
  - “Consumerization” of attacks.
  - Breeches are more public.

What activities are in a Vulnerability Management program?

1. Inventory
2. Scan
   - Operating Systems
   - Major Components
   - Applications
3. Remediate
   - Patches
   - Code changes
   - Manual fixes
4. Verify and Monitor



Westat's Vulnerability Management Program

- Defense-in-depth approach, which means layers of detection.
- Process
  - Weekly system scans
  - Applications scanned before going live
  - Applications scanned if code change
  - Weekly patching
  - Log file reviews
  - Weekly meetings between security and system admins
- Tools
  - Juniper Intrusion Detection
  - Tenable Security Center – Nessus
  - IBM's AppScan
  - Trend Deep Security
  - Trend Deep Discovery for breech detection

What do you do if a scan detects a possible breech?

- Vulnerability management is a preventative activity.
- There may be a time where a scan identifies, or leads to discovery of a possible breech.
- High Level Steps:
  - Convene Incident Response Team
  - Containment
  - Investigation
  - Eradication
  - Recovery
  - Reporting

Questions?

Dennis Pickett, CISSP
Westat
Senior Manager of Information Security
301-251-8203
dennispickett@westat.com