OWASP
Open Web Application Security Project

Vulnerability Management

elizabeth.belousov@owasp.org

Vulnerability Management Outline

What skills would you need:

- Business Process Engineering
- Communication Skills
- Knowledge of Information Security

Seamlessly embed your Vulnerability Management program with other business processes in your organization in order to succeed

Before you Start

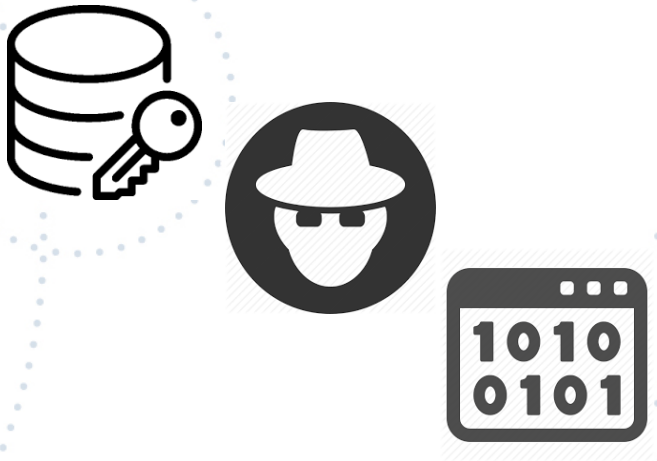
Questions to Answer:

- What is your security posture?
- What is your (applicable) framework?
- Do you know your assets?

Before you start your vulnerability management program:
What is your security posture-means what do you tell your customers?
What is your compliance framework?
Do you know your assets? You would be surprised! and that why you need vulnerability scans!

Threat Modeling Drawbacks

- Focus on Assets
- Focus on Attackers
- Focus on Software



Ransomware business strives on reactive approach to InfoSec. Threat modeling is a proactive measure that an organization can use early in the design.
“Focus on Assets” drawbacks: If you have a diverse set of assets, layer your defenses could be expensive.
“Focus on Attacker” drawbacks: chase “your tale”.
“Focus on Software” drawbacks: missing defense in depth

Threat Modeling

STRIDE

- S-Spoofing
- T-Tampering
- R-Repudiation
- I-Information disclosure
- D-Denial of Services
- E-Elevation of privileges

DREAD

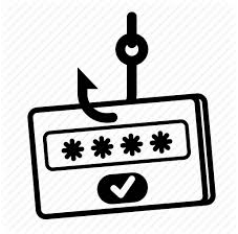
- Damage potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Frameworks

- ISO 27001
- NIST Special Publication 800-37
- OCTAVE-operationally critical threat, asset, and vulnerability evaluation
- FAIR- factor analysis of information risk
- TARA- threat agent risk assessment (TARA)

Vulnerability Management Checklist

- Map your assets
  - External IP scans by function, by location
  - Web Application (third party or own)
    - Dynamic scans
    - Static scans
- Select your tools
  - SCAP or ISO certified
  - Cloud infrastructure Auditing Capability
  - Internal Authenticated Scans
- Prepare Awareness Training
  - Change Management (patching)
  - Social Engineering
  - Phishing



Advisory and Patching

- Sign up for vendors updates
- Sign up for US-CERT
- Sign up for FTC scam alerts
- Employ task management system
- Ensure capacity/readiness to deploy patches

KPI

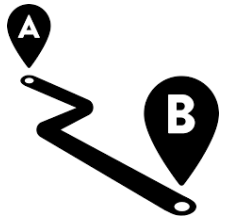
- What is your KPI?
- Does your management understand your KPI
- Severity: critical, high, medium, low
- Over what time: 30, 90, 180, 365 days
- How many Recurring vs. New
- Source of Threat

What is your metrics? If you can't measure you can't manage.
Does your management understand your KPI? How many critical and high vulnerabilities do you have ? Over what time 30 days, 90 days, 180 days a year? How many recurring vs. new vulnerabilities? Where are the threats are coming from? by functional areas of implementation? by area of technology? Revisit your internal procedures or policies.

How-to in glance:

- Create Consistent Vulnerability Scanning Process
- Announce it for ALL in your company
- Distribute Vulnerability Report to your management and responsible stakeholders
- Create Vulnerability Registry
- Create Vulnerability Work Instructions
- Enforce a deadline to fix
- Implement Exception Process
- Feed Auditing

What is Outcome?



- Incident Cost vs. Preventative Measures Cost
- Strategy for Layered Defense
- Gap Analysis
- Know Your Environment, Know Your Vulnerabilities
  - Inventory your assets—monthly
  - Train your resources —quarterly
  - Inventory your policies— yearly

Formalize

- Review and Repeat Policy Periodically
- Update Threat Modeling
- Maintain Risk Matrix
- Improve Change Management
- Provide a Baseline for Audit

OWASP
Open Web Application Security Project

Questions

elizabeth.belousov@owasp.org

When reusing this material please cite
OWASP Vulnerability Management Project
https://owasp.org/www-project-vulnerability-management-guide/