# Vulnerability management

## *Introduction & discussion*

Daniel Schatz

2014-10-07

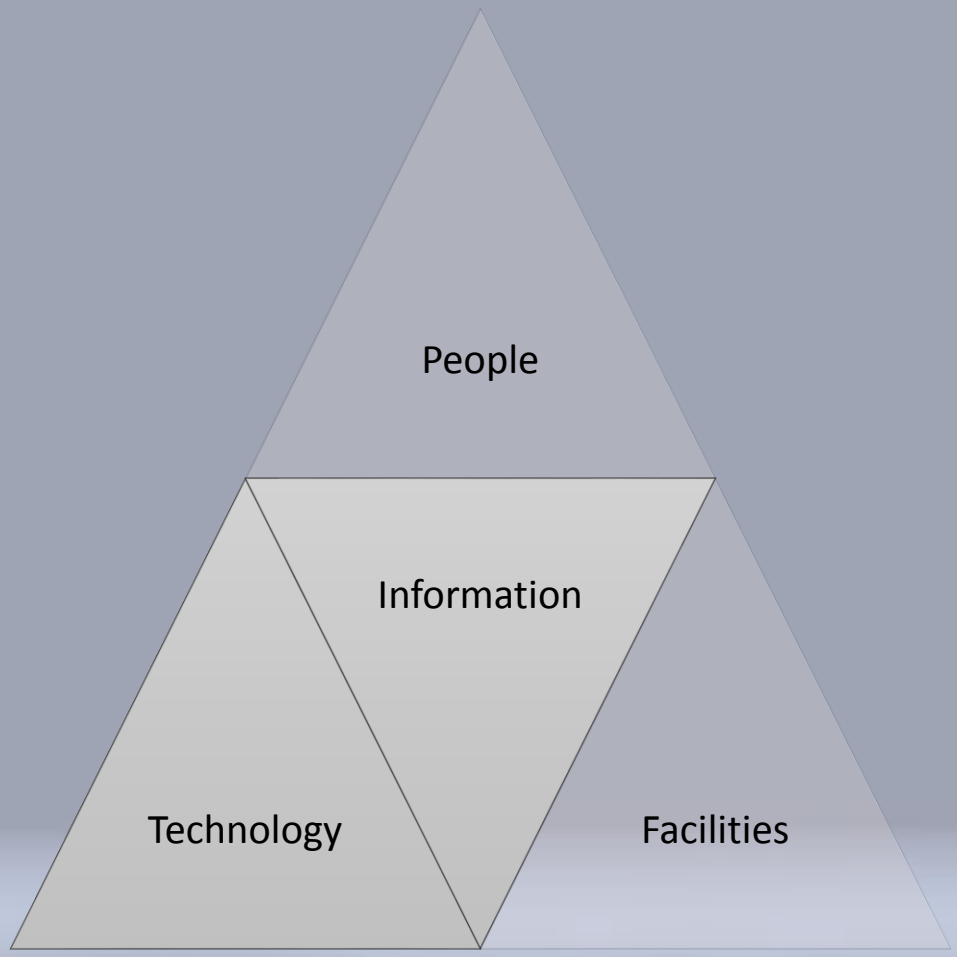
# About:

- What is Vulnerability Management about (Focus: VA)
- What are some key points of a VM program
- How to implement a VM program
- Tools
- Challenges

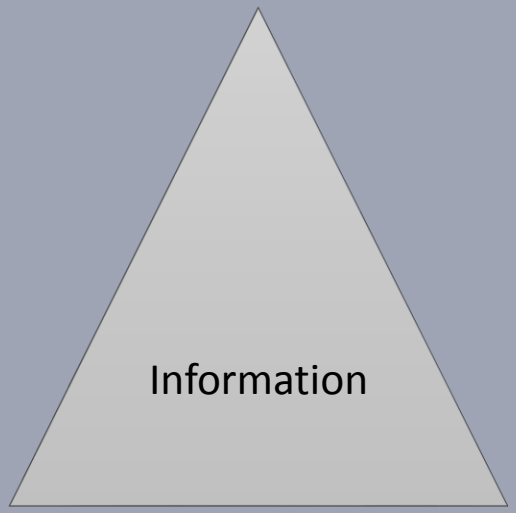
# Vulnerability Management

- In a nutshell –
  - what are my assets
  - what weakness do they have
  - what is their exposure
  - who is likely to exploit them
  - why would they do this
  - How do I handle it

# Assets?

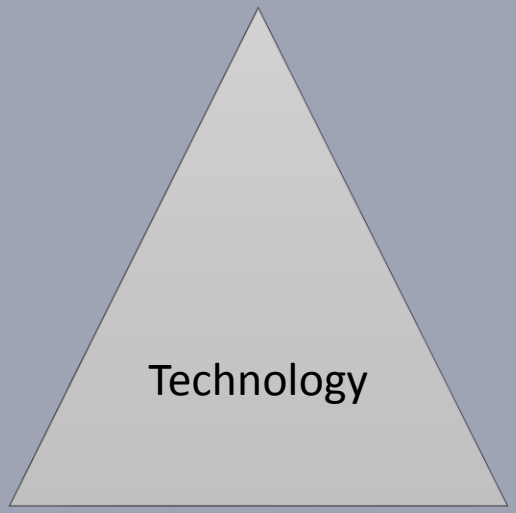


# Assets?




- Customer data
- Business processes
- Business strategy
- Financial data
- Research data
- Employee data
- Brand
- …

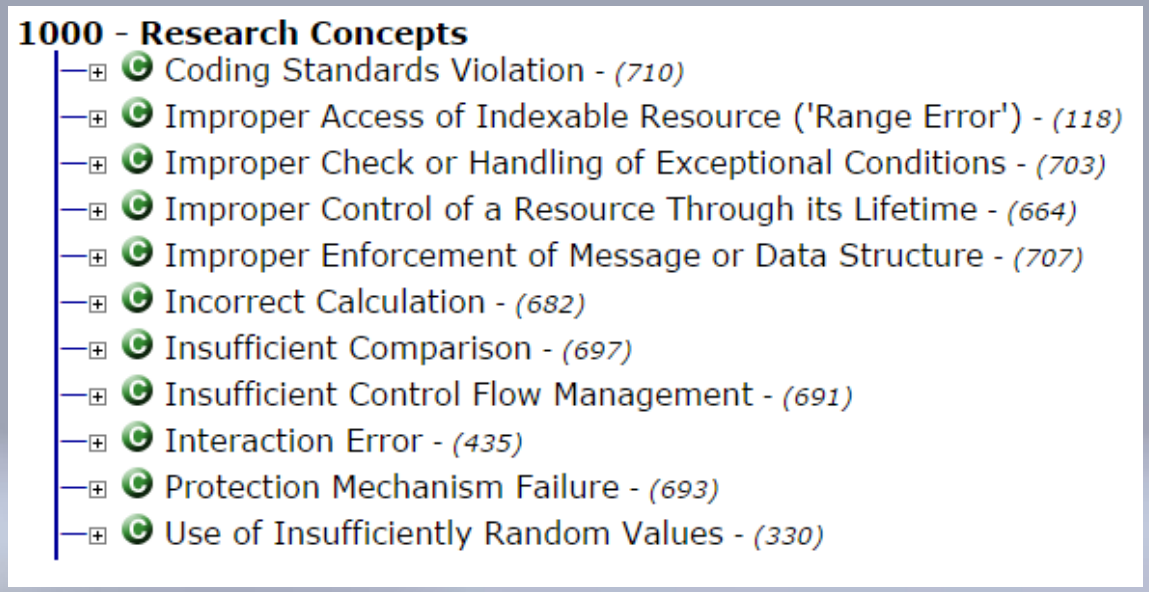
# Assets?




- Servers
- Desktop/Laptops
- Tablets/Smartphone
- Software
- Router/Switch
- Mainframes
- POS
- PaaS/SaaS/IaaS
- …

# Weakness?

- A cause of (software) security vulnerabilities as they are found in code, design, or system architecture
- Common Weakness Enumeration (CWE) provides a framework to map weakness characteristics to vulnerabilities




http://cwe.mitre.org/

# Exposure?

**As defined by MITRE an "exposure" describes a state in a computing system that:**

- **allows an attacker to conduct information gathering activities**
- **allows an attacker to hide activities**
- **includes a capability that behaves as expected, but can be easily compromised**
- **is a primary point of entry that an attacker may attempt to use to gain access to the system or data**

**e.g. open access to your internal network range, weak controls for services, …**

# Side note - Common Vulnerabilities and Exposures

***CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."***

***Mitre.org***

**National Cyber Awareness System**

**Vulnerability Summary for CVE-2014-0160**

**Original release date:** 04/07/2014

**Last revised:** 07/24/2014

**Source:** US-CERT/NIST

## Overview

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

## Impact

**CVSS Severity (version 2.0):**

**CVSS v2 Base Score:** 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)

**Impact Subscore:** 2.9

**Exploitability Subscore:** 10.0

**CVSS Version 2 Metrics:**

**Access Vector:** Network exploitable

**Access Complexity:** Low

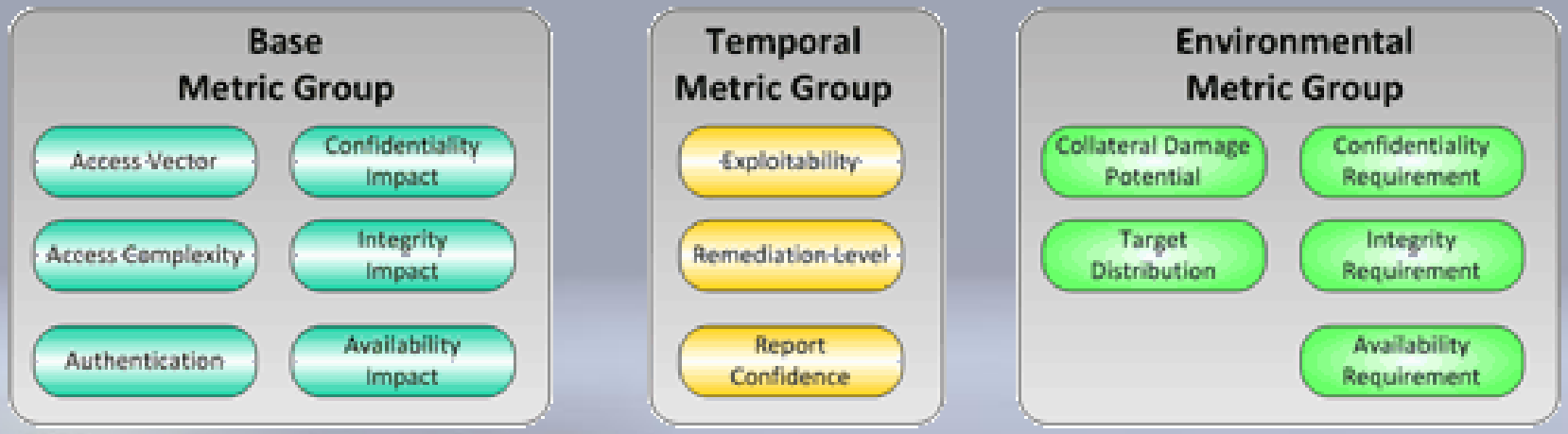
**Authentication:** Not required to exploit

**Impact Type:** Allows unauthorized disclosure of information

# Side note - CVSS

***"CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability."***

***FIRST.ORG***




*http://www.first.org/cvss/cvss-guide*

# Attacker / Threat agent?

**As detailed as necessary but usually categorized similar to this**

- **Unskilled**
- **Script Kiddies**
- **Hacker/Hacktivist**
- **Organized crime**
- **Nation state**

# Attacker / Threat agent?

| Threat Attributes | | Employee Reckless | Employee Untrained | Info Partner | Anarchist | Civil Activist | Competitor | Corrupt Official | Data Miner | Employee Disgruntled | Cyberwarrior | External Spy | Internal Spy | Irrational Individual | Leg Adve |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Non-hostile | | | Hostile | | | | | | | | | | |
| Initial Access | Internal | x | x | x | | | | | | x | | | x | | |
| | External | | | | x | x | x | x | x | | x | x | | x | |
| Trust Advantage | None | | | | x | x | x | x | x | | x | x | | x | |
| | Partial Trust | | | x | | | | | | | | | | | |
| | Employee | x | x | | | | | | | x | | | x | x | |
| | Administrator | | | | | | | | | | | | x | | |
| Motivation | Accidental/Mistake | | x | x | | | | | | | | | | | |
| | Don't Care | x | | | | | | | | | | | | | |
| | Immoral | x | | | x | | | | | | | | | x | |
| | Social/Moral Gain | | | | x | x | | x | | | | | | | |
| | Emotional Gain | | | | x | | | | | x | | | | x | |
| | Financial Gain | | | | | | x | x | x | | | | | | |
| | Ideological | | | | | | x | | | | x | | | | |
| | Political | | | | | | | | | | x | x | x | | |
| Outcomes / Goal (1-2) | Acquisition/Theft | | | | | | | | | | | | x | | |
| | Business Advantage | | | | | | x | x | x | | | x | | | |
| | Damage | x | x | x | x | | | | | x | x | | | x | |
| | Embarrassment | x | x | x | | x | | | | x | x | | | x | |
| | Tech Advantage | | | | | | x | x | x | | | x | x | | |
| Intended Actions (1 or more) | Copy | | | | | x | x | | x | | | x | x | | |
| | Deny | | | | | | | x | | | x | | | | |
| | Destroy | | | | x | | | | | x | x | | | | |
| | Damage | | | | | | x | | | x | x | | | | |
| | Take | | | | | | | | | | | | | | |
| | Penetrate | | | | | | x | | x | x | x | x | x | | |
| | Control | | | | | | | | x | x | x | x | x | x | |

# Attacker / Threat agent?

**Typically actor and intention is closely related**

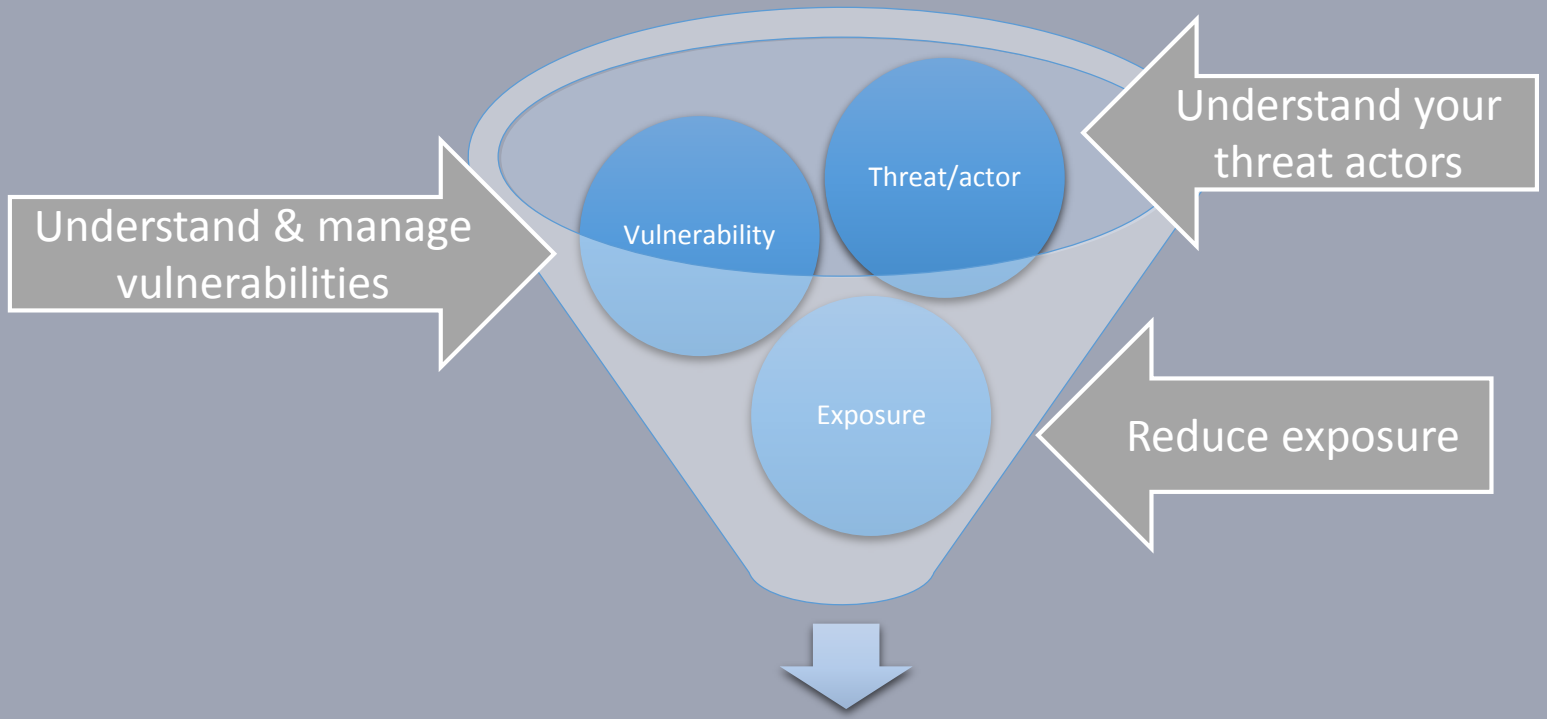
- **Script Kiddie – curiosity / malice**
- **Hacktivist – attention for a cause**
- **Organized crime – value extraction**
- **State sponsored – information extraction**

**Whatever the business is, there is always something of value**

**Basic vulnerability management capabilities (AV, VA, patching) keeps basic attackers at bay**

**Advanced attackers require additional sophistication on the defenders side**

# Dealing with the situation



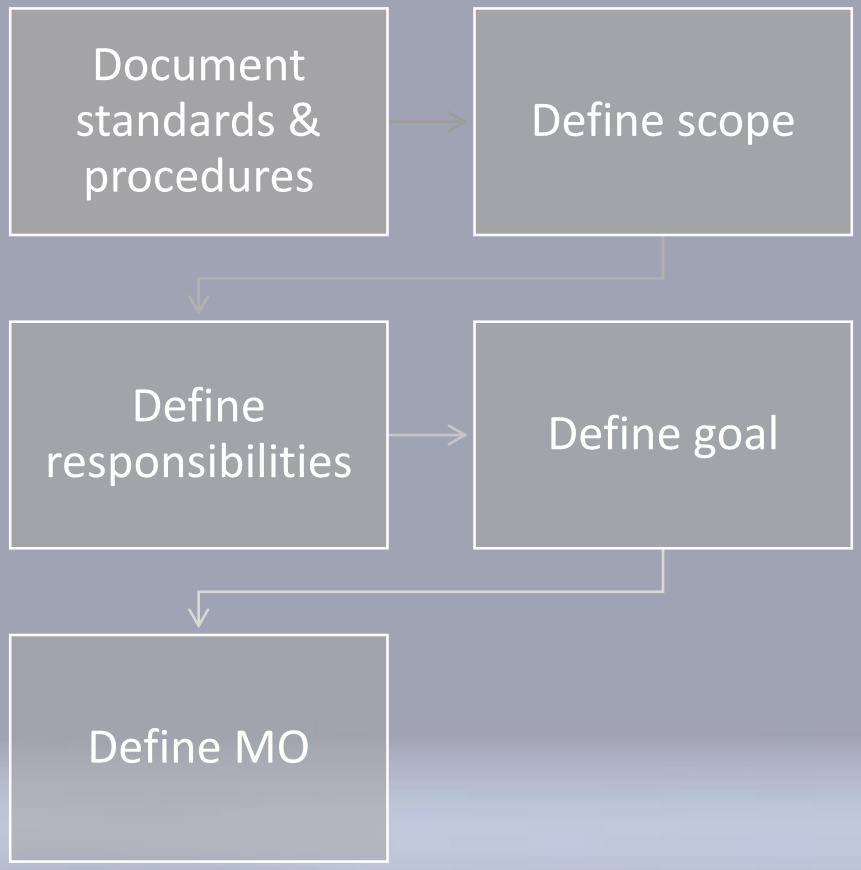
# ISF SoGP

| CONTROL FRAMEWORK (continued) | | Page | Type |
|---|---|---|---|
| **CF9 Network Management (continued)** | | | |
| CF9.7 | Voice over IP (VoIP) Networks | 136 | S |
| CF9.8 | Telephony and Conferencing | 137 | S |
| **CF10 Threat and Vulnerability Management** | | | |
| CF10.1 | System and Software Vulnerability Management | 138 | F |
| CF10.2 | Malware Awareness | 141 | F |
| CF10.3 | Malware Protection Software | 142 | F |
| CF10.4 | Security Event Logging | 144 | F |
| CF10.5 | System/Network Monitoring | 146 | F |
| CF10.6 | Intrusion Detection | 148 | F |
| **CF11 Incident Management** | | | |
| CF11.1 | Information Security Incident Management | 150 | F |
| CF11.2 | Cybercrime Attacks | 153 | S |
| CF11.3 | Emergency Fixes | 155 | F |
| CF11.4 | Forensic Investigations | 157 | S |
| **CF12 Local Environments** | | | |
| CF12.1 | Local Environment Profile | 159 | S |
| CF12.2 | Local Security Co-ordination | 161 | S |
| CF12.3 | Office Equipment | 163 | S |
| **CF13 Desktop Applications** | | | |
| CF13.1 | Inventory of Desktop Applications | 165 | S |
| CF13.2 | Protection of Spreadsheets | 167 | S |
| CF13.3 | Protection of Databases | 169 | S |
| CF13.4 | Desktop Application Development | 171 | S |

| CONTROL FRAMEWORK (continued) | | Page | Type |
|---|---|---|---|
| **CF17 System Development Management** | | | |
| CF17.1 | System Development Methodology | 201 | F |
| CF17.2 | System Development Environments | 203 | F |
| CF17.3 | Quality Assurance | 204 | F |
| **CF18 Systems Development Lifecycle** | | | |
| CF18.1 | Specifications of Requirements | 205 | F |
| CF18.2 | System Design | 207 | F |
| CF18.3 | System Build | 209 | F |
| CF18.4 | Systems Testing | 211 | F |
| CF18.5 | Security Testing | 213 | F |
| CF18.6 | System Promotion Criteria | 215 | F |
| CF18.7 | Installation Process | 217 | F |
| CF18.8 | Post-implementation Review | 218 | F |
| **CF19 Physical and Environmental Security** | | | |
| CF19.1 | Physical Protection | 219 | F |
| CF19.2 | Power Supplies | 221 | F |
| CF19.3 | Hazard Protection | 222 | F |
| **CF20 Business Continuity** | | | |
| CF20.1 | Business Continuity Strategy | 223 | S |
| CF20.2 | Business Continuity Programme | 225 | S |
| CF20.3 | Resilience | 227 | S |
| CF20.4 | Crisis Management | 229 | F |
| CF20.5 | Business Continuity Planning | 231 | F |
| CF20.6 | Business Continuity Arrangements | 233 | F |
| CF20.7 | Business Continuity Testing | 235 | F |

F Fundamental topic S Specialised topic

# Vulnerability Management framework



# ISF SoGP CF 10.1

**CF10.1.1 [*Standard & Procedures*]**
**There should be documented standards/procedures for system and software vulnerability management**

**CF10.1.2 [*Define scope*]**
**Standards/procedures should be supported by a system and software vulnerability management process to manage system and software vulnerabilities**

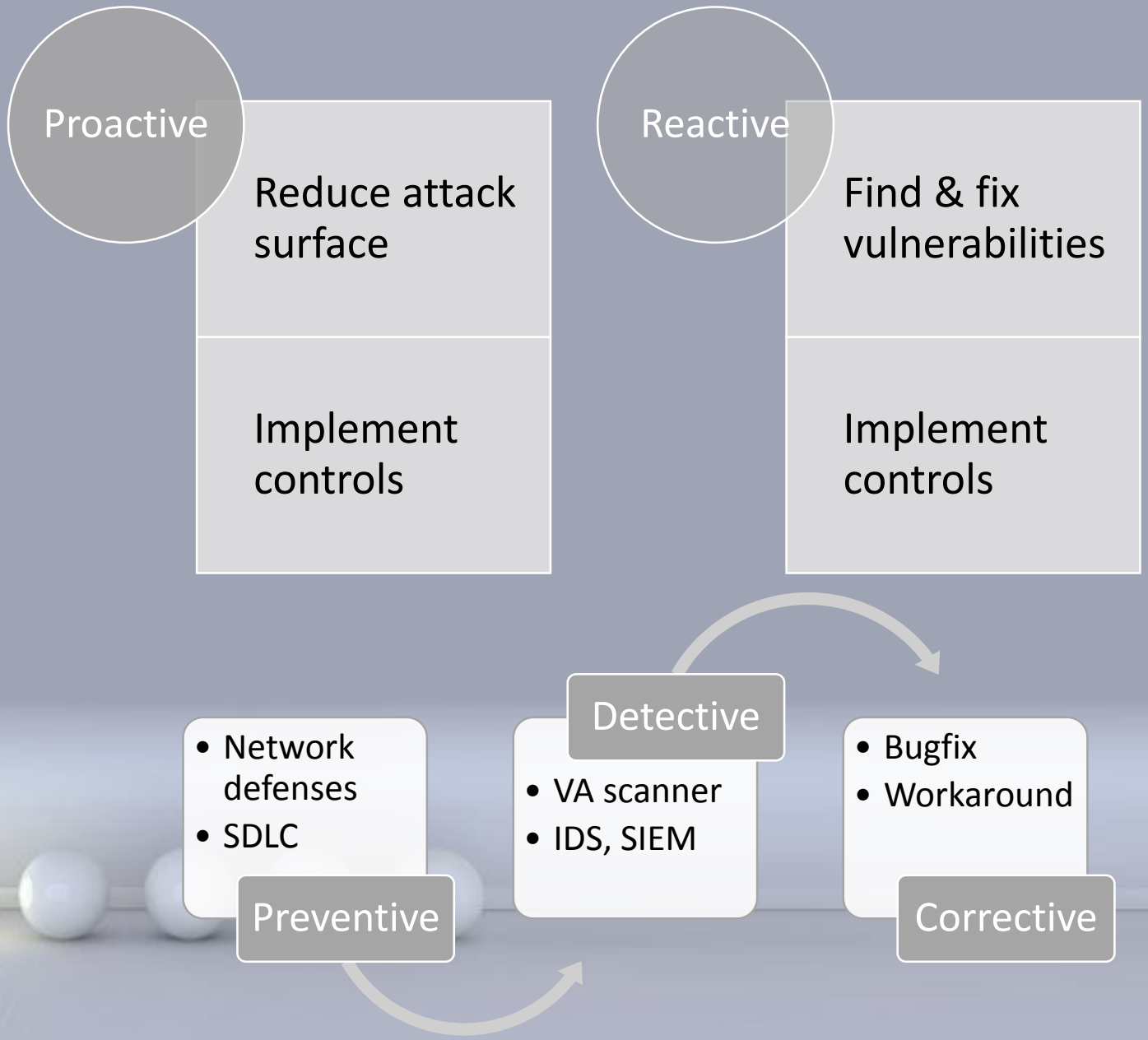
**CF10.1.3**
**The system and software vulnerability management process should be documented, approved, …**

# ISF SoGP CF 10.1

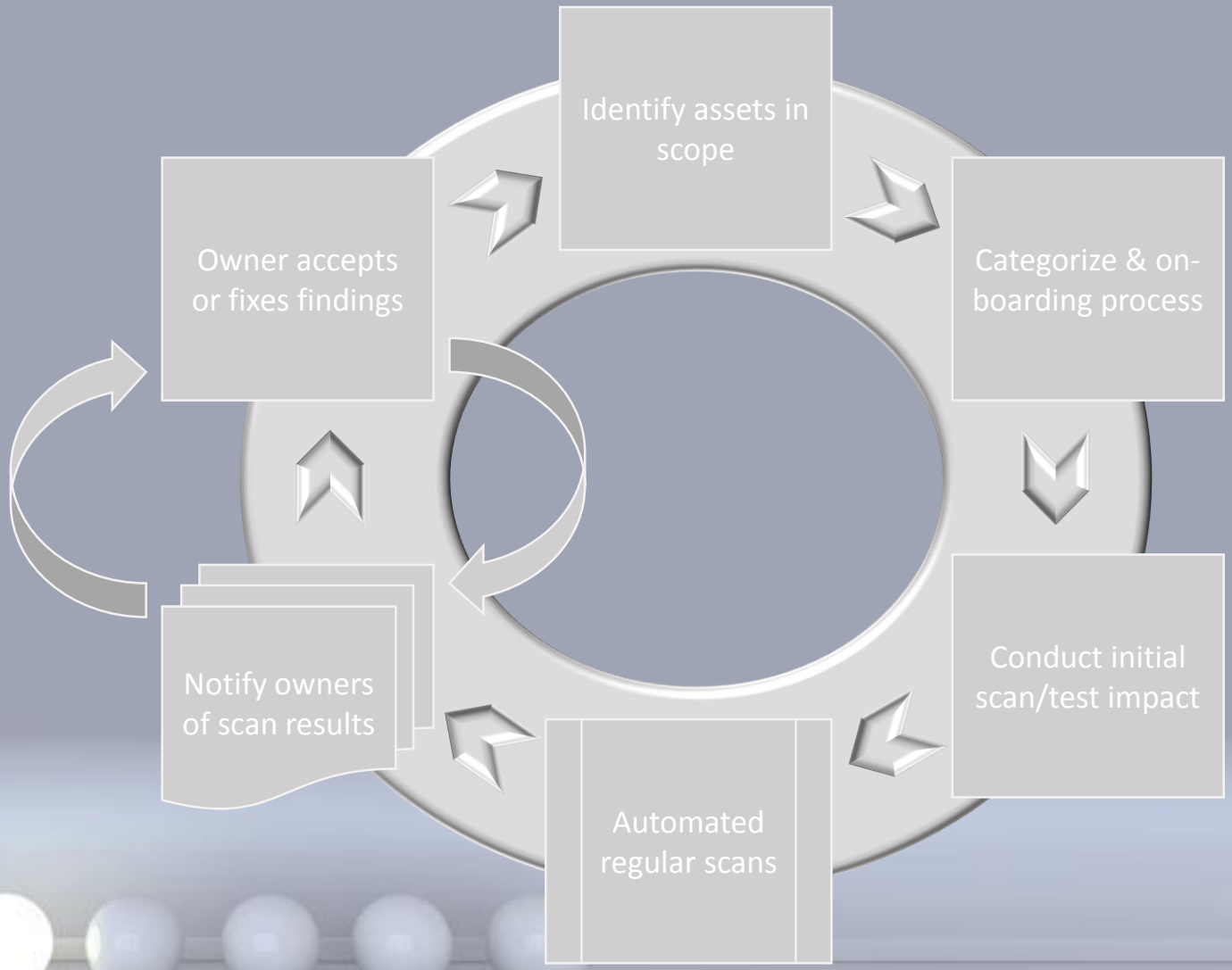
**CF10.1.4**
**The system and software vulnerability management process should be used by business owners and system owners to help:**

a) **determine the importance of business applications, information systems and networks to help identify the extent of vulnerabilities and timescales/priorities for remediating vulnerabilities**
b) **discover system and software vulnerabilities as soon as they become know**
c) **determine whether software code that can exploit a new vulnerability is publicly available, either as a 'proof of concept' or as actual malicious code**
d) **identify and obtain patches when they are available to remediate discovered vulnerabilities**
e) **decide when to deploy patches e.g. by assessing potential post-deployment impact to the organisation, determining the criticality of patches and analysing the results of testing patches**
f) **record patches that have been applied**

# How to manage?



# Asset vulnerability assessment lifecycle



# Implementation

**Identify assets in scope**

- Focus on most valuable assets supporting the business' goal
- InfoSec team provides input but doesn't decide priority of business assets

**Categorize & on-board**

- Understand properties of assets (location, technology, purpose) and prioritize those with high risk profile or regulatory requirements
- Involve asset owners & support teams early so they can schedule time to help
- Identify quick wins and early adopters to help get traction
- Make the process as simple as possible to the asset owners

**Initial scan/impact test**

- Work with stakeholder to run a test assessment on a representative sample (Lab, QA, PPE, Prod)
- Ensure all usual change management procedures are followed
- Take extra care to provide feedback on concerns and explain findings/expectations

# Implementation

**Conduct automated regular scans**

- Following successful onboarding & testing the asset will be included in regular scan schedules
- Frequency depends on requirements (policy, regulatory, SLA impact, risk profile, …)

**Distribute findings report**

- Asset owners need to know what vulnerabilities exist on their assets
- Ensure the right contacts get the results and that they know what to do with it

**Vulnerability treatment**

- Ensure vulnerabilities are treated within agreed timelines as per policy requirements
- Verify treatment was implemented correctly
- Escalate where treatment did not take place
- Always be cooperative and helpful

# Implementation

## Discovery

- Regularly monitor your networks (esp. perimeter) for new & unexpected assets
- Identify owners and follow on-boarding process
- Make friends in the M&A department

## Metrics

- Identify KPI for your program and start measuring asap
- Review KPI with stakeholder over time to ensure usefulness
- Drive improvements based on KPI

| Metric | Measure |
|---|---|
| External IP address space scanned for vulnerabilities | % |
| Internal IP address space scanned for vulnerabilities | % |
| Number of scanned assets | Absolute number |
| Number of assets without identified owner | Absolute number |
| Assets without identified owner | %Chg previous period |
| Assets with critical vulnerabilities (sev 4/5) | Absolute number |
| Assets with medium vulnerabilities (sev 3) | Absolute number |
| Assets with critical vulnerabilities (sev 4/5) | %Chg previous period |
| Assets with medium vulnerabilities (sev 3) | %Chg previous period |
| Accepted risk (SARR) for critical vulnerabilities (sev 4/5) | Absolute number |
| Accepted risk (SARR) for medium vulnerabilities (sev 3) | Absolute number |
| Policy breach - mitigation time sev 4/5 | Absolute number |
| Policy breach - mitigation time sev 3 | Absolute number |
| Policy breach - mitigation time sev 4/5 | %Chg previous period |
| Policy breach - mitigation time sev 3 | %Chg previous period |
| Mean time to remediation (sev3/4/5) | Avg/days |

# Ok, but do i have to?

The organization should conduct vulnerability assessments throughout the lifecycle of the system as part of the vulnerability management strategy. **[Australian Government Information Security Manual: Controls]**

Vulnerability scanning of business applications, information systems, and network devices should be performed on a regular basis (e.g., daily). **[The Standard of Good Practice for Information Security, 2013]**

Is vulnerability testing conducted on a quarterly basis? **[OECD / World Bank Technology Risk Checklist, Version 7.3]**

External vulnerability scans must be conducted quarterly by an Approved Scanning Vendor that is approved by the Payment Card Industry Security Standards Council. **[PCI DSS Requirements, 3.0]**

The system must run scanning tools on a daily basis to check for open ports, patch levels, services, configuration files, and software version. **[Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, Version 4.0]**

Systems should be checked regularly to ensure they are in compliance with the information security standards. This check can be accomplished either manually or with an automated tool. The checks should be performed by authorized personnel in compliance with the information security standards. **[ISO 27002 Code of practice for information security management, 2005]**

The organization must periodically scan for vulnerabilities in the system and hosted applications and when new potential vulnerabilities are identified. **[NIST SP 800-53]**

An accredited independent assessor must conduct vulnerability scanning on the Operating Systems, the operating infrastructure, web applications, and databases annually. **[FedRAMP Baseline Security Controls]**

# VA Technology

**Vulnerability assessment tools are aimed to assist with identification of vulnerabilities in an automated way**

**Various different approaches, architectures and scopes**









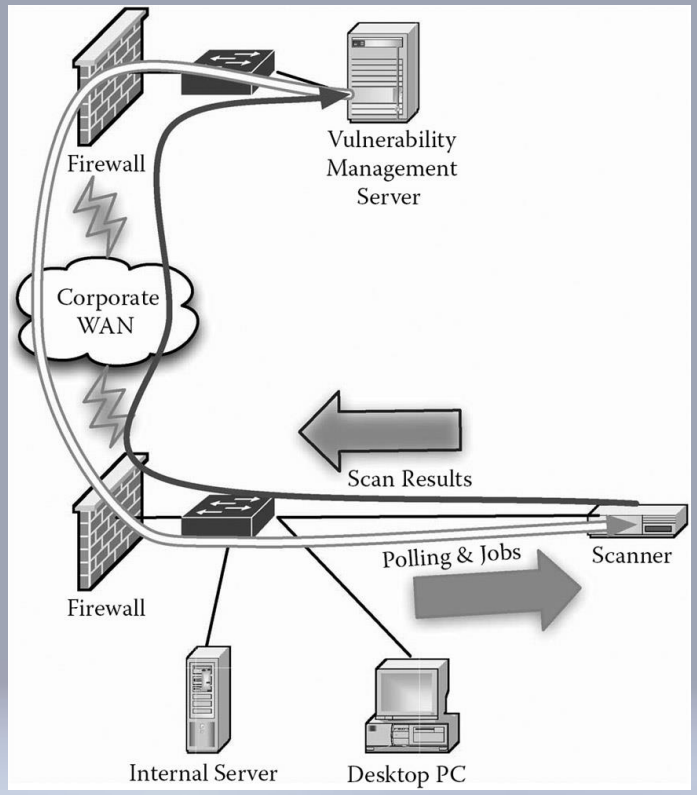
# VA Technology

**Right solution depends on the requirements of the organisation**

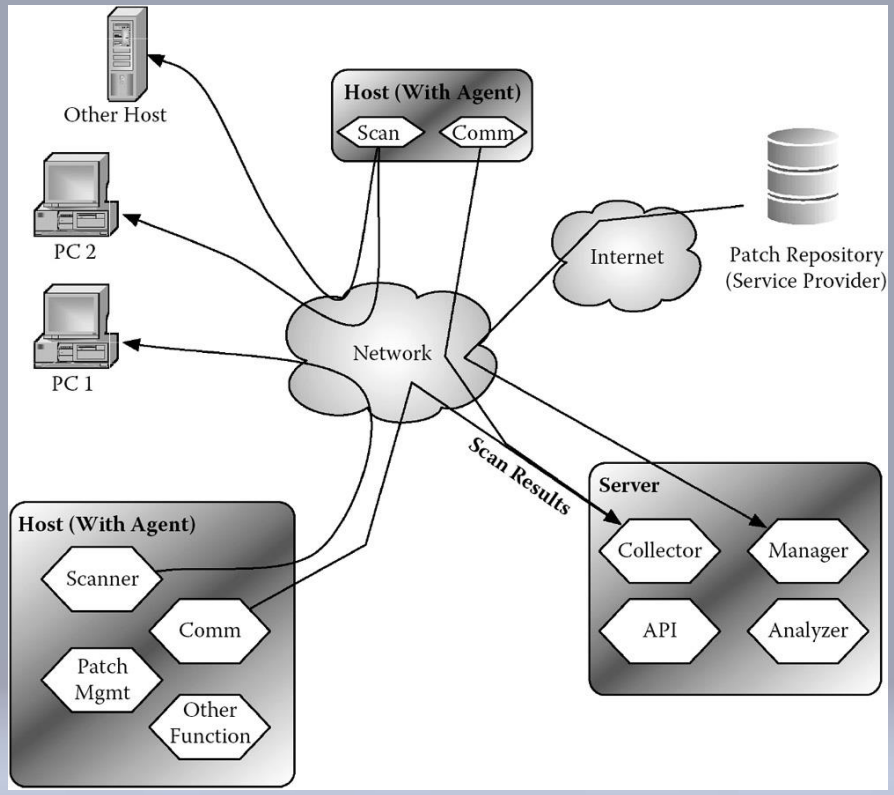
- Deployed, SaaS or mixed?
  - Internal/external environment
  - Scale of organisation
  - IT staff to manage deployed
- Licensing model?
  - Per asset/IP
  - Per scanner
  - Flat fee / mixed
- Enterprise Management?
  - Rapid deployment option
  - Centralized management console
- Technology stack?
  - Windows, Linux, other
  - Scan performance/Network speed
  - API available
- Supported Technologies?
  - Key vendors supported?
- Commercial or Open Source?

# VA Technology

## Appliance based approach

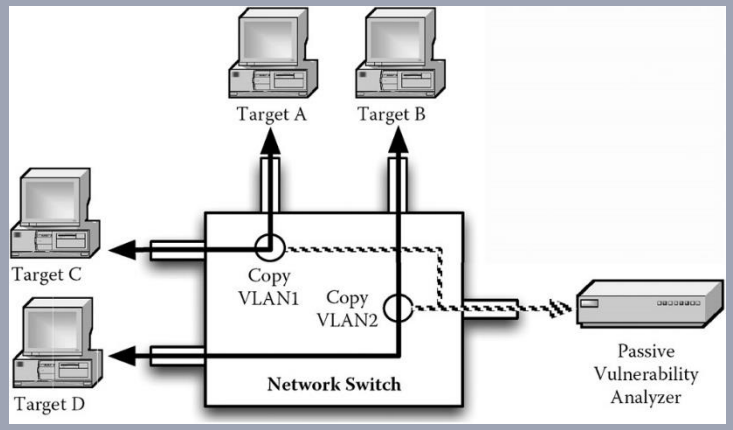



## Agent based approach



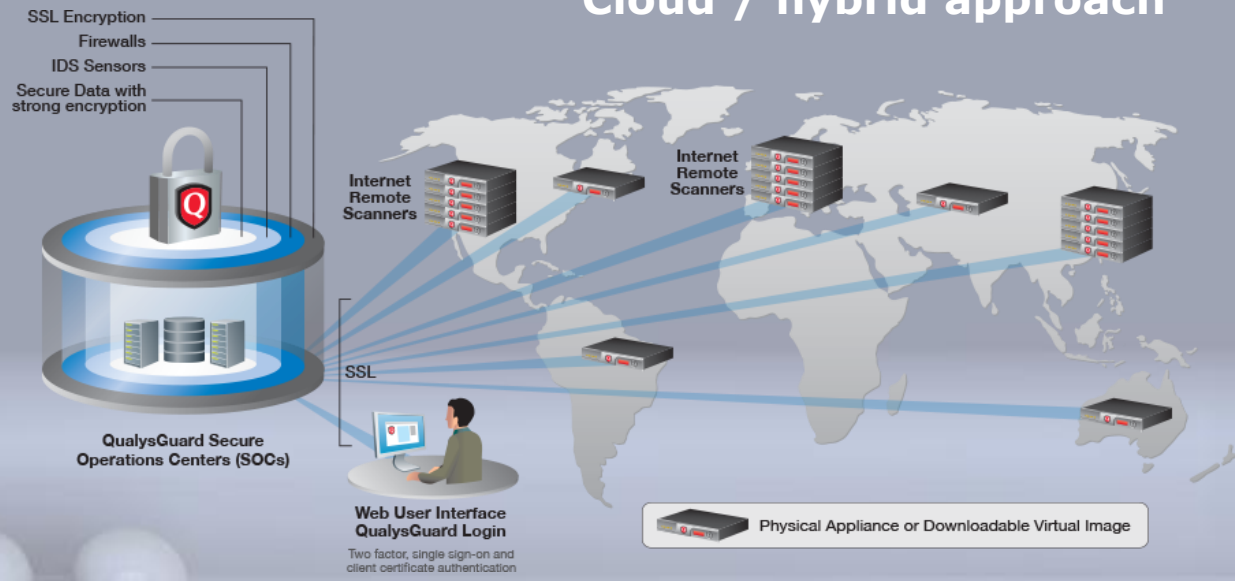

*Source: Foreman, Park (2009), Vulnerability Management, Auerbach Publications*

# VA Technology




**Passive vulnerability analysis approach**

**Cloud / hybrid approach**




*Source: Foreman, Park (2009), Vulnerability Management, Auerbach Publications & Qualys Inc.*

# Discussion

**Medium size organisation, generally risk averse**
**Relatively small IT team, largely Microsoft shop**
**Strict SLA for their services**

**HQ London/UK (1000 FTE)**
- **Managed Datacentre (PPE/Prod)**
- **Some use of cloud services**

**Branch offices Sydney & Austin/TX (200 FTE each)**
- **No DC, but IT rooms**
- **Good but saturated comm links**

**You, the new InfoSec Manager, are asked to implement a VA solution. What are the key points you'd consider?**

# Discussion

**You successfully deployed your new Vulnerability Management program across parts of the organisation. Shortly after you arrive at the office you notice a high priority message -**

**You know that your organisation invested a considerable amount of money in the VM program and your boss will be calling you shortly to ask what you're doing about this issue.**

**What do you do next?**

# Challenges

**Technology**

- What technology does the solution support on the assessment side
- How quickly does the vendor provide updates for new vulnerabilities
- What is the False Positive and False Negative rate
- How difficult is the solution to deploy/use
- Is the solution itself secure
- Does it integrate with standard enterprise solutions (SIEM, Password Vaulting, etc.)

**Resources**

- Is the technology optimized to conserve resources (CPU, network, storage)
- Are processes optimized to reduce analyst time required (ease of use, automation, value add information, …)
- Is sufficient documentation and/or vendor training available
- Are there enough FTE, is the program pace aligned with available FTE

# Challenges

**Cost**

- What cost model is most appropriate (capex vs opex)
- Does the solution cost scale well with the program roadmap
- How high is the lock in cost

**Culture**

- Does senior management support the program
- Is staff in support of security or is it unwelcome additional workload
- Do asset owner resist in fear of what may be found

# Questions?