# LECTURE 6
# VULNERABILITY MANAGEMENT



Dr Warusia Mohamed Yassin

# Topics

- Vulnerability Management
- VM Lifecycle
- Important of VM
- Penetration Testing
- Vulnerability Scanning

# Organizations are Feeling the Pain

***1. What causes the damage?***

**95% of breaches target known vulnerabilities**

***2. How do you prevent the damage? What are your options?***

**RISK=**

**Assets x *Vulnerabilities* x Threats**

**You *can* control vulnerabilities.**

***3. How do you successfully deal with vulnerabilities?***

- **Vulnerabilities**
- **Business complexity**
- **Human resources**
- **Financial resources**

***4. How do you make the best security decisions?***

**Focus on the *right assets*, *right threats*, *right measures*.**

# What Is Vulnerability Management?

- A process to determine whether to **eliminate**, **mitigate** or **tolerate** vulnerabilities based upon risk and the cost associated with fixing the vulnerability.

# What Is Vulnerability Management?

- At a high level, the "***intelligent confluence***" of…

**Assessment**
What assets?

+

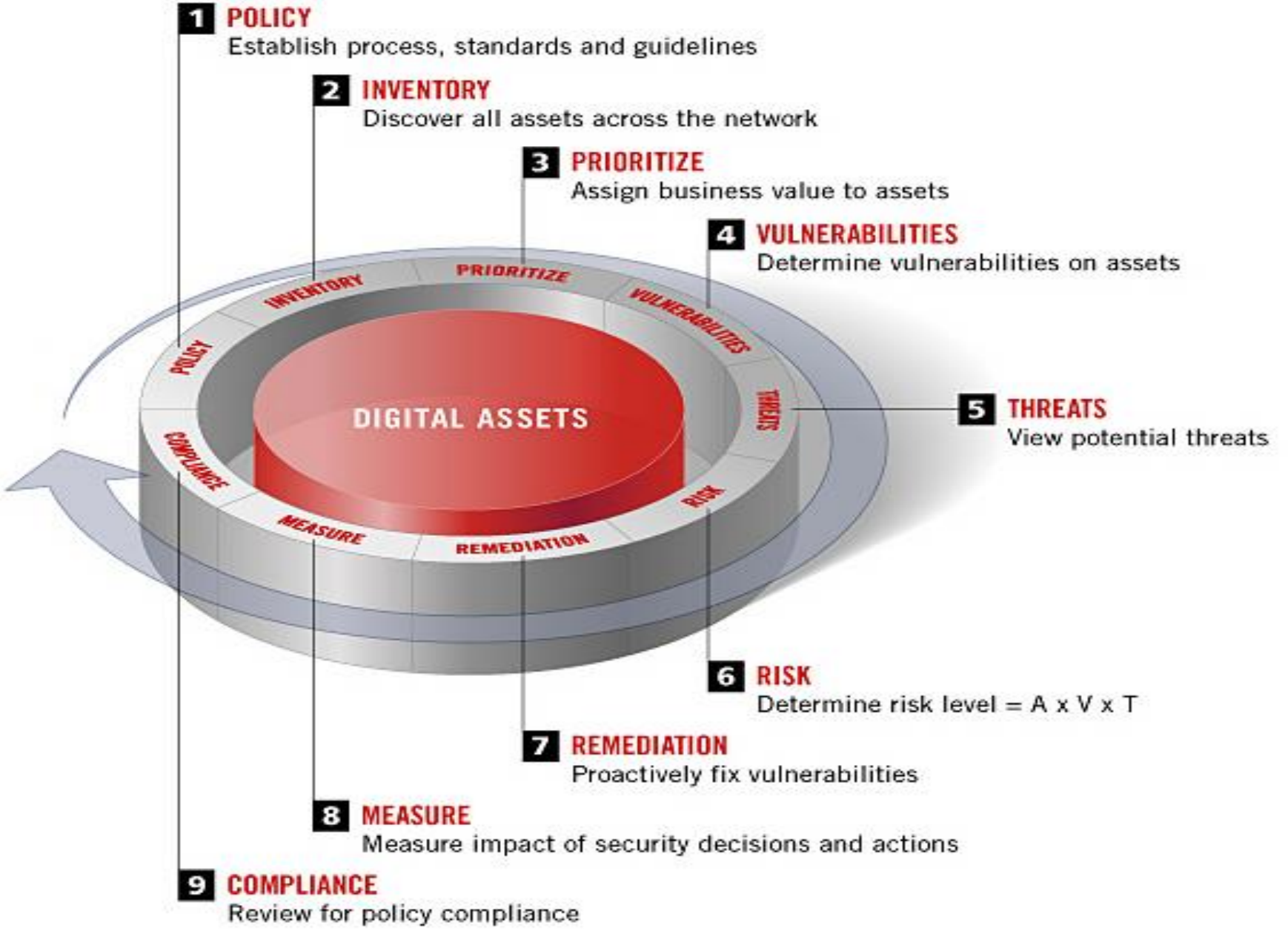
**Analysis**
What to fix first?

+

**Remediation**
Fix the problem

- Component of Risk Management
- Balance the demands of business goals and processes

# Vulnerability Management Lifecycle



# Successful Approaches:
## Implementing An Effective VM Strategy

- Focus on four key areas:
  - Prioritize Assets
  - Determine Risk Level (assets, threats, vulnerabilities)
  - Remediate Vulnerabilities
  - Measure

# Successful Approaches:
## Implementing An Effective VM Strategy

- **Assets**

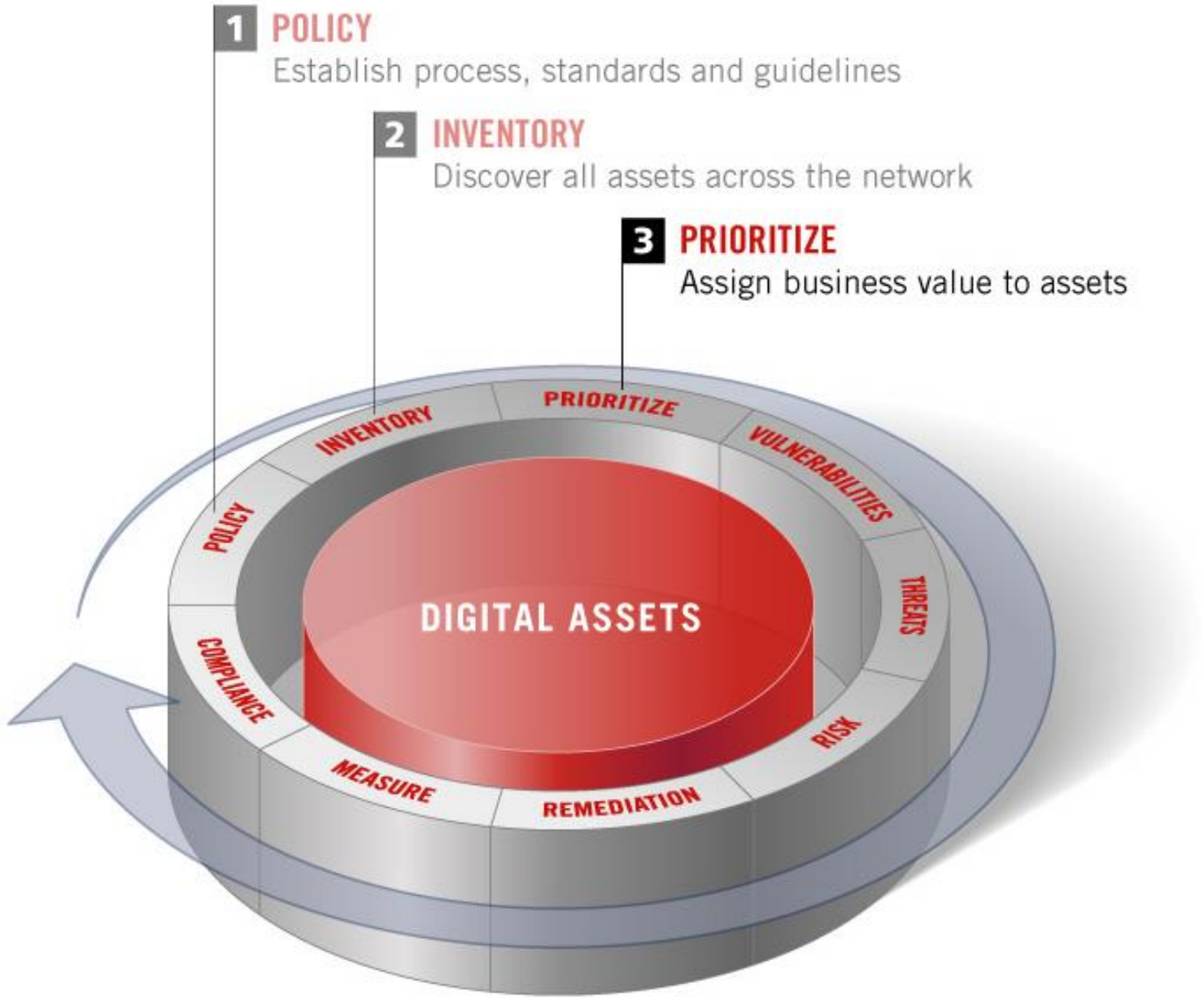
Any function, task, capability, equipment or information that has value to the organization or supports the ability of the organization to conduct business

- **Threats**

Any person, circumstance or event that has the **potential** to cause **damage** to an organizational asset or business function

- **Vulnerabilities**

Any **flaw** in the design, implementation or administration of a system that provides a mechanism for a threat to **exploit** the weakness of a system or process




# Prioritize Asset

# Asset Prioritization

**Identify assets by:**

**Networks**

Logical groupings of devices

Connectivity - None, LAN, broadband, wireless

**Network Devices**

Wireless access points, routers, switches

**Operating System**

Windows, Unix

**Applications**

IIS, Apache, SQL Server

**Versions**

IIS 5.0, Apache 1.3.12, SQL Server V.7

**Example:**

**Network-based discovery**

- ✓ Known and “unknown” devices
- ✓ Determine network-based applications
- ✓ Excellent scalability

**Agent-based discovery**

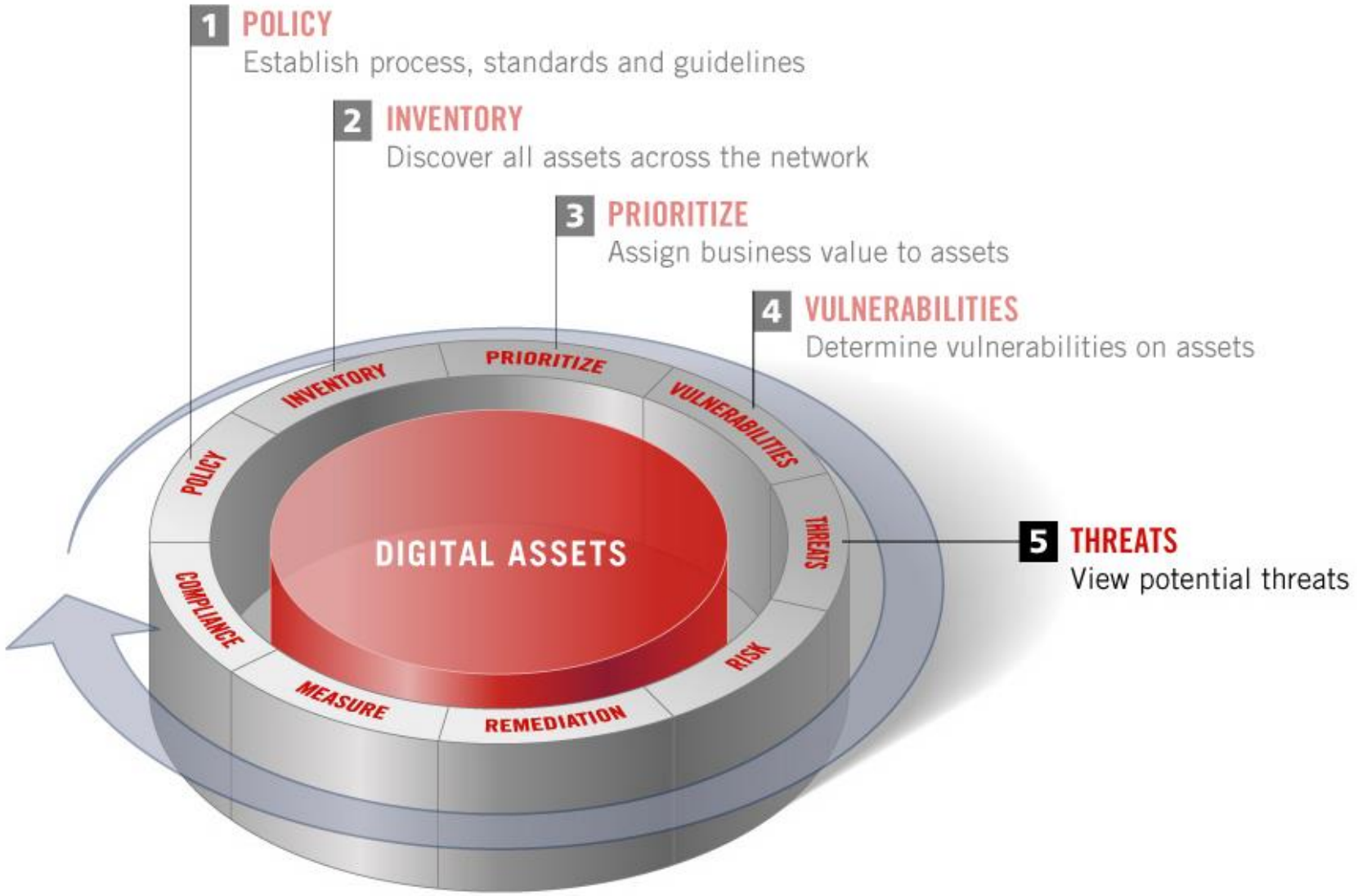
- ✓ In-depth review of the applications and patch levels
- ✓ Deployment disadvantages

**Network- and agent-based discovery techniques are optimal**

- ✓ *Agents* - Cover what you already know in great detail
- ✓ *Network* - Identify rogue or new devices

**Frequency**

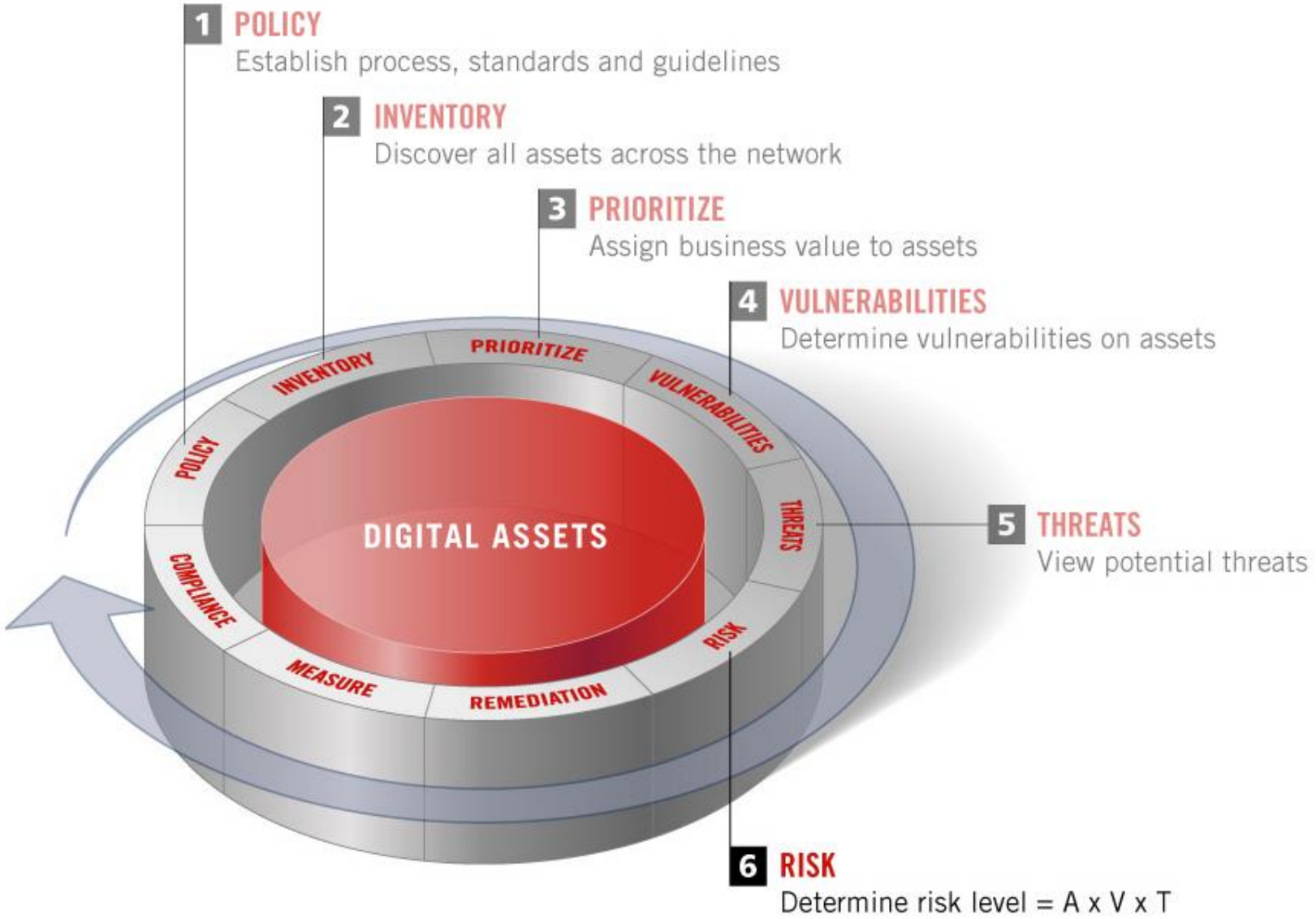
- ✓ Continuous, daily, weekly
- ✓ Depends on the asset



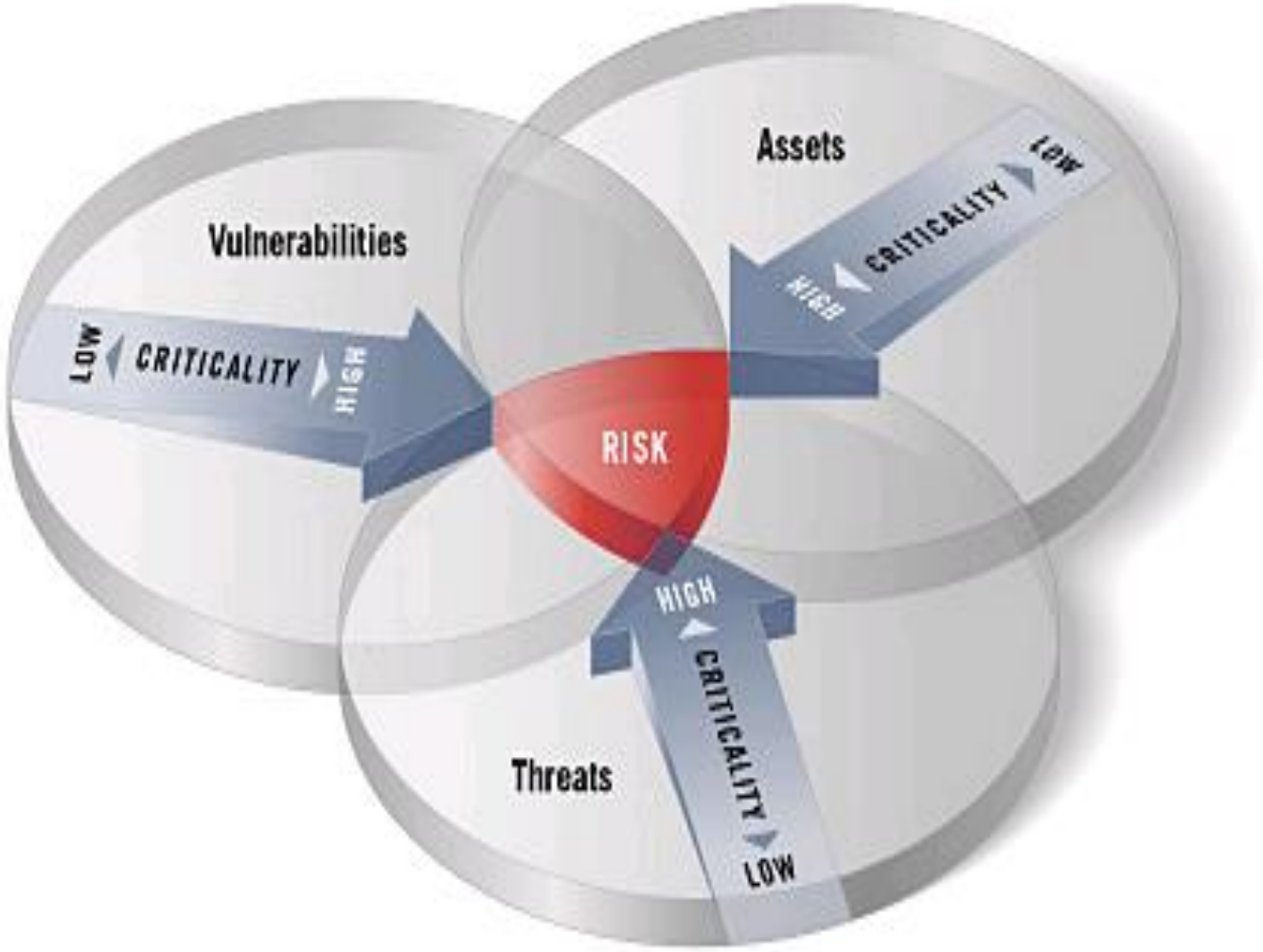

**Correlate Threats**

# Correlate Threats

- Not all threat and vulnerability data have equal priority
- Primary goal is to rapidly protect your most critical assets
- Identify threats
  - ✓ Worms
  - ✓ Exploits
  - ✓ Wide-scale attacks
  - ✓ New vulnerabilities
- Correlate with your most critical assets
- Result = Prioritization of vulnerabilities within your environment



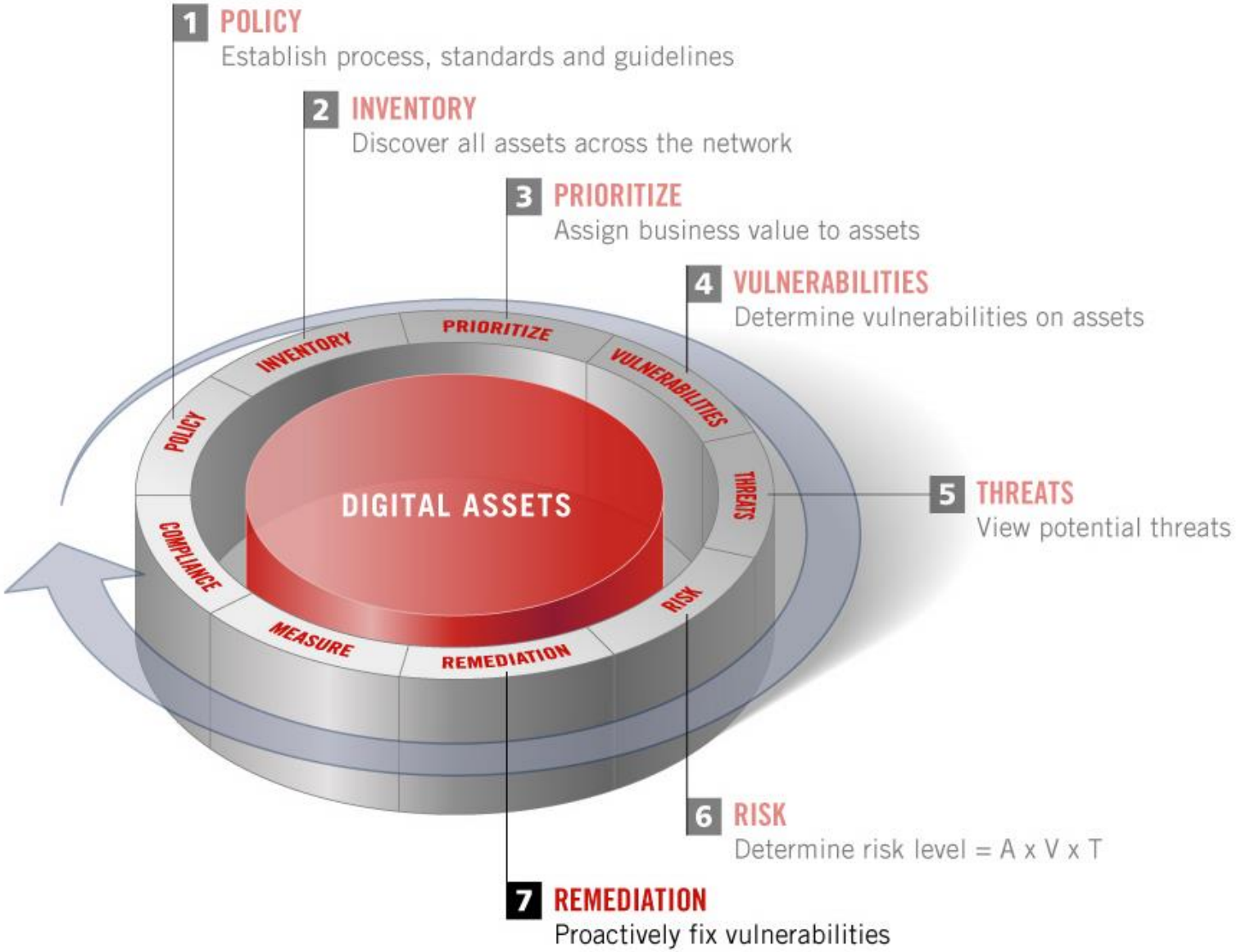

# Determine Risk Level




## Risk Calculation

- The Union of:
  - ✓ **V**ulnerabilities
  - ✓ **A**ssets
  - ✓ **T**hreats
- Based upon the criticality of VAT
- Focus your resources on the *true* risk

# Remediation



# Remediation

- Perfection is unrealistic (zero vulnerabilities)
  - ✓ Think credit card fraud – will the banks ever eliminate credit card fraud?
- You have *limited* resources to address issues
- The question becomes:
  - ✓ Do I address or not?
- Factor in the business impact costs + remediation costs
  - ✓ If the risk outweighs the cost – eliminate or mitigate the vulnerability!

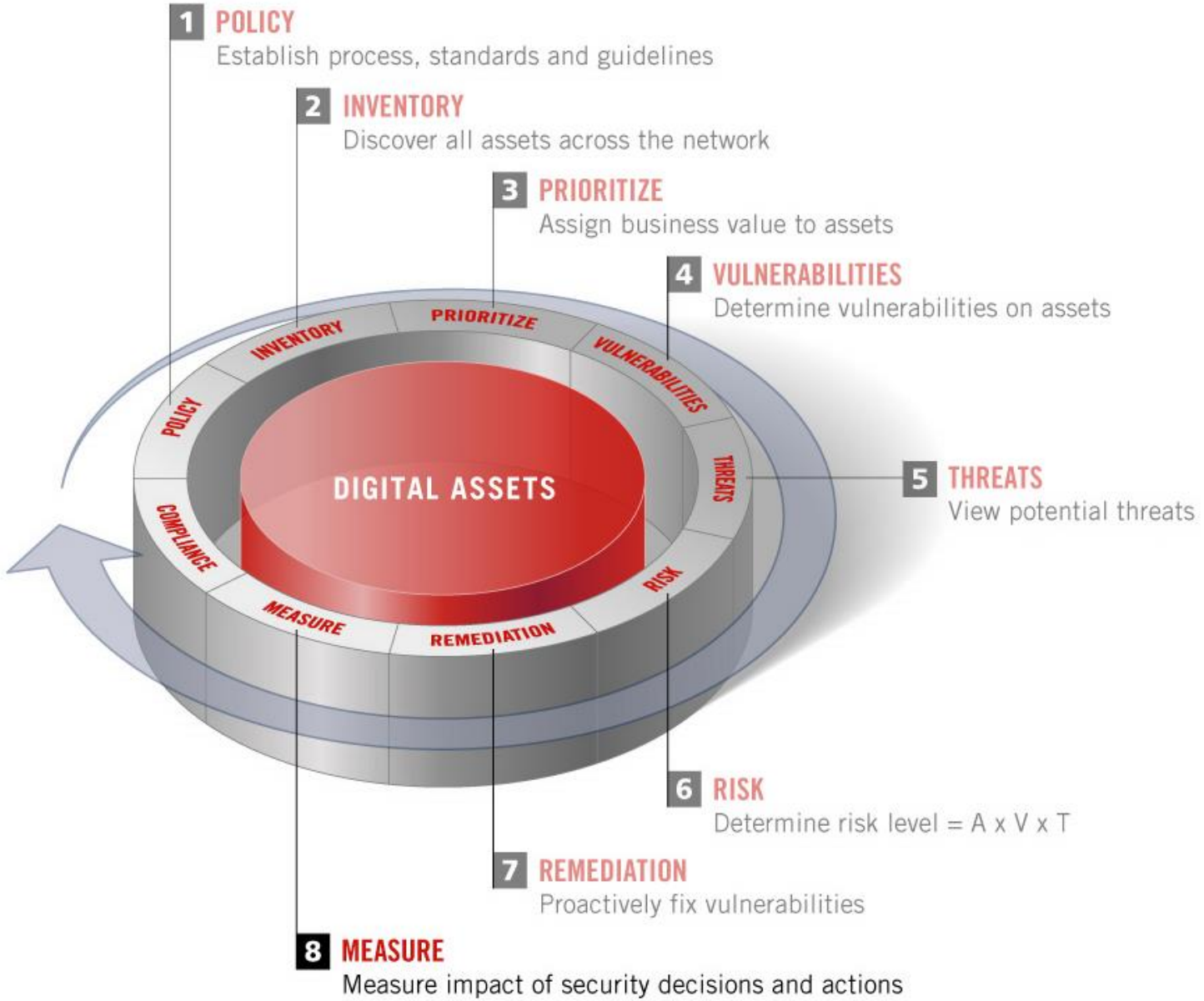
# Remediation / Resolution

## Apply the Pareto Principle – the 80/20 rule

- Focus on the *vital few* not the *trivial many*
- 80% of your risk can be eliminated by addressing 20% of the issues
- The Risk Union will show you the way
  - ✓ Right assets
  - ✓ Relevant threats
  - ✓ Critical vulnerabilities

## Patch or Mitigate

- Impact on availability from a bad patch vs. the risk of not patching
- Patch or mitigate
- Recommendations:
  - ✓ QA security patches 24 hours
  - ✓ Determine if there are wide spread problems
  - ✓ Implement defense-in-depth


1 POLICY
Establish process, standards and guidelines
2 INVENTORY
Discover all assets across the network
3 PRIORITIZE
Assign business value to assets
4 VULNERABILITIES
Determine vulnerabilities on assets
5 THREATS
View potential threats
6 RISK
Determine risk level = A x V x T
7 REMEDIATION
Proactively fix vulnerabilities
8 MEASURE
Measure impact of security decisions and actions
DIGITAL ASSETS
POLICY
INVENTORY
PRIORITIZE
VULNERABILITIES
THREATS
RISK
REMEDIATION
MEASURE
COMPLIANCE

# Measure

# Measure

## Current state of security metrics

- You can't manage what you can't measure
- No focus on quantifying "Security"
  - ✓ What is my *real* risk?
- Only a relative scale of risk, not an absolute
- Return on Security Investment (ROSI) is extremely difficult to calculate
- No accountability in security

## Future Look:

- Accountability
- A universal standard to quantify risk
- Common nomenclature
- Dashboard view of risk and vulnerabilities across disparate organizations
- Technologies that will help answer the questions:
  - ✓ Am I secure?
  - ✓ Who is accountable and by when?
  - ✓ Am I getting better or worse?
  - ✓ How am I trending over time?
  - ✓ How do I compare to my peers?
  - ✓ How do I compare outside my industry?

# 10 Steps to Effective Vulnerability Management

1. Identify all the assets in your purview
2. Create an Asset Criticality Profile (ACP)
3. Determine exposures and vulnerabilities
4. Track relevant threats – realized and unrealized
5. Determine Risk  - union of vulnerabilities x assets x threats
6. Take corrective action if risk > cost to eliminate or mitigate
7. Create meaningful metrics and hold people accountable
8. Identify and address compliance gaps
9. Implement an automated vulnerability management
10. ***Convince someone with a budget that vulnerability management is important***

# Need for Vulnerability Management

Vulnerabilities on a network are GOLD to cyber criminals:

- Provide unauthorized entry to networks
- Can expose confidential information, fuel stolen identities, violate privacy laws, or paralyze operations
- Exposure is extreme for networks with vulnerable devices connected by IP

**Sources of Vulnerabilities**

- ☒ Programming errors
- ☒ Unintentional mistakes or intentional malware in General Public License software
- ☒ Improper system configurations
- ☒ Mobile users sidestepping perimeter security controls
- ☒ Rising attacks through viewing popular websites

# Need for Vulnerability Management

## Despite utilization of basic defenses, network security breaches abound

- TJX exposed 46M records
- DSW exposed 1.4M records
- Card Systems exposed 40M records
- 215M+ reported record exposures since 2005 (actual is significantly higher)

## Automation is Crucial

- Manual detection and remediation workflow is too slow, too expensive and ineffective

### Attack Trends

- ☒ Increased professionalism and commercialization of malicious activities
- ☒ Threats that are increasingly tailored for specific regions
- ☒ Increasing numbers of multistage attacks
- ☒ Attackers targeting victims by first exploiting trusted entities
- ☒ Shift from “Hacking for Fame” to “Hacking for Fortune”

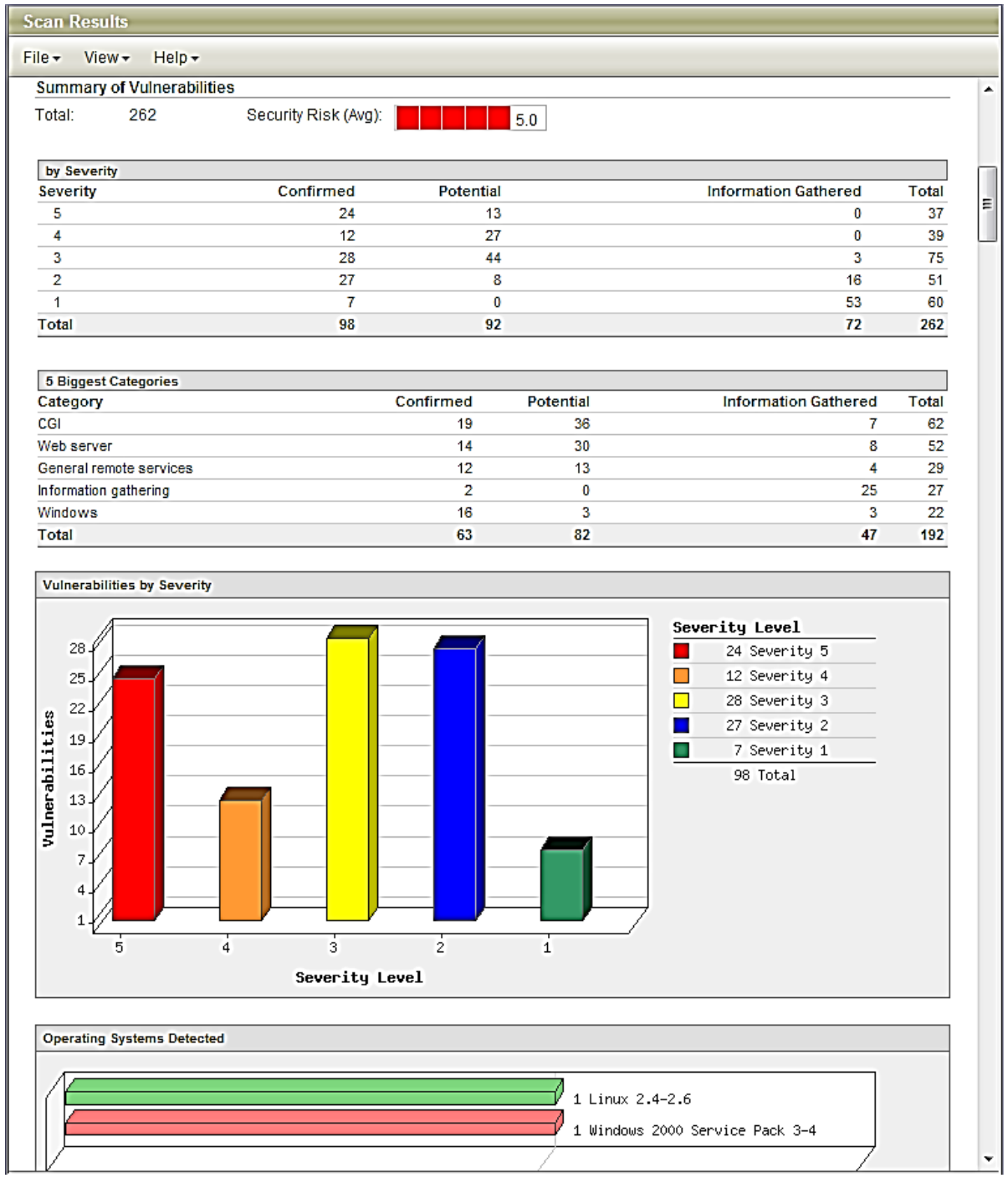
# Need for Vulnerability Management

## Did we learn our lessons?

- Most vulnerabilities are long known before exploited
- Successful exploitation of vulnerabilities can cause substantial damage and financial loss
- A few vulnerable systems can disrupt the whole network
- System misconfiguration can make systems vulnerable

## Challenges IT Security Face

- ☒ NOT enough TIME, PEOPLE, BUDGET
- ☒ Prioritization of efforts for minimize business risks and protecting critical assets. We can't fix all problems - what can we live with?
- ☒ Adapting to accelerating change in sophistication of attacks.




# Vulnerability Scanning

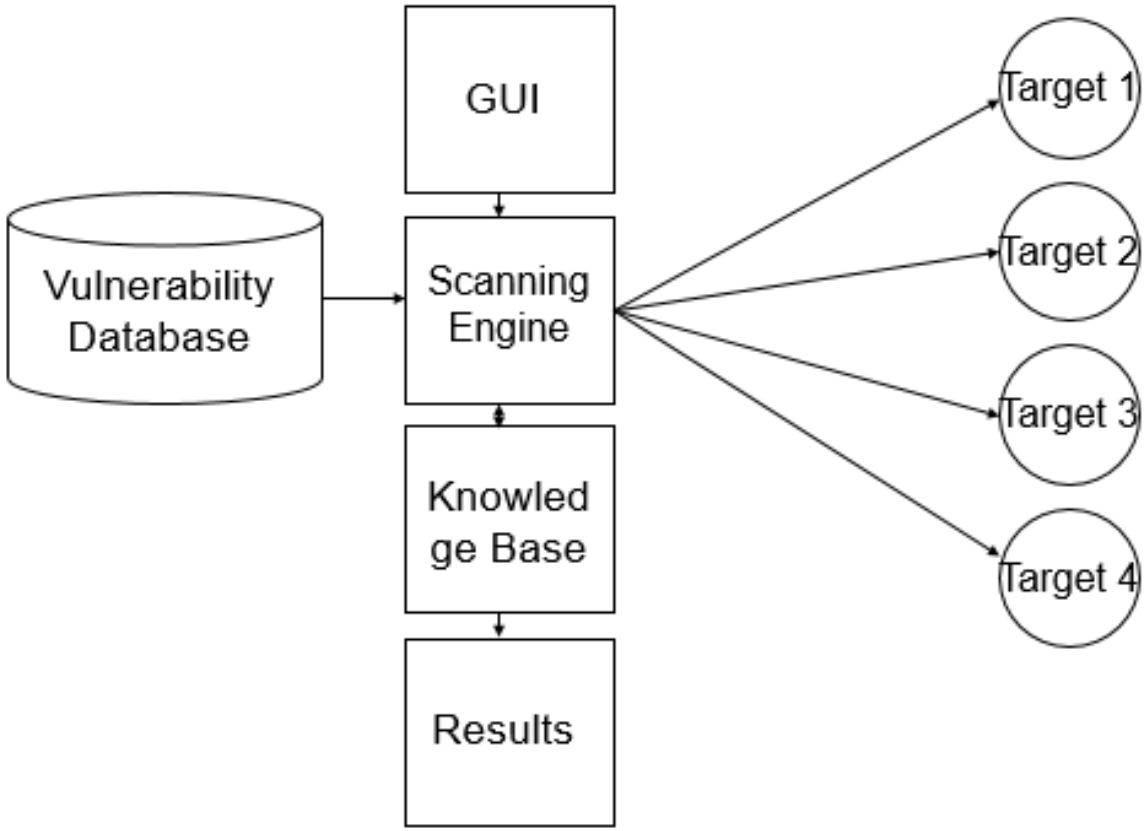
## Scanning:

- takes an “outside-in” and “inside-in” approach to security, emulating the attack route of a hacker
- tests effectiveness of security policy and controls by examining network infrastructure for vulnerabilities

## Vulnerability Scanners

- Vulnerability scanners are automated tools that scan hosts and networks for known vulnerabilities and weaknesses

# How Vulnerability Scanning Work




Similar to virus scanning software:

- Contain a database of vulnerability signatures that the tool searches for on a target system
- Cannot find vulnerabilities not in the database
  - ✓ New vulnerabilities are discovered often
  - ✓ Vulnerability database must be updated regularly

# Typical Vulnerabilities

- Network vulnerabilities
- Host-based (OS) vulnerabilities
  - ✓ Misconfigured file permissions
  - ✓ Open services
  - ✓ Missing patches
  - ✓ Vulnerabilities in commonly exploited applications (e.g. Web, DNS, and mail servers)

# Vulnerabilities Scanning Benefits

- Very good at checking for hundreds (or thousands) of potential problems quickly
  - ✓ Automated
  - ✓ Regularly
- May catch mistakes/oversights by the system or network administrator
- Defense in depth

# Vulnerabilities Scanning Drawbacks

- Report “potential” vulnerabilities
- Only as good as the vulnerability database
- Can cause complacency
- Cannot match the skill of a talented attacker
- Can cause self-inflicted wounds

# Vulnerabilities Scanning Drawbacks

- Report “potential” vulnerabilities
- Only as good as the vulnerability database
- Can cause complacency
- Cannot match the skill of a talented attacker
- Can cause self-inflicted wounds

# Vulnerabilities Scanning Tools

1. Port scanner (Nmap, Nessus)
2. Network enumerator
3. Network vulnerability scanner (BoomScan)
4. Web application security scanner
5. Database security scanner
6. Host based vulnerability scanner (Lynis, ovaldi, SecPod Saner)
7. ERP security scanner
8. Computer worm

# Example of Vulnerabilities Report

**Table 7.4** Vulnerabilities with respect to malicious threats

| Threat | Vulnerability | Description |
|---|---|---|
| DDoS attack on the central system | Inadequate attack detection and response on central system | New forms of DDoS attacks are continuoust being developed to defeat existing countermea sures. Due to the challenges of keeping th central system running 24/7, combined wit the lack of a strong tradition for cybersecurit awareness in the power distribution domai (which has not traditionally operated in cy berspace), countermeasures to various forms c DDoS attacks on the central system are rarel updated and may therefore be out of date |
| Tampering with all or most control data in transit from the central system to the choke component | Weak encryption and integrity check | The encryption of messages between the cen tral system and the metering node may be wea compared to the current standard. The same ap plies to the integrity checking of received mes sages. This applies in particular at the meterin nodes, which have relatively little computin power and are rarely replaced |

# Roadmap/Mind Map