Threat-Based Metrics for Continuous Enterprise Network Security Management

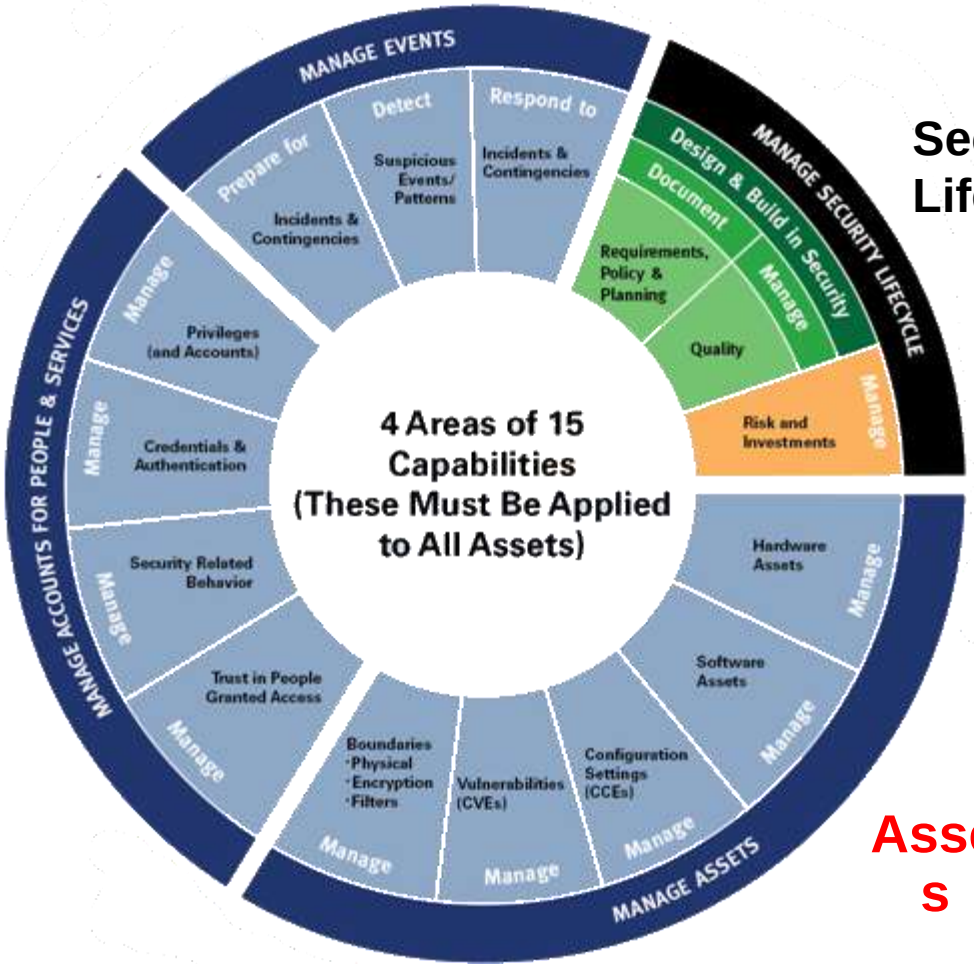
Richard Lippmann and James Riordan
MIT Lincoln Laboratory
{lippmann,james.riordan}@ll.mit.edu

To be Presented at IFIP Working Group 10.4 Workshop on Security Assessment: Metrics and Methods
24 January 2014

*This work is sponsored by the Department of Homeland Security under Contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government.

15 Security Capabilities that Must be Managed (U.S. Department of Homeland Security)

Events



Security Lifecycle

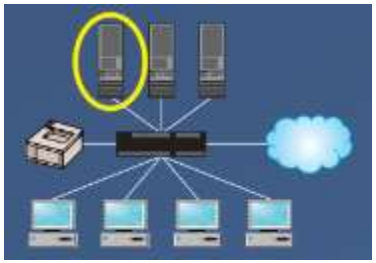
Accounts for People and Services

Assets

A Continuous Diagnostics and Mitigation (CDM) Process Controls Risk for Each Capability

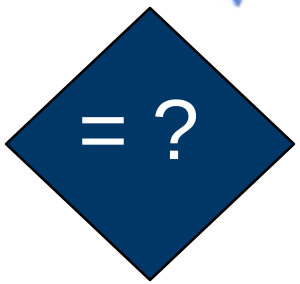
3. Prioritize Risks and Decide on Actions

4. Act
- **Mitigate Risk**
- **Refine Specifications**
- **Correct Observations**



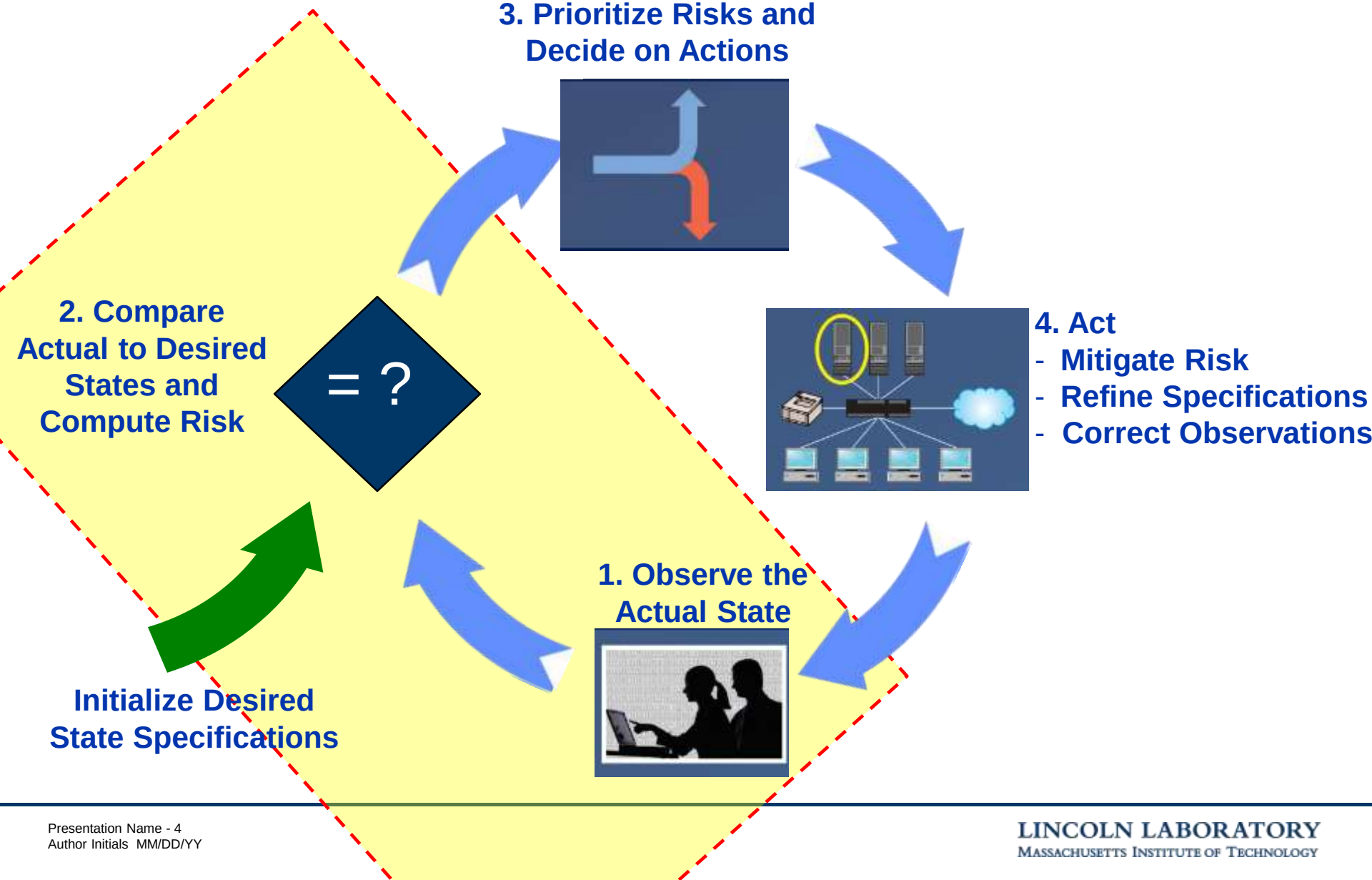
1. Observe the Actual State

2. Compare Actual to Desired States and Compute Risk

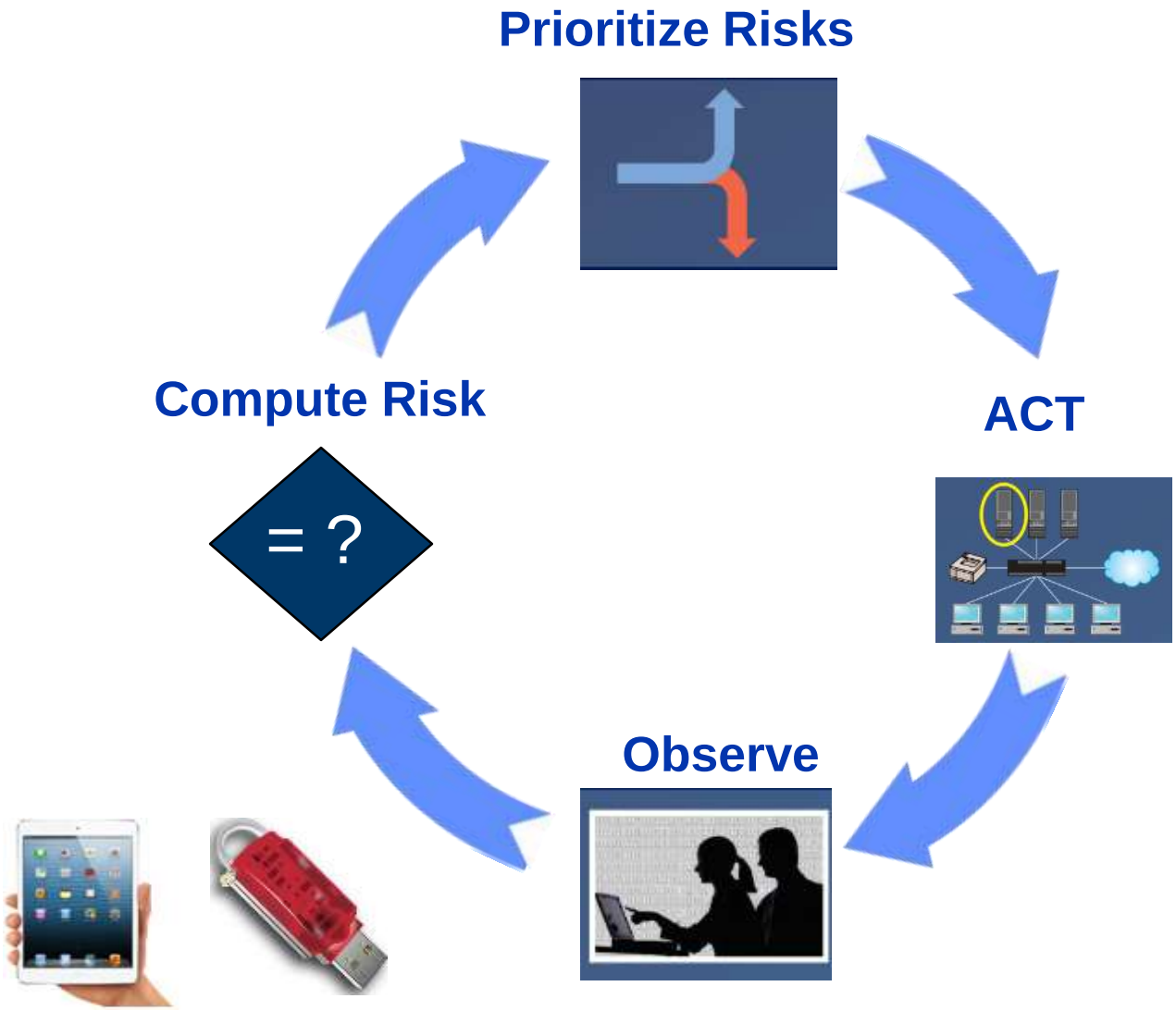


Initialize Desired State Specifications

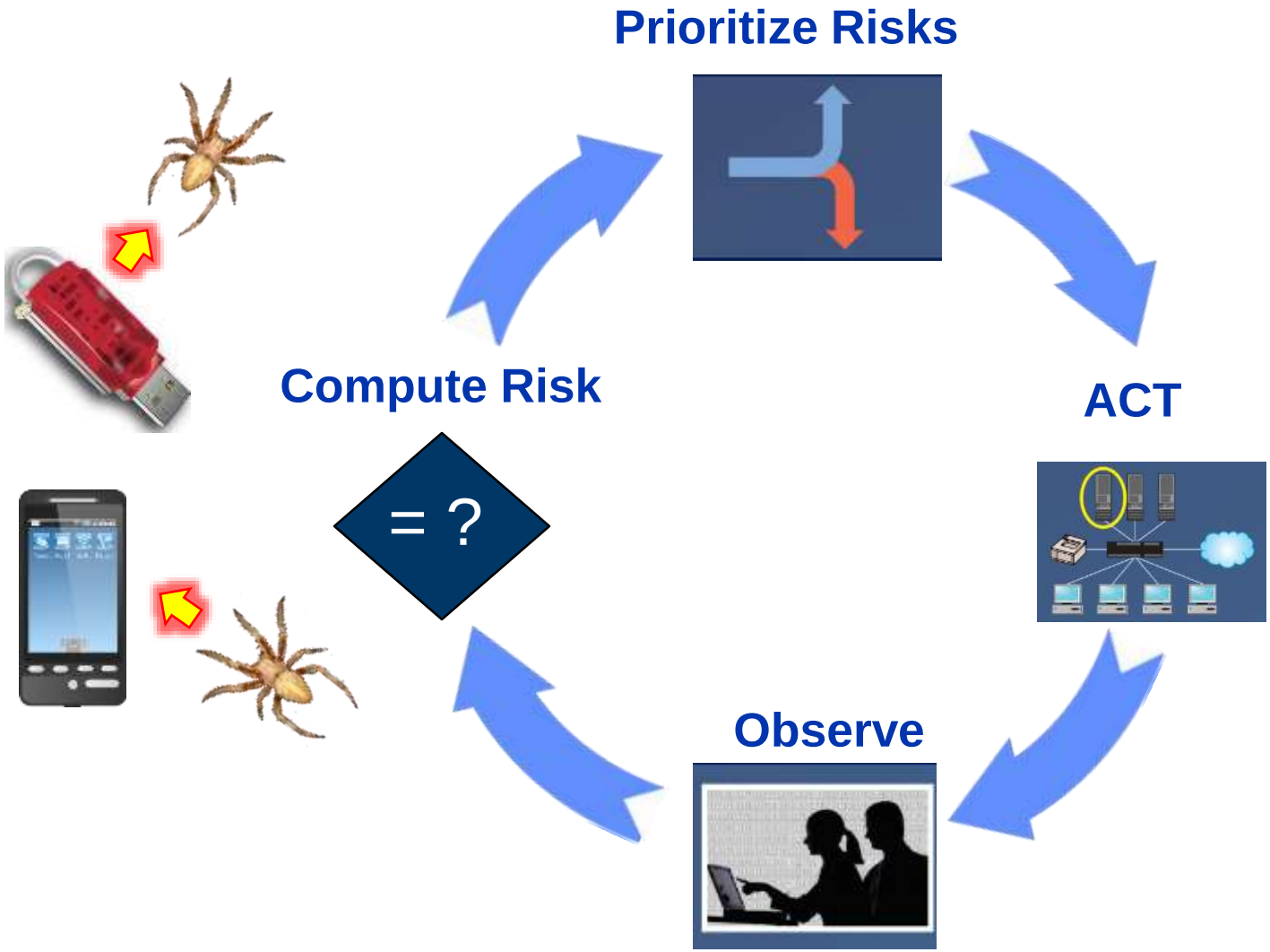
A Continuous Diagnostics and Mitigation (CDM) Process Controls Risk for Each Capability



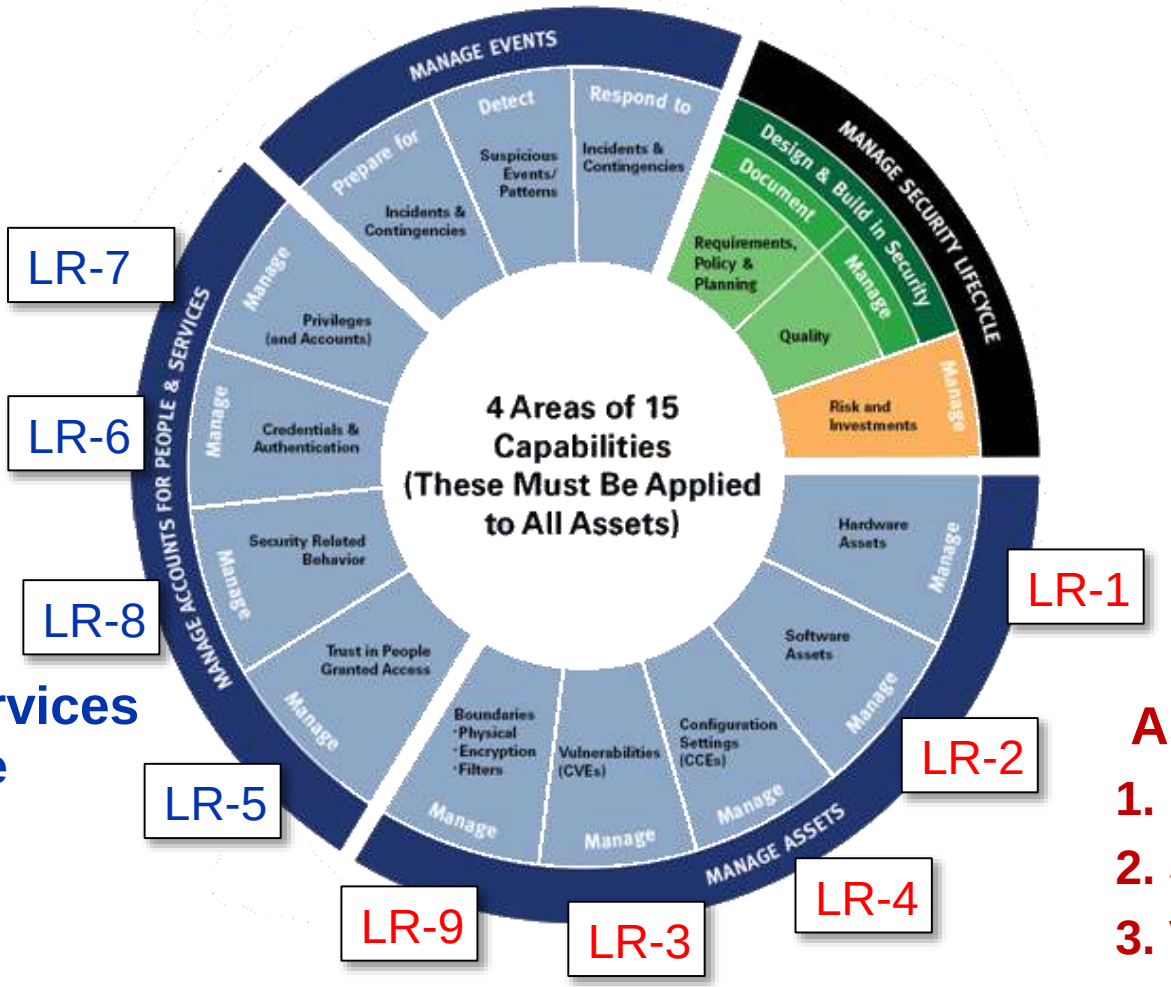
One Example is Managing the Use of Unauthorized Devices on a Network



Attackers can Either Observe and Compromise Insecure Devices or Spread from Already Infected Devices



We Have Created Metrics for Nine of Fifteen Capabilities



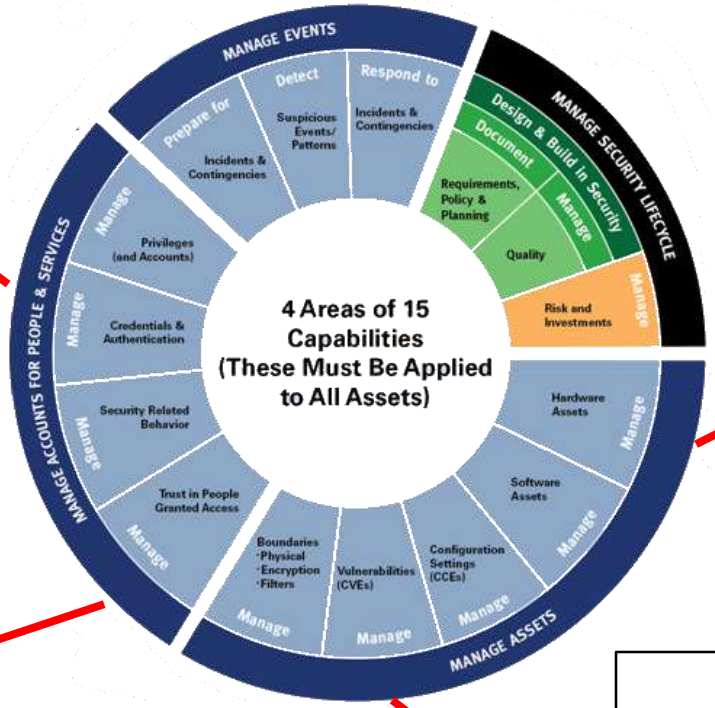
People and Services

5. Trust in People
6. Credentials
7. Accounts and Privileges
8. Behavior and Training

Assets

1. Hardware
2. Software
3. Vulnerabilities
4. Configuration
9. Boundaries

Each Metric Focuses on the Most Important Attack(s) for one Capability



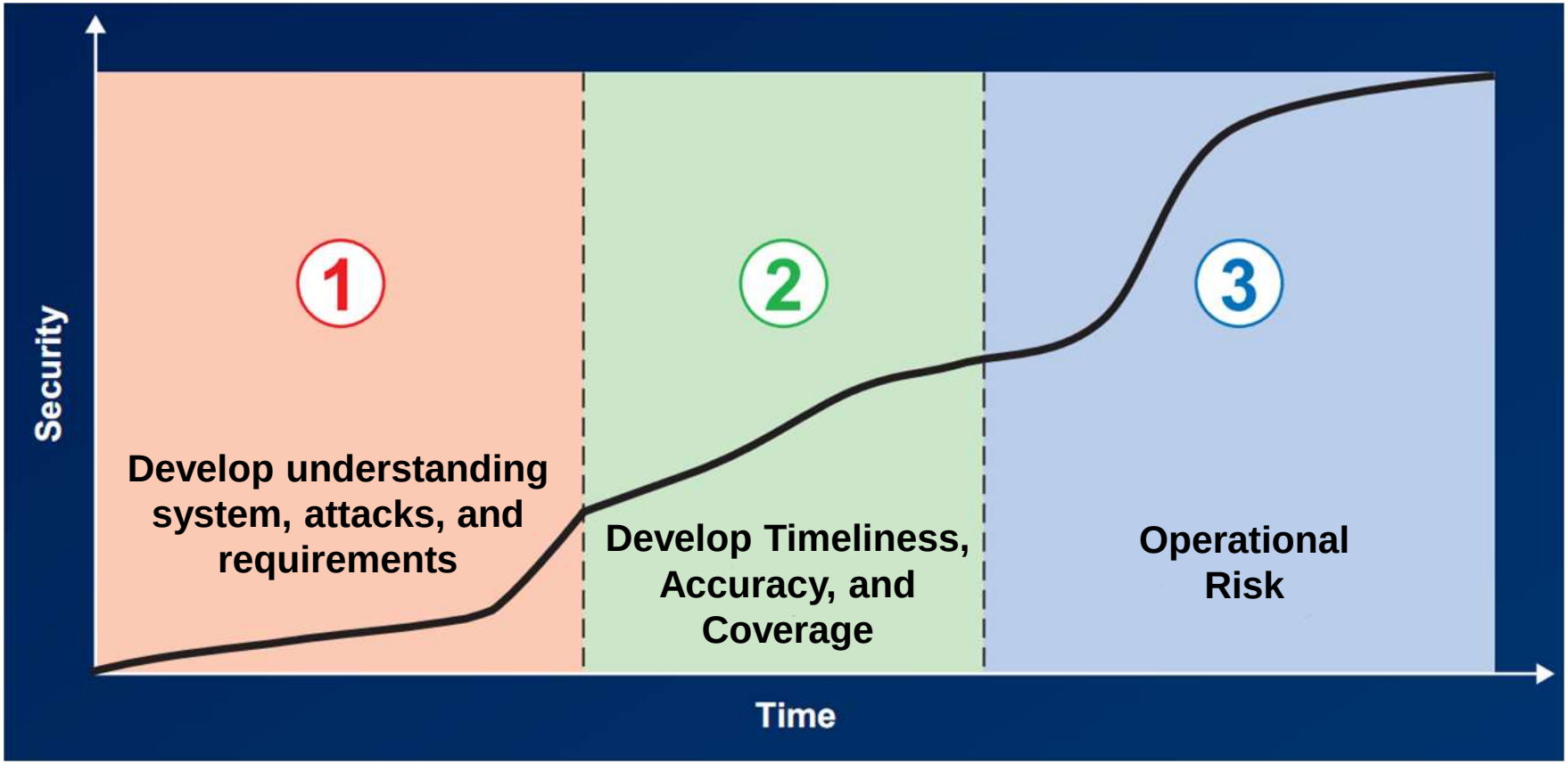
Client Side

Google

Java

Firefox

A Three-Stage Security Metric Maturity Model



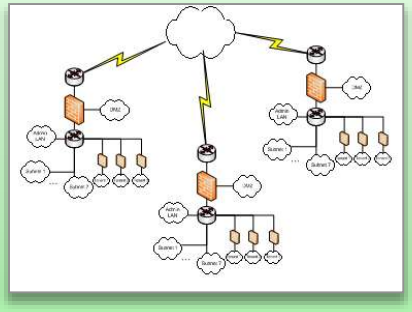
Checklist Metric

Capability Deficit Metric

Operational Risk Metric

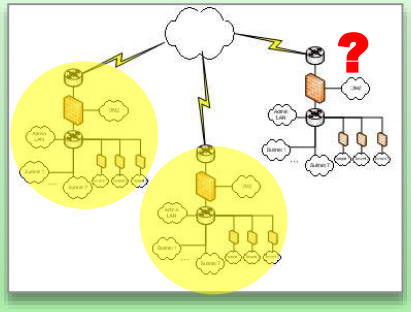
Level 2 Capability Deficit Metrics Determine If Risk Can Be Computed Accurately

Specification



Define what is required / permitted

Coverage



Perform measurements across all entities

There are few standard aspects to the Capability Deficit metric…

Timeliness

Observe frequently enough to reliably detect a short duration security event

Test Error

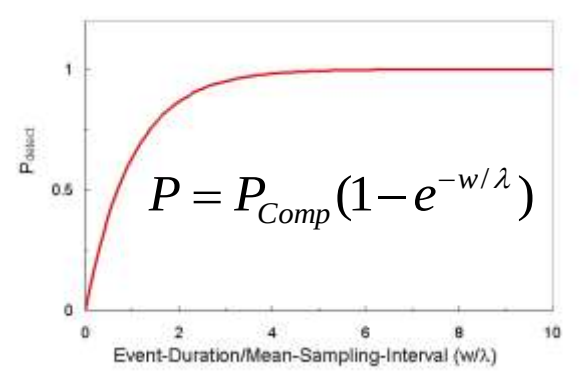
Insecure states are correctly classified

(no misclassification)

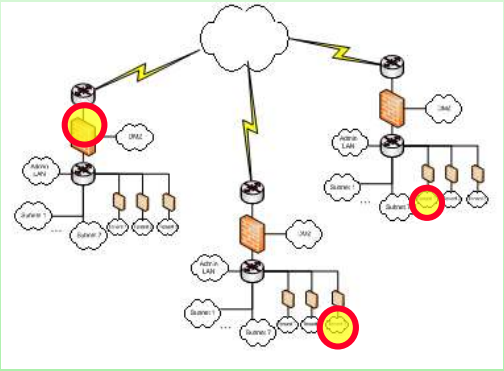
Level 3 Operational Risk Metrics Estimate the Risk Based on the Observed State

Risk = Probability of Successful Attack x Impact

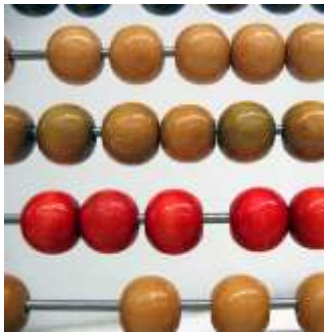
Compute Probability of Attack Success



Compute Attack Impact Based on Affected Devices



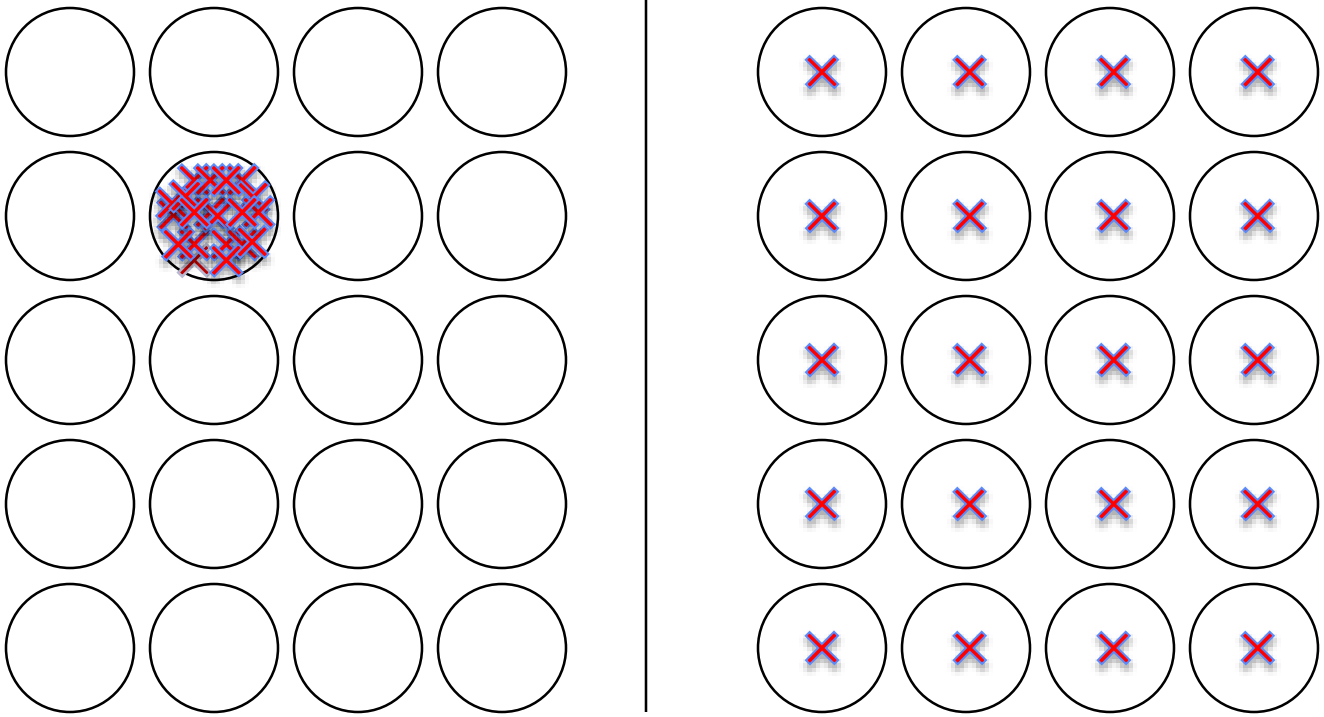
Existing Risk Metrics Can Not be Used in a Real-Time Diagnostic and Mitigation Loop



- Count- and percentage-based assessments do not model attackers correctly
  - Percentage of devices behind firewall / with anti-virus software
  - Mean / median lag of patch installation

- Other approaches are subjective and can't be automated
  - Annual Loss Expectancy = (Annual Rate)×(Loss)
  - Business Adjusted Risk = (Impact)×(Risk of Exploit)
  - Mission Oriented Risk and Design Analysis (MORDA)

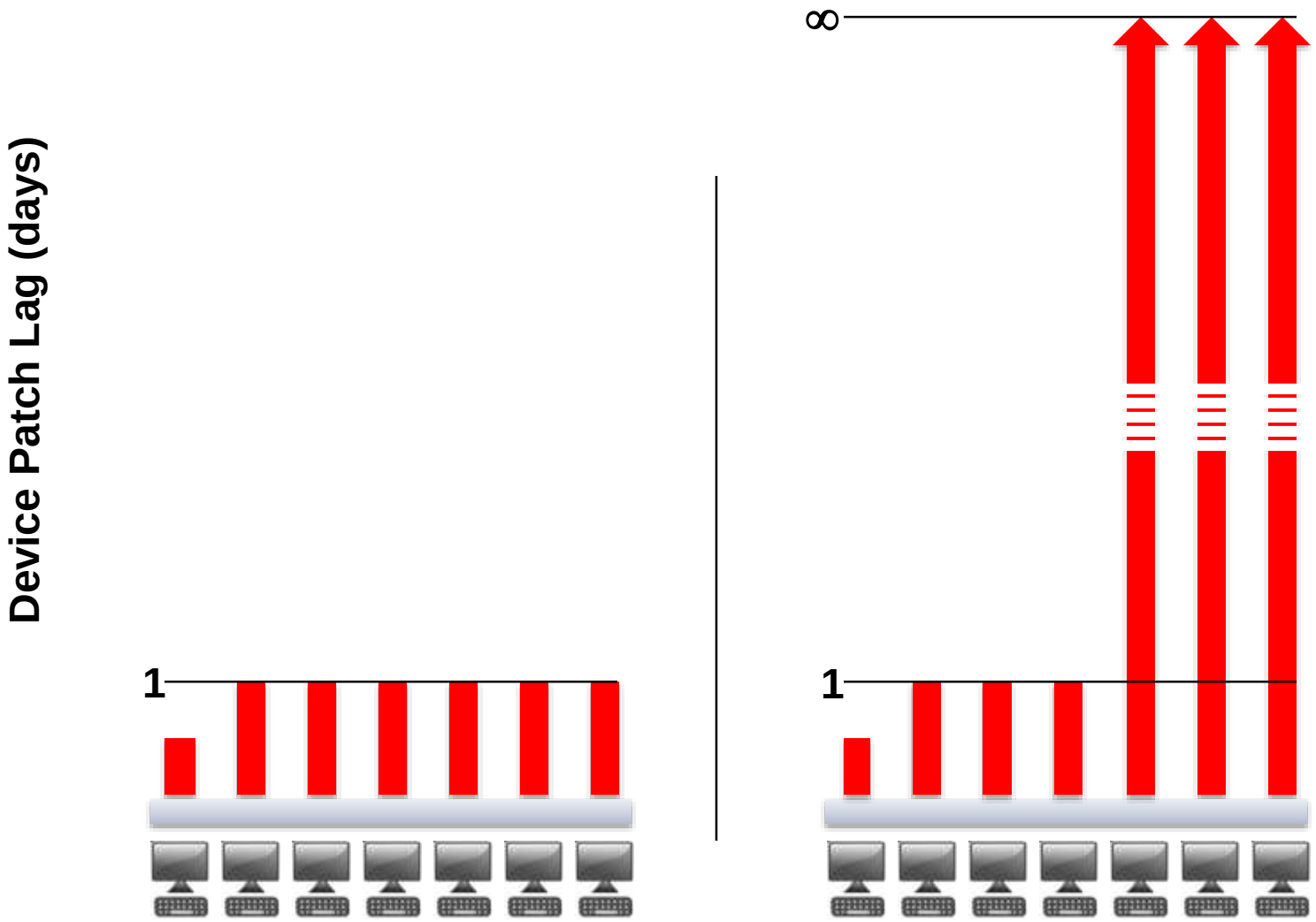
A Count of Serious Vulnerabilities Can be Misleading



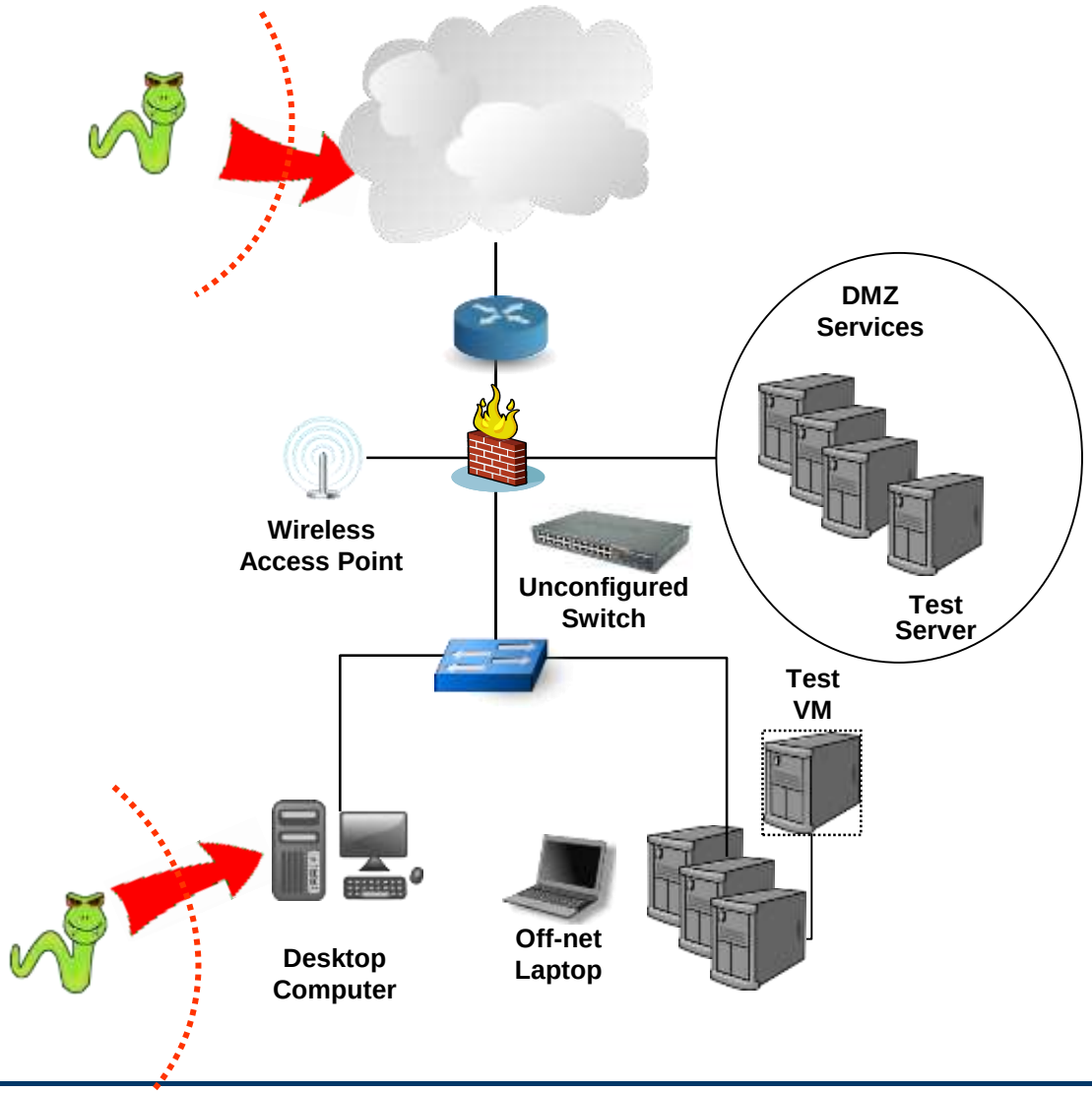
One machine with twenty serious vulnerabilities

Twenty machines each with one serious vulnerability

Median Patch Lag is Difficult to Interpret



One Attack Model in LR-1 is Attackers Looking for and Compromising Insecure Unauthorized Devices



- Assume unauthorized devices are unmanaged, hence vulnerable
- Attackers observe the network to look for these devices
- Attacker may be internal or external

Defenders Continuously Search for and Process Discovered Unauthorized Devices

Authorized Device List

Subnet	IP Addr	MAC
ALAN	10.1.2.3	aa:12:bb:34:cc:56
BLAN	10.4.5.6	cc:12:bb:34:cc:54
DMZ	18.9.2.14	2d:ab:99:ff:83:83

Discovered Device

Observe Network

Compare

In Authorized List

OK

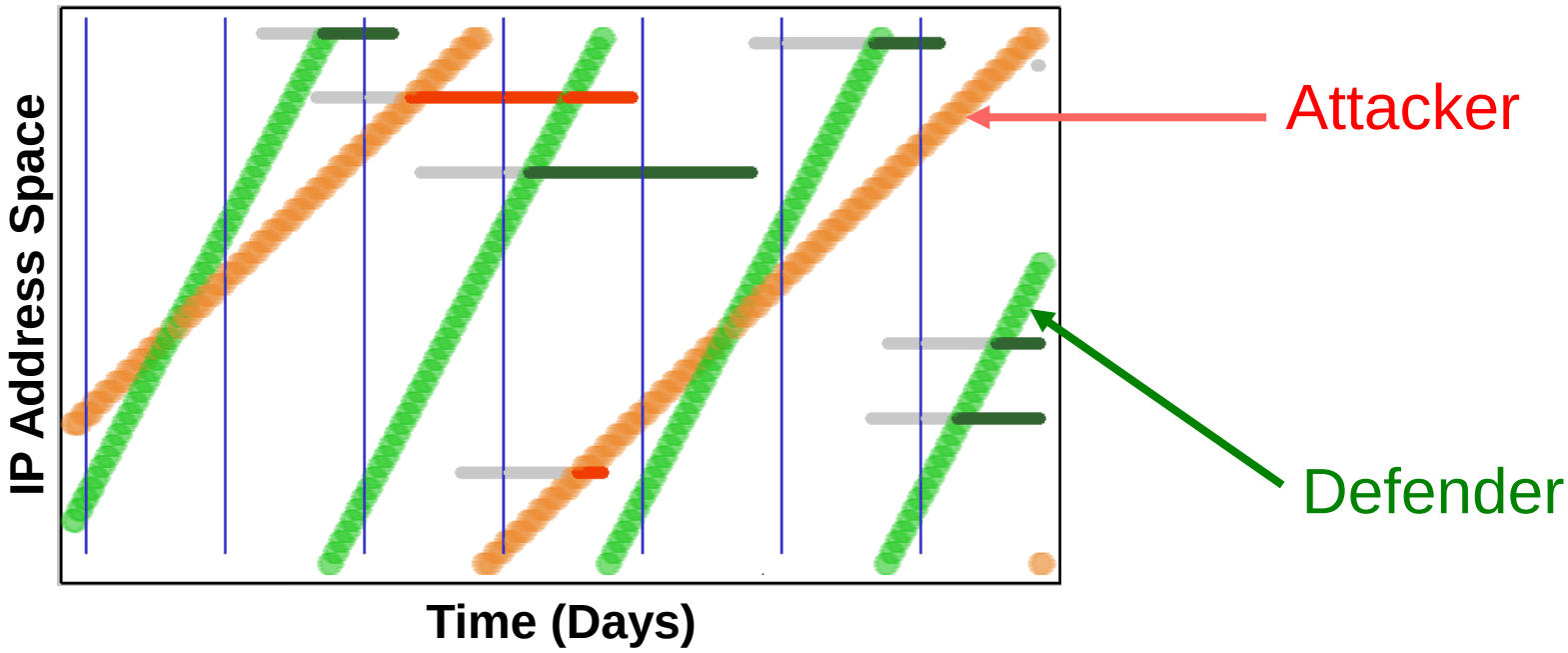
Not In Authorized List

Process

Authorize

Remove

We can Compute the Probability of Detecting a Finite Duration Event by Scanning

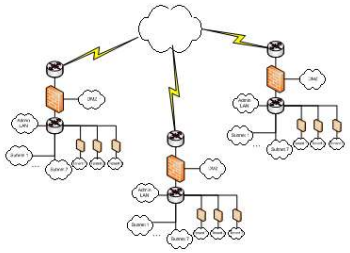


- **The probability of detection of an event of duration w with a scan interval δ is given by**

$$P_{\text{Observe}}(w,\delta) = \min\left(1, \frac{w}{\delta}\right)$$

LR-1 Capability Deficit Metric Components

Specification Deficit



$$SpecD_{subnet}(i) = 1 - I_{inventory\_specified}(i)$$

Coverage Deficit

$$CovD_{subnet}(i) = 1 - I_{covered}(i)$$

Timeliness Deficit

Probability of missing an event of a specified duration W

$$TimeD\left(W, \{\delta_j\}, i\right) = \sum_{i=0}^{n-1} \left[\frac{\max\left(0, \delta_{j+1} - \delta_j - W\right)}{\left(m_{\text{end}} - m_{\text{start}} - W\right)} \right]$$

Test Error

$$TestD = P_{miss}(i)$$

given the insecure condition was observed but not recognized

Overall Capability Deficit Metric

$$CD = 1 - (1 - TimeD) \cdot (1 - CovD) \cdot (1 - TestD) \cdot (1 - SpecD)$$

The LR-1 Operational Metric Is the Asset Value of the Expected Compromised Unauthorized Devices

Sum over all unauthorized devices of the probability of each being compromised

$$OM_{Unauth} = \sum_{\substack{Unauthorized \\ Devices}} AV \cdot P(Comp \mid Observed) \cdot P_{Observed}$$

Compute probability of attacker observing the unauthorized device from the window of presence and attacker scan rate

$$P_{\text{Observed}}(w, \Delta) = \min\left(1, \frac{w}{\Delta}\right)$$

w = Window of time unauthorized device is present

Δ = Attacker device sampling interval

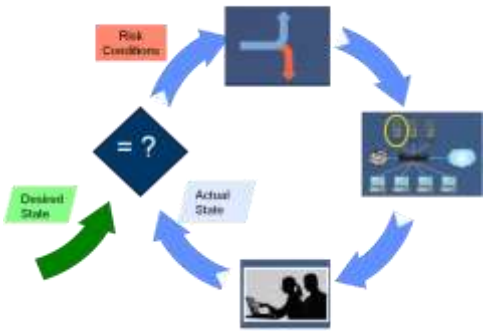
P(Comp|Observed) = Probability device is compromised given the it is observed by an attacker

AV = Asset Value for an unauthorized device

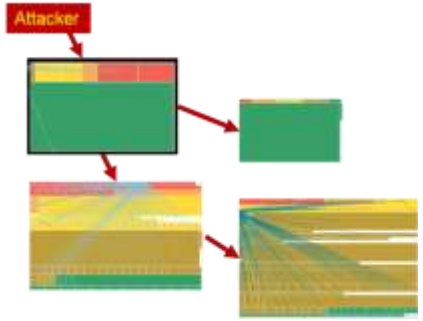
Summary

- The U.S. Department of Homeland Security (DHS) is implementing a Continuous Diagnostics and Mitigation (CDM) strategy for protecting government networks
- We will be creating metrics for 15 capabilities
- Each metric:
  - Includes up to date attacker models
  - Estimates risk from attackers
  - Includes a capability deficit component to determine if risk computations are accurate
- We are completing descriptions for the first nine metrics
- These will be used by the DHS to support continuous monitoring and risk mediation

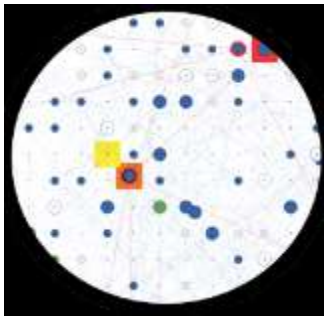
Roadmap for the Future



Continuous Diagnostics and Mitigation
(Accurate Continuous Observations,
Assess First-Step Risk,
Real-Time Operational Mitigations)



Attack Graph Analysis
(Assess Multi-Step Risk,
Prioritize and Evaluate Mitigations,
Assess Different Attackers)



Network Simulations
(Long-Term Modeling of Attacker
and Defense Strategies
and Policies)

Security Maturity Level →