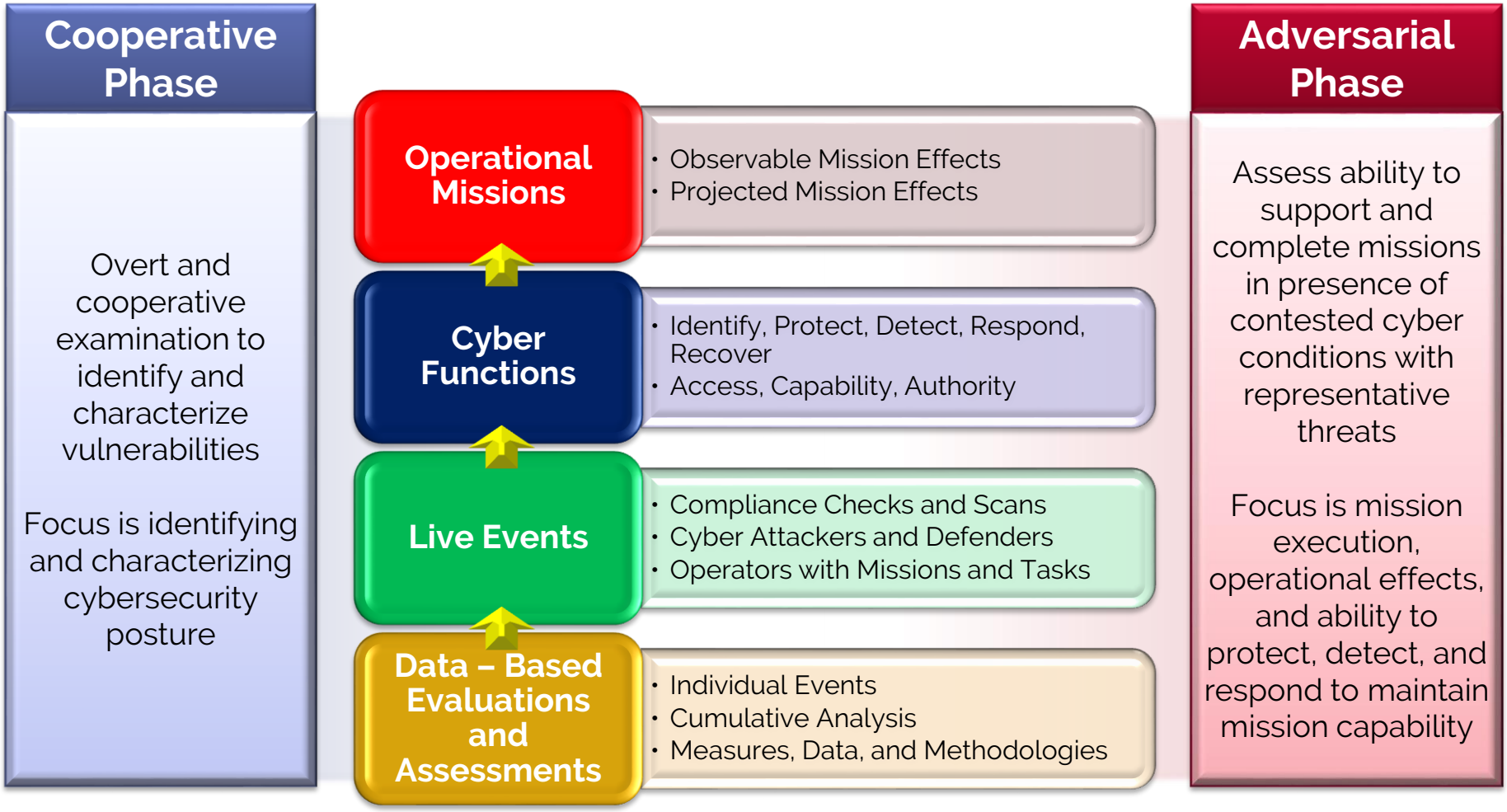
Method for Evaluating the Quality of Cybersecurity Defenses

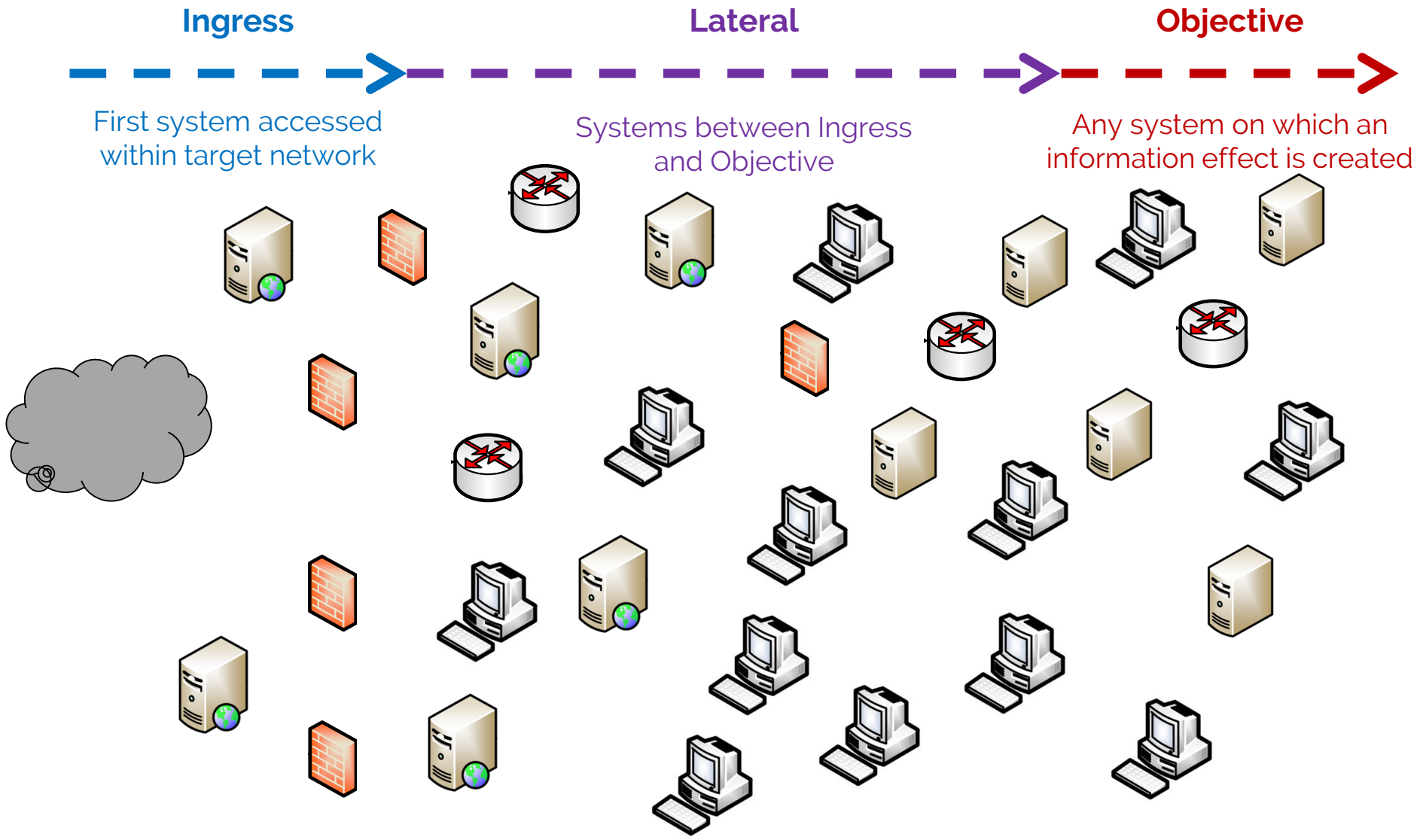
Shawn C. Whetstone
Vikram Kulkarni

March 21, 2018

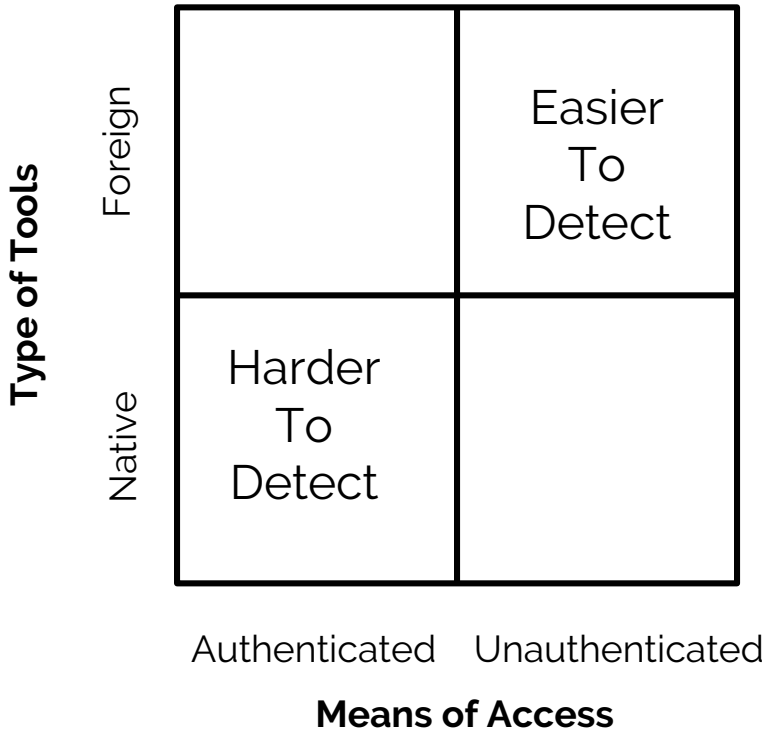
The Analytical Approach is Built from Data-Based Evaluations to Assess Cyber Effects on Operational Missions



Attacker as Part of the Test Team Enables Insights on Actions Taken Against Individual Systems



Defensive Strategy - Take Advantage of Easier-to-Detect Adversary Actions



Force More Detectable Types of Actions

Unauthenticated Access

Foreign Tools

Increase Detection Opportunities

Access Control Checkpoints

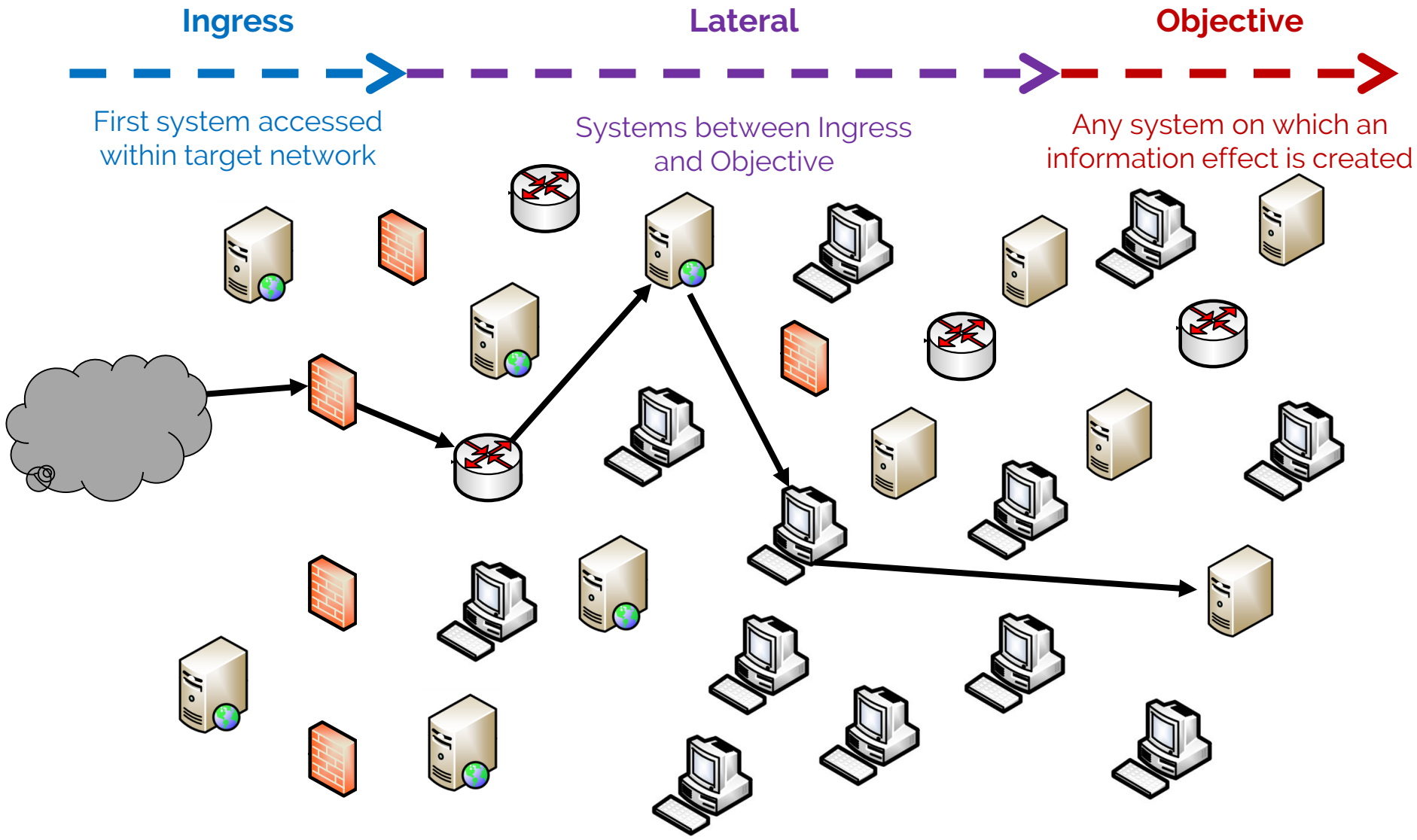
Means of Access

- **Authenticated:** Access to data and services achieved by presenting valid credential
- **Unauthenticated**: Access to data and services achieved without valid credential

Type of Tool

- **Native:** Action is completed using a tool that network owners authorize for use
- **Foreign**: Action is completed using a tool that network owners do not authorize for use

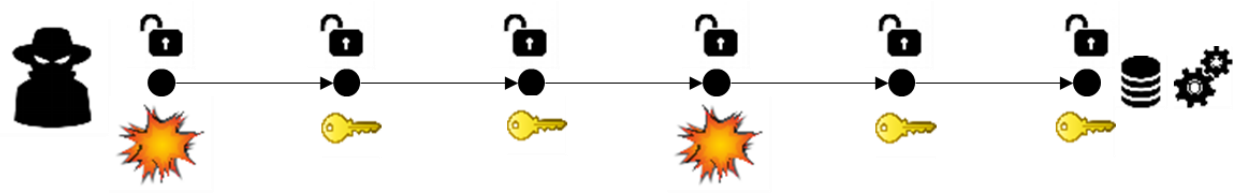
Attackers Also Provide Insights on How Individual Actions Link in Attack Threads



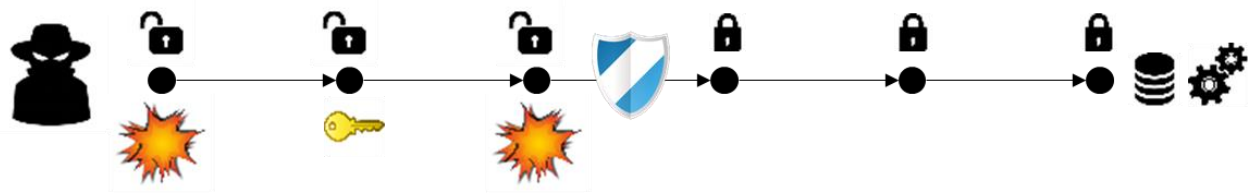
Evaluation Approach Considers Logically Completed Cyber Attacks

Attack threads: a logically connected series of adversarial activities starting at ingress and ending with

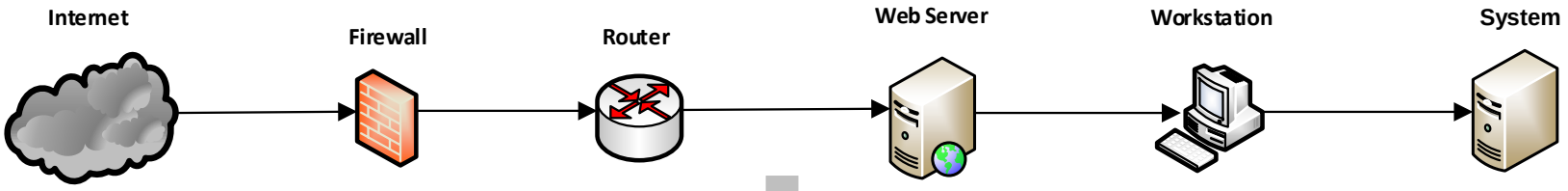
An effect on mission data or services



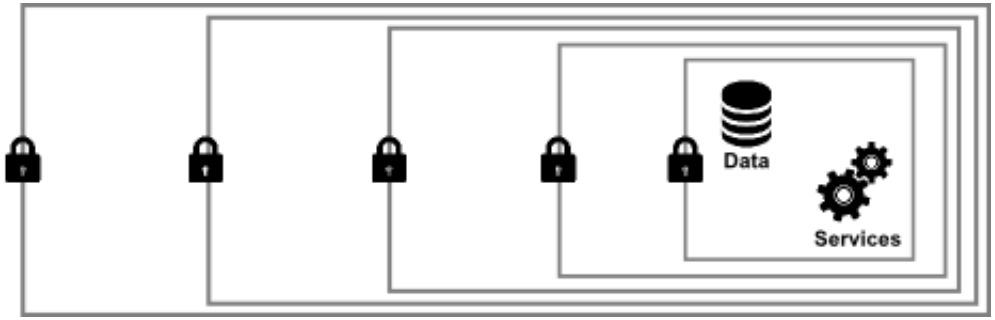
A successful defense



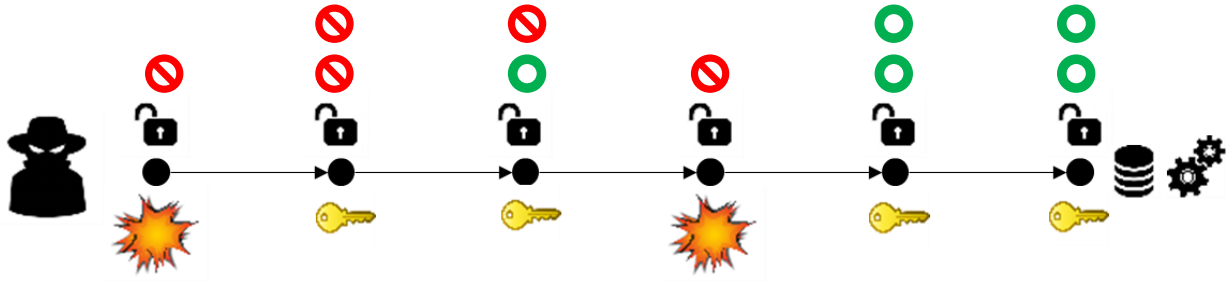
Conceptual Viewpoint for Cyber Attack Threads

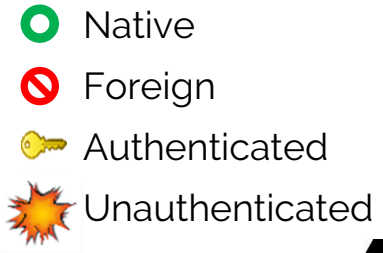


A series of checkpoints and actions that each provide an opportunity for defense



and through which the adversary progresses using
authenticated or unauthenticated means with native or foreign tools





Example Attack Thread

Access 1 – Workstation 1

- Boot from Kali Linux DVD
- Replace system files

Access 2 – Workstation 1

- Reboot to Windows gaining SYSTEM command prompt
- Query Domain for usernames, groups, privileges, file shares finding local administrator username

$$x = \frac{unauthenticated\ access\ attempts}{total\ access\ attempts} = \frac{2}{5} = 0.4$$

$$y = \frac{\#\ foreign\ tools\ used}{\#\ total\ tools\ used} = \frac{3}{10} = 0.3$$

Access 3 – Workstation 2

- Login as local administrator to workstation using guessed keyboard walk password
- Notice a domain administrator also is logged in, capture clear-text credentials from memory

Access 4 – Domain Controller

- Login to domain controller using domain administrator credentials
- Acquire and crack hashes for users, administrators throughout domain

Access 5 – Web Server

- Login to web server using cracked credentials
- Download and exfiltrate mission-critical documents

Authenticated
Unauthenticated
Native
Foreign

Analytical Approach is Conditional Probability to Detect using Two-Factor Logistic Regression

Binary Response: Detected/Undetected
Continuous Factor: Fraction of Unauthenticated Accesses in Thread
Continuous Factor: Fraction of Foreign Tools Used in Thread

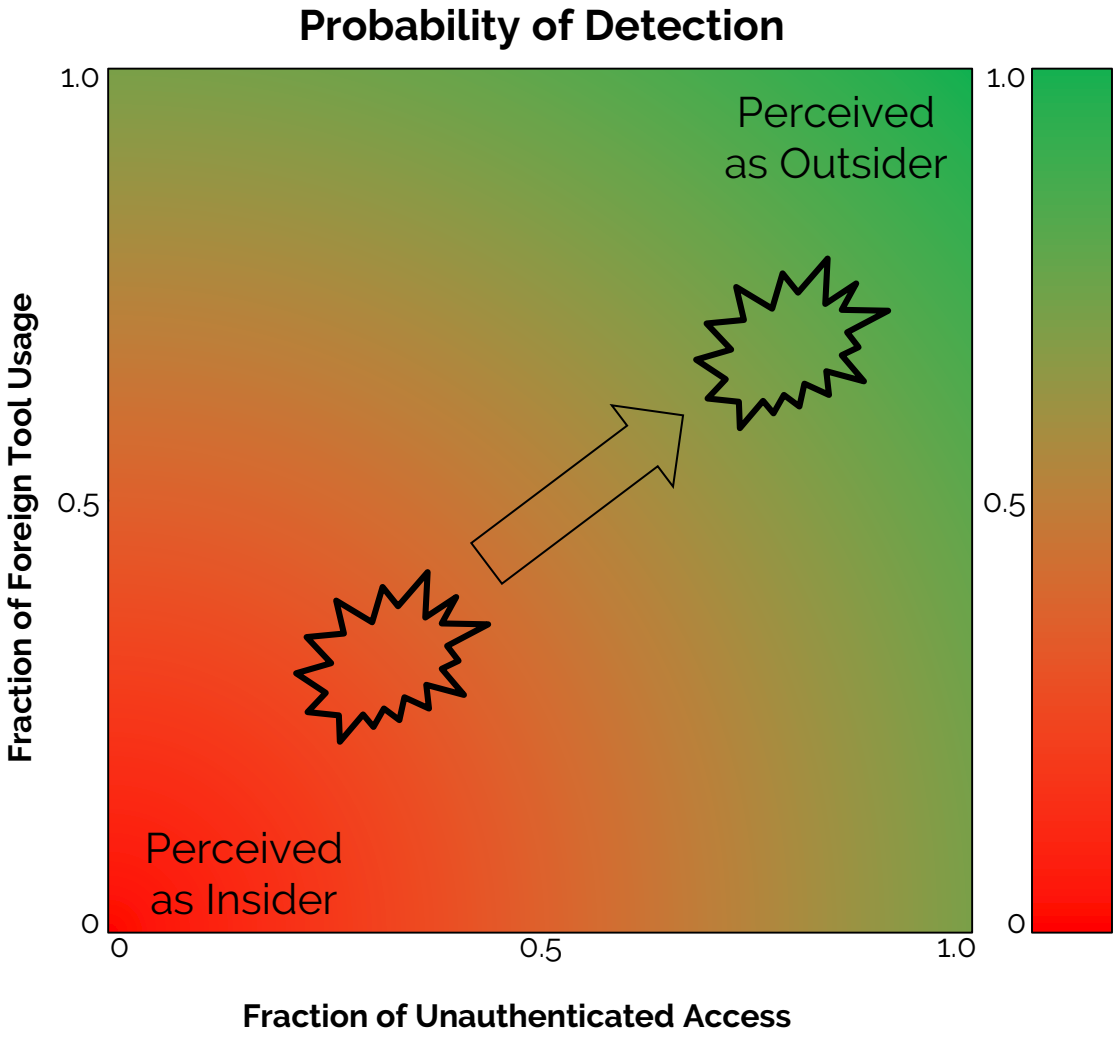
$$P(Detect|x,y) = \frac{e^{f(x,y)}}{1+e^{f(x,y)}}$$ Conditional Probability to Detect

$$f(x,y) = \underbrace{\beta_0 + \beta_1 x + \beta_2 y}_{\text{Linear Terms}} + \underbrace{\beta_{1,2}(x-\bar{x}) * (y-\bar{y})}_{\text{Interaction Term}}$$

$$x = \frac{unauthenticated\ access\ attempts}{total\ access\ attempts} \qquad \text{y} = \frac{\#\ foreign\ tools\ used}{\#\ total\ tools\ used}$$

(for each thread)

Two-Factor Model Provides Insights on Detection Performance

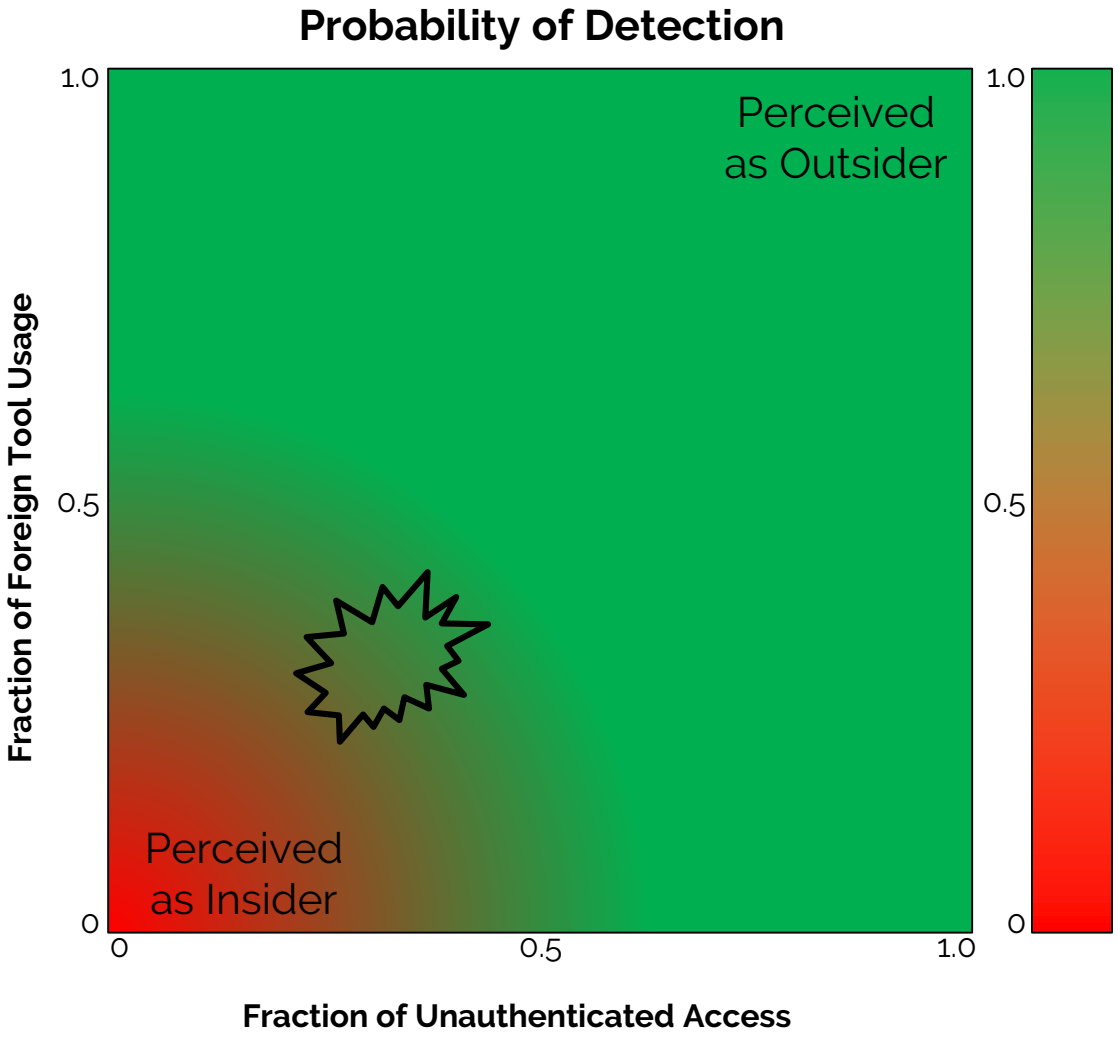


Regions of Perception

"Safe" Operating Space for Attacker

Modify Attacker Options or Behavior

Two-Factor Model Provides Insights on Detection Performance



Regions of Perception

"Safe" Operating Space for Attacker

Modify Attacker Options or Behavior

Improve Defenses to Shrink Safe Operating Space

Method of Simple Two-Factor Model Proved Useful in Analysis of Cyber Attacks in Assessments

Insights from Analytical Approach

- Confirmed that detection improving but not perfect
- Mapped detection strengths and weaknesses
- Insights into areas and specific actions to force behavior changes
- Revealed anomalous performance region and cause

Future Efforts

- Explore performance effects from actions to force behavior changes and improve detection
- Expand to additional factors and responses
- Explore implications for test procedures and designs