# Breach Preparedness

Kevin Hamako – DHS/HSI Investigator

Justin Edgar – Security Systems Engineer

# Outline

- Introductions
- Bottom Line Up-Front
- Attack Lifecycle
- Incident Response; What and Why
- Attack Lifecycle
- Preparing for the Inevitable; How
- Summary

# Introductions

- Kevin Hamako
  - DHS/HSI Special Agent
  - Cyber intrusion investigations group, San Diego
  - Counter-proliferation background
  - AF veteran

# Introductions

- Justin Edgar
  - Mandiant / FireEye Veteran
  - Product Consulting / Training
  - EY Alum
  - Army Veteran
  - Hubs/Daddy/etc.,

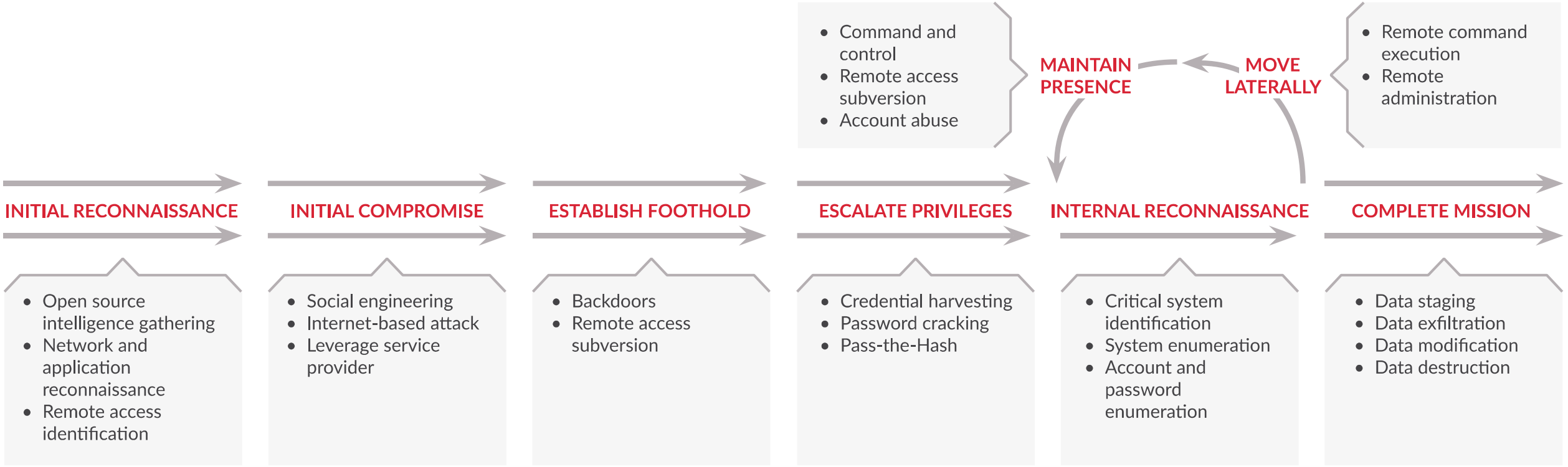

# B.L.U.F.

- Incident response is an attainable capability.
- Short-term instrumentation facilitates near-term operationalization.
- Skilled personnel can be “outsourced” while internal assets are trained.

# Attack Lifecycle

- Not all breaches are the same
  - Attacker types and motivations
    - Data theft
    - Reputation effect
    - Financial gain
    - Corporate competition
  - Attribution (or not)
  - Prosecution (or not)

# Attack Lifecycle

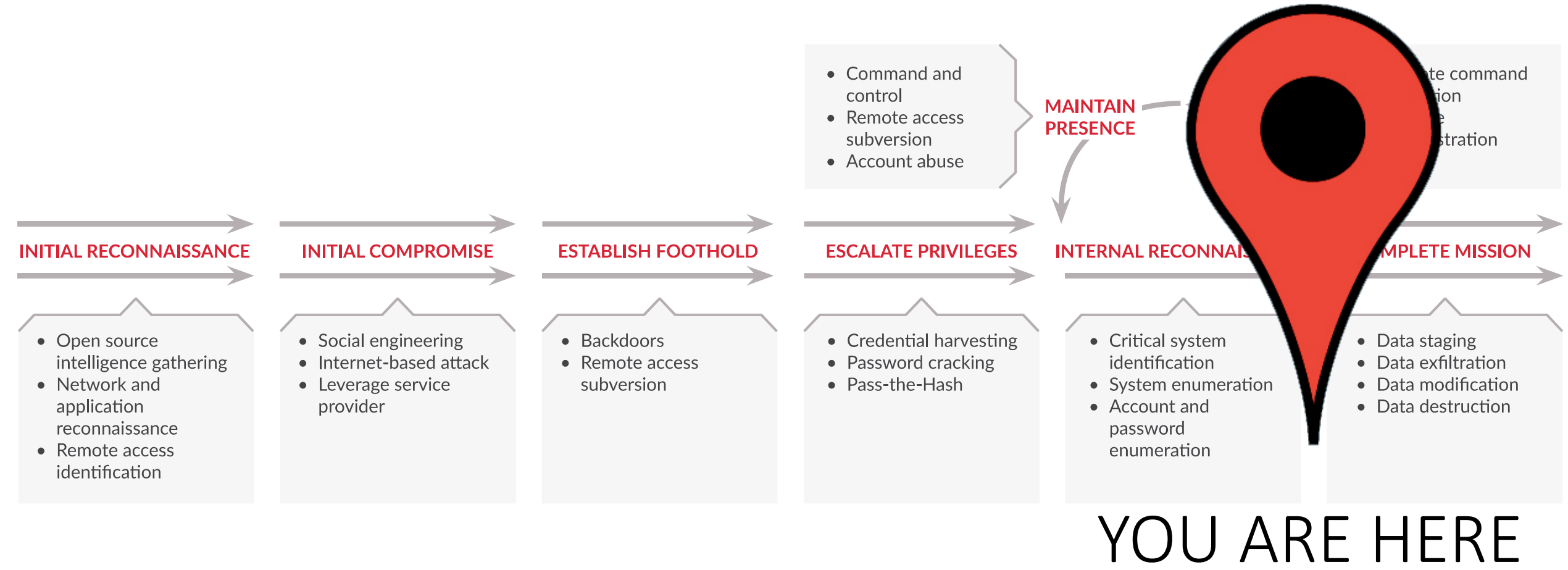



**69** % OF COMPANIES NOTIFIED OF BREACH BY EXTERNAL ENTITY

**32** DAYS TO BEGIN BREACH RESPONSE

**205** MEDIAN NUMBER OF DAYS BEFORE DETECTION

# Attack Lifecycle




YOU ARE HERE

**69** % OF COMPANIES NOTIFIED OF BREACH BY EXTERNAL ENTITY

**32** DAYS TO BEGIN BREACH RESPONSE

**205** MEDIAN NUMBER OF DAYS BEFORE DETECTION

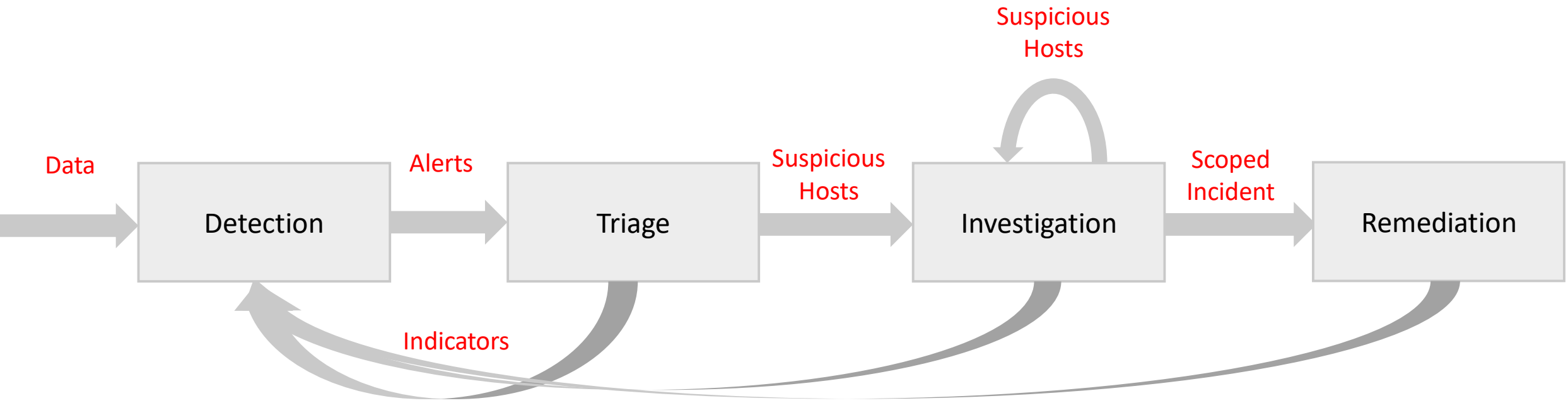
# Notification Process

- Common Scenario and Flow
  - Incident response / investigation at victim
  - Investigation identifies adversary infrastructure (domain, IP)
  - Court order yields historical or current netflow from adversary infrastructure
  - Netflow identifies connections to other possible victims
  - Victim notification
    - IOCs based on infrastructure we're watching
    - Adversary background
    - TTPs we observed at previous victim

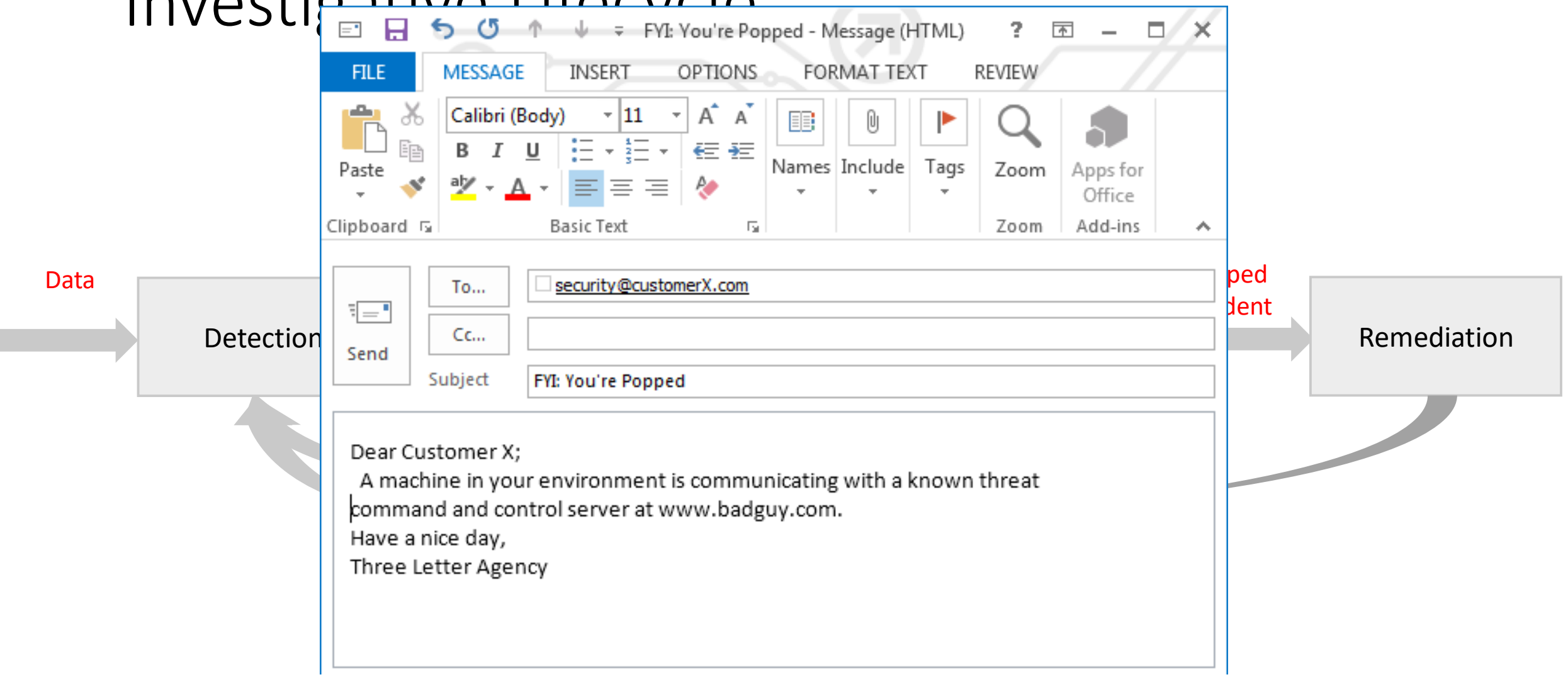
# Incident Response: The “What” and “Why”

- Telling the breach story
  - Compile artifacts
  - Create logical connections
    - Zoom in / zoom out
    - Temporal and physical associations
- Internal and external requirements
  - Compliance
  - Breach notification regulations
  - Incident scoping

# Investigative Lifecycle



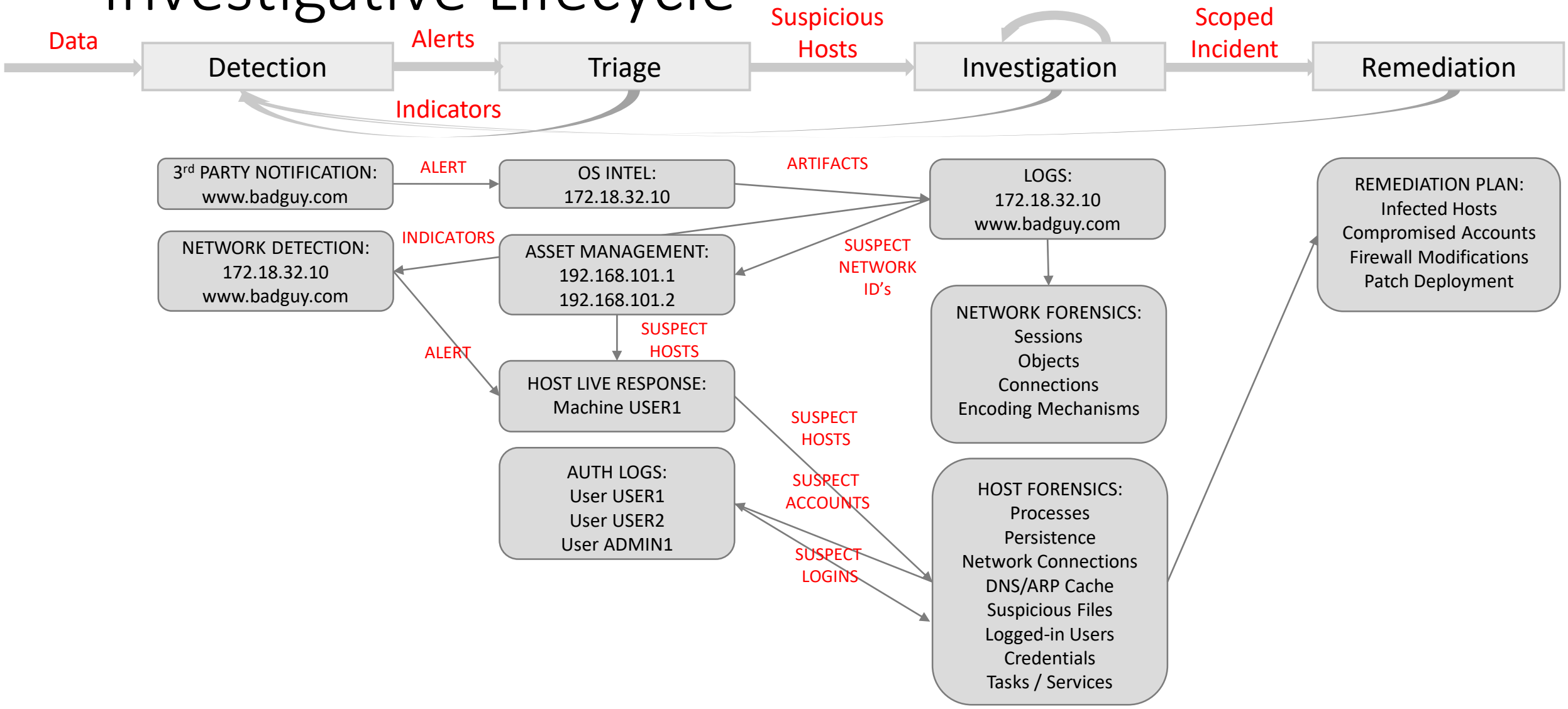
# Investigative Lifecycle



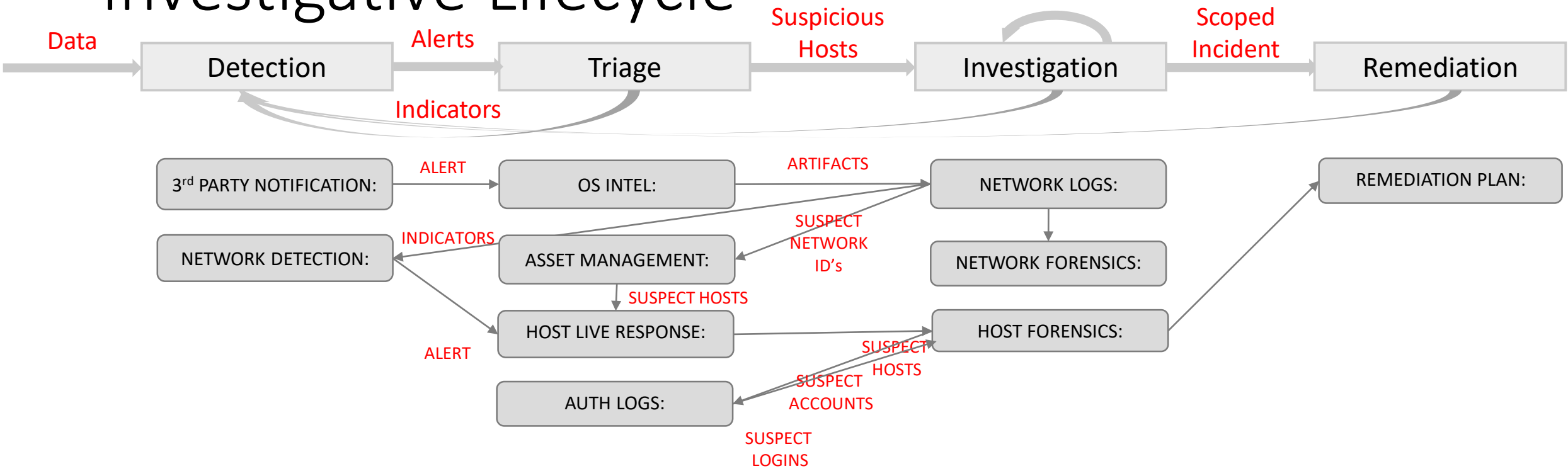
# Incident Response: “How”

- Instrumentation
  - Indicator application
    - Network
    - Host
  - Historical queries
    - Connections
    - Authorizations
    - Asset attribution
    - Detections?
  - Comprehensive examination
    - Network
    - Host
- Skillsets
  - Network
    - Derive and apply indicators
    - Review packet capture
  - Host
    - Collect forensic data
    - Derive and apply indicators
  - Intelligence
    - Understand threat MO
    - Communicate hypotheses
    - Build and tell the story
      - Defeat cognitive bias

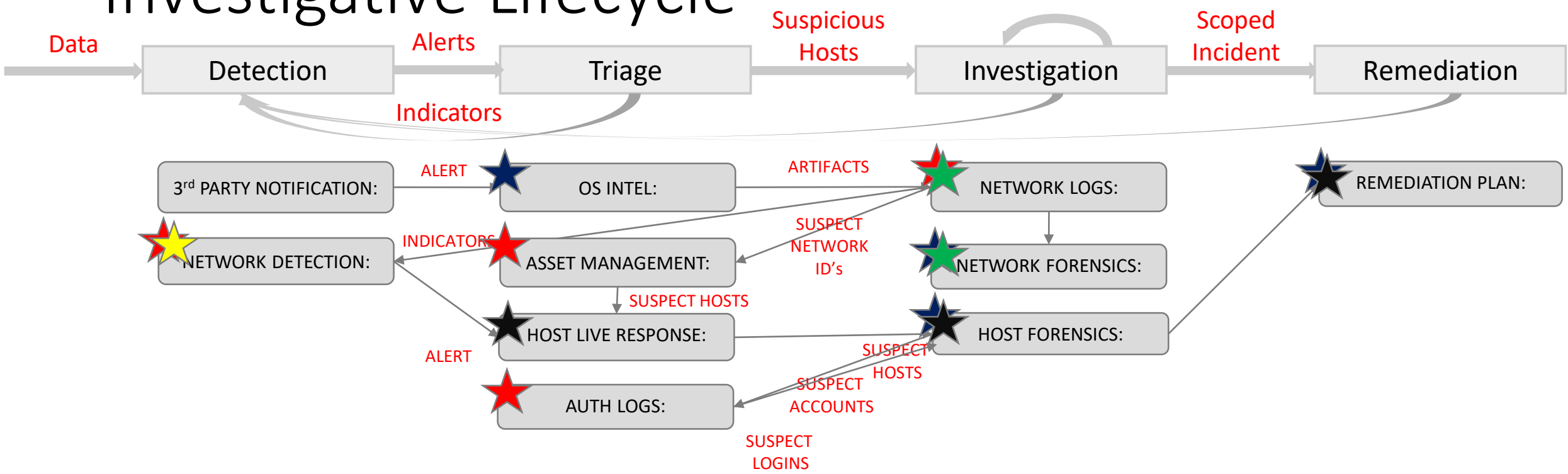
# Investigative Lifecycle



# Investigative Lifecycle



# Investigative Lifecycle




| Logging: | Detection: | Intel Feed: | Network Forensics: | Host Forensics: |
|---|---|---|---|---|
| Network transactions | Network indicators | Network indicators | Connections | Triage |
| Asset attribution | Host indicators | Host indicators | Packets | Live response data |
| Authorization | | Threat TTPs | Session contents | Timeline |
| | | Threat motivations | C2 de-obfuscation | File acquisition |
| | | | | Remediation? |

# Skillsets for Incident Response

- Host forensic skills
  - Live data collection and analysis
  - Memory collection and analysis
  - File system timeline analysis
  - SANS FOR508: Adv. Digital Forensics, Incident Response, Threat Hunting
- Network forensic skills
  - Netflow and PCAP collection and analysis
  - Log aggregation and analysis
  - Protocol understanding
  - SANS FOR572: Adv. Network Forensics and Analysis

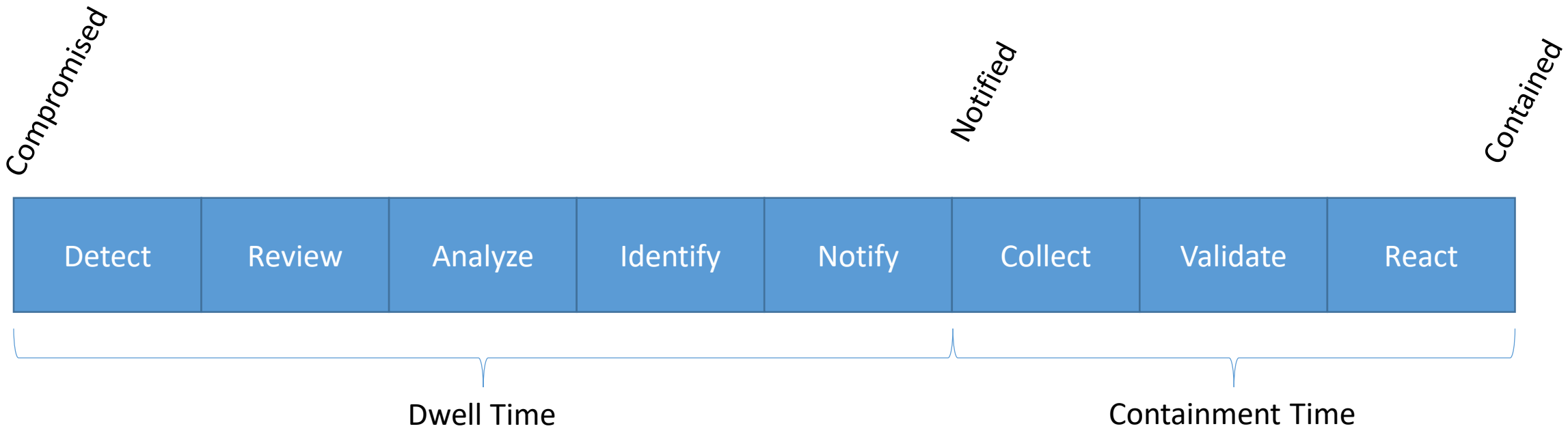
# Summary

- Incident response is an attainable capability.
- Short-term instrumentation facilitates near-term operationalization.
- Skilled FTEs can be “outsourced” while internal assets are trained.

# Questions

# BACKUP SLIDES

# DRAIN CVR


Compromised
Notified
Contained
Detect
Review
Analyze
Identify
Notify
Collect
Validate
React
Dwell Time
Containment Time