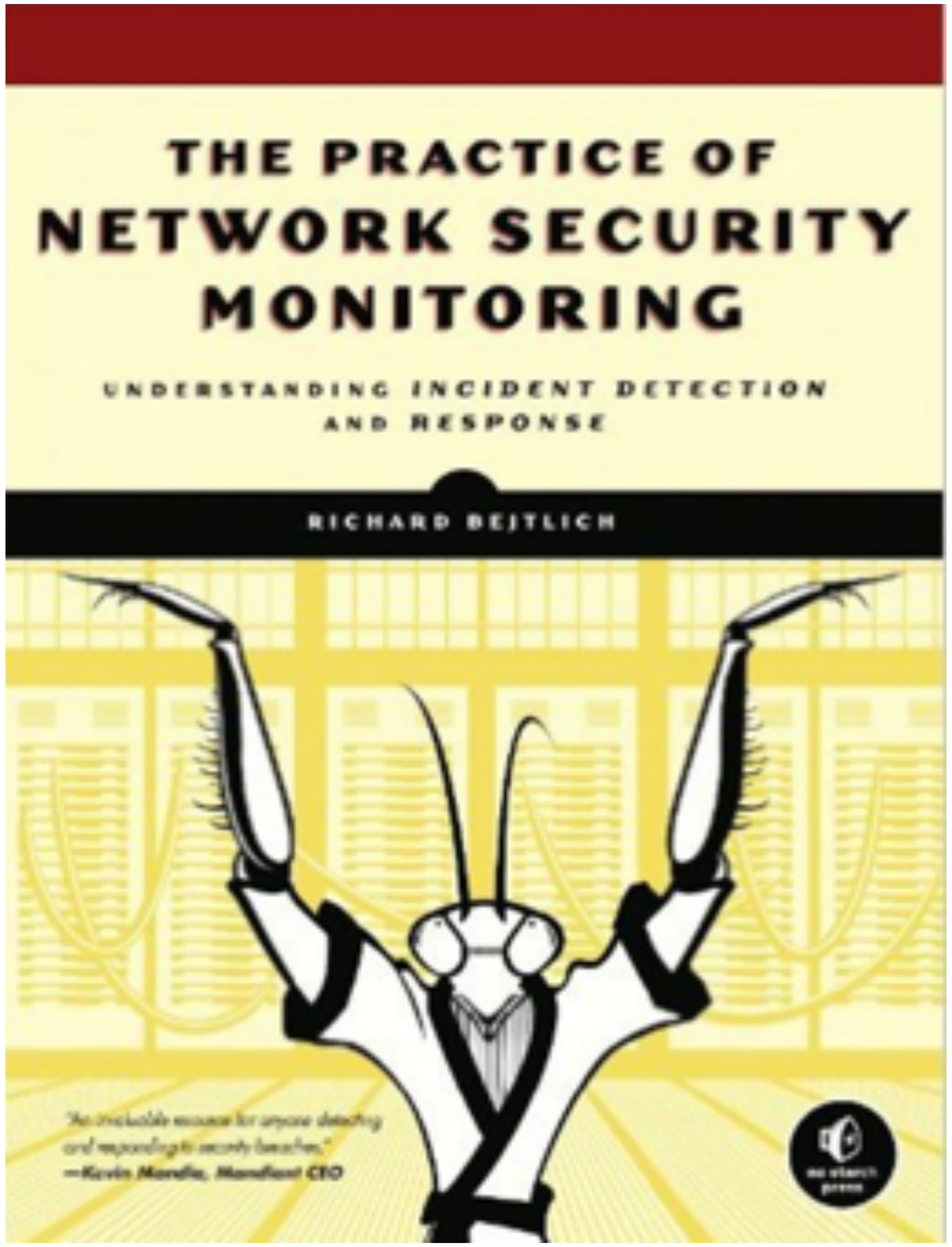
CNIT 50: Network Security Monitoring

9 NSM Operations


THE PRACTICE OF NETWORK SECURITY MONITORING
UNDERSTANDING INCIDENT DETECTION AND RESPONSE
RICHARD BEJTLICH
"An invaluable resource for anyone detecting and responding to security breaches."
—Kevin Mandia, Mandiant CEO
no starch press

Topics

- **The Enterprise Security Cycle**
- **Collection, Analysis, Escalation, and Resolution**
- **Remediation**

Introduction

- Methodology is more important than tools
- Don't specify roles by tools
  - SIEM tem, AV team, DLP team
- Give teams missions
  - They will find or build tools as needed

The Enterprise Security Cycle

Four Phases

- Planning
- Resistance
- Detection
- Response

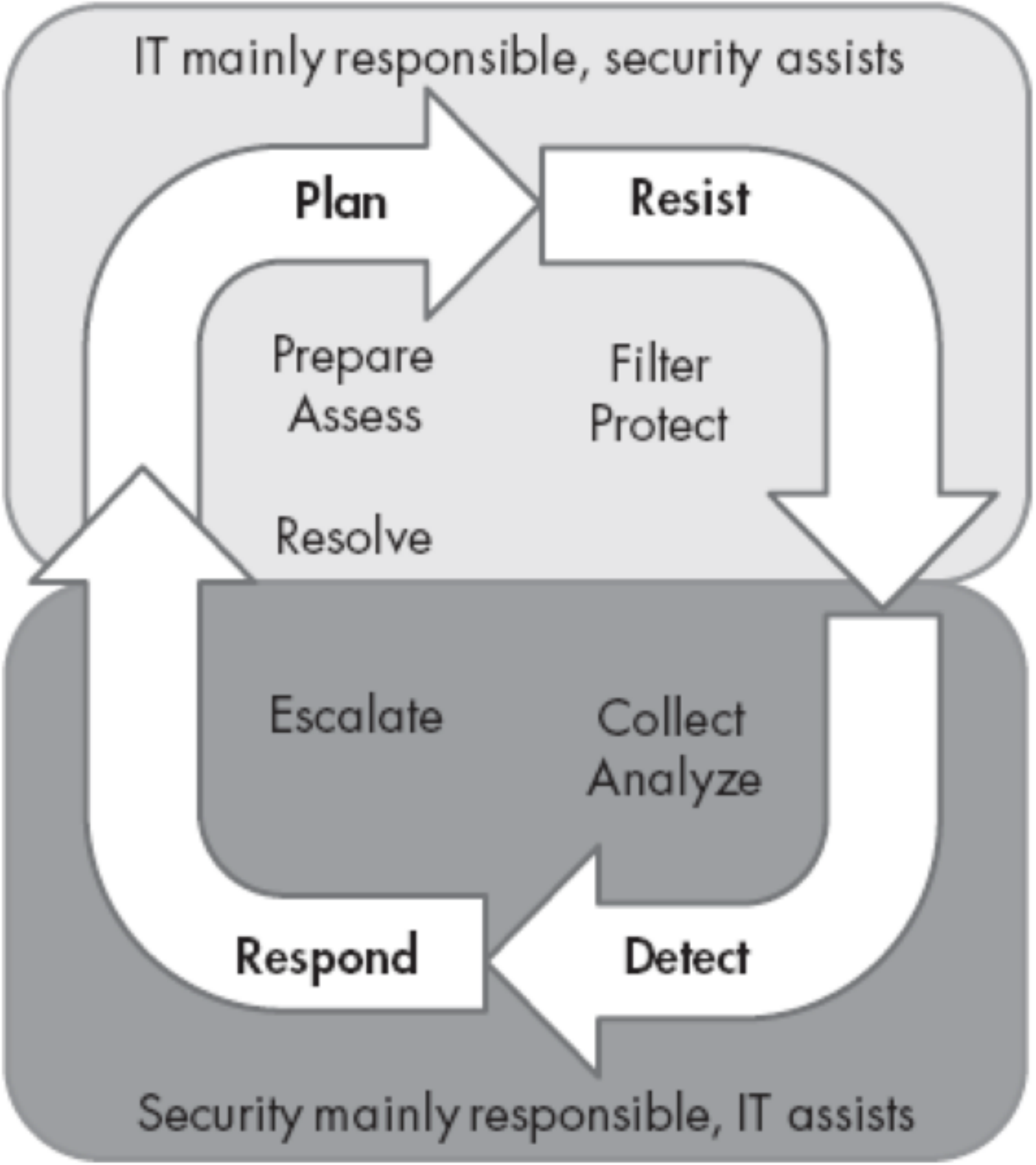

IT mainly responsible, security assists
Plan
Resist
Prepare
Assess
Filter
Protect
Resolve
Escalate
Collect
Analyze
Respond
Detect
Security mainly responsible, IT assists

Figure 9-1. Enterprise security cycle

Planning

- **Goals**
  - Position organization to resist intrusions
  - Counter weaknesses being exploited by intruders
- IT and Security teams **prepare** and **assess** situation

Planning

- **Preparation**
  - Budgeting, auditing, compliance checks, training, secure software development
- **Assessment**
  - Adversary simulation, penetration testing, red teaming

Resistance

- **Filter** and **protect**
- Automated countermeasures
    - Firewalls, antivirus, data-leakage protection, whitelisting
- Administrative countermeasures
    - Security awareness training, configuration and vulnerability management

Detection and Response

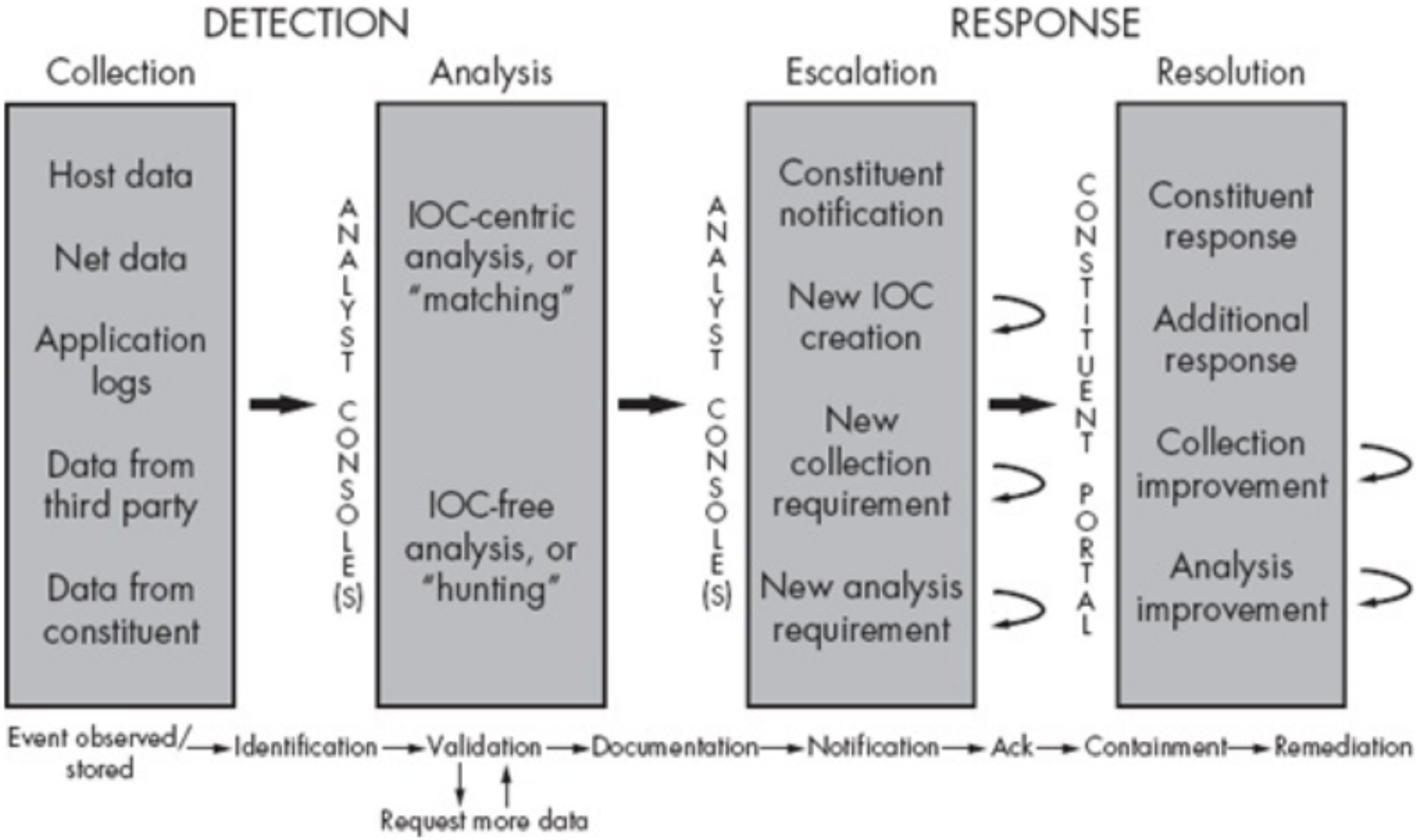


Figure 9-2. NSM process

Collection, Analysis, Escalation, and Resolution

Collection, Analysis, Escalation, and Resolution

- **Collection**
  - Gathering data required to decide if activity is normal, suspicious, or malicious
- **Analysis**
  - Validating what we suspect about the status of an event. Two types of analysis: focused on Indicators of Compromise (IOCs" and not

Collection, Analysis, Escalation, and Resolution

- **Escalation**
  - Notifying a constituent about the status of a compromised asset
- **Resolution**
  - Action taken by a constituent or security team member to reduce the risk of loss

Collection

- **Technical processes**
  - Endpoints or hosts, including computers, servers, mobile devices, etc.
  - Network
  - Logs created by applications, devices, and related sources
- **Nontechnical collection processes**
  - Third parties like partners law enforcement, intelligence agencies
  - Constituents

Technical Sources

- Commercial platforms like **Mandiant for Intelligent Response (MIR)** which asks questions of endpoints via software
    - Enables CIRTs to *sweep* the enterprise for signs of intruder activity
    - Conduct targeted analysis of potential victim computers
- Commercial version of **F-Response**
    - Basic remote access to hard drives and RAM
    - Native windows tools such as Windows Management Instrumentation Command-line (WMIC) and SysInternals psexec

Network Collection

- Tools we've covered collect network-derived data
- Layers of interpretation transform raw network information into indicators of compromise
- Application logs like Apache and antivirus are a primary source of technical data

Log Collection Requirements

- **Log source** creates application data
- **Log collector** accepts and stores the data
- **Transport method** moves logs from source to collector
- Ex: ELSA might collect logs from a proxy server, and syslog might be the transport method

Host Data

- Host data is often acquired on demand
- Different from logs that are created by a regularly scheduled process
- MIR can remotely query for host data
    - Like a mutex in memory or an artifact in Windows Registry

Nontechnical Sources

- Only 1/3 of intrusions are detected by the attacked organization

- The other 2/3 learn about them from external parties

- Reports from users are often critical

  - Such as phishing attempts

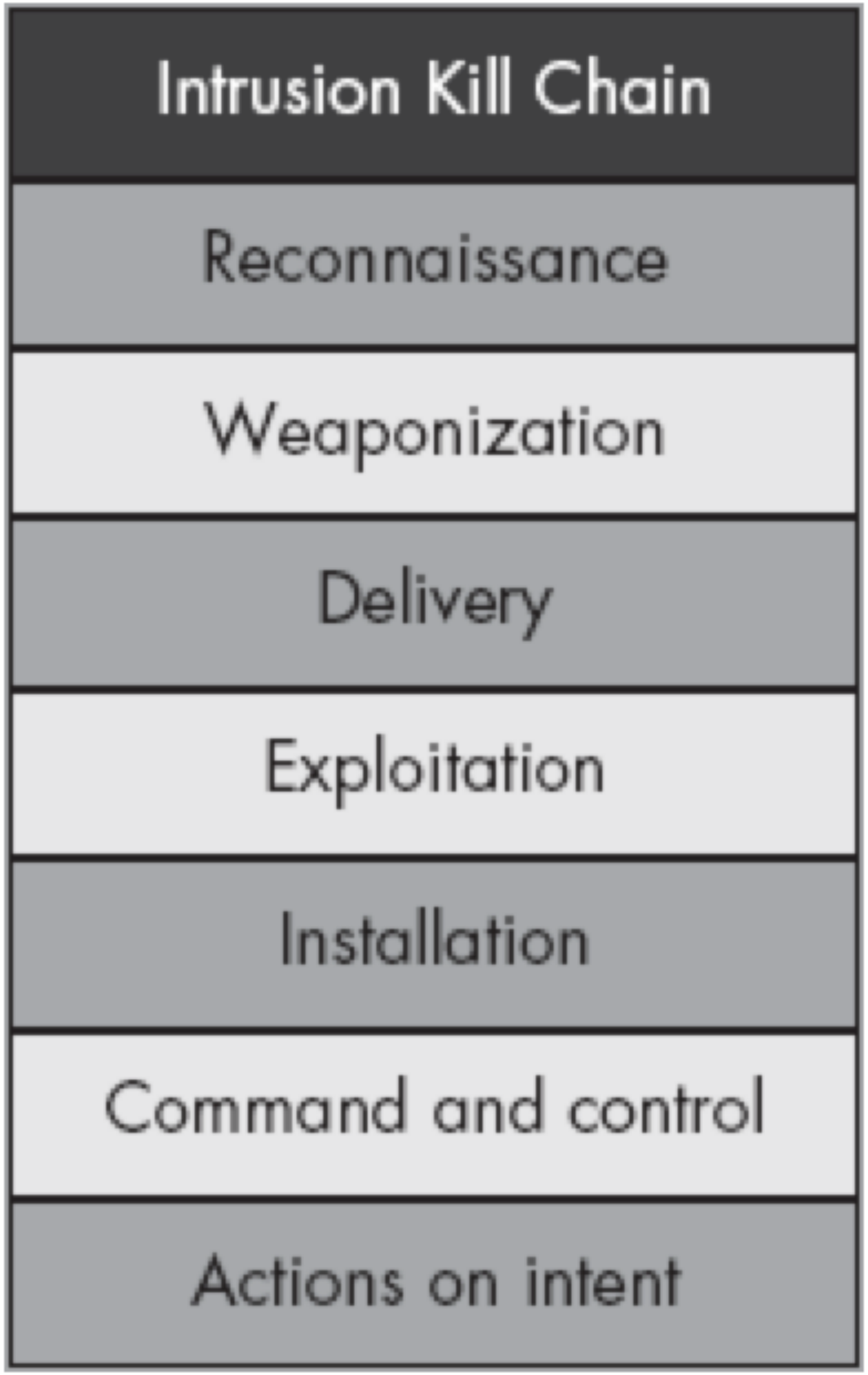
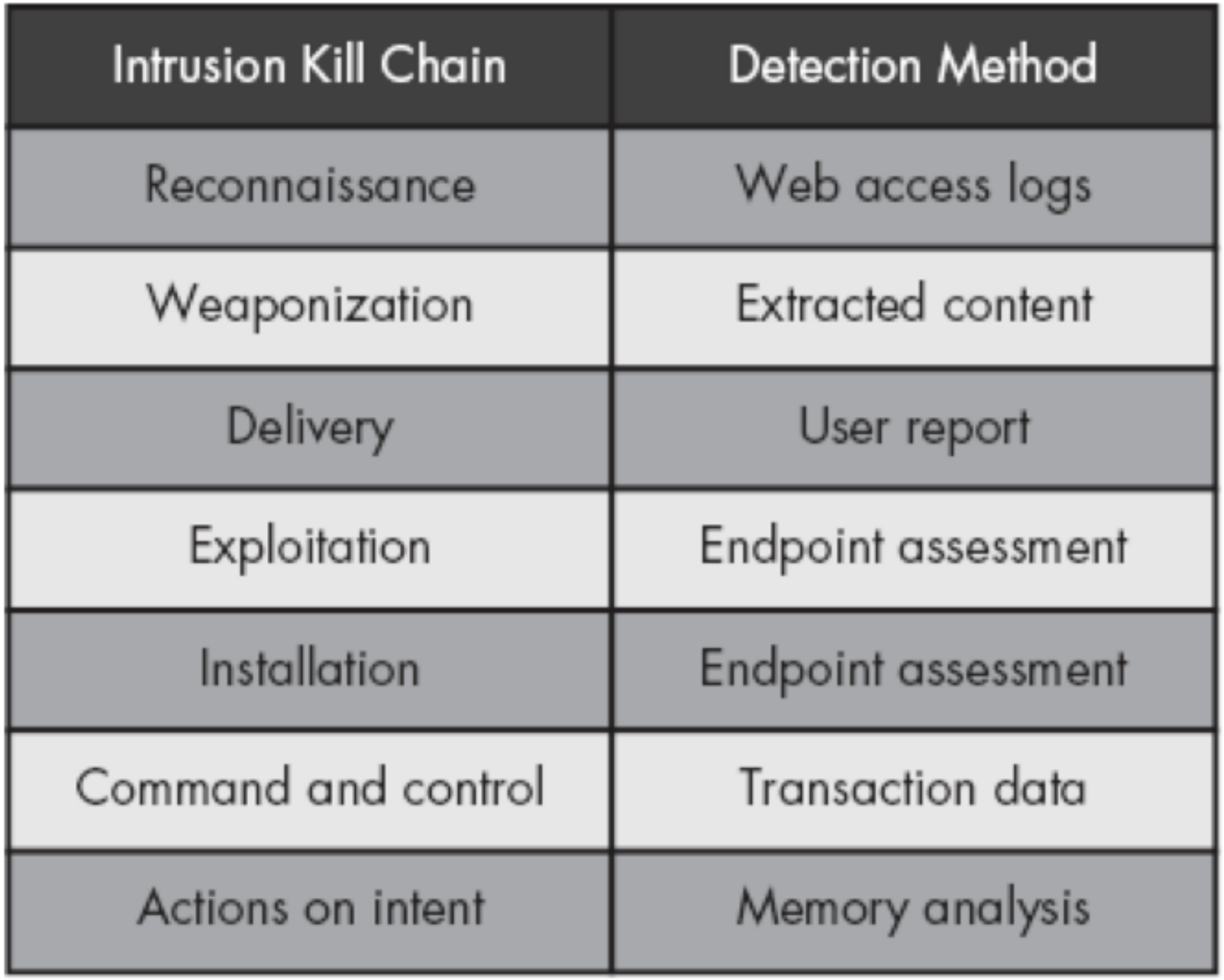


Figure 9-3. Intrusion kill chain model



Intrusion Kill Chain	Detection Method
Reconnaissance	Web access logs
Weaponization	Extracted content
Delivery	User report
Exploitation	Endpoint assessment
Installation	Endpoint assessment
Command and control	Transaction data
Actions on intent	Memory analysis

Figure 9-4. Intrusion kill chain and possible detection sources and methods

Collection Components

- **Data** from host, network, and applications
- **Process** to accept reports from third parties and constituents to gather nontechnical data
- **Database**, ticketing system, or other platform to manage this information

Analysis

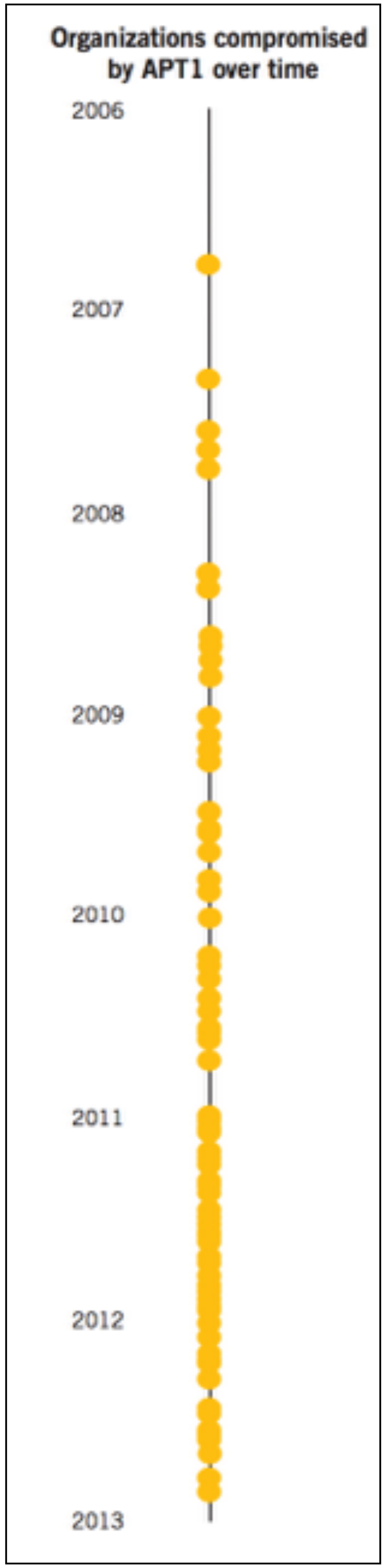
- The process of identifying and validating normal, suspicious, and malicious activity
- IOCs expedite this process
- IOCs are observable evidence of adversary activity
- Mandiant APT1 IOCs include IP addresses, domain names, and MD5 hashes

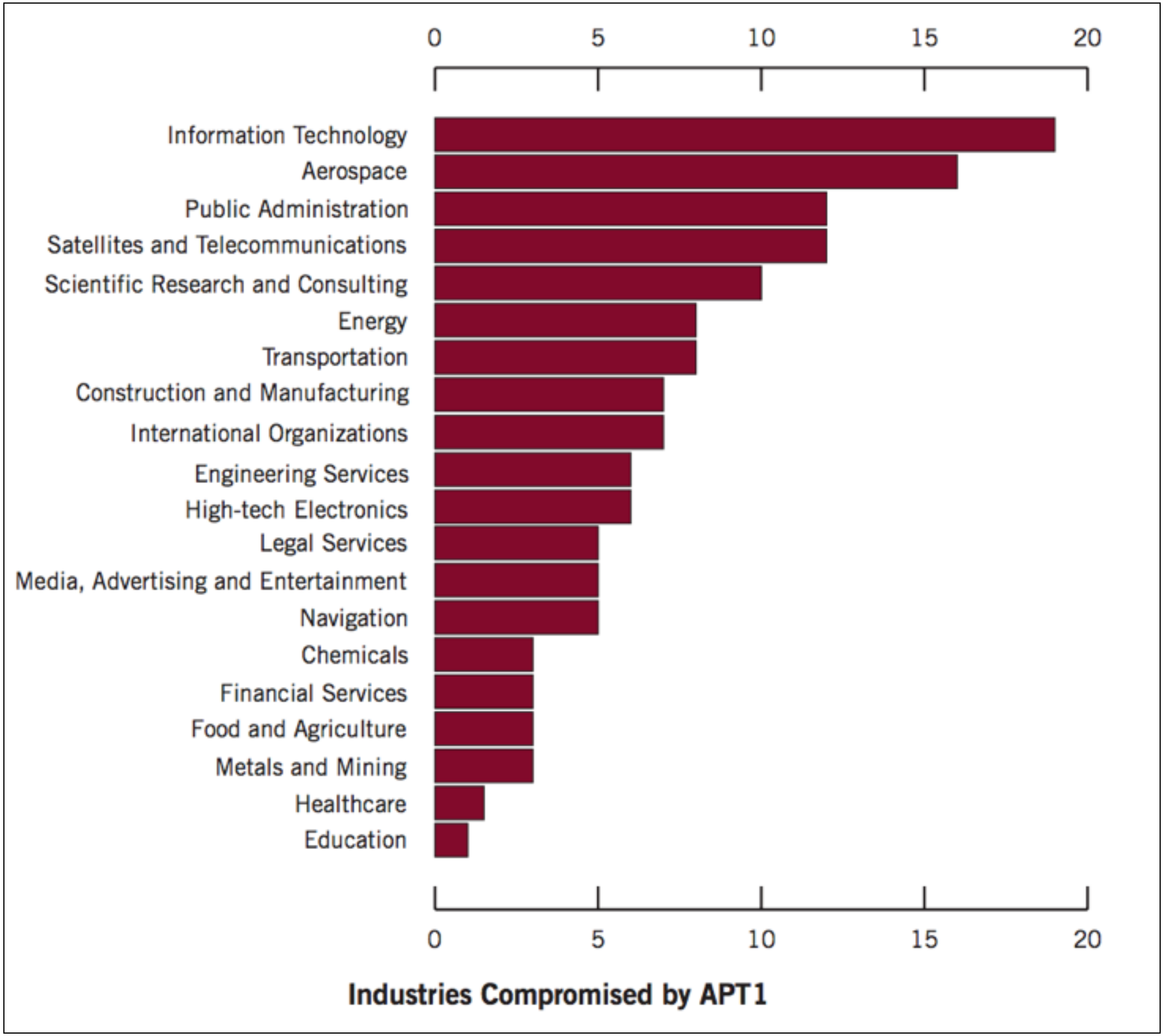
MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

- **Link Ch 9a**


Organizations compromised by APT1 over time
2006
2007
2008
2009
2010
2011
2012
2013

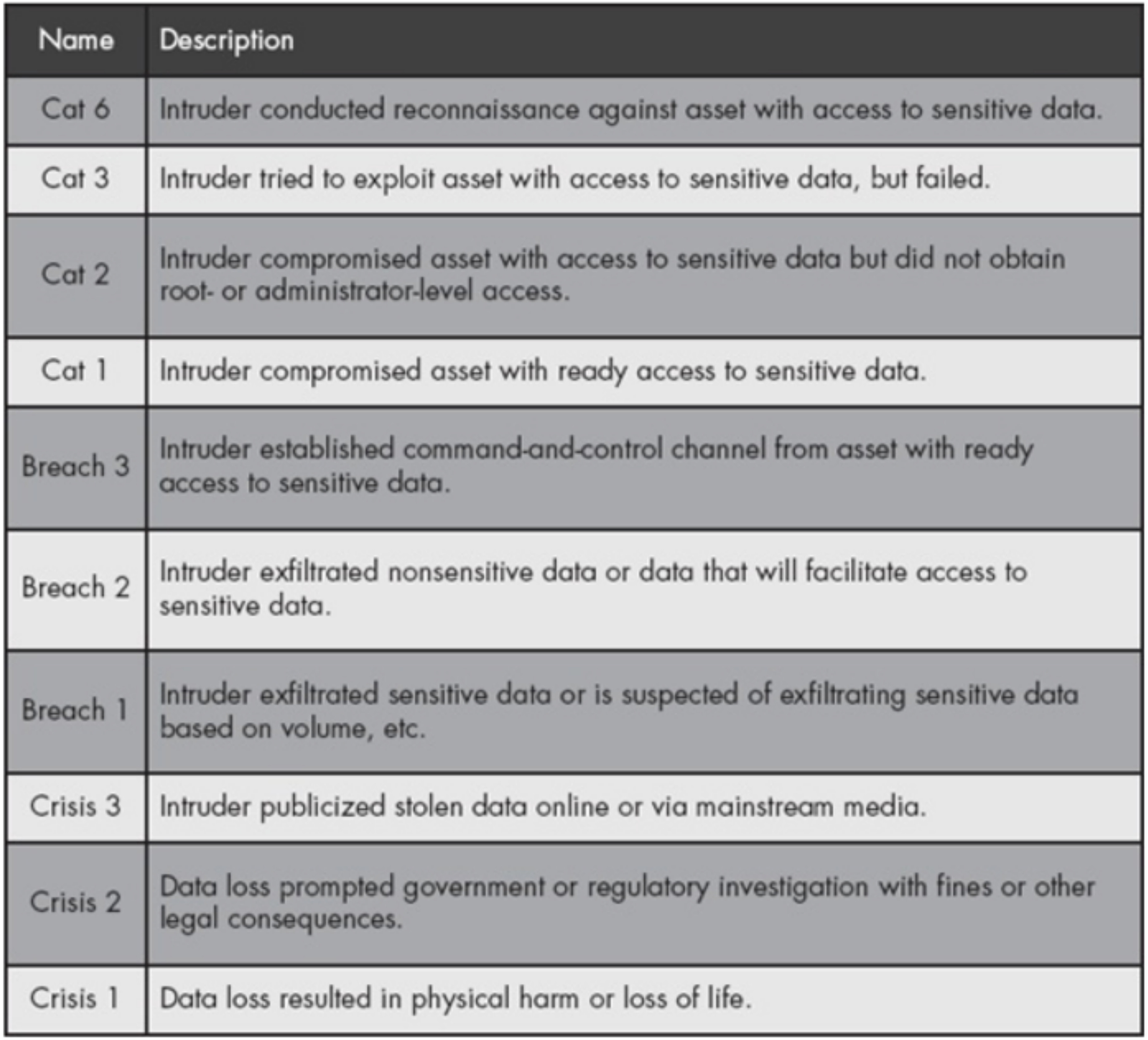

0
5
10
15
20
Information Technology
Aerospace
Public Administration
Satellites and Telecommunications
Scientific Research and Consulting
Energy
Transportation
Construction and Manufacturing
International Organizations
Engineering Services
High-tech Electronics
Legal Services
Media, Advertising and Entertainment
Navigation
Chemicals
Financial Services
Food and Agriculture
Metals and Mining
Healthcare
Education
0
5
10
15
20
Industries Compromised by APT1

IOC-Free Analysis

- Also called **hunting**
- Security experts perform **friendly force projection** on their networks
- Examining data and sometimes occupying the systems themselves in order to find advanced threats
- Senior investigators perform network **hunting trips** guiding junior investigators through data and systems looking for signs of the adversary

Intrusions and Incidents

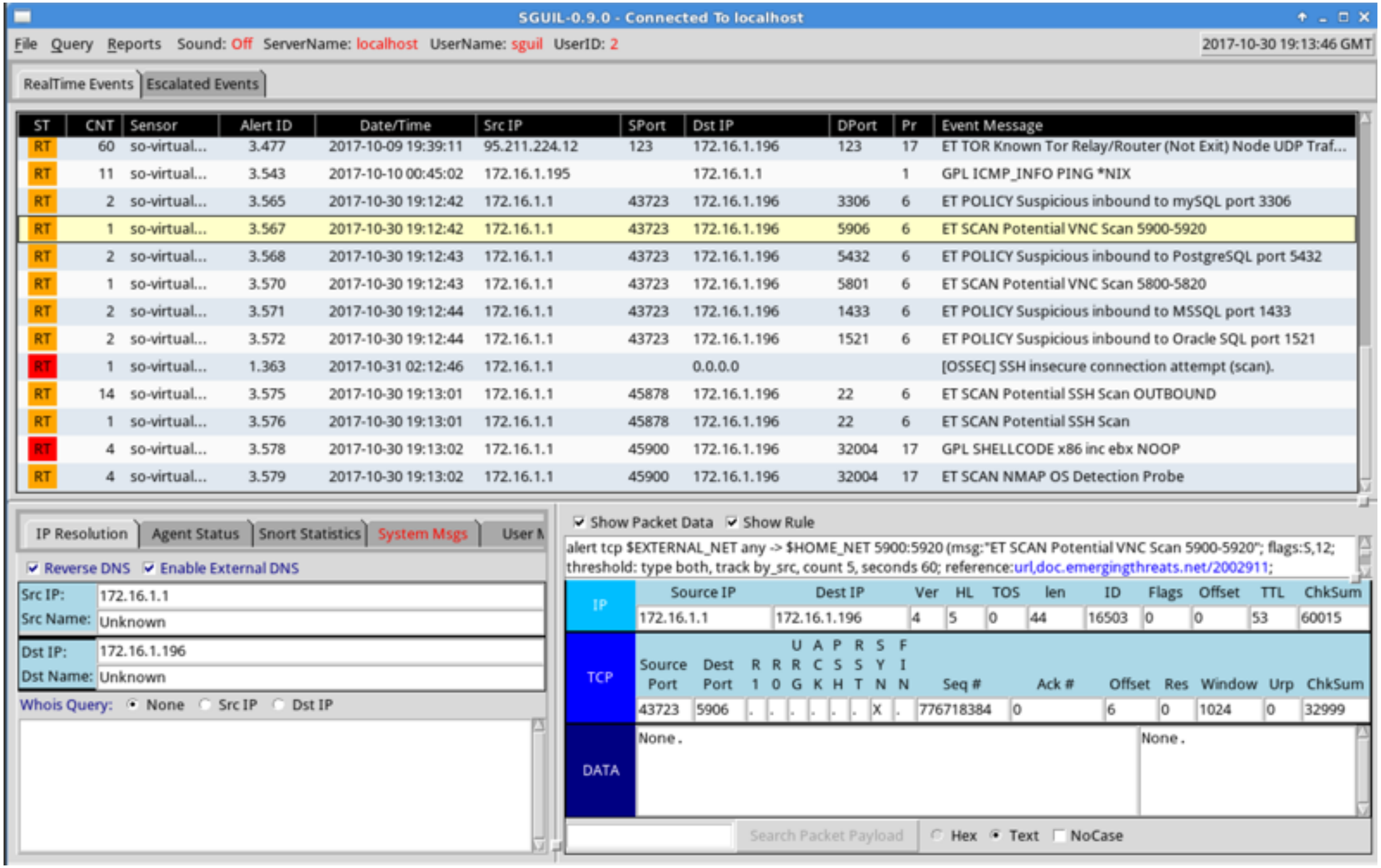
- **Intrusions** are policy violations or incidents
- An **incident** is "any unlawful, unauthorized, or unacceptable action" involving a computer or network
- Intrusion categories on next slide



Name	Description
Cat 6	Intruder conducted reconnaissance against asset with access to sensitive data.
Cat 3	Intruder tried to exploit asset with access to sensitive data, but failed.
Cat 2	Intruder compromised asset with access to sensitive data but did not obtain root- or administrator-level access.
Cat 1	Intruder compromised asset with ready access to sensitive data.
Breach 3	Intruder established command-and-control channel from asset with ready access to sensitive data.
Breach 2	Intruder exfiltrated nonsensitive data or data that will facilitate access to sensitive data.
Breach 1	Intruder exfiltrated sensitive data or is suspected of exfiltrating sensitive data based on volume, etc.
Crisis 3	Intruder publicized stolen data online or via mainstream media.
Crisis 2	Data loss prompted government or regulatory investigation with fines or other legal consequences.
Crisis 1	Data loss resulted in physical harm or loss of life.

Figure 9-5. Suggested intrusion categories

Event Classification by Sguil



Sound: Off ServerName: localhost UserName: sguil UserID: 2 2017-10-30 19:13:46 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	60	so-virtual...	3.477	2017-10-09 19:39:11	95.211.224.12	123	172.16.1.196	123	17	ET TOR Known Tor Relay/Router (Not Exit) Node UDP Traf...
RT	11	so-virtual...	3.543	2017-10-10 00:45:02	172.16.1.195		172.16.1.1		1	GPL ICMP_INFO PING *NIX
RT	2	so-virtual...	3.565	2017-10-30 19:12:42	172.16.1.1	43723	172.16.1.196	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	1	so-virtual...	3.567	2017-10-30 19:12:42	172.16.1.1	43723	172.16.1.196	5906	6	ET SCAN Potential VNC Scan 5900-5920
RT	2	so-virtual...	3.568	2017-10-30 19:12:43	172.16.1.1	43723	172.16.1.196	5432	6	ET POLICY Suspicious inbound to PostgreSQL port 5432
RT	1	so-virtual...	3.570	2017-10-30 19:12:43	172.16.1.1	43723	172.16.1.196	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	2	so-virtual...	3.571	2017-10-30 19:12:44	172.16.1.1	43723	172.16.1.196	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	2	so-virtual...	3.572	2017-10-30 19:12:44	172.16.1.1	43723	172.16.1.196	1521	6	ET POLICY Suspicious inbound to Oracle SQL port 1521
RT	1	so-virtual...	1.363	2017-10-31 02:12:46	172.16.1.1		0.0.0.0			[OSSEC] SSH insecure connection attempt (scan).
RT	14	so-virtual...	3.575	2017-10-30 19:13:01	172.16.1.1	45878	172.16.1.196	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	so-virtual...	3.576	2017-10-30 19:13:01	172.16.1.1	45878	172.16.1.196	22	6	ET SCAN Potential SSH Scan
RT	4	so-virtual...	3.578	2017-10-30 19:13:02	172.16.1.1	45900	172.16.1.196	32004	17	GPL SHELLCODE x86 inc ebx NOOP
RT	4	so-virtual...	3.579	2017-10-30 19:13:02	172.16.1.1	45900	172.16.1.196	32004	17	ET SCAN NMAP OS Detection Probe

☑ Reverse DNS ☑ Enable External DNS

Src IP:	172.16.1.1
Src Name:	Unknown
Dst IP:	172.16.1.196
Dst Name:	Unknown

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5900:5920 (msg:"ET SCAN Potential VNC Scan 5900-5920"; flags:S,12;
threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002911;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	172.16.1.1	172.16.1.196	4	5	0	44	16503	0	0	53	60015

TCP	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	43723	5906	.	.	.	.	.	.	X	.	776718384	0	6	0	1024	0	32999

DATA		
	None .	None .

○ Hex ● Text □ NoCase

Event Classification

- Should include
  - User ID of analyst making the decision
  - Time of the classification
  - Optional comments field
- Forwarding events to senior analysis is helpful
- Collaboration and social discussions of incident data is helpful

Two Key Metrics

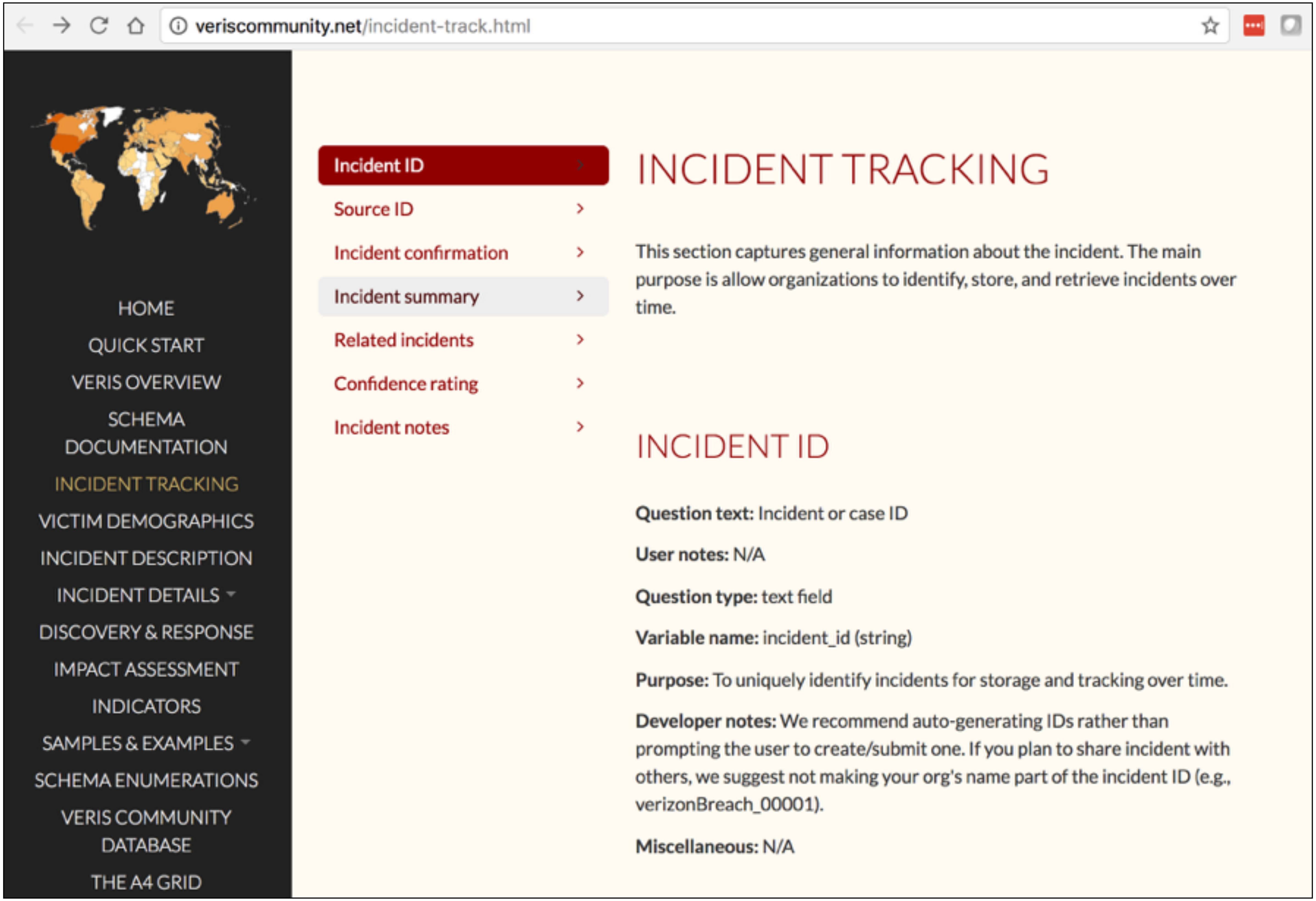
- **Count and classification** of incidents
- **Time elapsed** from incident detection to containment
- Important for internal reports and when reporting to external bodies

Escalation

- The process the CIRT uses to
  - Document its findings
  - Notify its constituents
  - Receive acknowledgment from the constituents of the incident report

Documentation of Incidents

- Creates a record of the event and the CIRT's work to handle it
- Assign a different incident number to each victim computer
  - So you can measure incident response metrics
- Vocabulary for Event Recording and Incident Sharing (VERIS) (link Ch 9b)



INCIDENT TRACKING

This section captures general information about the incident. The main purpose is allow organizations to identify, store, and retrieve incidents over time.

INCIDENT ID

Question text: Incident or case ID

User notes: N/A

Question type: text field

Variable name: incident_id (string)

Purpose: To uniquely identify incidents for storage and tracking over time.

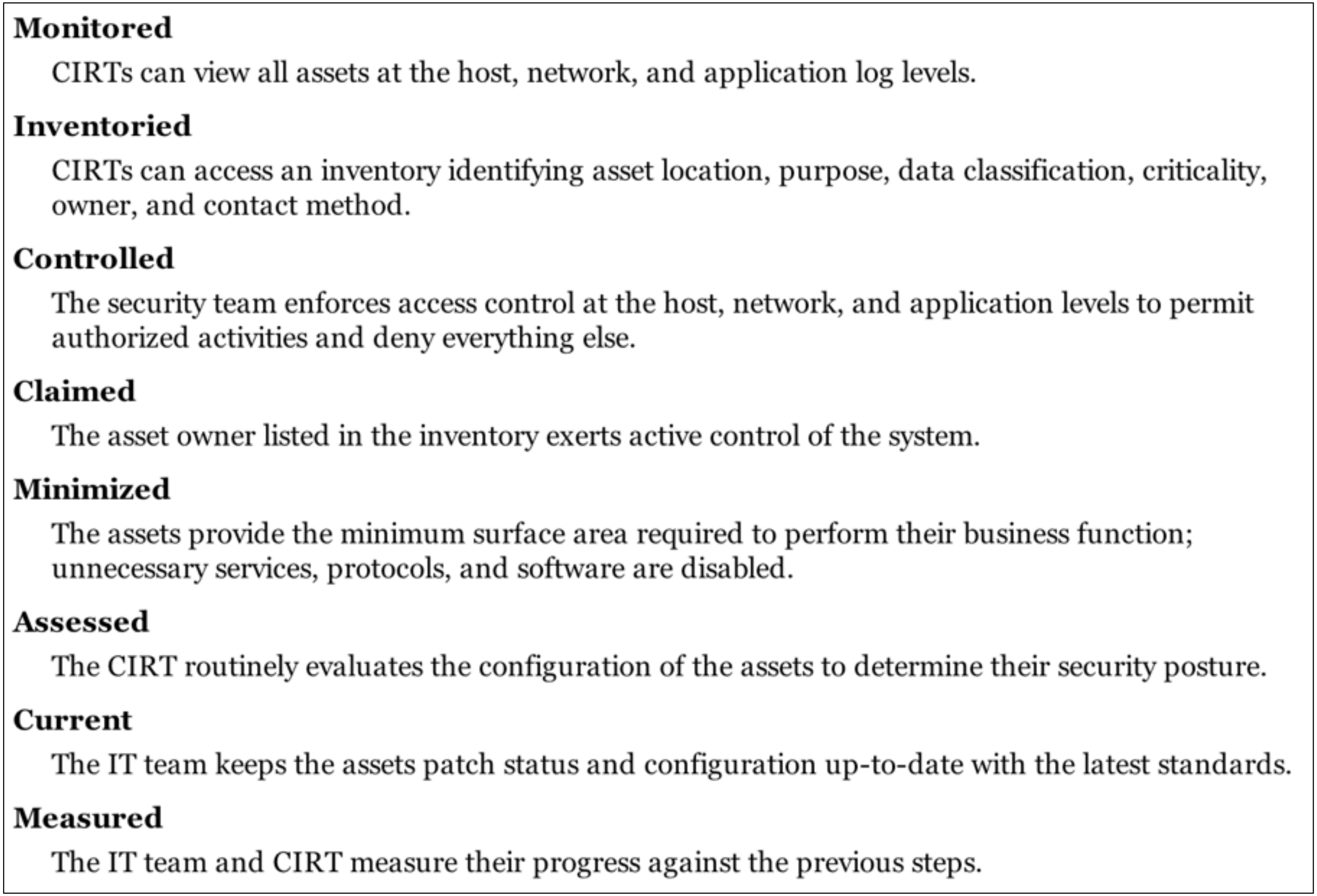
Developer notes: We recommend auto-generating IDs rather than prompting the user to create/submit one. If you plan to share incident with others, we suggest not making your org's name part of the incident ID (e.g., verizonBreach_00001).

Miscellaneous: N/A

Notification of Incidents

- Identify the compromised asset
- Find a person or group responsible for the victim
- Deliver an incident report to the affected party

Defensible Network Architecture



Monitored

CIRTs can view all assets at the host, network, and application log levels.

Inventoried

CIRTs can access an inventory identifying asset location, purpose, data classification, criticality, owner, and contact method.

Controlled

The security team enforces access control at the host, network, and application levels to permit authorized activities and deny everything else.

Claimed

The asset owner listed in the inventory exerts active control of the system.

Minimized

The assets provide the minimum surface area required to perform their business function; unnecessary services, protocols, and software are disabled.

Assessed

The CIRT routinely evaluates the configuration of the assets to determine their security posture.

Current

The IT team keeps the assets patch status and configuration up-to-date with the latest standards.

Measured

The IT team and CIRT measure their progress against the previous steps.

Kahoot!

Identifying Systems and Owners

- Notification is impossible if the CIRT cannot:
  - Map an IP address or hostname to a real computer
  - Determine its owner
  - Contact the owner

Incident Severity

- Notification depends on incident severity
- Different expected response times depending on severity
  - Telephone or IM for urgent notification
  - Backup notification plans in case primary contacts are unresponsive

Incident Acknowledgement

- Some constituents don't care to know that their computers are compromised
    - Or are swamped with other work
- Others have no IT or security abilities
    - Depend completely on CIRT for next steps
- Track acknowledgement time and method in your incident reporting system to help improve overall security process

Incident Communication Considerations

- If your organization is compromised, assume adversary has access to your email

- Encrypt CIRT-to-constituent emails

- Exchange truly sensitive information by phone

- If your VoIP is compromised, use cell phones

- Another option: use Gmail or another provider

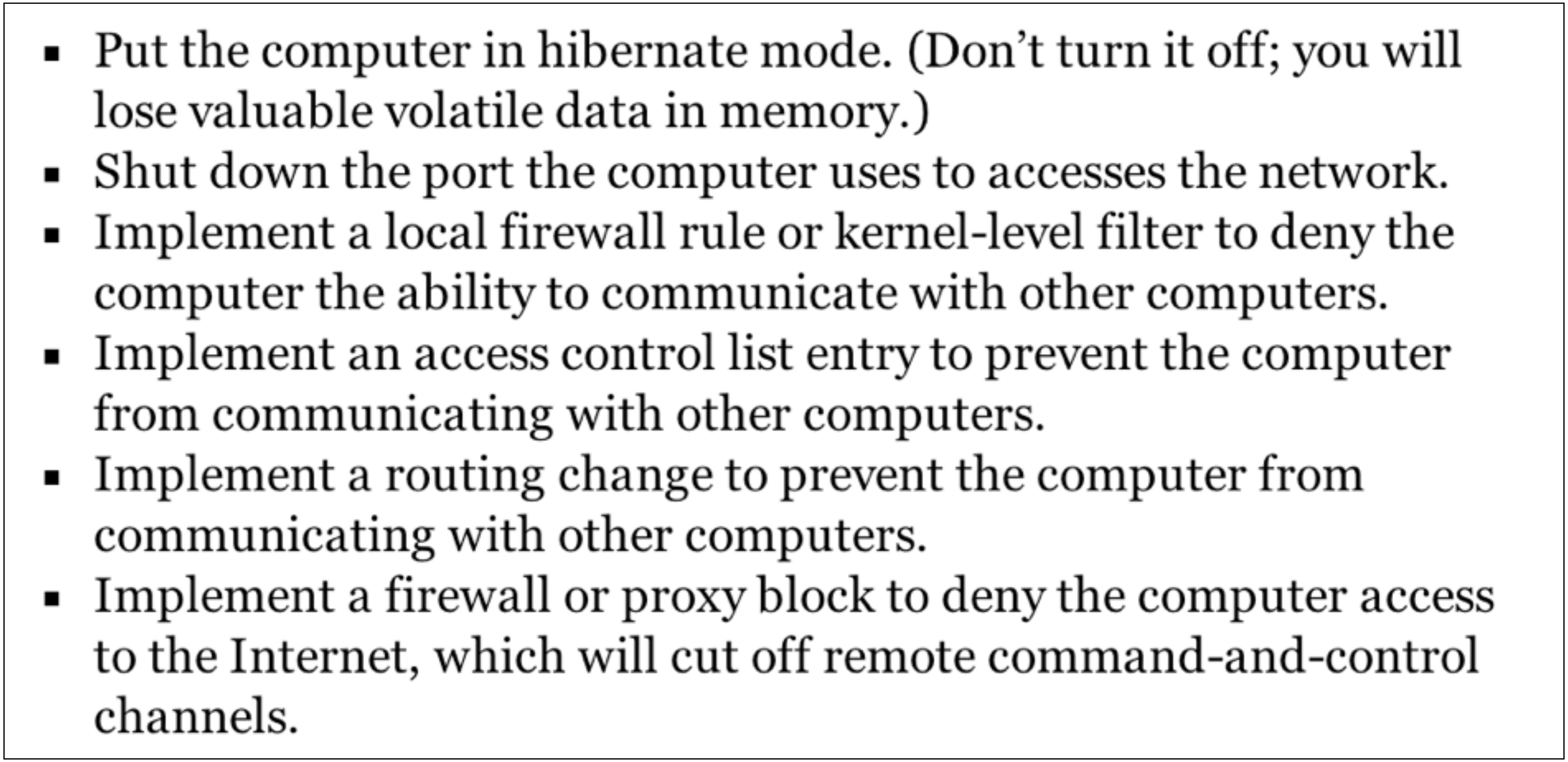
Resolution

- The process CIRTS and constituents use to transition compromised systems from an at-risk state to a trustworthy state
- Must balance risk of data loss, alteration, or denial of service against the business requirement of the compromised assets
- CIRT often wants the compromised computer off the network immediately
- Business owner wants it online no matter what the cost

Risk-Mitigation Guidelines

- When an asset is compromised
  - Constituent must take at least one measure to reduce risk of data loss, alteration, or denial of service
  - Taking no action is not an option
  - Tolerating an intruder is at best poor practice and at worst an invitation for a lawsuit or other penalty

Containment Techniques



- Put the computer in hibernate mode. (Don’t turn it off; you will lose valuable volatile data in memory.)
- Shut down the port the computer uses to accesses the network.
- Implement a local firewall rule or kernel-level filter to deny the computer the ability to communicate with other computers.
- Implement an access control list entry to prevent the computer from communicating with other computers.
- Implement a routing change to prevent the computer from communicating with other computers.
- Implement a firewall or proxy block to deny the computer access to the Internet, which will cut off remote command-and-control channels.

Honeynet

- Move the intruder to a honey network of simulated computers for study in a "safe" environment

Speed of Containment

- A hot debate
- Fast containment lowers risk
- Slower containment provides more time to learn about an adversary
- Best: contain incidents as quickly as possible, as long as the CIRT can **scope the incident** to the best of its capability

Scoping the Incident

- Understanding the intruder's reach
- One computer, or the whole active directory domain?
- A CIRT's speed making the containment decision is one of the primary ways to measure its maturity

Slow Detection

- CIRT that cannot find intrusions and learns about them from external parties
  - Rapid containment won't be effective
  - Intrusion has spread too far
  - "Pulling the plug" on the first identified victim will leave other victims online and available to the adversary

Fast Detection

- CIRT that develops its own threat intelligence, maintains pervasive visibility, and quickly finds intruders on its own
    - Likely to scope an incident quickly
    - Can contain the victim(s0 in time to limit the adversary's options

Threat-Centric

- Focus on presumed nature of the adversary
- A mature CIRT tracks many distinct threat groups
- Recognizes a sophisticated or damaging threat
    - Acts quickly to contain it
- Also notices more routine event involving a criminal
    - More leisurely response

Asset-Centric

- Focuses on presumed nature of the victim computer
- CIRT works with mature IT and business organization
- Understands sensitivity of the data and the roles of systems processing that data
- If incident affects a business-critical asset
  - CIRT acts quickly
- If incident affects less important asset, such as an employee laptop,
  - CIRT acts less quickly

Playbooks and Campaigns

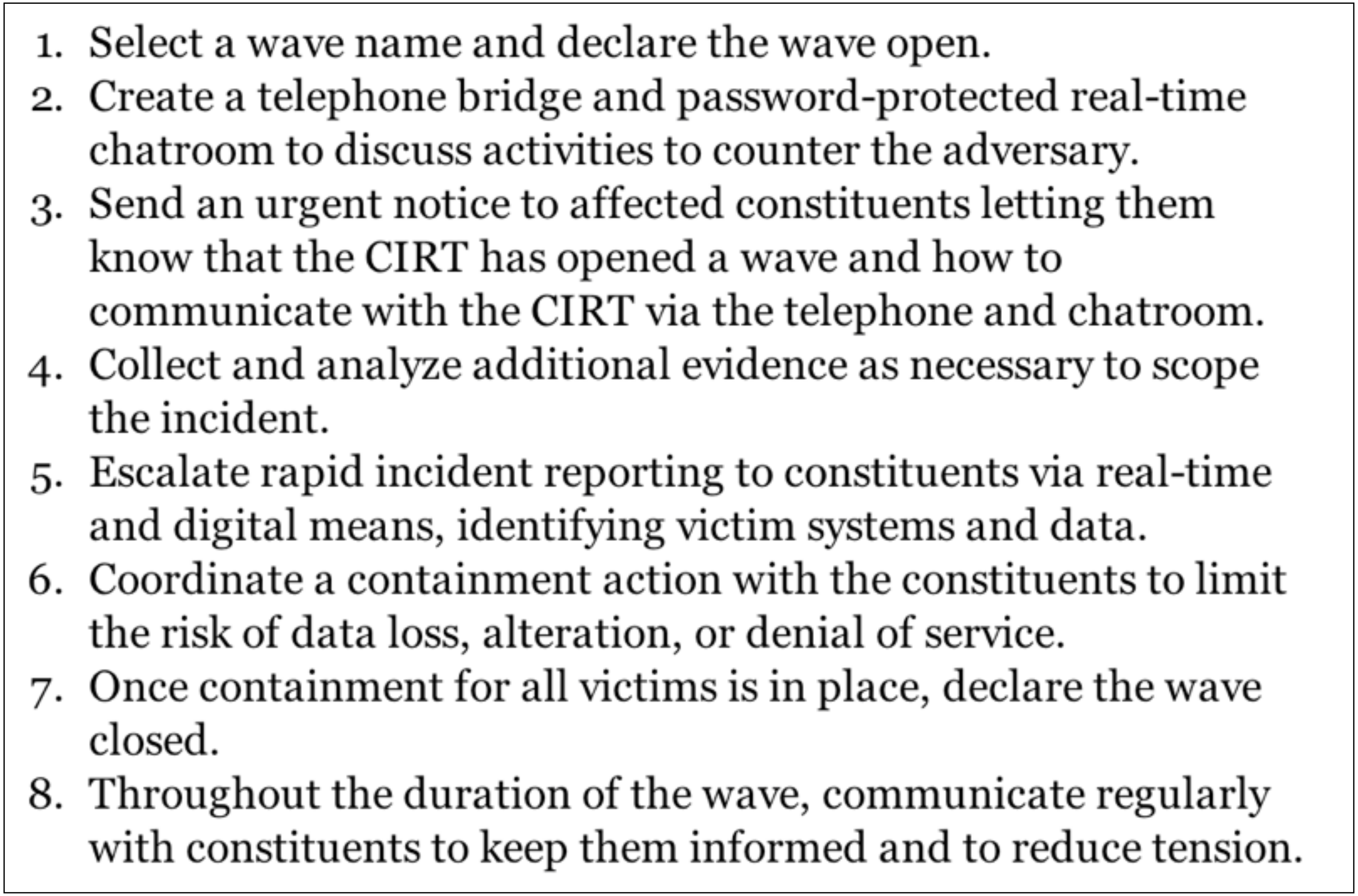
- CIRTs should document their processes in **playbooks**

  - Outline responsibilities and actions to be taken by CIRTs and constituents

- CIRT should track intruder actions

- Identifying **campaigns** -- long-term operations by an adversary, usually to steal information

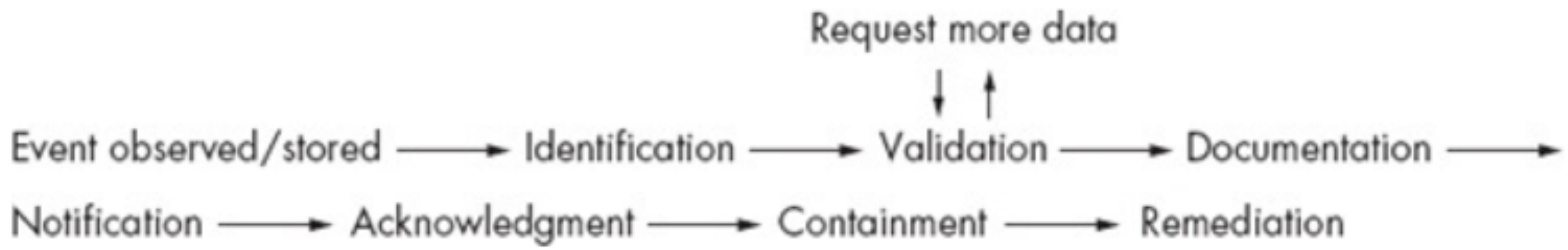
Waves



1. Select a wave name and declare the wave open.
2. Create a telephone bridge and password-protected real-time chatroom to discuss activities to counter the adversary.
3. Send an urgent notice to affected constituents letting them know that the CIRT has opened a wave and how to communicate with the CIRT via the telephone and chatroom.
4. Collect and analyze additional evidence as necessary to scope the incident.
5. Escalate rapid incident reporting to constituents via real-time and digital means, identifying victim systems and data.
6. Coordinate a containment action with the constituents to limit the risk of data loss, alteration, or denial of service.
7. Once containment for all victims is in place, declare the wave closed.
8. Throughout the duration of the wave, communicate regularly with constituents to keep them informed and to reduce tension.

Measure Times

- Of key steps in the detection and response process



Request more data

Event observed/stored → Identification → Validation → Documentation →

Notification → Acknowledgment → Containment → Remediation

Figure 9-6. Events for which time should be recorded

Detection and Response

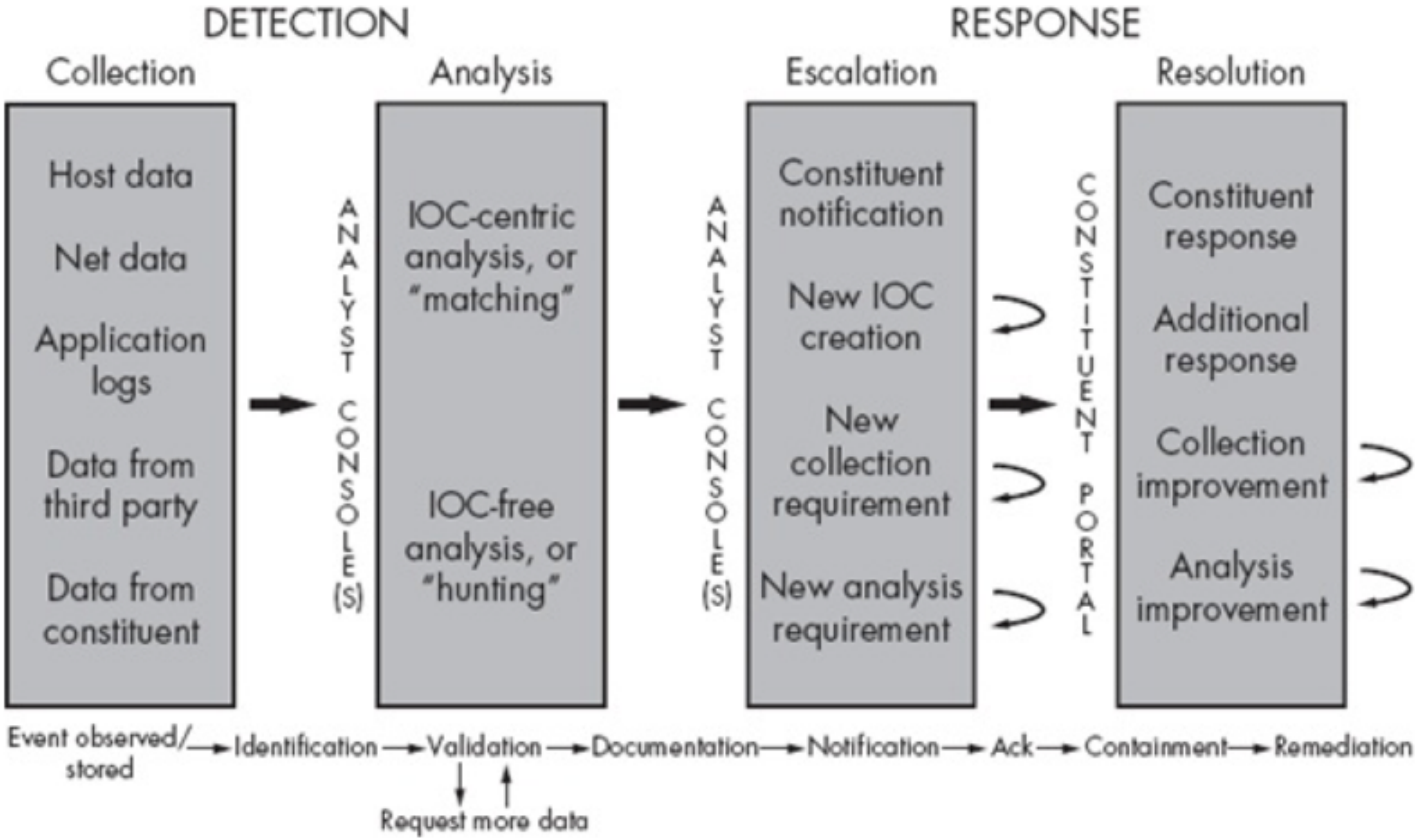


Figure 9-2. NSM process

Remediation

Actions

- "**Clean**" systems by removing intruder's tools, persistence mechanisms, and access methods

- **Rebuild** systems from installation media or trustworthy backups

- **Reflash or abandon hardware**, because attackers can implant persistence mechanisms in hardware

Rebuilding

- Rebuild any system with which the adversary was known to interact

    - Forensic reason to believe adversary acquired and used unauthorized access to the victim

- But only after fully scoping the incident

- A CIRT can never be sure of all the actions an intruder took on any victim

Remediation Speed

- Some CIRTs try to get from *detection* to *containment* in one hour
- Other try to get from *adversary access* to *remediation* in one hour
- Getting from *detection* to *containment* might take weeks
- Record these metrics to measure improvement

Using NSM to Improve Security

Example: NetFlow Probe

- A vendor offers equipment to analyze NetFlow records from border routers

- But CIRT already gathers session data using Argus and Bro on gateways with SO so this is redundant

Example: APT1 Report

- Mandiant's APT1 report includes more than 3000 indicators
    - CIRT can use them for IOC-matching
- The report also includes 100 pages of tools used by APT1 actors
    - CIRT can use that for IOC-free hunting analysis

Example: Asset Inventory

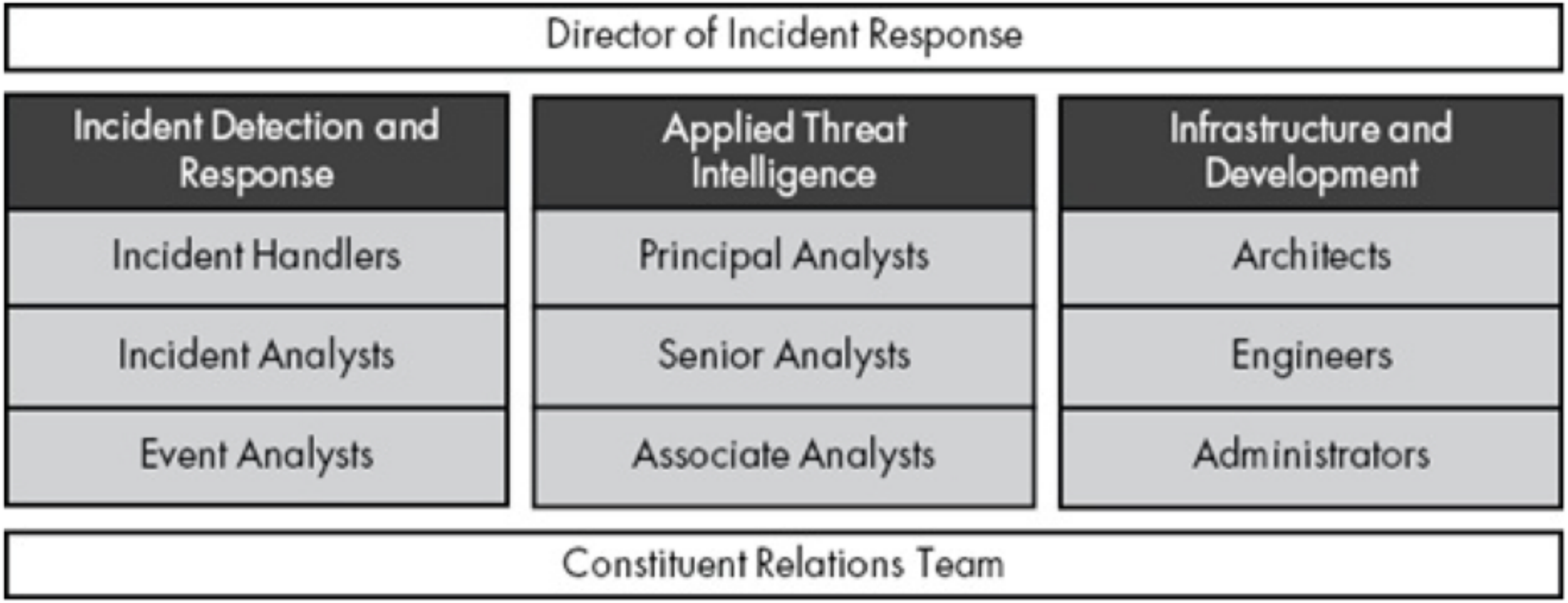
- Time between *detection* to *containment* is weeks
- CIO wants to decrease it to under one hour
- Vendor proposes a new asset management system
- Multiple business lines express enthusiasm for the new tool and form a working group
- CIRT endorses new system

Example: NAC

- Networking team tries a Network Access Control (NAC) solution
- IT resists the program, fearing it will impede user productivity
- CIRT recommends the NAC because it will help during resolution
- CIRT convinces the IT team to support the NAC

Building a CIRT

- You may be working alone, without a CIRT
- To justify adding staff, track these key metrics
  - Classification and count of incidents
  - Time from incident detection to containment
- Ask management if they are satisfied with these numbers



Director of Incident Response

Incident Detection and Response	Applied Threat Intelligence	Infrastructure and Development
Incident Handlers	Principal Analysts	Architects
Incident Analysts	Senior Analysts	Engineers
Event Analysts	Associate Analysts	Administrators

Constituent Relations Team

Figure 9-7. General CIRT structure

Director of Incident Response

- Organizes, trains, and equips the CIRT to succeed
- Selects a deputy from one of the three CIRT components to assist with this mission
- Keeps management away from the CIRT so the CIRT can do its job

Incident Detection and Response (IDR) Center

- Group responsible for daily analysis and escalation of security incidents
  - **Incident Handlers** (IHs) -- experienced analysts tasked with hunting
  - **Incident Analysts** (IAs) -- mid-level analysts who combine hunting with matching
  - **Event Analysts** (EAs) -- beginning analysts who focus on matching

Incident Detection and Response (IDR) Center

- Analysts at all levels have access to all datatypes
- But EAs and IAs may classify only events for which they are responsible
- IHs train IAs and EAs, take them on digital hunting trips, and operationalize lessons into the repeatable playbooks EAs use to identify intrusions
- IHs open, manage, and close waves

Applied Threat Intelligence (ATI) Center

- Responsible for digital intelligence activities, internal security consulting, adversary simulation, red teaming, and penetration testing
  - **Intelligence Team** provides reporting support during waves and regular briefings and updates on adversary activity to the CIRT and constituents. Also searches for IOCs, adversary tools, techniques, and procedures

Applied Threat Intelligence (ATI) Center

- **Red Team** proactively assesses and tests the organization to determine its security posture by simulating a wide variety of threats. They provide a metric to measure CIRT response.

- **Blue Team** members act as internal security consultants, helping to improve security

Infrastructure and Development (ID) Center

- Enables the other two CIRT components by employing software developers who code production-grade tools

- Designs, builds, deploys, and runs the collection, analysis, and escalation tools

- Leads development of new detection and response techniques

- Assumes responsibility for tools which begin as proof-of-concept tools from other teams

Constituent Relations Team

- Intermediary between the CIRT and its constituents
- Represent the CIRT outside the company itself

Kahoot!