MIS 4596

Unit#20

Network Security Monitoring and Incident Response

Agenda

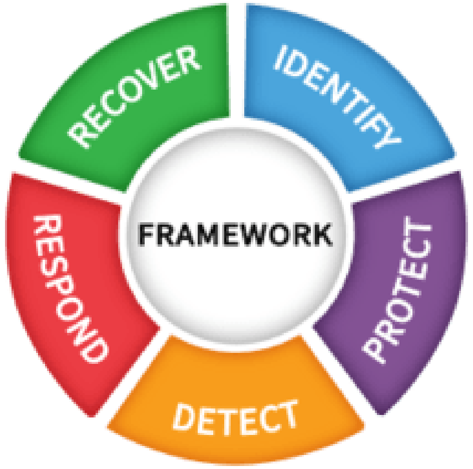
- A bit more on Social Engineering & Physical Attacks and employee mistakes
- NIST Cybersecurity Framework
- Computer security incident response vocabulary
- Attackers and detection
- Handling an incident
  - Preparation
  - Detection and analysis
  - Containment, eradication and recovery
  - Incident response workflow
- Incident case: South Carolina Department of Revenue

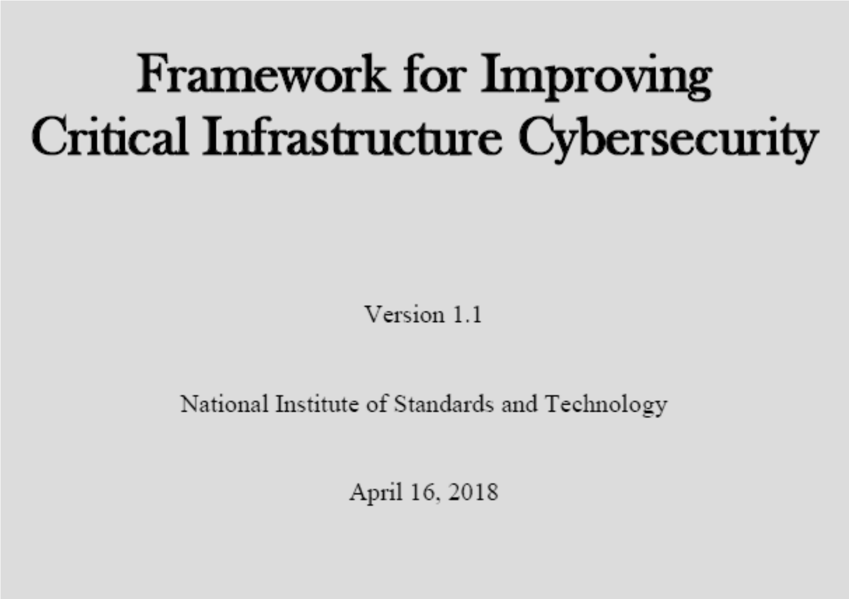
Social Engineering & Physical Attacks

- Vishing (Voice social engineering) and impersonation with employee mistakes
- Sprouts: https://abc7.com/1303739/

xhibitio

NIST Cybersecurity Framework


RECOVER
IDENTIFY
FRAMEWORK
RESPOND
PROTECT
DETECT



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

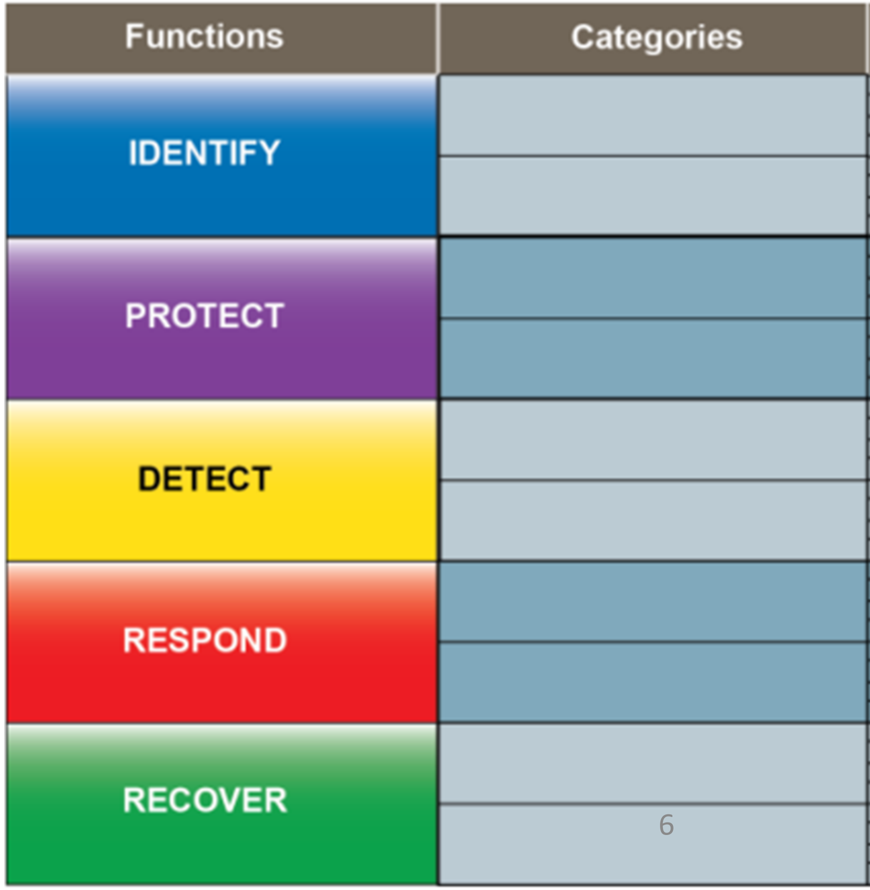
What assets need protection?

What safeguards are available ?

What techniques can identify incidents ?

What techniques can contain impacts of incidents ?

What techniques can restore capabilities?



Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	

NIST Cybersecurity Framework

What assets need protection?

What safeguards are available ?

What techniques can identify incidents ?

What techniques can contain impacts of incidents ?

What techniques can restore capabilities ?

Function Unique Identifier	Function	Category
ID	Identify	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management
PR	Protect	Identity Management and Access Control
		Awareness and Training
		Data Security
		Information Protection Processes and Procedures
		Maintenance
		Protective Technology
DE	Detect	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
RS	Respond	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
RC	Recover	Recovery Planning
		Improvements
		Communications

Computer security incident response - vocabulary

Event – any observable occurrence in a system or a network, e.g.

- User sending an email
- User connecting to a file share (i.e. file folder on another computer)
- Server receiving a request for a web page
- Firewall blocking a connection attempt

Adverse event – is an event with a negative consequence, e.g.

- System crash
- Execution of malware that destroys data
- Unauthorized use of system privileges

Computer security incident response - vocabulary

Computer security incident – is a violation (or imminent threat) of computer security policies, acceptable use policies, or standard practices, e.g.

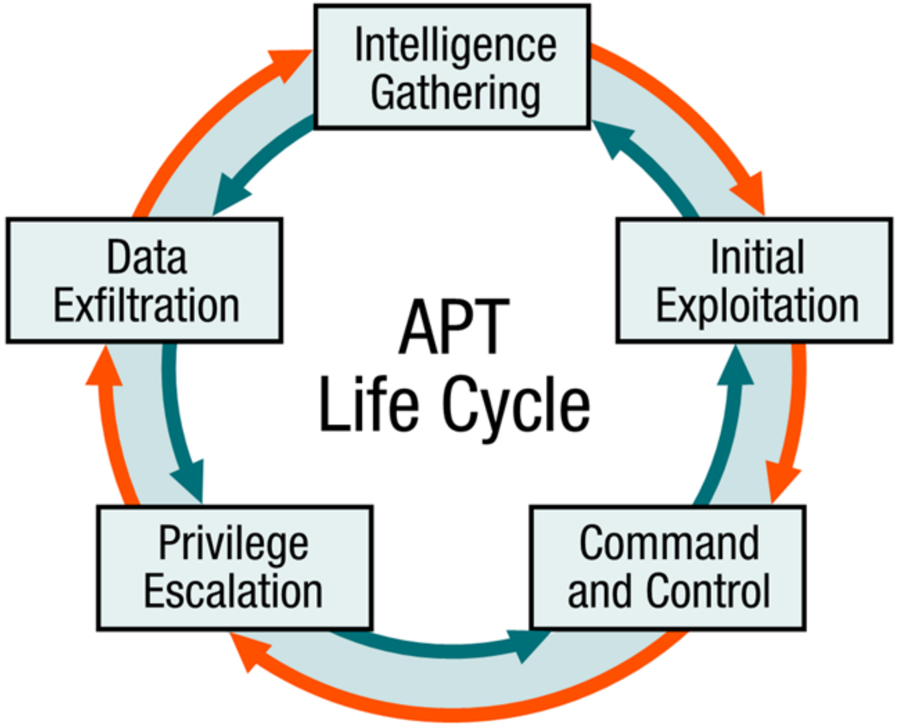
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money
- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
- A user provides or exposes sensitive information to others by mistake or on purpose

Computer security incident response

Is necessary because…

- Computer security controls, systems, and processes are not perfect
- Protections designed to protect information and information systems eventually fail
- Security breaches are inevitable

Anatomy of Advanced Persistent Threats



APT Life Cycle

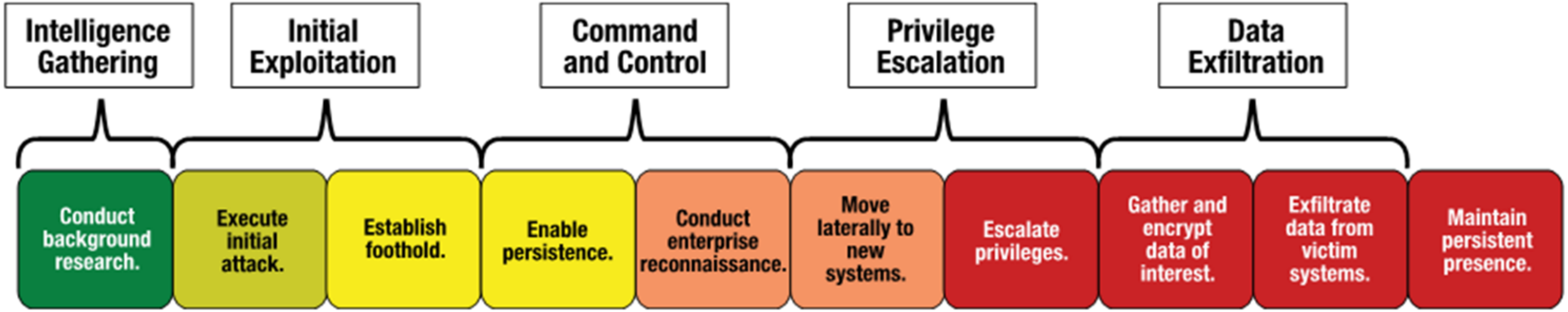
Intelligence Gathering

Initial Exploitation

Command and Control

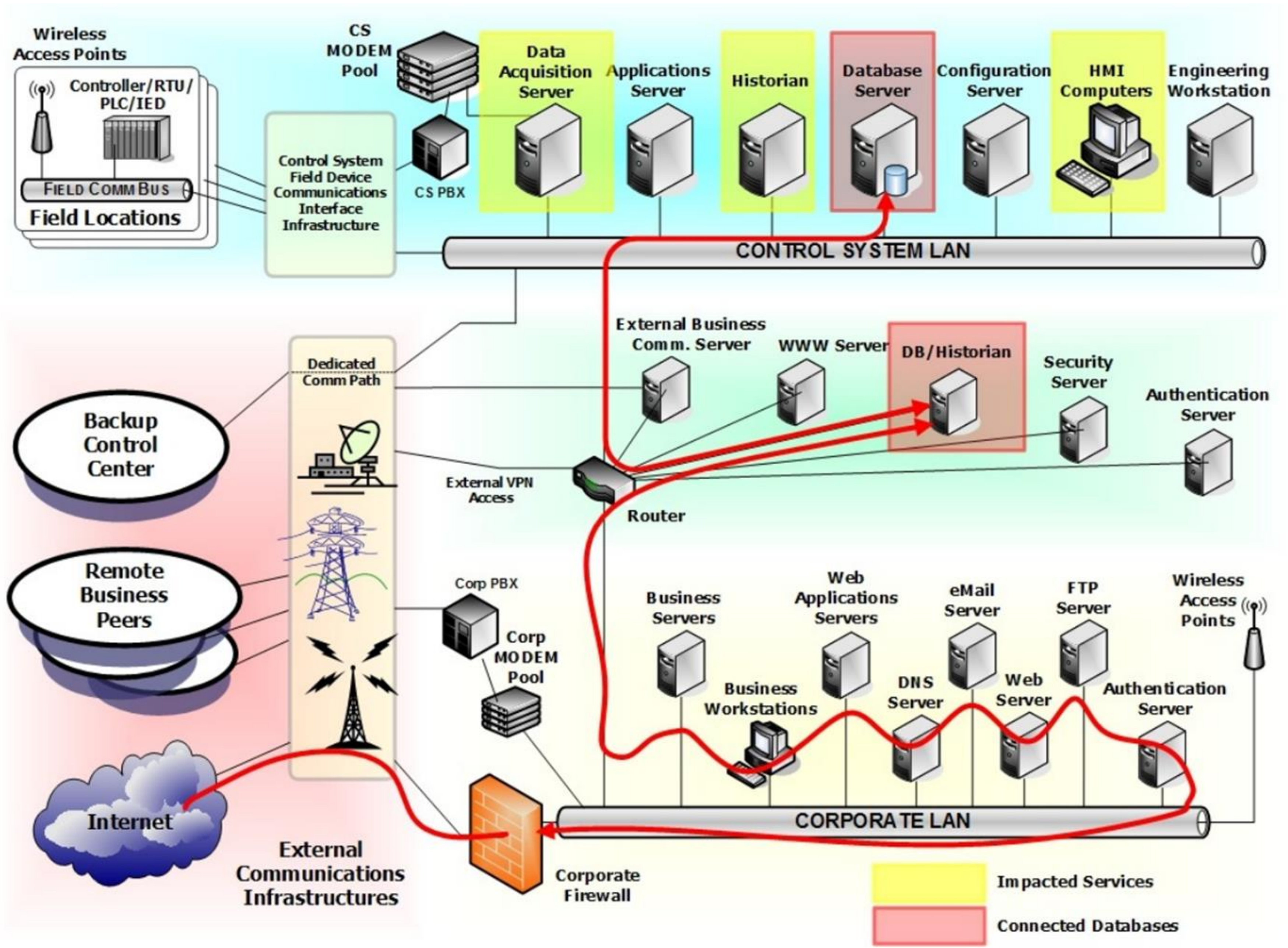
Privilege Escalation

Data Exfiltration



- **Intelligence Gathering**
  - Conduct background research.
- **Initial Exploitation**
  - Execute initial attack.
  - Establish foothold.
- **Command and Control**
  - Enable persistence.
  - Conduct enterprise reconnaissance.
- **Privilege Escalation**
  - Move laterally to new systems.
  - Escalate privileges.
- **Data Exfiltration**
  - Gather and encrypt data of interest.
  - Exfiltrate data from victim systems.
- Maintain persistent presence.

Example of Network Intrusion


Wireless Access Points
Controller/RTU/PLC/IED
FIELD COMM BUS
Field Locations
Control System Field Device Communications Interface Infrastructure
CS MODEM Pool
CS PBX
Data Acquisition Server
Applications Server
Historian
Database Server
Configuration Server
HMI Computers
Engineering Workstation
CONTROL SYSTEM LAN
Dedicated Comm Path
External Business Comm. Server
WWW Server
DB/Historian
Security Server
Authentication Server
Backup Control Center
External VPN Access
Router
Remote Business Peers
Corp PBX
Corp MODEM Pool
Business Servers
Web Applications Servers
eMail Server
FTP Server
Wireless Access Points
Business Workstations
DNS Server
Web Server
Authentication Server
Internet
CORPORATE LAN
External Communications Infrastructures
Corporate Firewall
🟨 Impacted Services
🟥 Connected Databases

Attackers and their tactics

“Attackers continue to grow more adept at working across a range of operating systems and device types, as well as in both on-premises and cloud architectures

Traditional barriers to attacker success continue to lessen over time. Put simply, more attackers can do more things in more diverse environments”

2020 M-TRENDS

FIREEYE MANDIANT SERVICES | SPECIAL REPORT

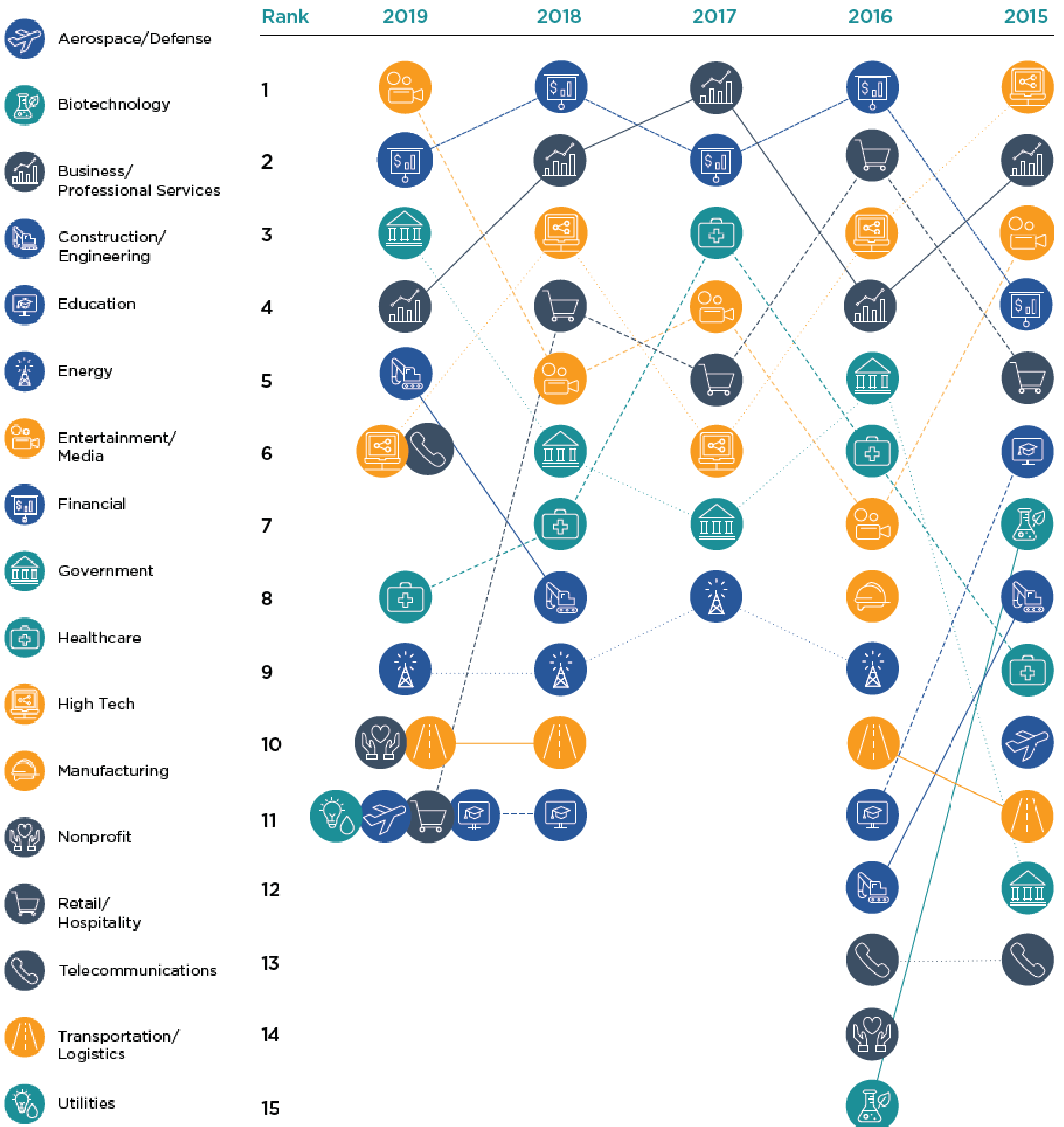
Table of Contents

Executive Summary 4

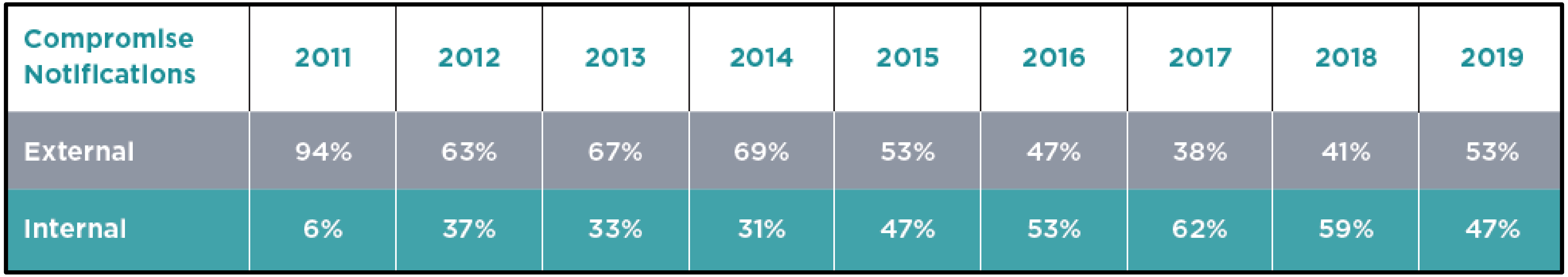
By the Numbers 8
Detection by Source 9
Dwell Time 11
Industry Targeting 16
Targeted Attacks and Retargeting 17
Threat Group 18
Malware 19
Threat Techniques 20

Who is being attacked?

M-TRENDS 2020
FIREEYE MANDIANT SERVICES | SPECIAL REPORT



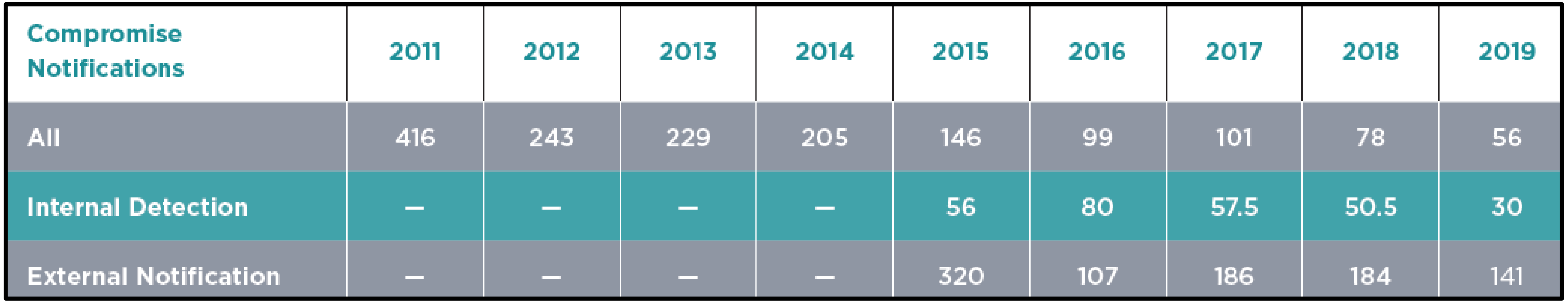
Who is detecting intrusions by attackers?



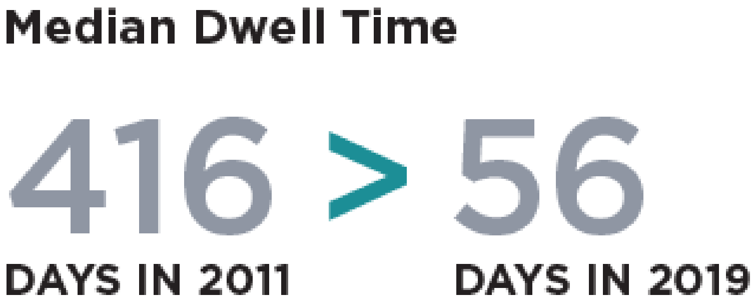
Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
External	94%	63%	67%	69%	53%	47%	38%	41%	53%
Internal	6%	37%	33%	31%	47%	53%	62%	59%	47%

M-TRENDS®
2020
FIREEYE MANDIANT SERVICES | SPECIAL REPORT

How long are attackers remaining in compromised systems?



Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
All	416	243	229	205	146	99	101	78	56
Internal Detection	–	–	–	–	56	80	57.5	50.5	30
External Notification	–	–	–	–	320	107	186	184	141



Median Dwell Time

416 > 56

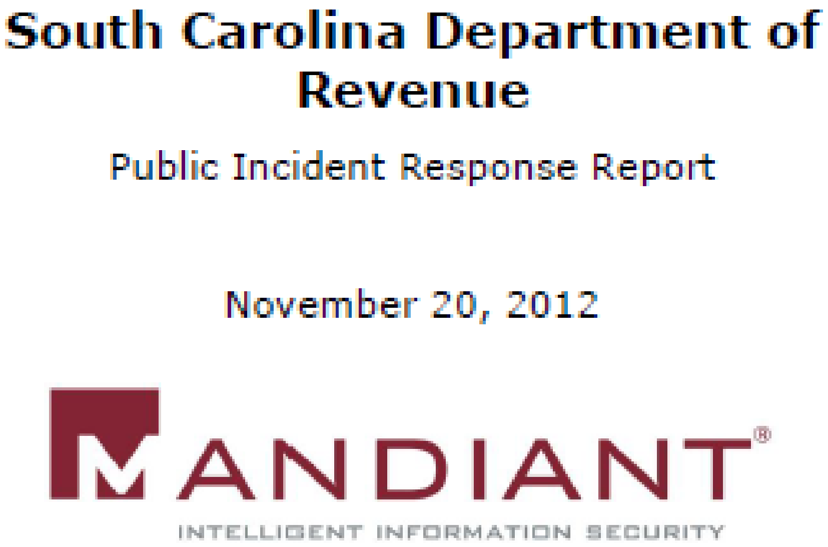
DAYS IN 2011

DAYS IN 2019

M-TRENDS®
2020
FIREEYE MANDIANT SERVICES | SPECIAL REPORT

“**Dwell time**” is “the number of days an attacker is present in a victim network before they are detected”

Incident Case: South Carolina Department of Revenue



South Carolina Department of Revenue

Public Incident Response Report

November 20, 2012

MANDIANT®

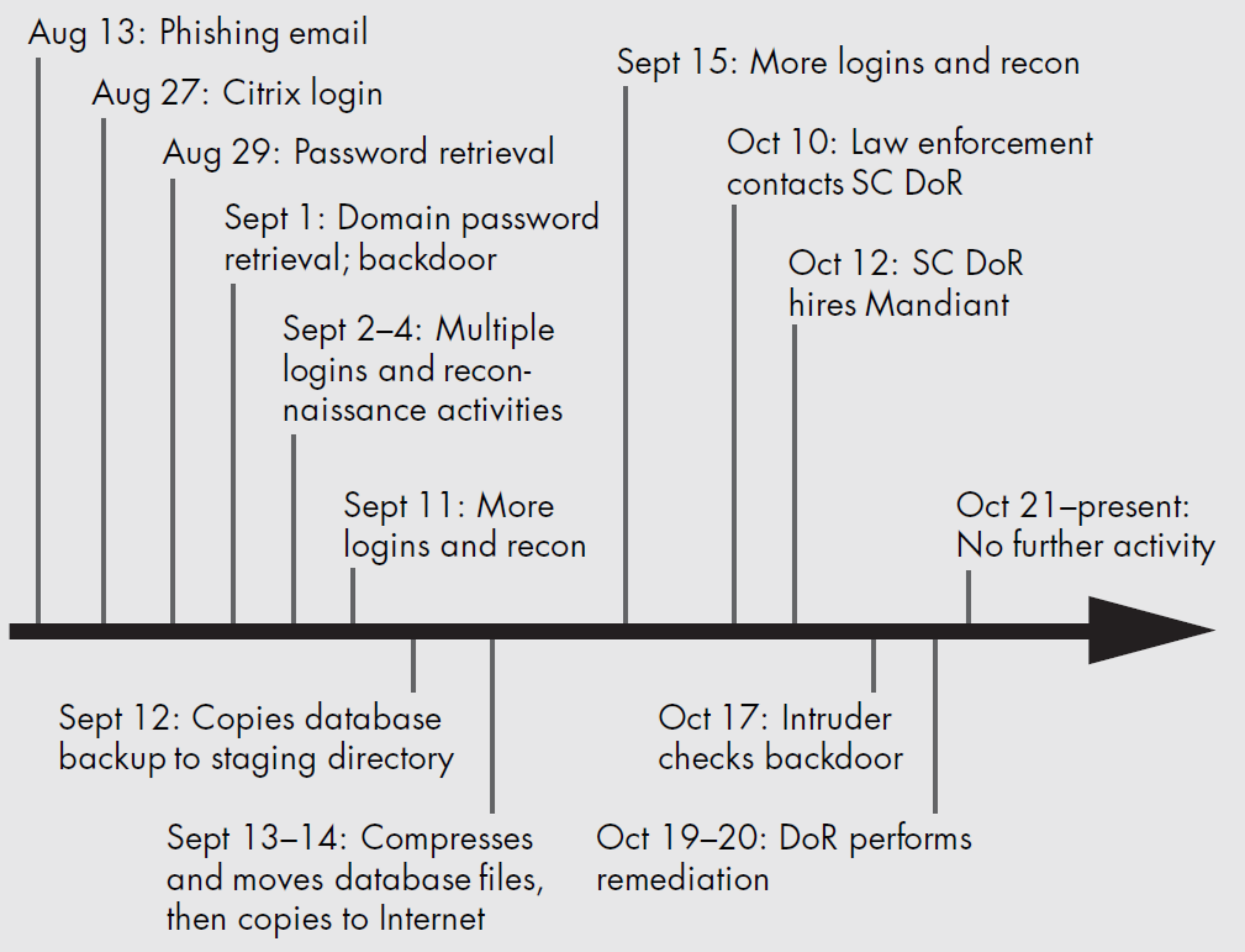
INTELLIGENT INFORMATION SECURITY

Meet in your breakout rooms, and answer the following questions:

1. How did the SC Department of Revenue (SCDR) find out about the breach i.e. internally or externally?
2. What was the dwell time?
3. How long did it take for the attackers to accomplish their mission?
4. At what points could SCDR have interdicted (i.e., cut off) the attackers, and prevented them from accomplishing their mission?

Answers:

1. SCDR was notified by “a law enforcement agency” (p. 1), so they were notified by an external party.
2. 54 days: August 27–October 19
3. It took attackers until September 14 to finish uploading the stolen data, or 19 days.
    - This means that if SCDR had detected and cut off the attackers before the uploading began on September 13, the breach could have been prevented.

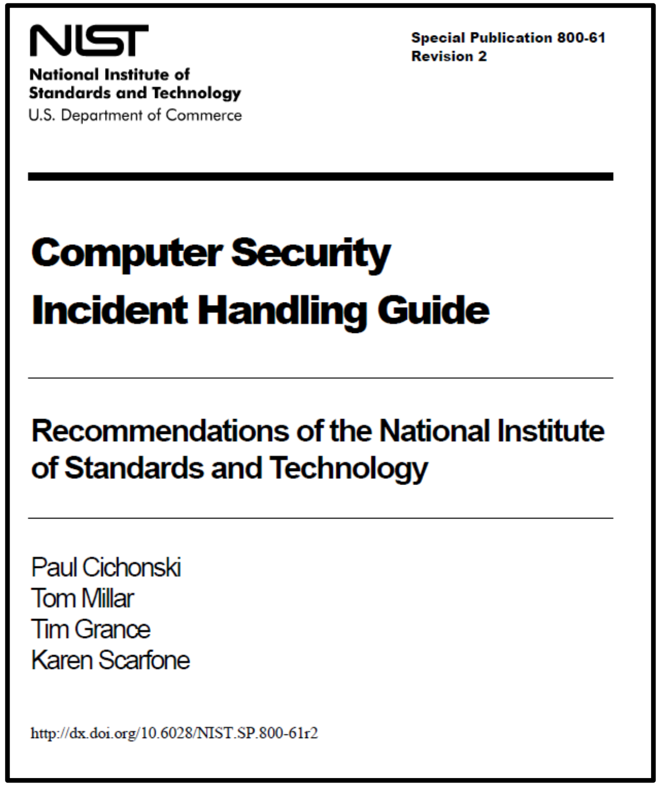

Aug 13: Phishing email
Aug 27: Citrix login
Aug 29: Password retrieval
Sept 1: Domain password retrieval; backdoor
Sept 2–4: Multiple logins and reconnaissance activities
Sept 11: More logins and recon
Sept 12: Copies database backup to staging directory
Sept 13–14: Compresses and moves database files, then copies to Internet
Sept 15: More logins and recon
Oct 10: Law enforcement contacts SC DoR
Oct 12: SC DoR hires Mandiant
Oct 17: Intruder checks backdoor
Oct 19–20: DoR performs remediation
Oct 21–present: No further activity

Possible points that SCDR could have interdicted the attackers were every time the attacker interacted with a system on SCDR’s network was an opportunity to detect and respond to the attackers.

Handling an Incident

Incident response process has several phases:

1. **Preparation** - the business attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments
   - **Residual risk** will inevitably persist after controls are implemented



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

2. **Detection and analysis** - of security breaches is necessary to alert the organization when incidents occur

3. **Containment, Eradication & Recovery** - the organization works to mitigate the impact of the incident by containing it and ultimately recovering from it
   - Activity often cycles back to detection and analysis
     E.g., to see if additional hosts are infected by malware while eradicating malware

4. **Post-Incident Activity** - After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents

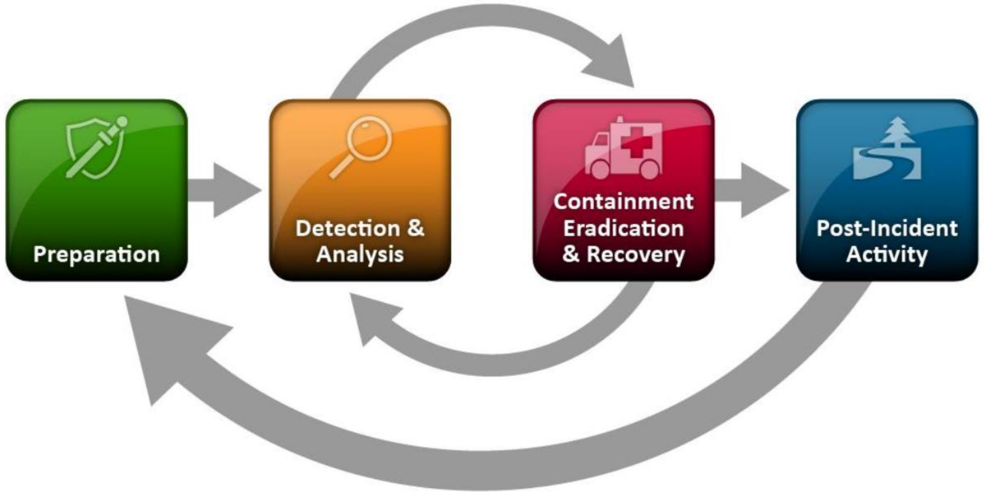
Handling an Incident - Preparation

Preventing Incidents – Keeping the number of incidents reasonably low is very important to protect the business processes of the organization

- If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team
- This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage, longer periods of service and data unavailability)

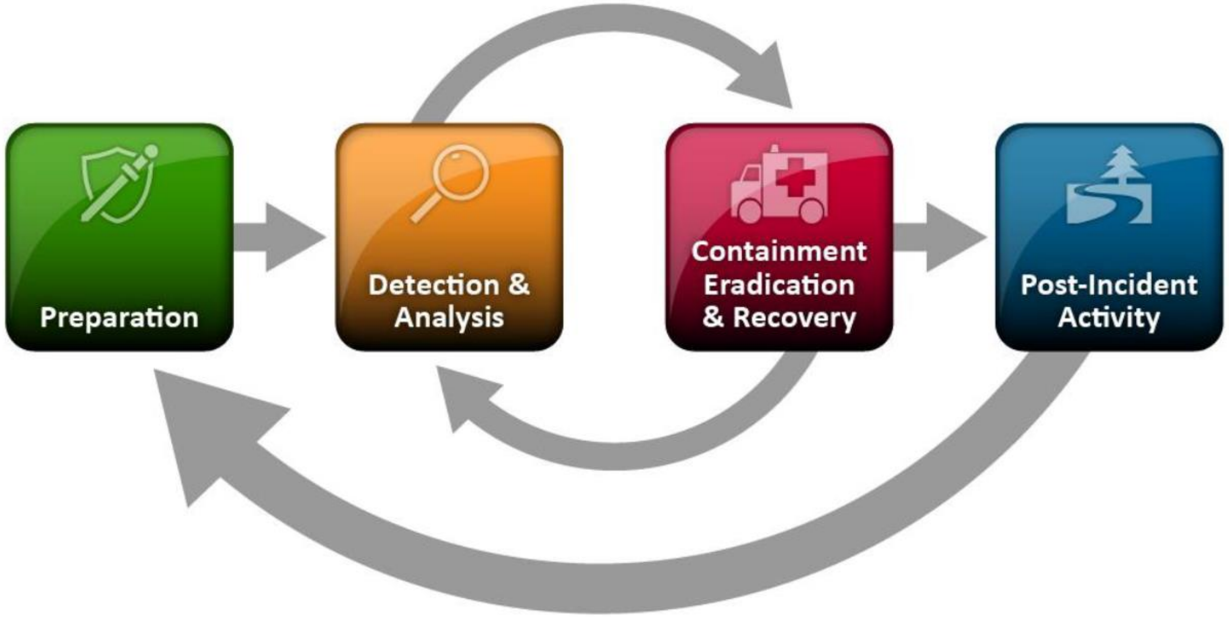
Incident response preparation includes preventing incidents by ensuring that systems, networks, and applications are sufficiently secure

- Risk Assessments
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Handling an Incident - Preparation

- Establishing and training an incident response team
- Acquiring the necessary tools and resources
  - Incident Handler Communication Facilities
  - Incident Analysis Hardware and Software
  - Incident Analysis Resources
  - Incident Mitigation Software


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

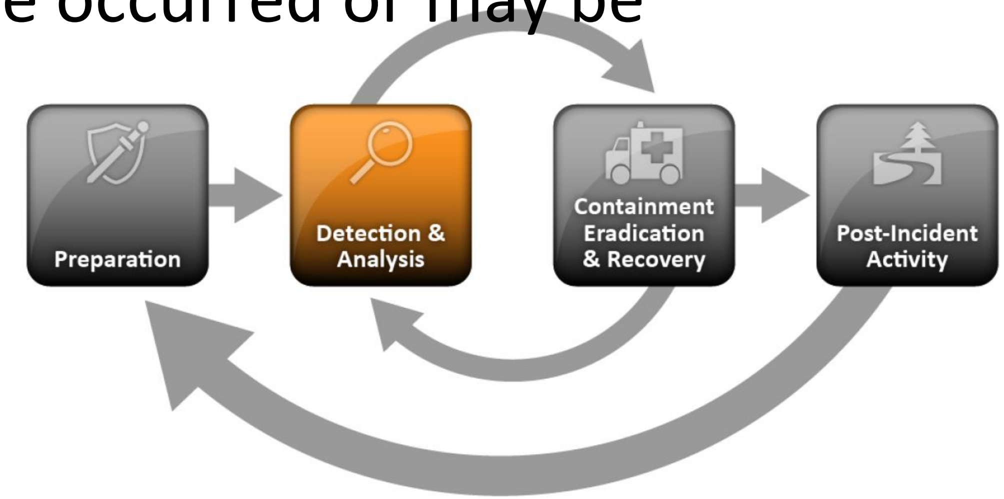
Handling an Incident – Detection and Analysis

Signs of an incident

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem

Signs of an incident fall into one of two categories:

1. **Precursors** – a sign that an incident may occur in the future
2. **Indicators** - a sign that an incident may have occurred or may be occurring now

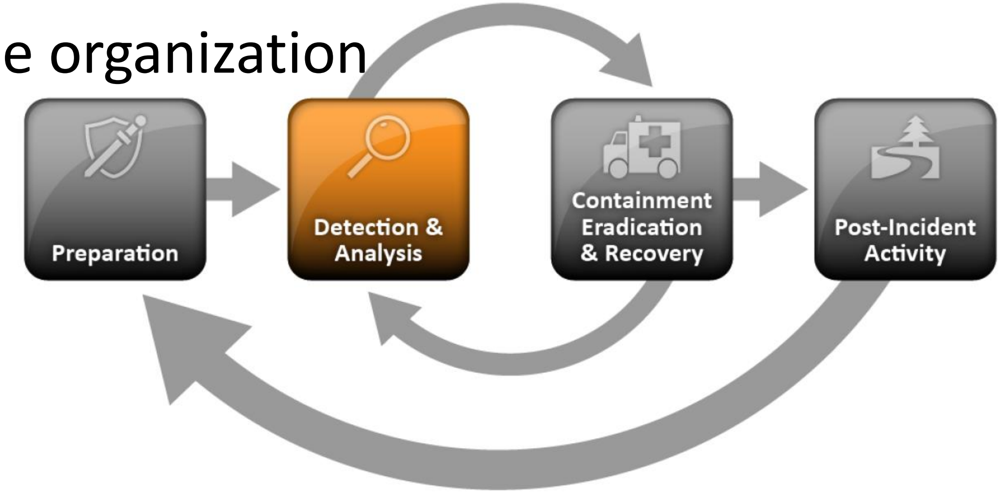

Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Handling an Incident – Detection and Analysis

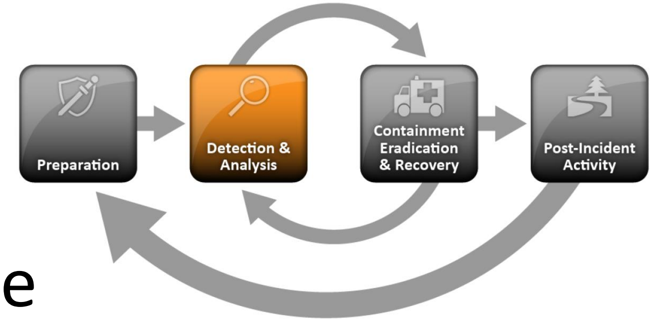
Precursors – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

Examples of precursors are:

- Web server log entries that show the usage of a vulnerability scanner
- NIST National Vulnerability Database (NVD) Announcement of a new exploit targeting a vulnerability of the organization’s mail server
- A threat from a group stating the group will attack the organization


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Detection and Analysis


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Indicators - While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:

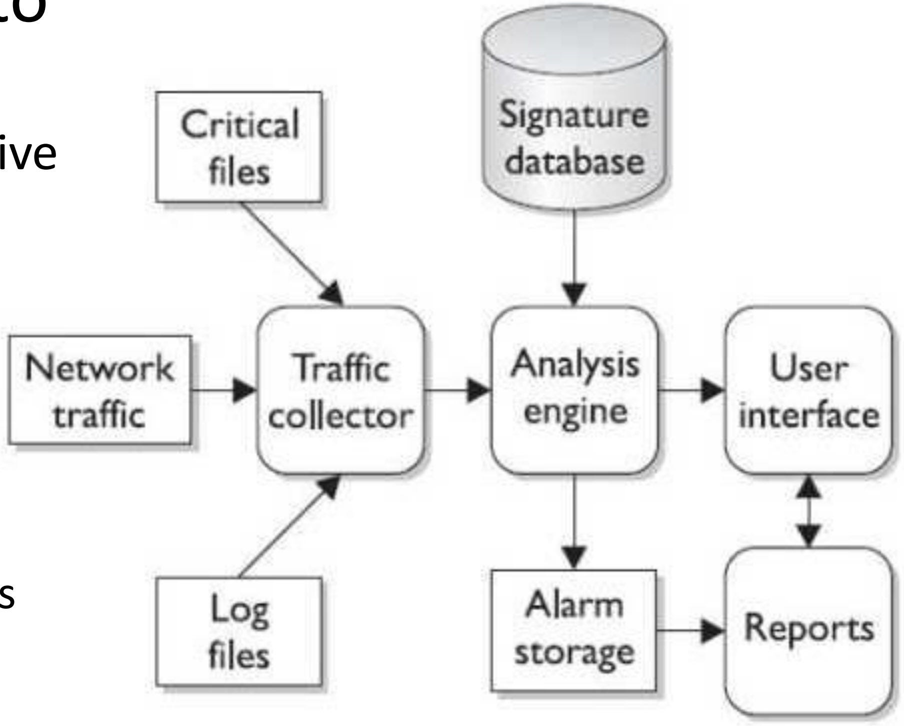
- An application logs multiple failed login attempts from an unfamiliar remote system
- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server
- A system administrator sees a filename with unusual characters
- Antivirus software alerts when it detects that a host is infected with malware
- A host records a configuration change in its log
- An email administrator sees a large number of bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

Intrusion Detection Systems (IDSs)

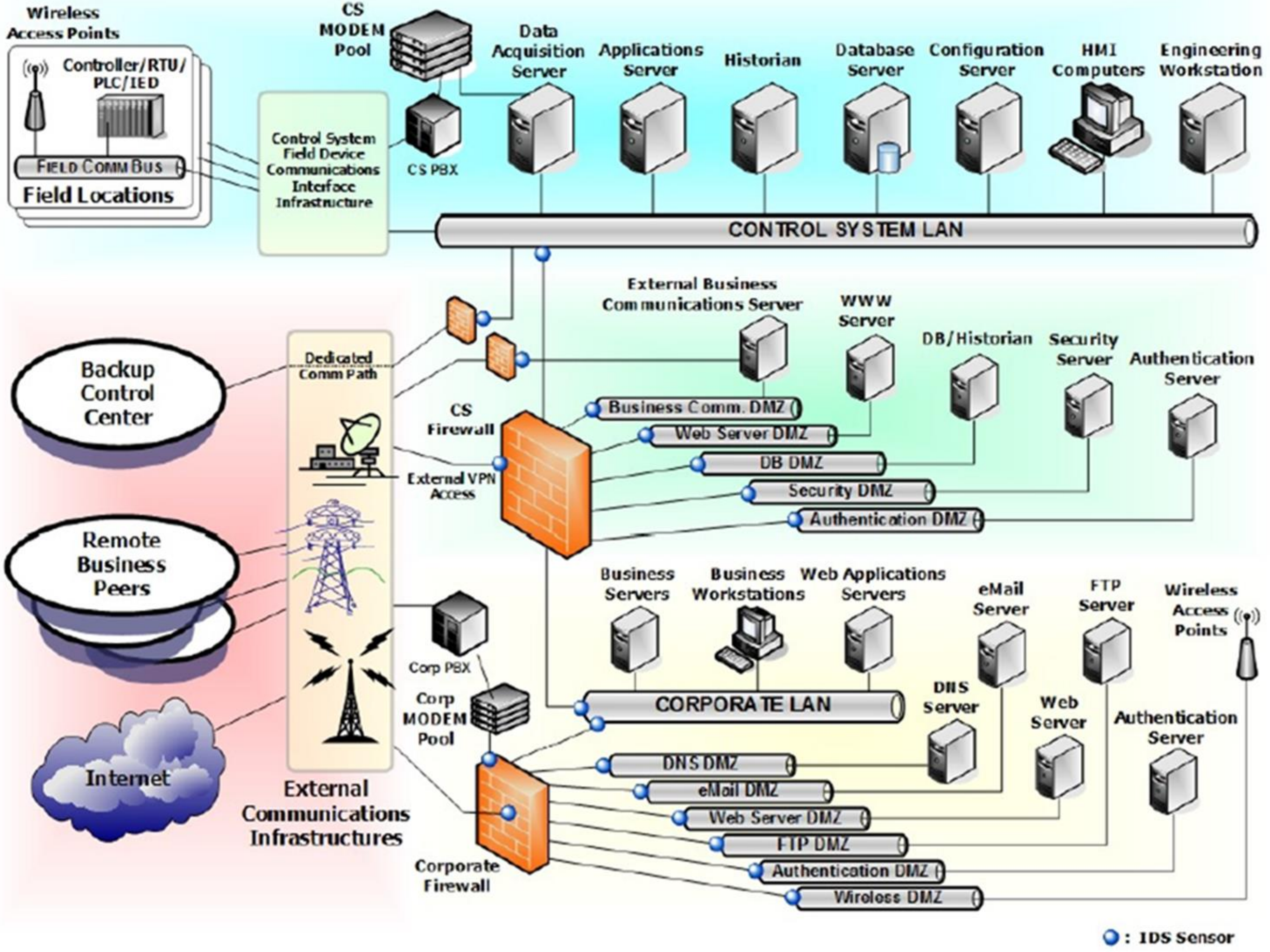
While firewalls and antivirus are preventive controls, IDS are access control monitoring devices designed to

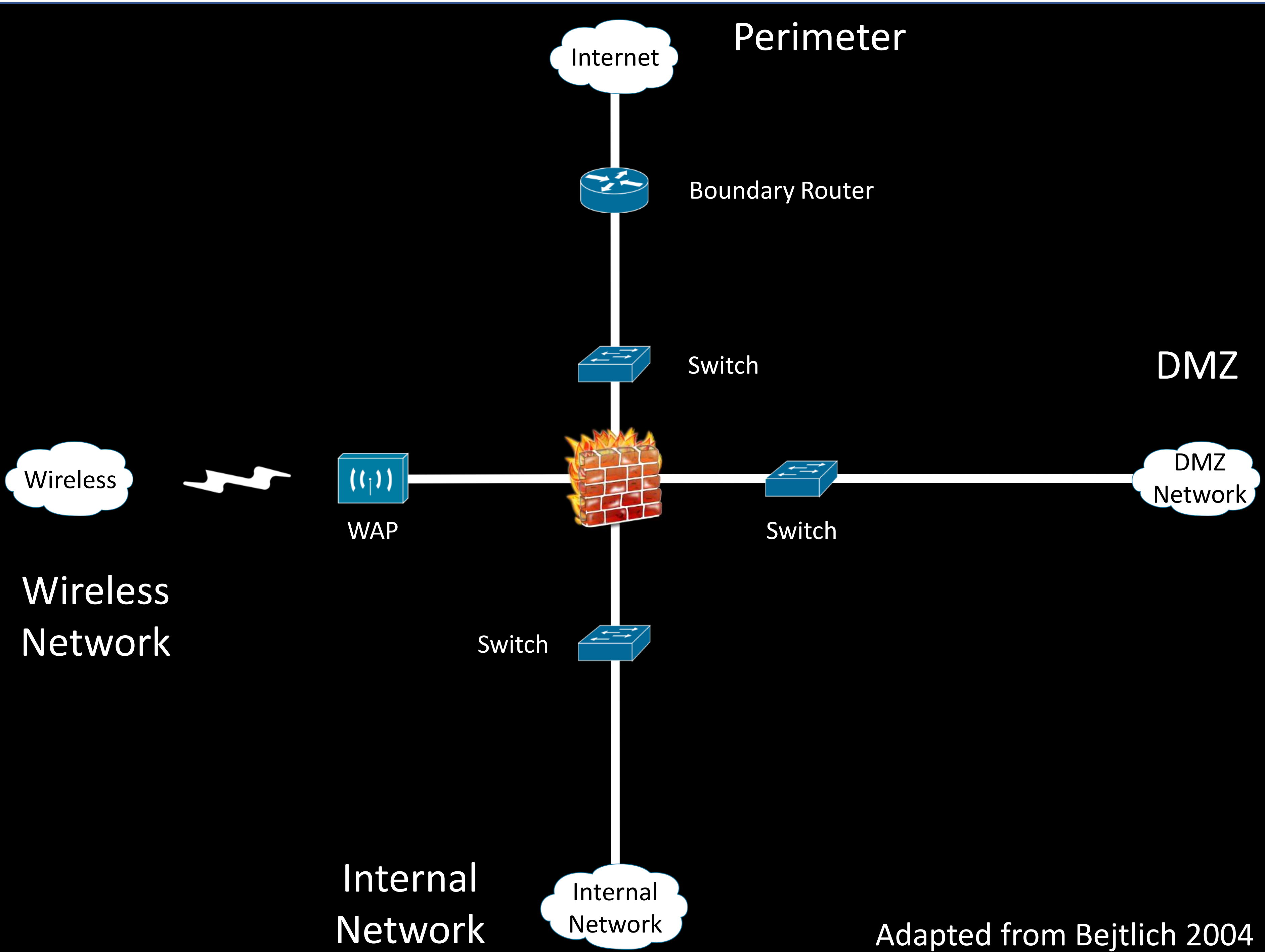
1. Detect a security breach
2. Aid in mitigating damage caused by hackers breaking into sensitive computer and network systems

- IDS' components
  1. Sensors
     - Collect and send traffic and user activity data to analyzers
  2. Analyzers
     - Look for suspicious activity and if found sends alert to administrator's interface
  3. Administrative interfaces


Critical files
Signature database
Network traffic
Traffic collector
Analysis engine
User interface
Log files
Alarm storage
Reports

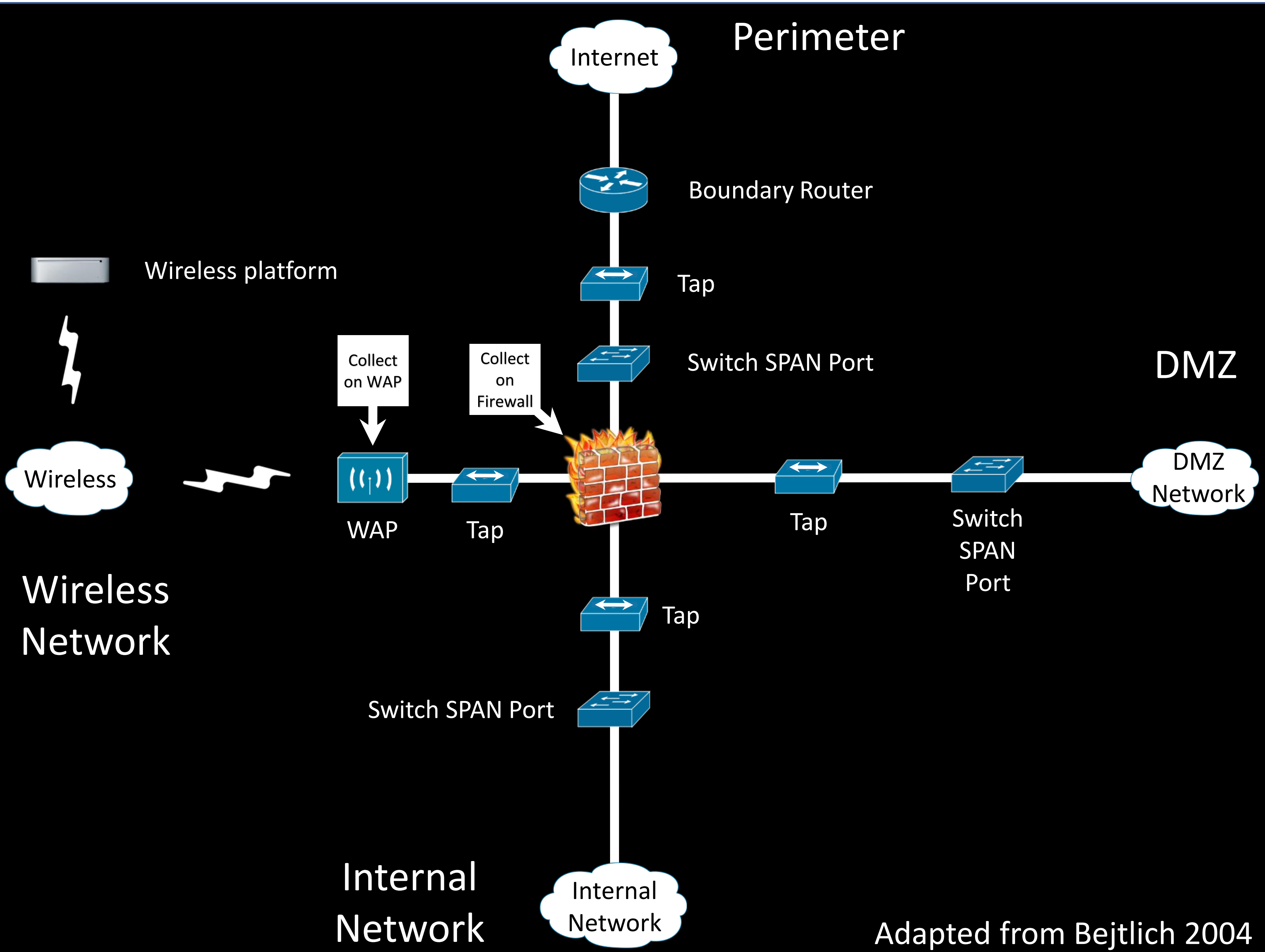
Example of IDS Locations


Wireless Access Points
Controller/RTU/ PLC/IED
FIELD COMM BUS
Field Locations
Control System Field Device Communications Interface Infrastructure
CS MODEM Pool
CS PBX
Data Acquisition Server
Applications Server
Historian
Database Server
Configuration Server
HMI Computers
Engineering Workstation
CONTROL SYSTEM LAN
External Business Communications Server
WWW Server
DB/Historian
Security Server
Authentication Server
Backup Control Center
Dedicated Comm Path
CS Firewall
External VPN Access
Business Comm. DMZ
Web Server DMZ
DB DMZ
Security DMZ
Authentication DMZ
Remote Business Peers
Internet
External Communications Infrastructures
Corp PBX
Corp MODEM Pool
Business Servers
Business Workstations
Web Applications Servers
eMail Server
FTP Server
Wireless Access Points
CORPORATE LAN
DNS Server
Web Server
Authentication Server
DNS DMZ
eMail DMZ
Web Server DMZ
FTP DMZ
Authentication DMZ
Wireless DMZ
Corporate Firewall
● : IDS Sensor



Internet
Perimeter
Boundary Router
Switch
DMZ
Wireless
WAP
Switch
DMZ Network
Wireless Network
Switch
Internal Network
Internal Network

Adapted from Bejtlich 2004



Perimeter

Internet

Boundary Router

Tap

Switch SPAN Port

DMZ

DMZ Network

Tap

Switch SPAN Port

Wireless platform

Wireless

Collect on WAP

Collect on Firewall

WAP

Tap

Wireless Network

Tap

Switch SPAN Port

Internal Network

Internal Network

Adapted from Bejtlich 2004

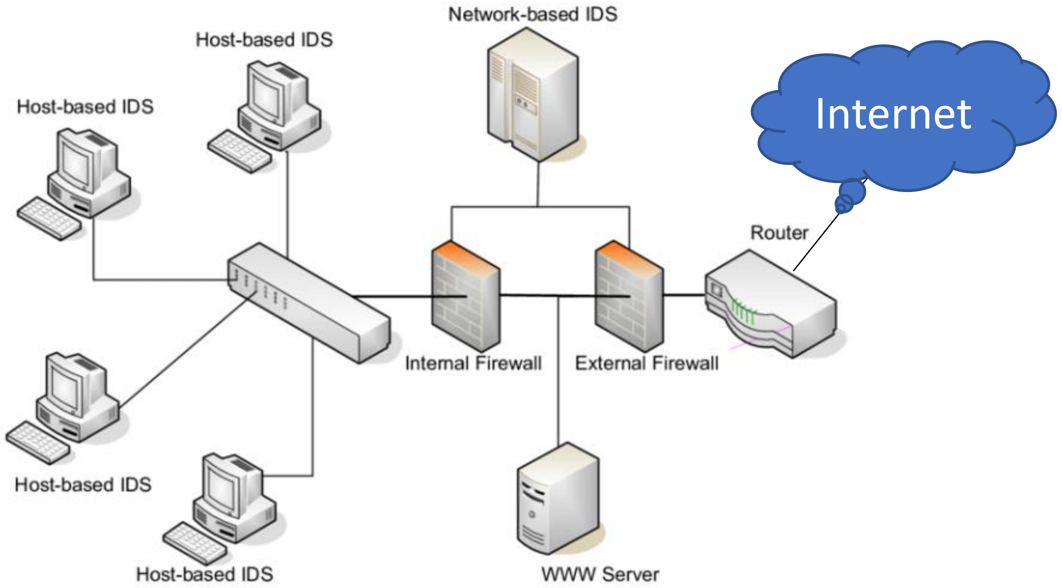
Intrusion Detection Systems (IDSs)

Two main types of IDS

1. **Host-based** for analyzing activity within a particular computer system
2. **Network-based** for monitoring network communications

IDS can be configured to:

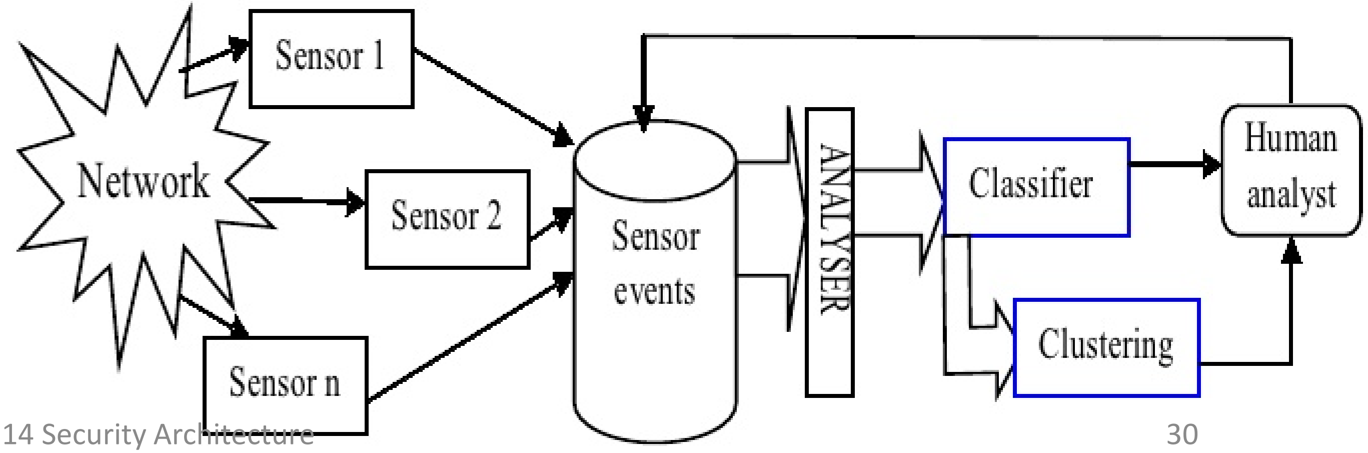
- Watch for attacks
- Alert administrator as attacks happen
- Expose a hacker & her/his techniques
- Work with firewalls to terminate a connection


Network-based IDS
Host-based IDS
Host-based IDS
Internet
Router
Internal Firewall
External Firewall
Host-based IDS
Host-based IDS
WWW Server

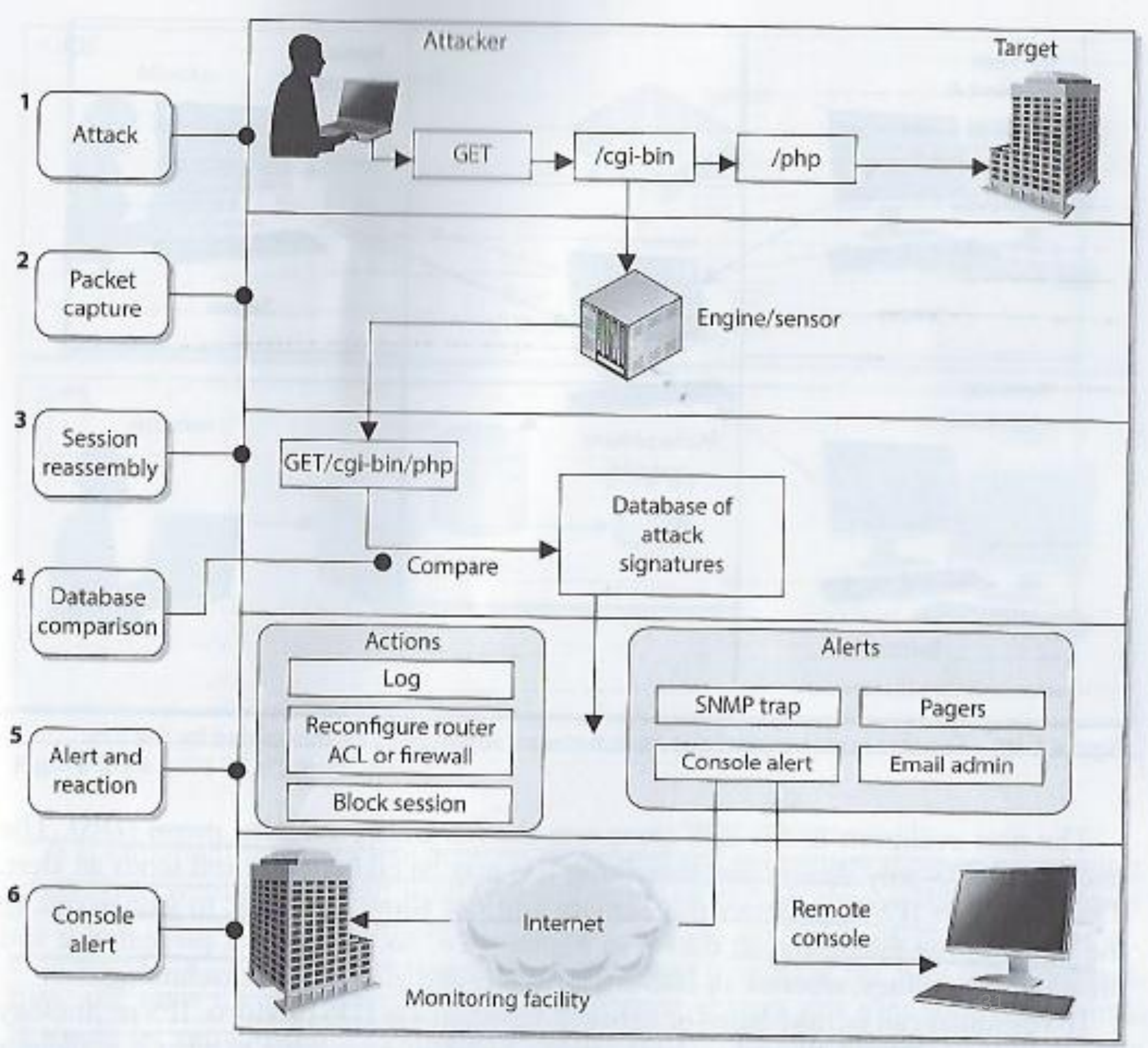
Intrusion Detection Systems (IDS)

Network-based IDS (NIDS)

- Uses sensors which can be either host computers with specialized software installed or dedicated appliances
  - Each have a NIC (network interface card)
    - NIC is configured in promiscuous mode to capture all traffic (rather than packets addressed to the host computer
    - Copies packets – sending one copy up the OSI stack (for normal processing or possible analysis with a HIDS), and another copy to analyzer looking for specific patterns in the network traffic
- Monitors network traffic, cannot see the activity happening within the higher levels of the OSI stack (HIDS is used for this)


Network
Sensor 1
Sensor 2
Sensor n
Sensor events
ANALYSER
Classifier
Clustering
Human analyst

Basic architecture of a Network IDS


1
Attack
Attacker
Target
GET
/cgi-bin
/php
2
Packet capture
Engine/sensor
3
Session reassembly
GET/cgi-bin/php
4
Database comparison
Compare
Database of attack signatures
5
Alert and reaction
Actions
Log
Reconfigure router ACL or firewall
Block session
Alerts
SNMP trap
Pagers
Console alert
Email admin
6
Console alert
Internet
Remote console
Monitoring facility

Harris, S. and Maymi, F. (2016) All In One CISSSP Exam Guide, Seventh Edition, McGraw-Hill Education

Intrusion Prevention Systems (IPS)

IDS – Detect something bad may be taking place and send an alert

Detective and "after the fact" response

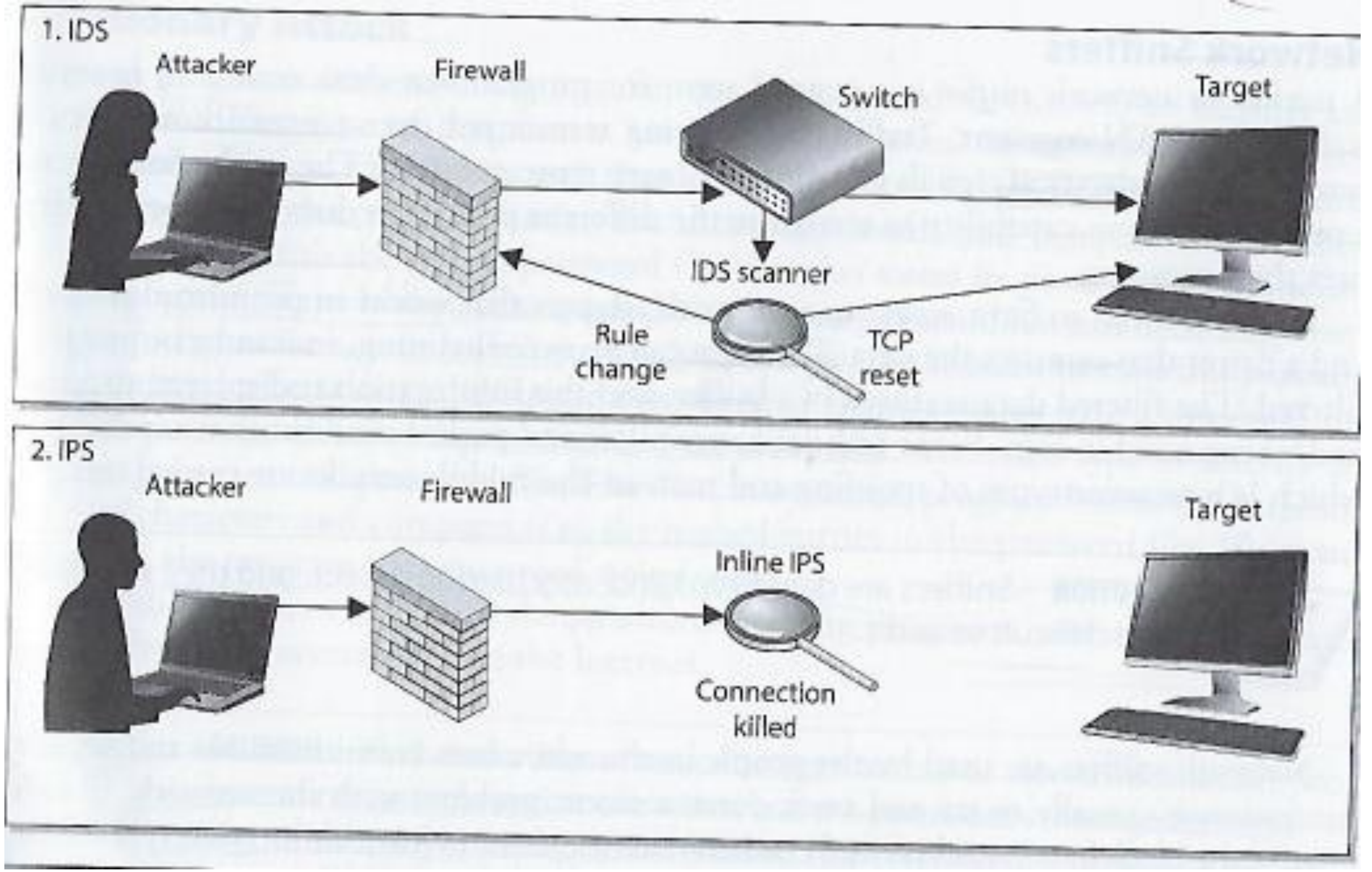
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
  - *Preventive and proactive response*

  - *IPS can be host-based or network-based (like IDS)*
  - *Can be content-based (looking deep into packets), conduct protocol analysis or be signature matching*
  - *Also can use rate-based metrics to identify suspicious increases in volumes of traffic*
    - *E.g. DoS – flood attack*
    - *Traffic flow anomalies – "slow and low" stealth attack attempting to be undetected*

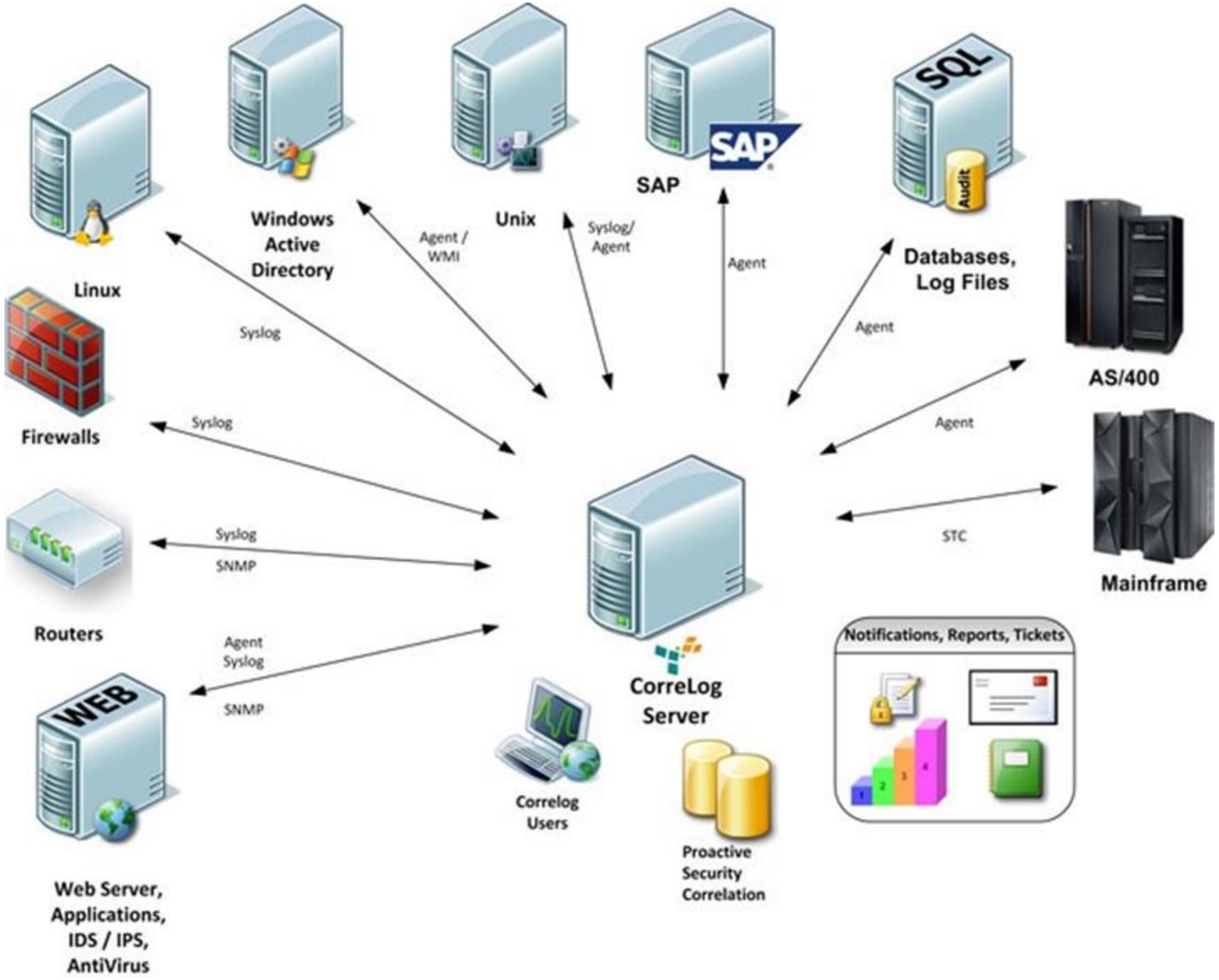
IDS versus IPS

Possible responses to a triggered event:

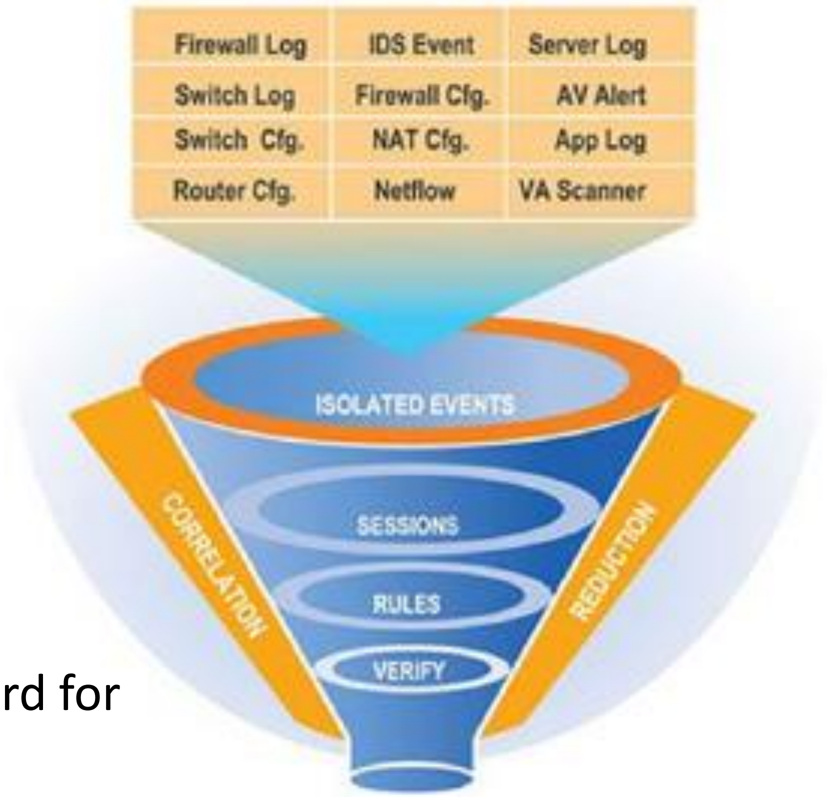
- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors and administrators


1. IDS
Attacker
Firewall
Switch
Target
IDS scanner
Rule change
TCP reset
2. IPS
Attacker
Firewall
Inline IPS
Target
Connection killed

Continuous monitoring with a Security Information and Event Management (SIEM) system


Windows Active Directory
Unix
SAP
SAP
Linux
Agent / WMI
Syslog/ Agent
Agent
Databases, Log Files
Audit
SQL
Syslog
Agent
AS/400
Firewalls
Syslog
Agent
Syslog
SNMP
STC
Mainframe
Routers
Agent Syslog
SNMP
WEB
CorreLog Server
Notifications, Reports, Tickets
Correlog Users
Proactive Security Correlation
Web Server, Applications, IDS / IPS, AntiVirus

SIEM’s help with Data Analysis and Correlation


Firewall Log
IDS Event
Server Log
Switch Log
Firewall Cfg.
AV Alert
Switch Cfg.
NAT Cfg.
App Log
Router Cfg.
Netflow
VA Scanner
ISOLATED EVENTS
SESSIONS
RULES
VERIFY
CORRELATION
REDUCTION

- Bring raw data events into one database
- Database software is programmed to look for “Notable events” or correlations
- Correlations will take seemingly isolated events and bring them forward for review/action:
  - **Windows Log:** Employee denied windows login (unknown user account)
  - **Identity Management System:** notes the user account was deleted because employee was terminated last month.
- Security Domains: Access, Endpoints, Networks, Identity

SIEM

- ***Security Information and Event Management (SIEM)*** market is defined by the customer's need to analyze event data in **real time.**

- Allows for the early detection of targeted attacks and data breaches

- Collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.

- Aggregates event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data.

Magic Quadrant

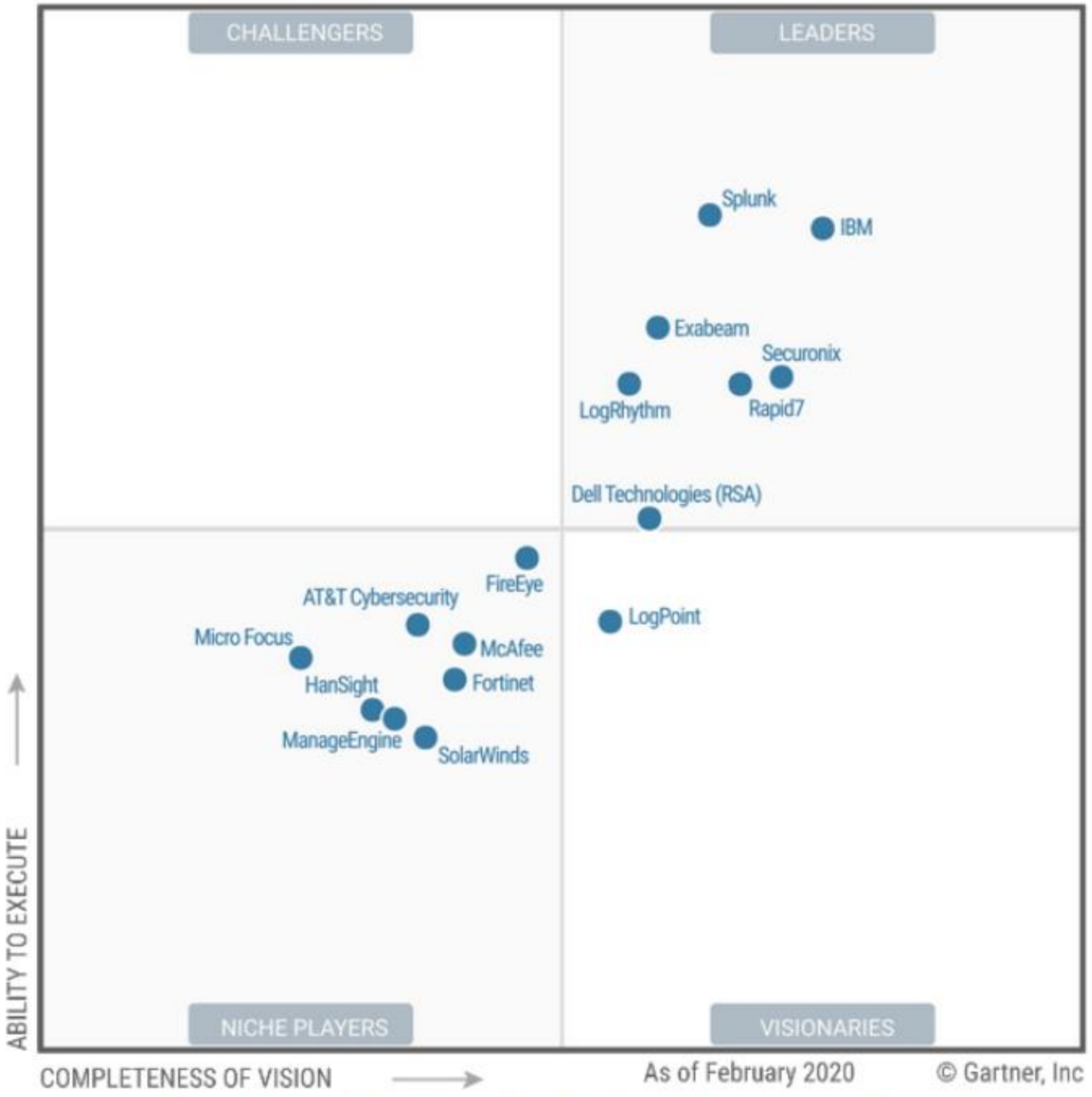
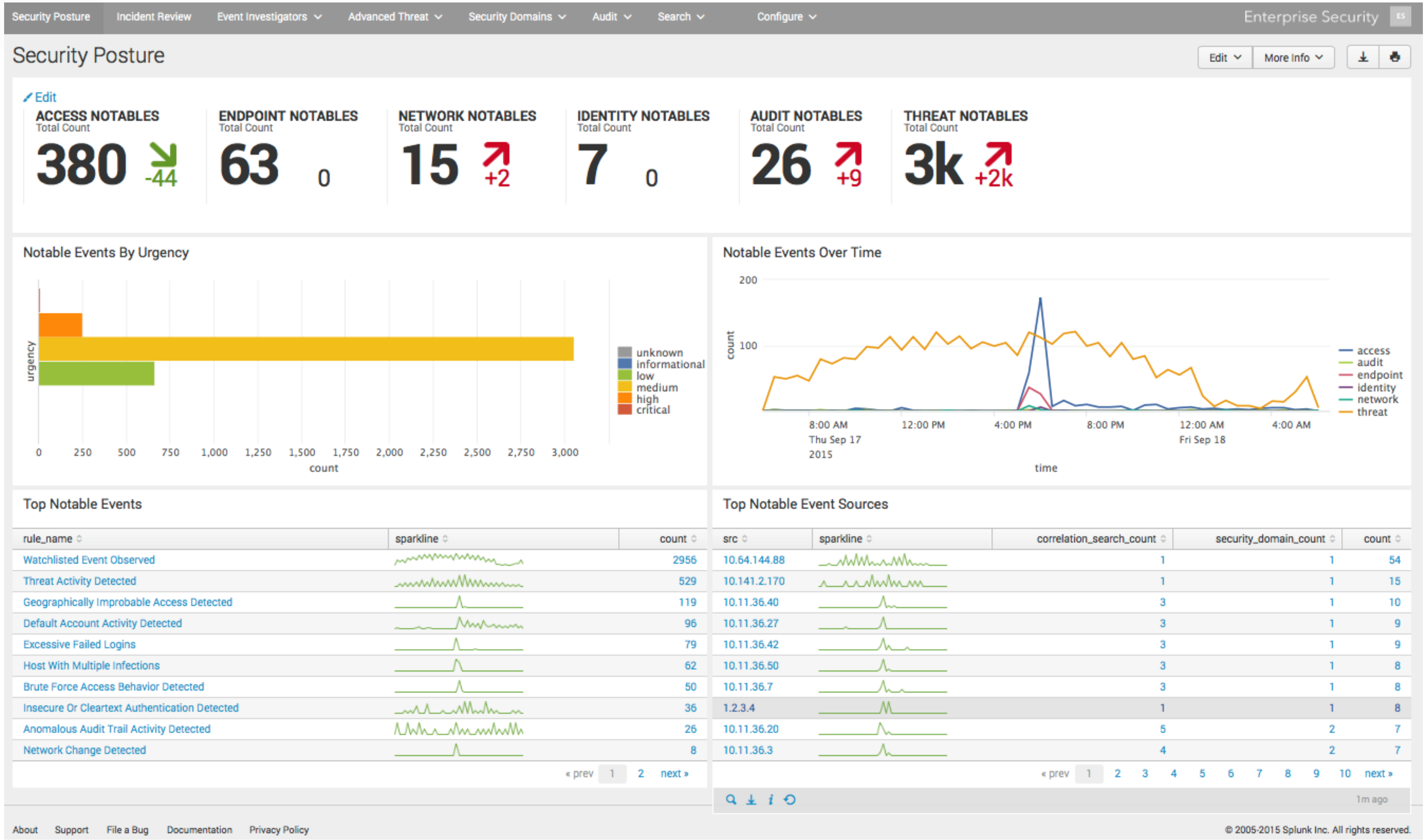


Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (February 2020)

splunk>


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Edit
More Info
Edit
Notable Events By Urgency
urgency
0
250
500
750
1,000
1,250
1,500
1,750
2,000
2,250
2,500
2,750
3,000
count
unknown
informational
low
medium
high
critical
Notable Events Over Time
200
100
count
8:00 AM
Thu Sep 17
2015
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Fri Sep 18
4:00 AM
time
access
audit
endpoint
identity
network
threat
« prev
1
2
next »
« prev
1
2
3
4
5
6
7
8
9
10
next »
1m ago
About
Support
File a Bug
Documentation
Privacy Policy

Security Posture

ACCESS NOTABLES
Total Count
380 -44

ENDPOINT NOTABLES
Total Count
63 0

NETWORK NOTABLES
Total Count
15 +2

IDENTITY NOTABLES
Total Count
7 0

AUDIT NOTABLES
Total Count
26 +9

THREAT NOTABLES
Total Count
3k +2k

Top Notable Events

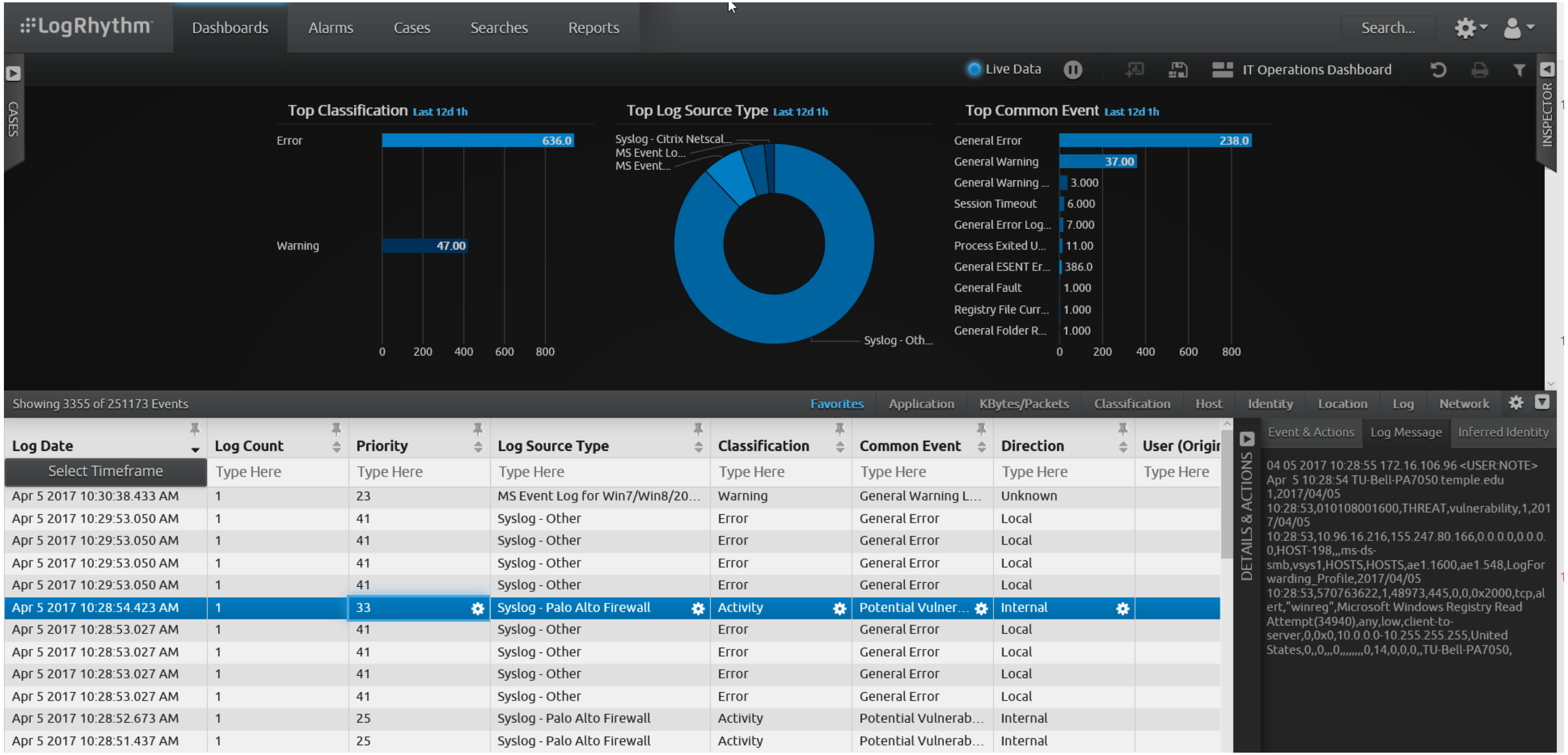
rule_name	sparkline	count
Watchlisted Event Observed		2956
Threat Activity Detected		529
Geographically Improbable Access Detected		119
Default Account Activity Detected		96
Excessive Failed Logins		79
Host With Multiple Infections		62
Brute Force Access Behavior Detected		50
Insecure Or Cleartext Authentication Detected		36
Anomalous Audit Trail Activity Detected		26
Network Change Detected		8

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.64.144.88		1	1	54
10.141.2.170		1	1	15
10.11.36.40		3	1	10
10.11.36.27		3	1	9
10.11.36.42		3	1	9
10.11.36.50		3	1	8
10.11.36.7		3	1	8
1.2.3.4		1	1	8
10.11.36.20		5	2	7
10.11.36.3		4	2	7

© 2005-2015 Splunk Inc. All rights reserved.

LogRhythm™

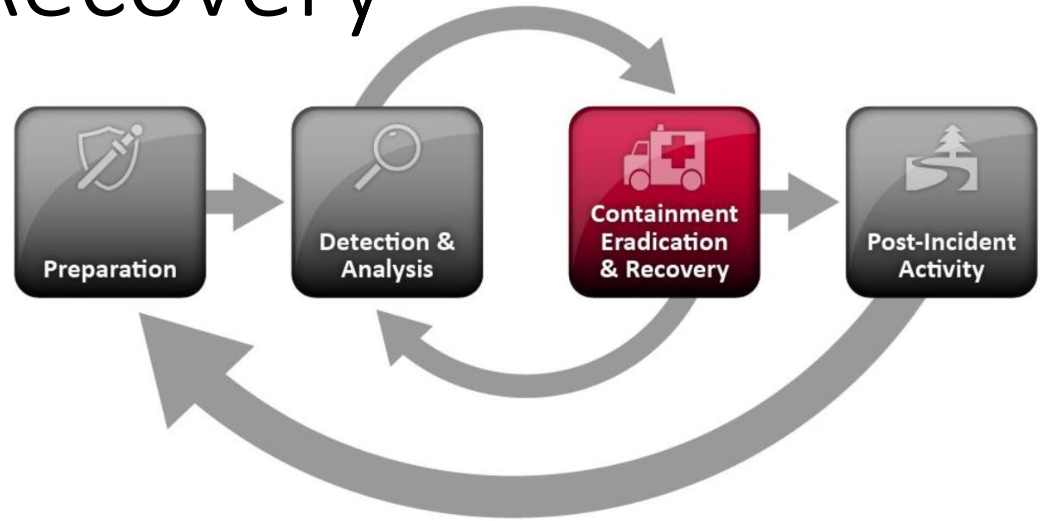

LogRhythm
Dashboards
Alarms
Cases
Searches
Reports
Search...
Live Data
IT Operations Dashboard
CASES
INSPECTOR
Top Classification Last 12d 1h
Error
636.0
Warning
47.00
0
200
400
600
800
Top Log Source Type Last 12d 1h
Syslog - Citrix Netscal...
MS Event Lo...
MS Event...
Syslog - Oth...
Top Common Event Last 12d 1h
General Error
238.0
General Warning
37.00
General Warning ...
3.000
Session Timeout
6.000
General Error Log...
7.000
Process Exited U...
11.00
General ESENT Er...
386.0
General Fault
1.000
Registry File Curr...
1.000
General Folder R...
1.000
0
200
400
600
800
Favorites
Application
KBytes/Packets
Classification
Host
Identity
Location
Log
Network
DETAILS & ACTIONS
Event & Actions
Log Message
Inferred Identity

Showing 3355 of 251173 Events

Log Date	Log Count	Priority	Log Source Type	Classification	Common Event	Direction	User (Origin
Select Timeframe	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here	Type Here
Apr 5 2017 10:30:38.433 AM	1	23	MS Event Log for Win7/Win8/20...	Warning	General Warning L...	Unknown	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:29:53.050 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:54.423 AM	1	33	Syslog - Palo Alto Firewall	Activity	Potential Vulner...	Internal	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:53.027 AM	1	41	Syslog - Other	Error	General Error	Local	
Apr 5 2017 10:28:52.673 AM	1	25	Syslog - Palo Alto Firewall	Activity	Potential Vulnerab...	Internal	
Apr 5 2017 10:28:51.437 AM	1	25	Syslog - Palo Alto Firewall	Activity	Potential Vulnerab...	Internal	

```
04 05 2017 10:28:55 172.16.106.96 <USER:NOTE>
Apr  5 10:28:54 TU-Bell-PA7050.temple.edu
1,2017/04/05
10:28:53,010108001600,THREAT,vulnerability,1,201
7/04/05
10:28:53,10.96.16.216,155.247.80.166,0.0.0.0,0.0.0.
0,HOST-198,,,ms-ds-
smb,vsys1,HOSTS,HOSTS,ae1.1600,ae1.548,LogFor
warding_Profile,2017/04/05
10:28:53,570763622,1,48973,445,0,0,0x2000,tcp,al
ert,"winreg",Microsoft Windows Registry Read
Attempt(34940),any,low,client-to-
server,0,0x0,10.0.0.0-10.255.255.255,United
States,0,,0,,,0,,,,,,,,0,14,0,0,0,,TU-Bell-PA7050,
```

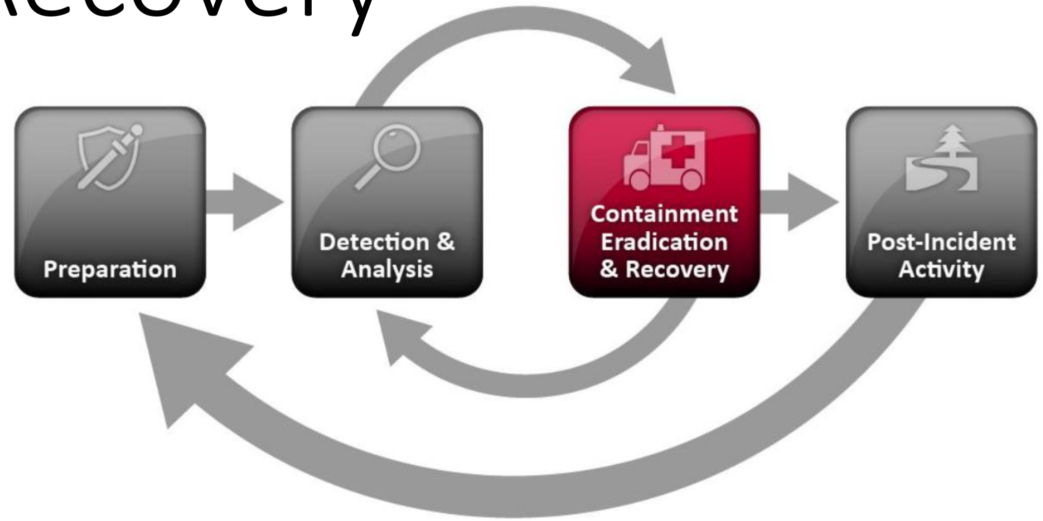
Containment, Eradication, and Recovery


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Containment - is important before an incident overwhelms resources or increases damage

- Most incidents require containment, which provides time for developing a tailored remediation strategy
- An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions)
- Criteria for selecting among containment strategies are based on type of incident:
  - Potential damage & theft of resources
  - Need for evidence preservation
  - Service availability requirements (e.g., network connectivity, services provided to external parties)
  - Time & resources needed to implement
  - Effectiveness (e.g., partial containment, full containment)

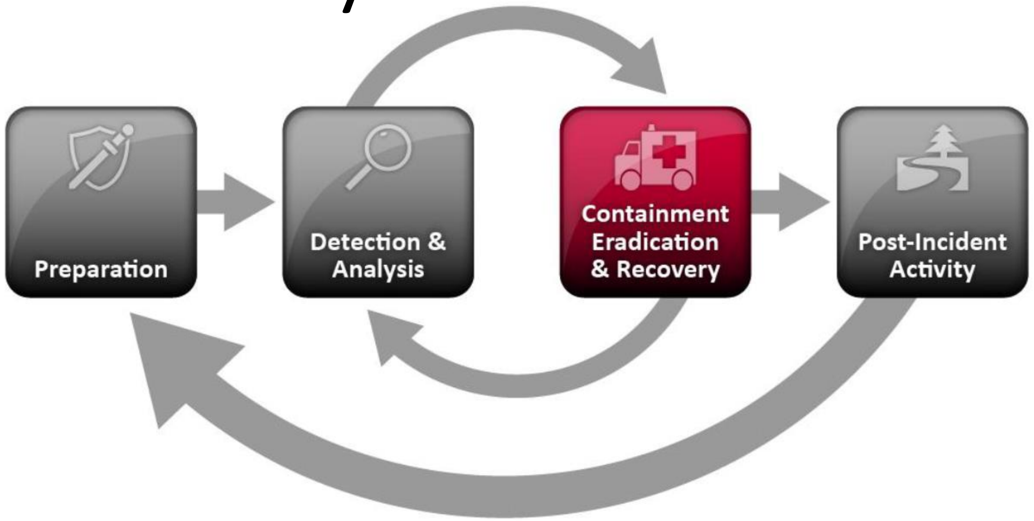
Containment, Eradication, and Recovery


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Eradication - After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as:

- Deleting malware
- Disabling breached user accounts
- Identifying and mitigating all vulnerabilities that were exploited
  - *During eradication, it is important to identify all affected hosts within the organization so that they can be remediated*

Containment, Eradication, and Recovery


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

Recovery - In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents

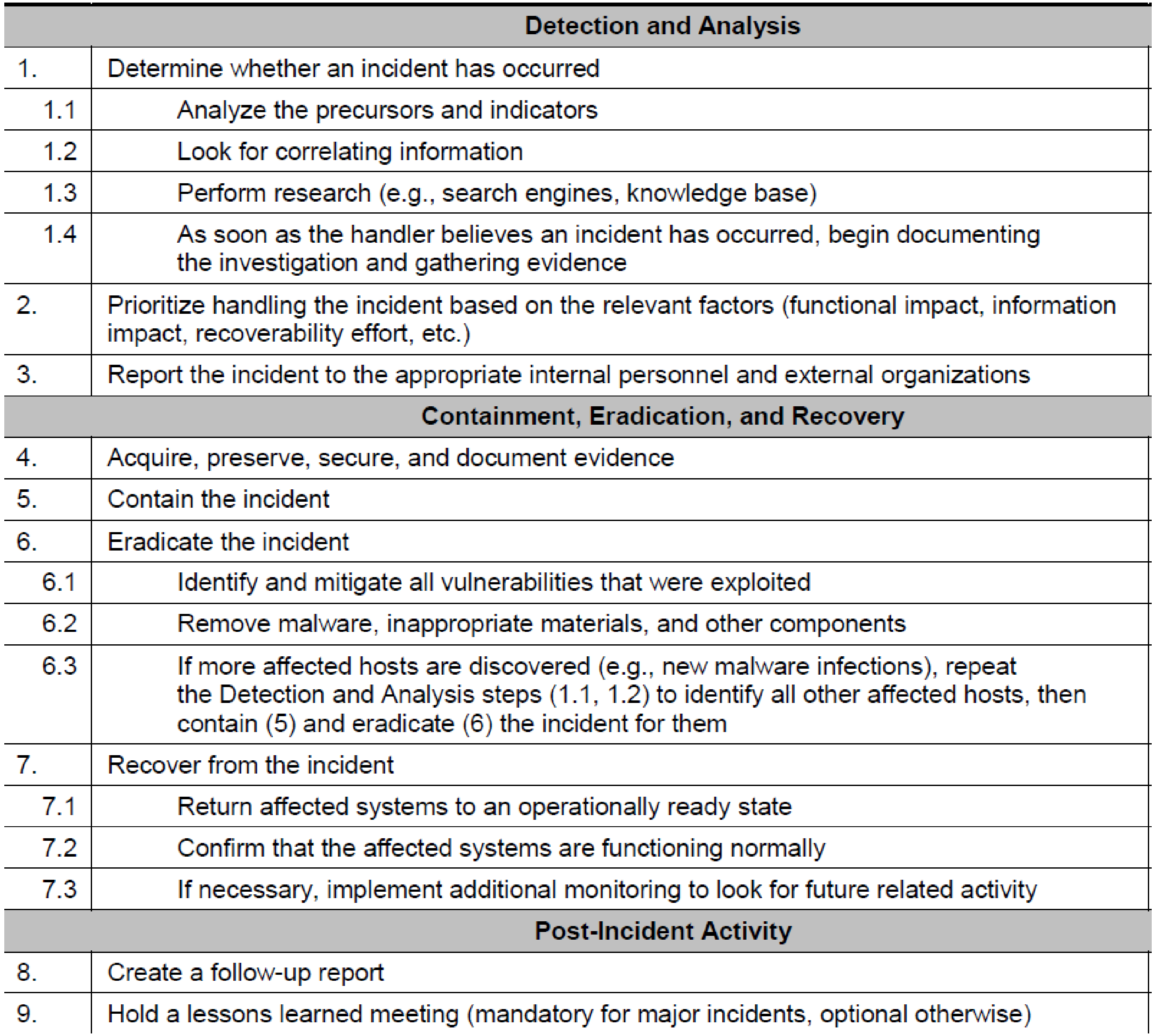
May involve such actions as:

- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g. firewall rules, boundary router access control lists, …)

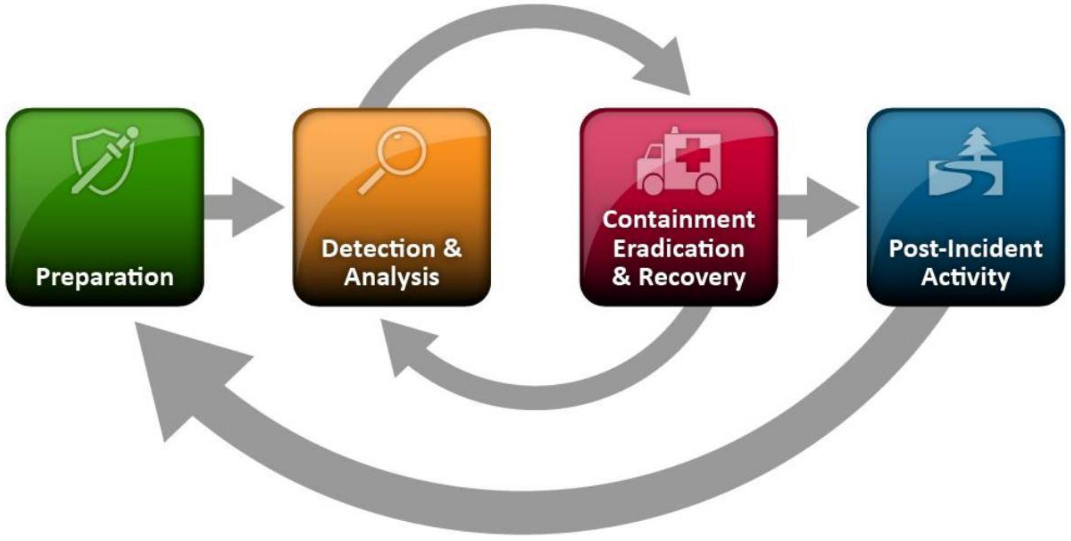
Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner

- As a result, higher levels of system logging or network monitoring are often part of the recovery process

Incident Response Workflow



	Detection and Analysis
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
	Containment, Eradication, and Recovery
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
	Post-Incident Activity
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)



Agenda

- ✓A bit more on Social Engineering & Physical Attacks and employee mistakes
- ✓NIST Cybersecurity Framework
- ✓Computer security incident response vocabulary
- ✓Attackers and detection
- ✓Handling an incident
  - ✓Preparation
  - ✓Detection and analysis
  - ✓Containment, eradication and recovery
  - ✓Incident response workflow
- ✓Incident case: South Carolina Department of Revenue