MIS 4596

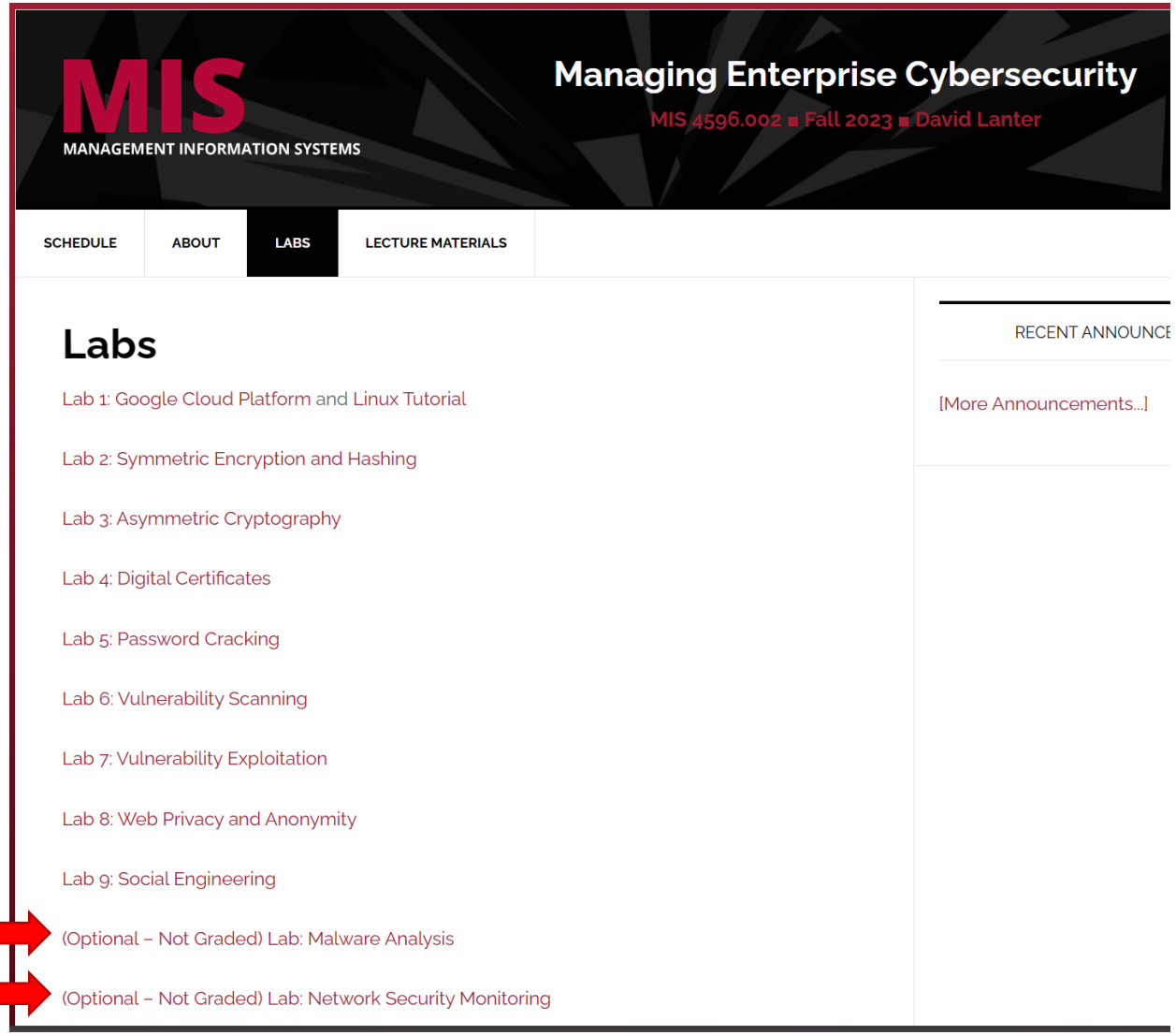
Unit#19

Network Security Monitoring and Incident Response

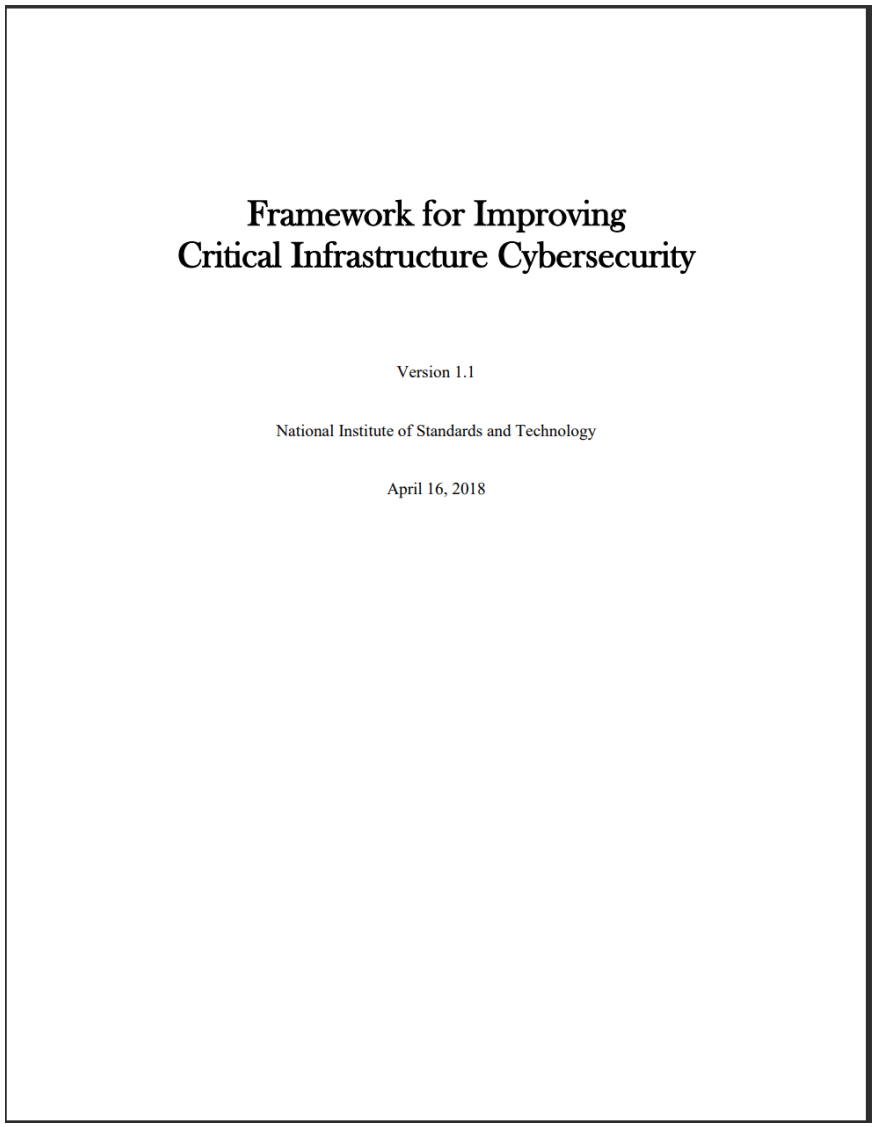
Agenda

- Labs 10 & 11
- 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

Labs 10 & 11 are “Optional – Not Graded”



NIST “Cybersecurity Framework”



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

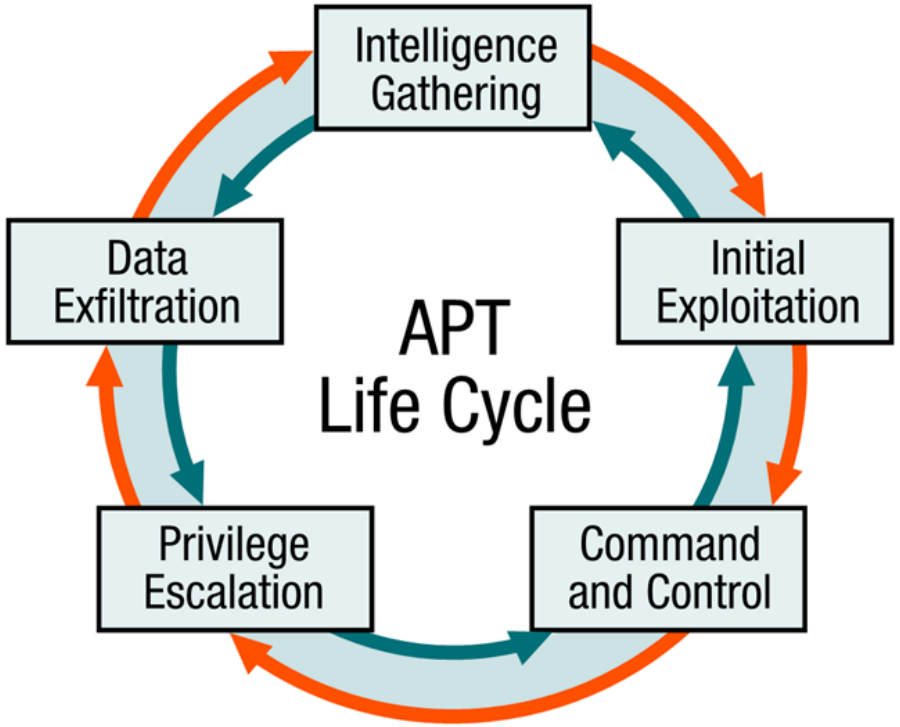
Computer security incident – is a violation (or imminent threat) of computer security policies, acceptable use policies, or standard practices, e.g.

- 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

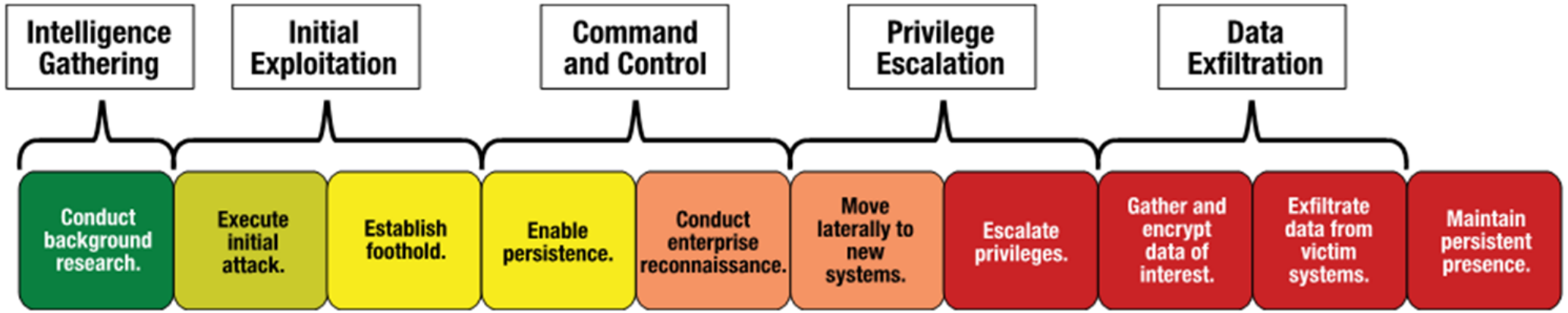
Computer security incident response

Is necessary because…

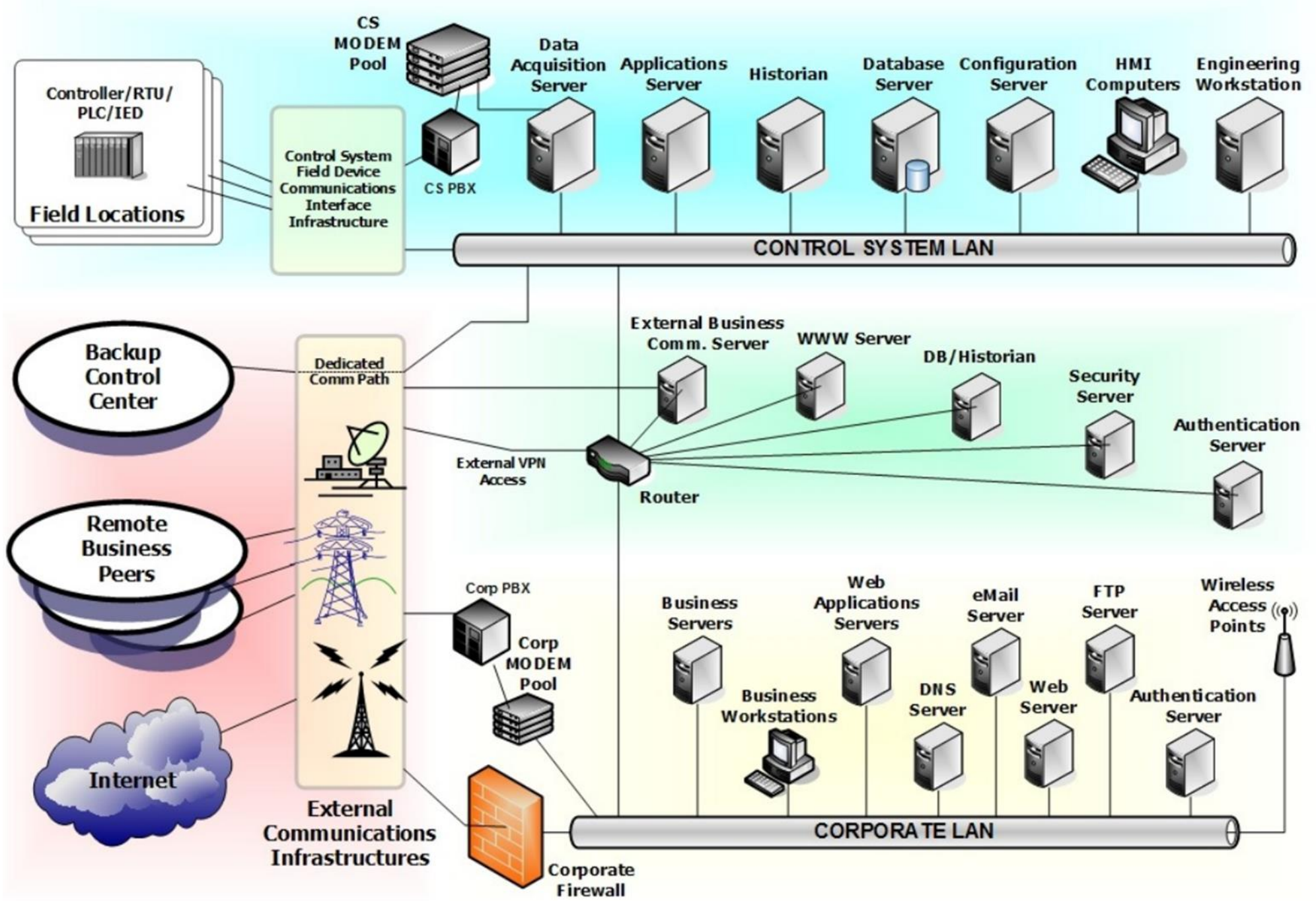
- Computer security controls, systems, and processes are not perfect
- Protections designed to protect information and information systems eventually fail
- Security breaches are inevitable



Anatomy of Advanced Persistent Threats

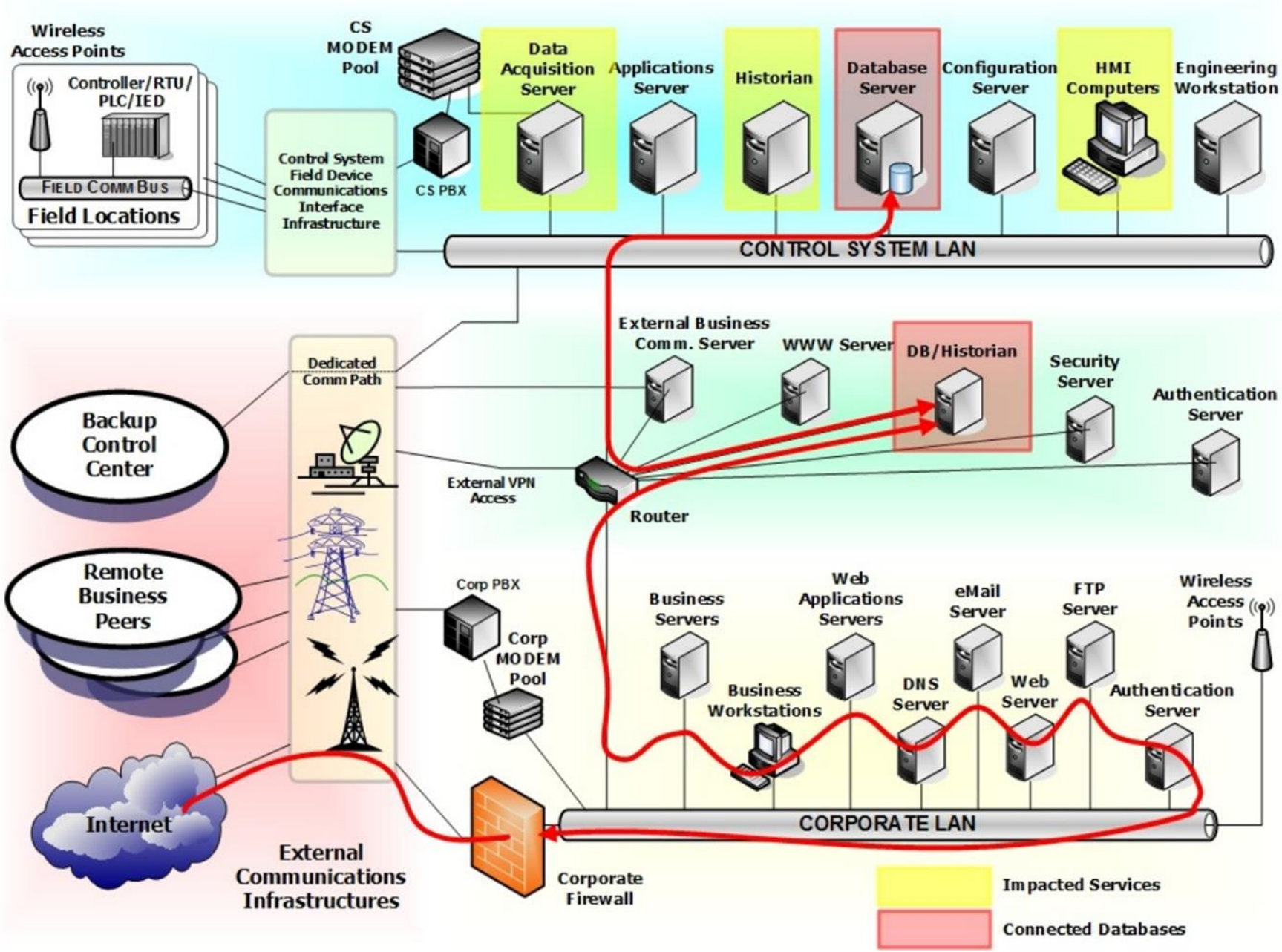


Example of a Network

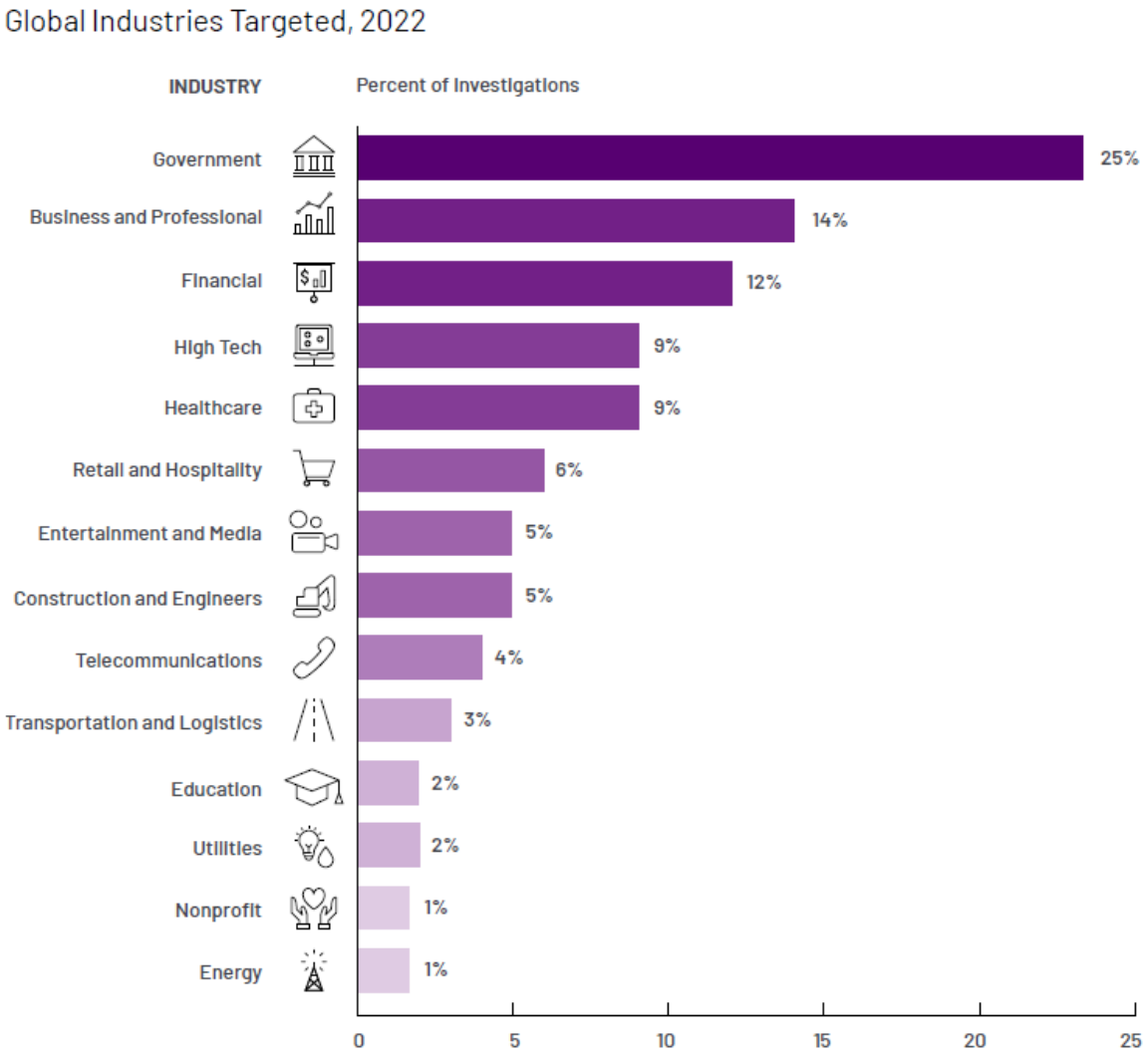


Integrated networks

Example of Network Intrusion

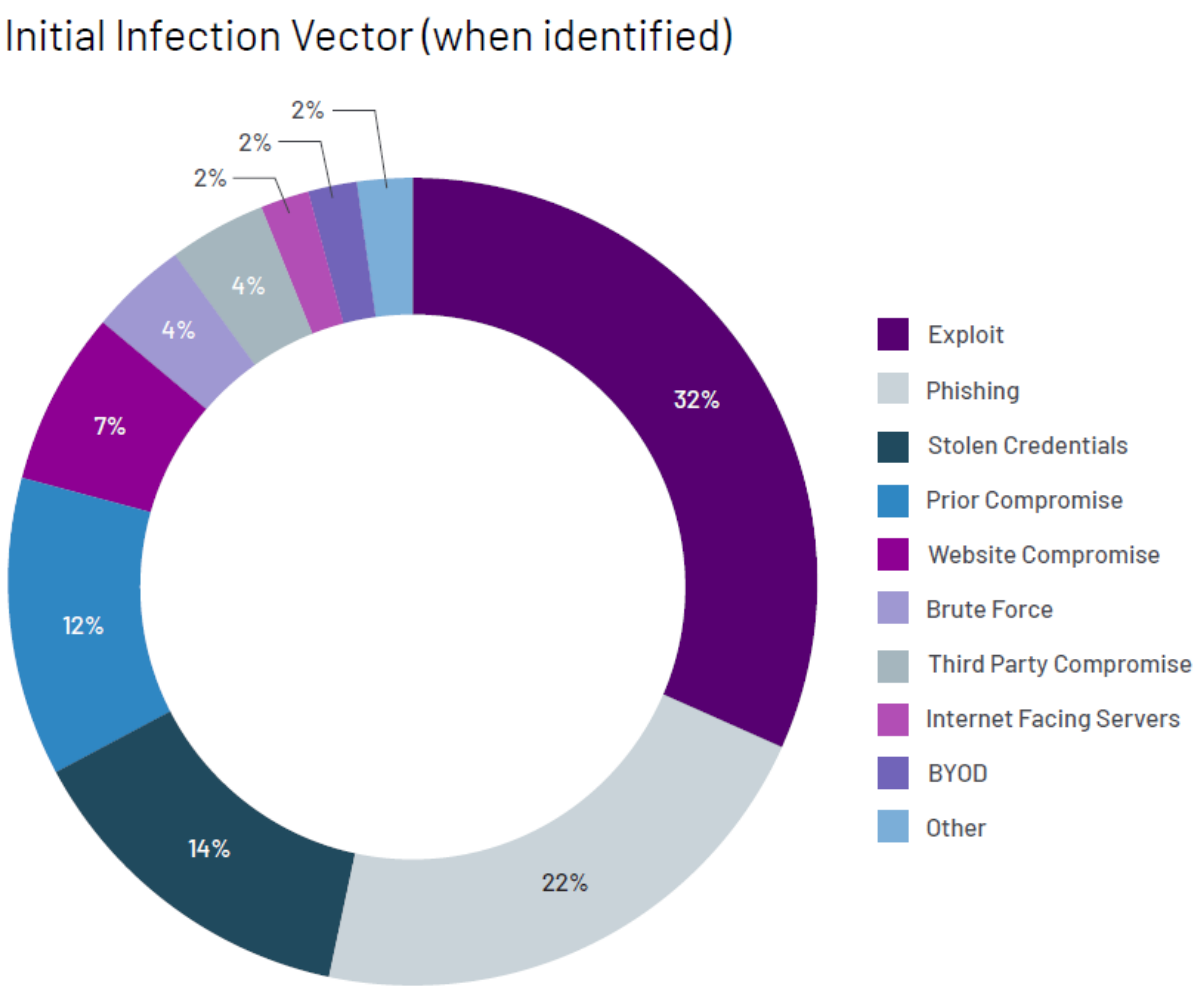


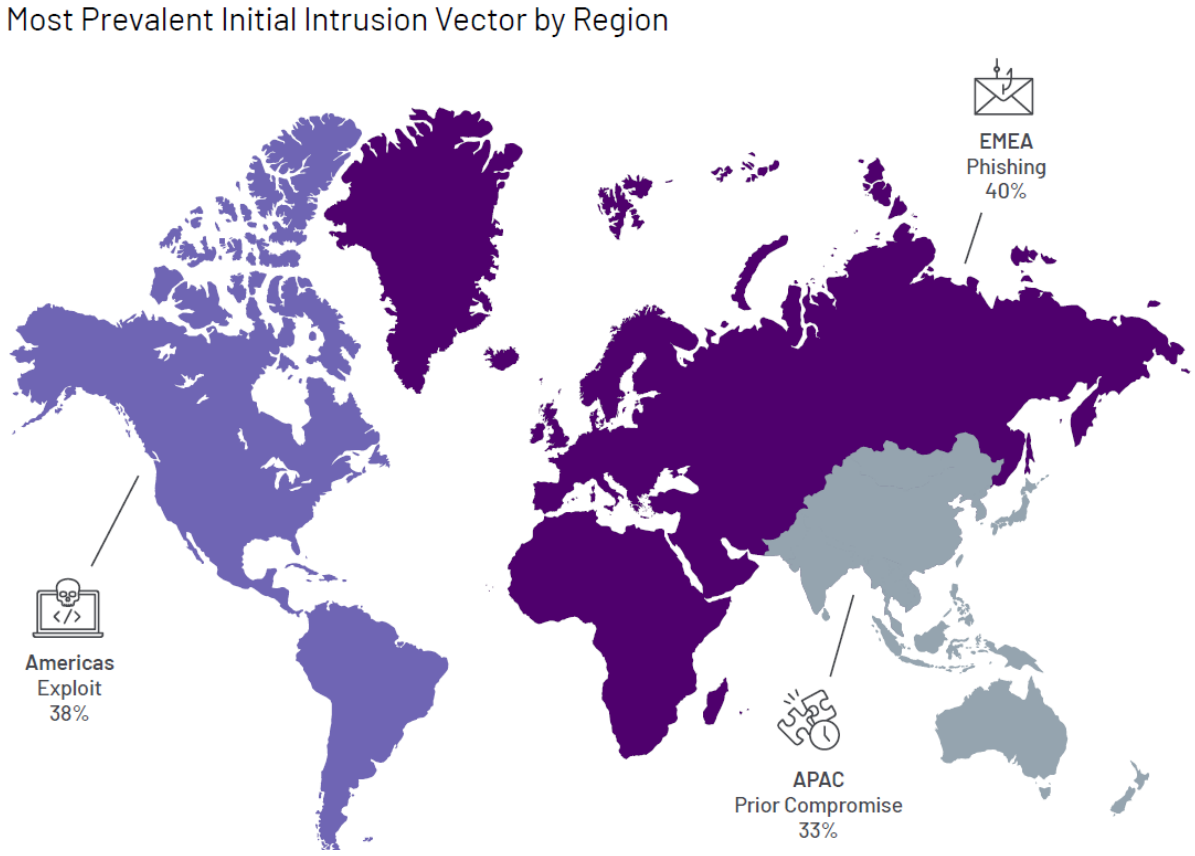
Industry Targeting



https://www.mandiant.com/m-trends

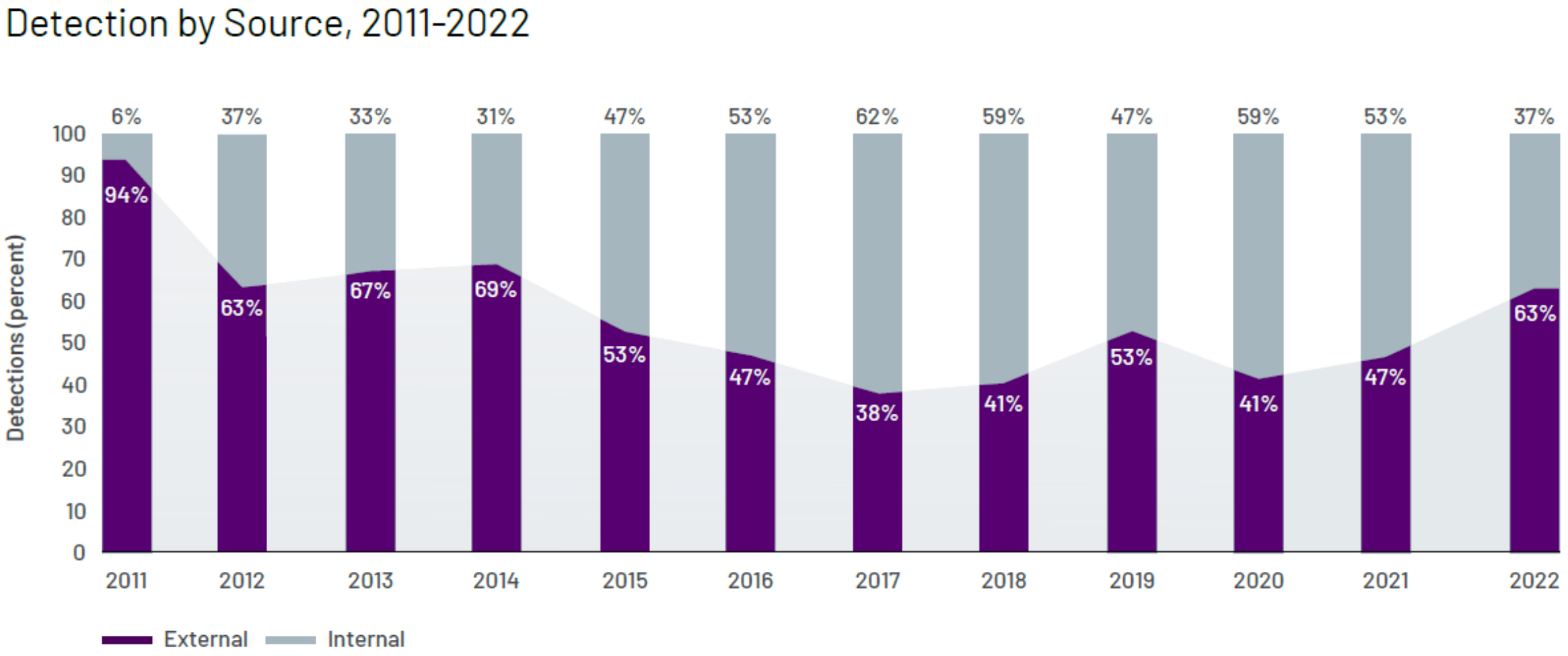
Intrusions initiated with an initial infection vector due to a prior compromise





https://www.mandiant.com/m-trends

Who is detecting intrusions by attackers?



https://www.mandiant.com/m-trends

How long are attackers remaining in compromised systems?

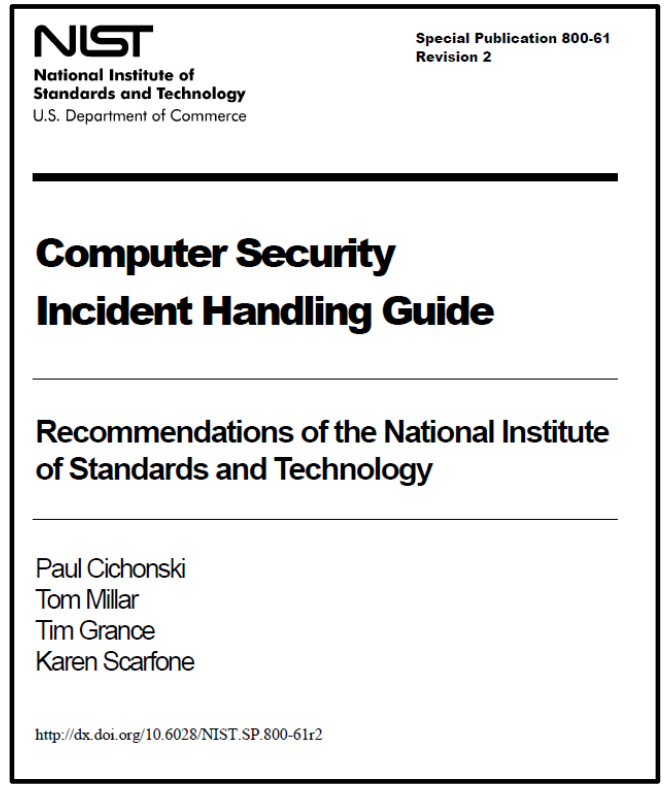
Global Median Dwell Time, 2011-2022

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	**416**	**243**	**229**	**205**	**146**	**99**	**101**	**78**	**56**	**24**	**21**	**16**
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

*"**Dwell time** is calculated as the number of days an attacker is present in a victim environment before they are detected."*

https://www.mandiant.com/m-trends

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

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

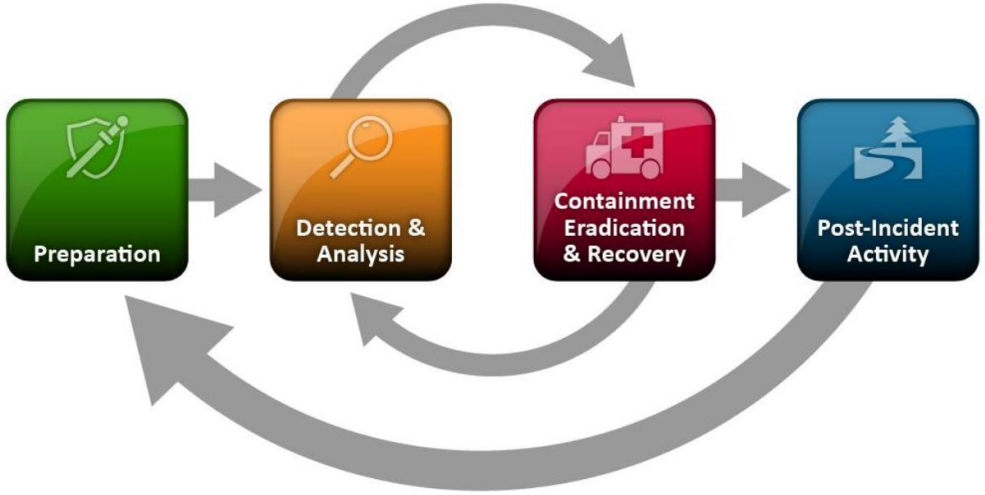
Handling an Incident - Preparation

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



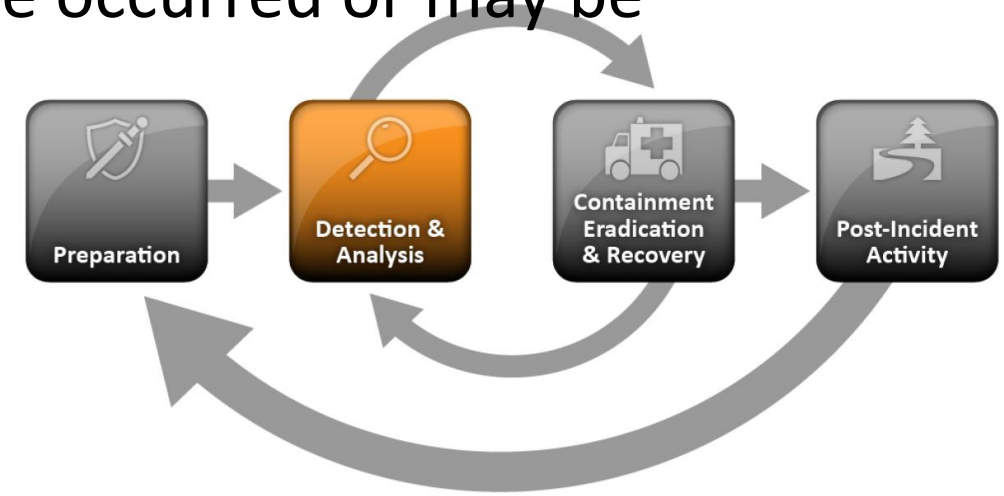
Handling an Incident – Detection and Analysis

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

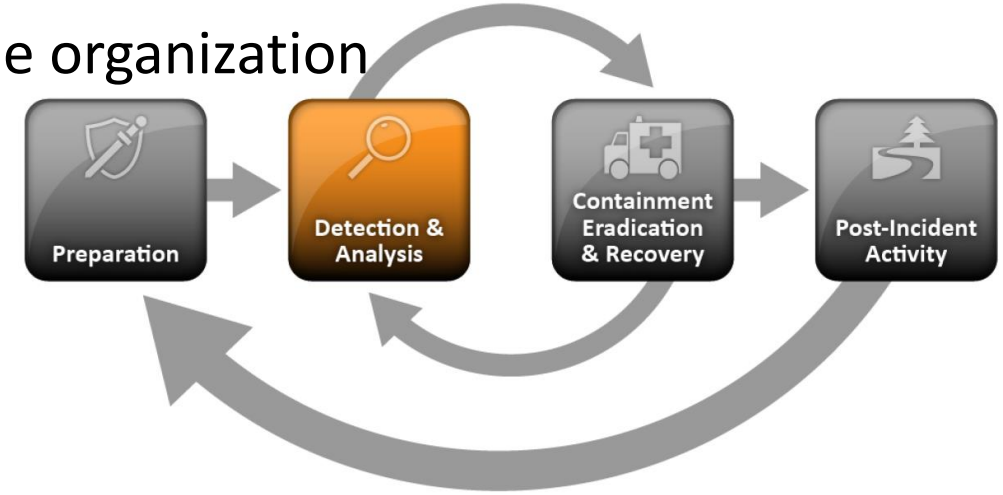


Handling an Incident – Detection and Analysis

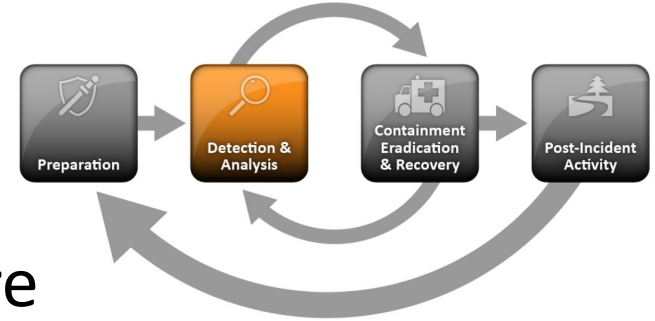
Precursors – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

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

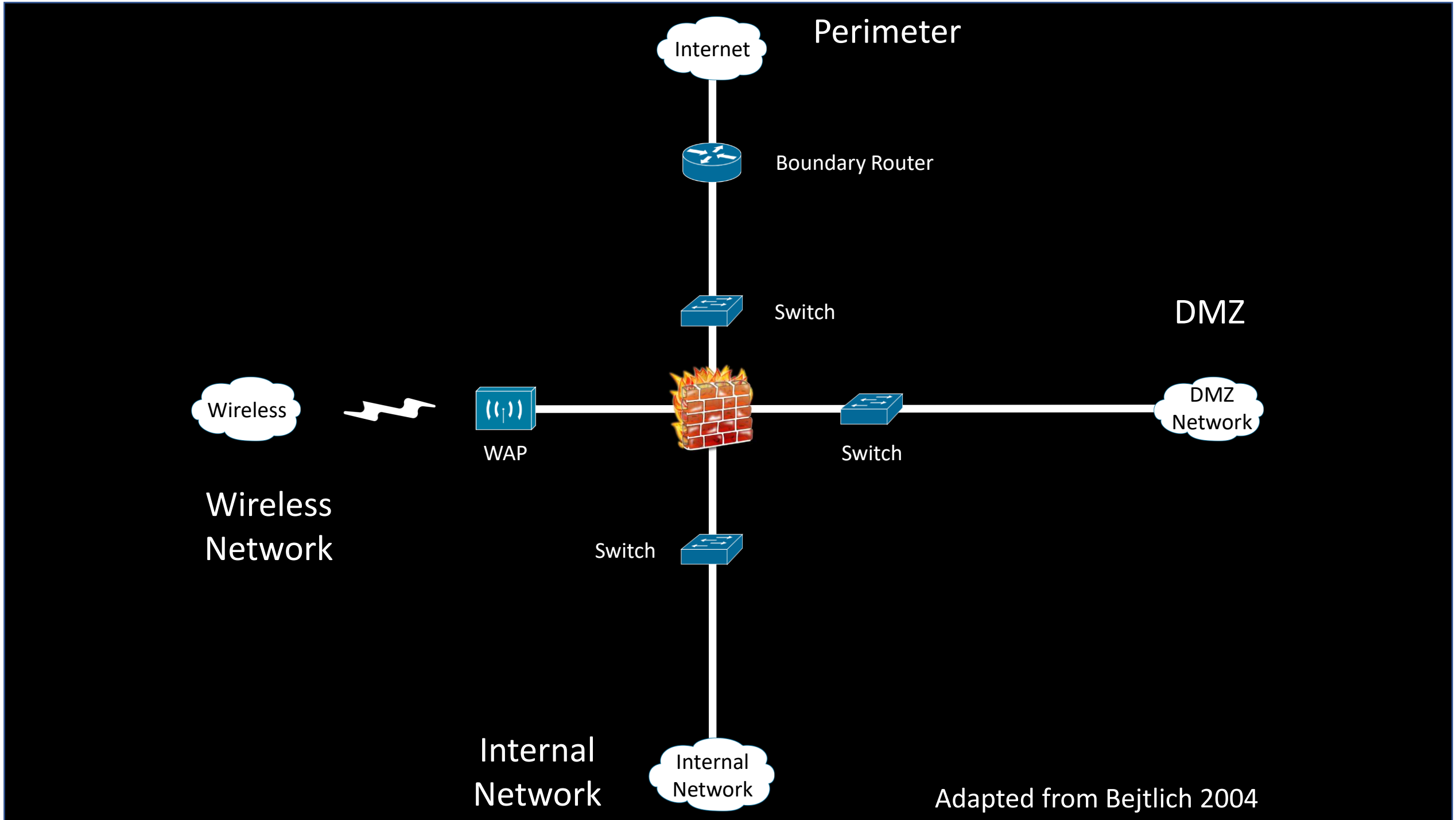


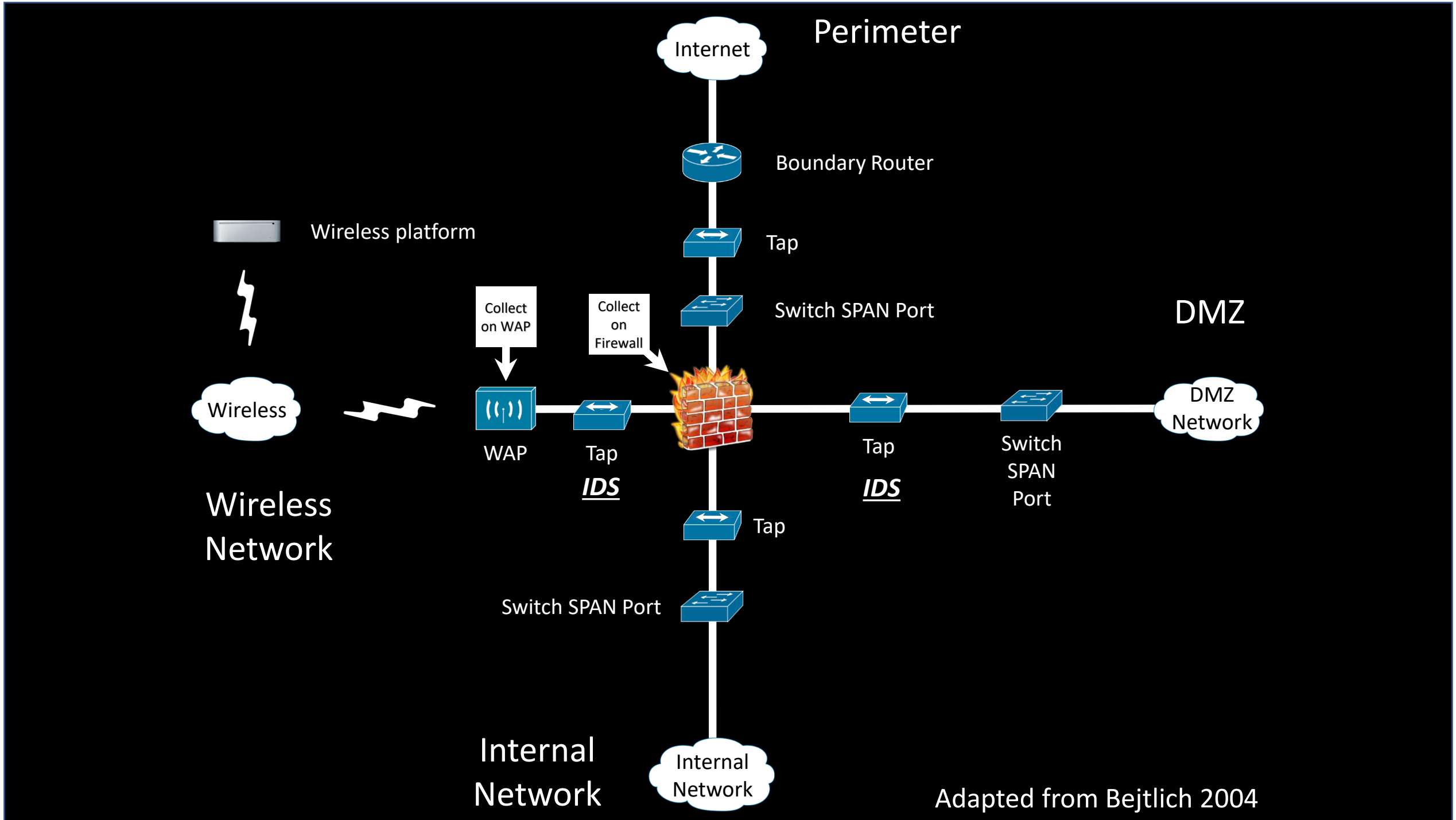
Detection and Analysis



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 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


Perimeter
Internet
Boundary Router
Switch
DMZ
Wireless
WAP
Switch
DMZ Network
Wireless Network
Switch
Internal Network
Internal Network
Adapted from Bejtlich 2004

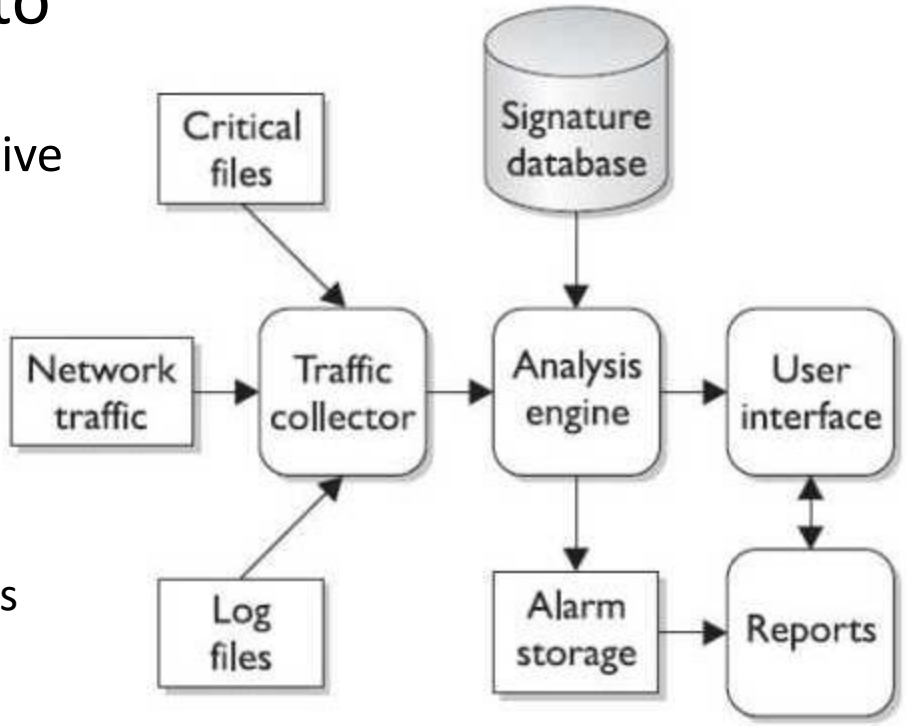

Perimeter
Internet
Boundary Router
Wireless platform
Tap
Collect on WAP
Collect on Firewall
Switch SPAN Port
DMZ
Wireless
WAP
Tap
IDS
Tap
IDS
Switch SPAN Port
DMZ Network
Wireless Network
Tap
Switch SPAN Port
Internal Network
Internal Network
Adapted from Bejtlich 2004

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



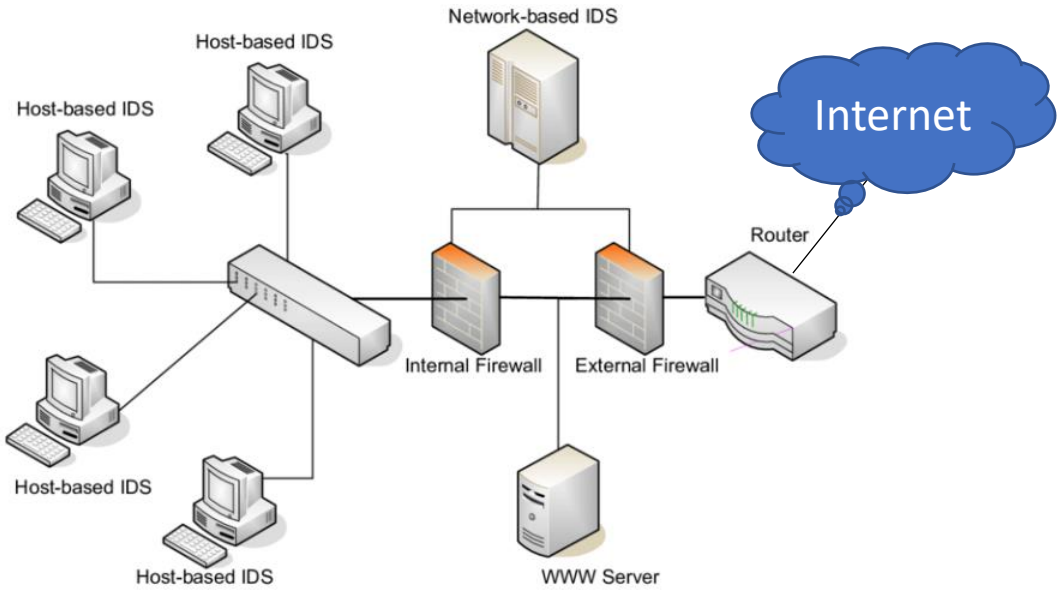
Intrusion Detection Systems (IDSs)

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



Intrusion Prevention Systems (IPS)

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

Detective and "after the fact" response

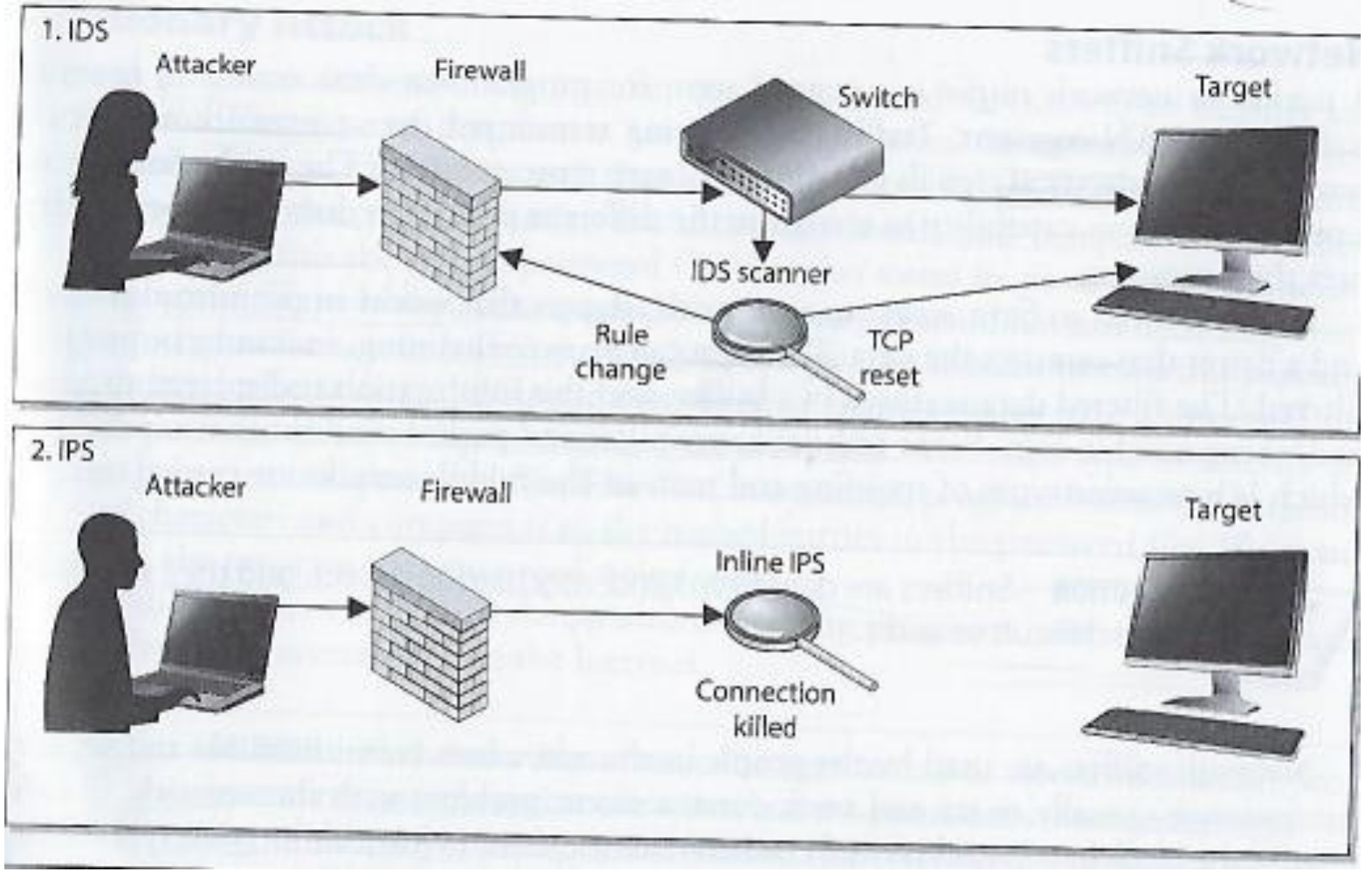
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
  - *Preventive and proactive response*

  - *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



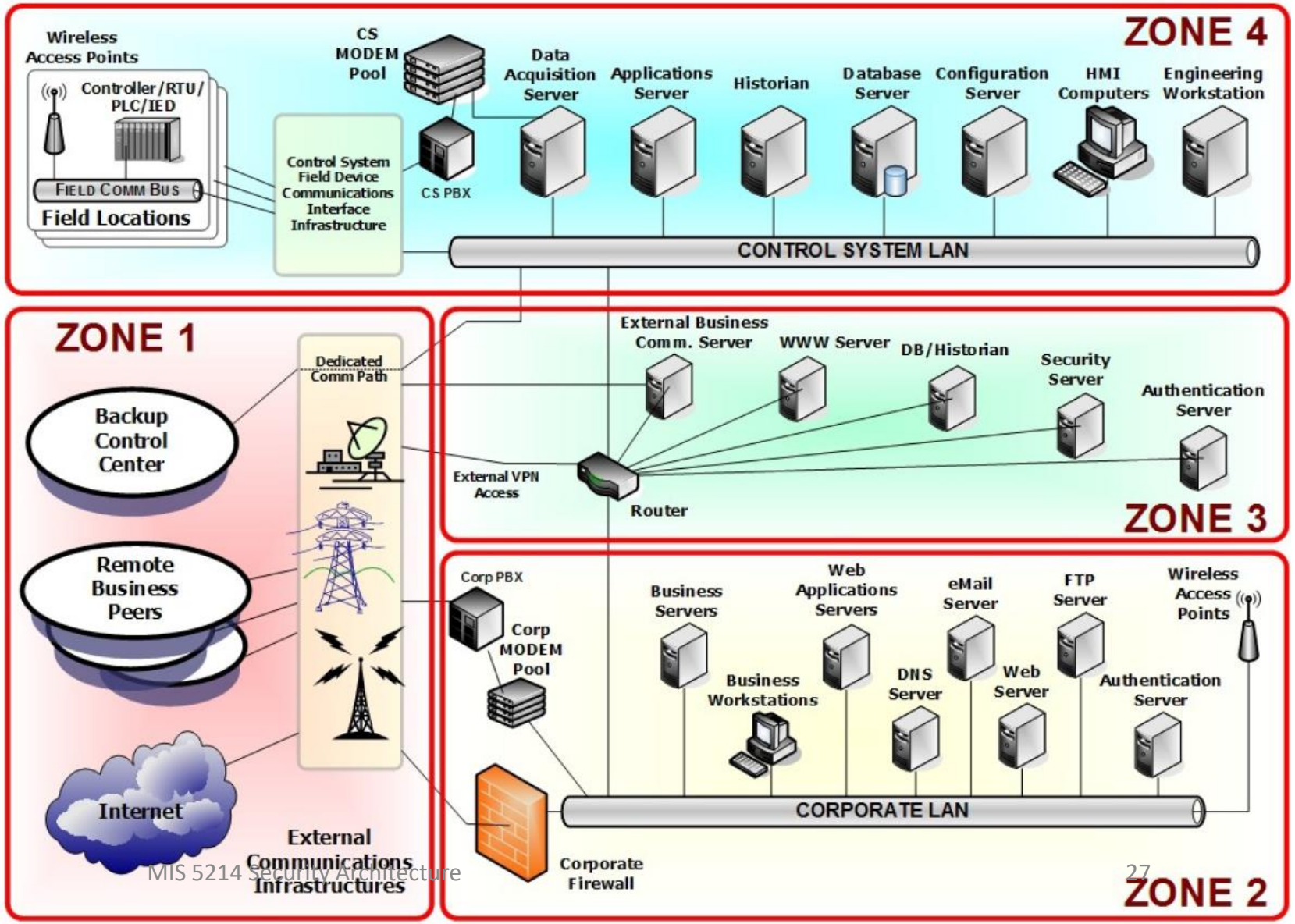
Network Security: Begins with understanding roles of assets in the topology of the network, and moves onto partitioning resources into distinct security zones…

Zone 1: External connectivity to the Internet, peer locations, and back- up facilities

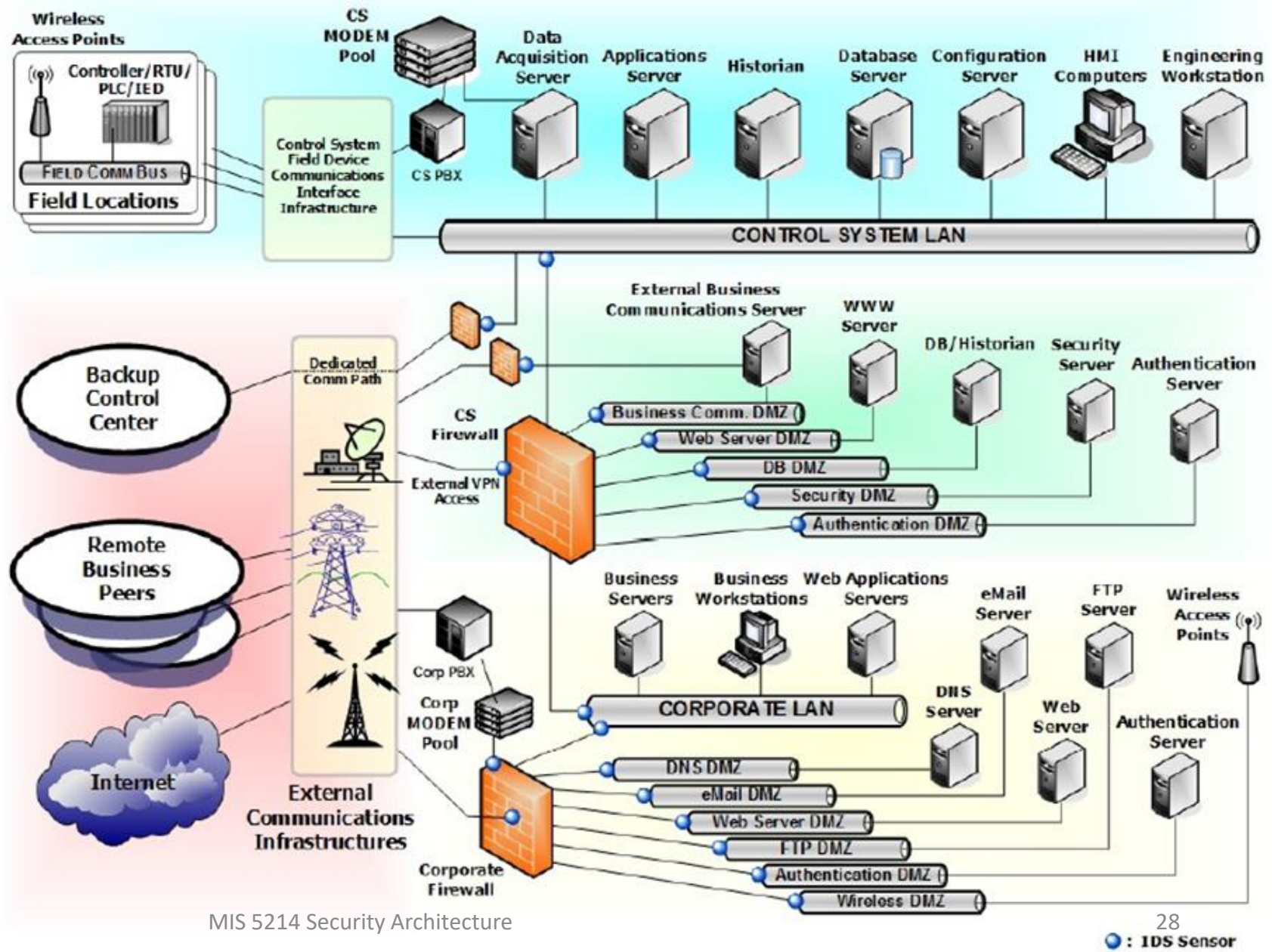
Zone 2: External connectivity and corporate communications

Zone 3: Control systems (in Zone 4) sending and receiving communications to/from external services

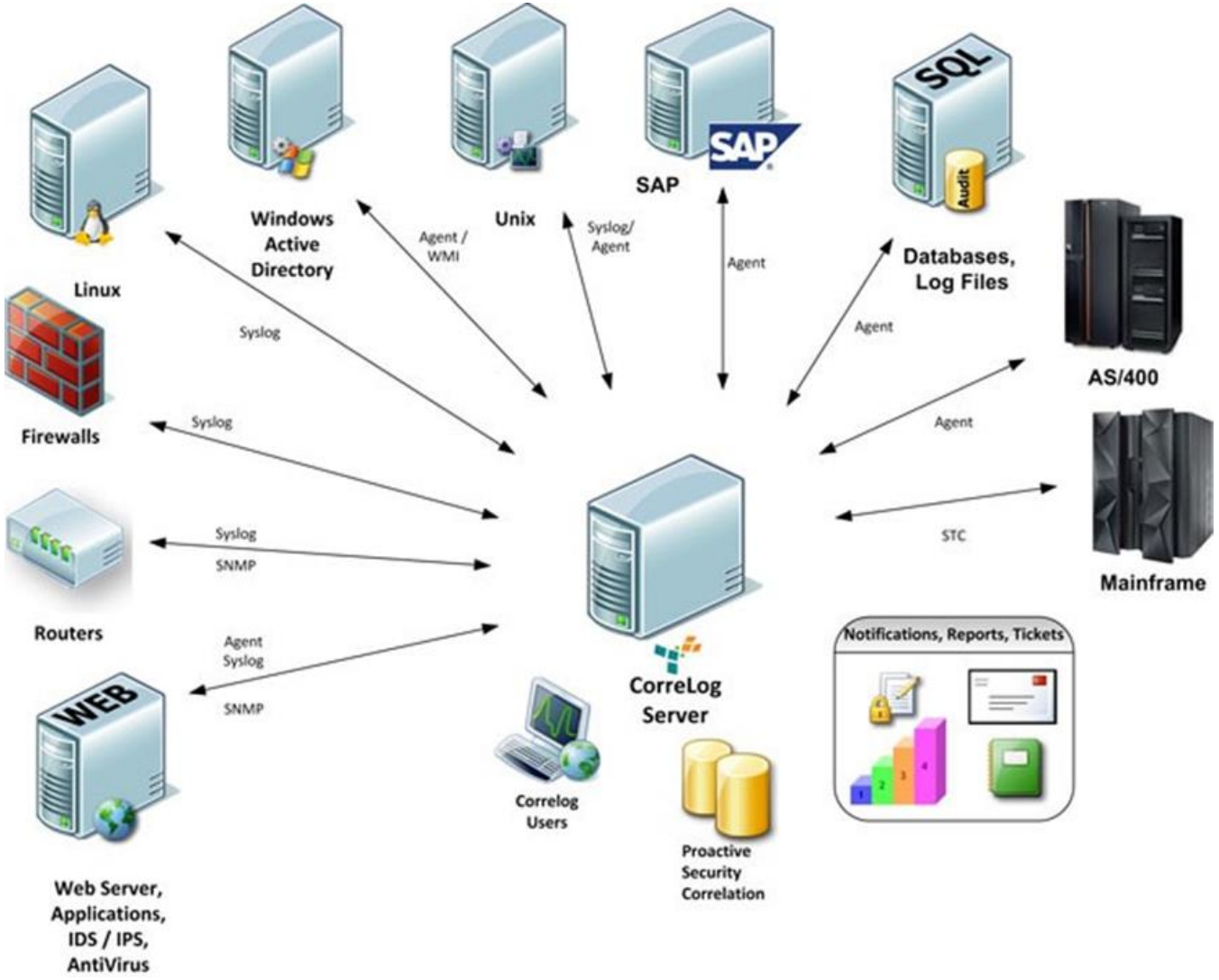
Zone 4: Control systems operations – process based or SCADA



Intrusion Detection System sensors and firewalls located throughout the network



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



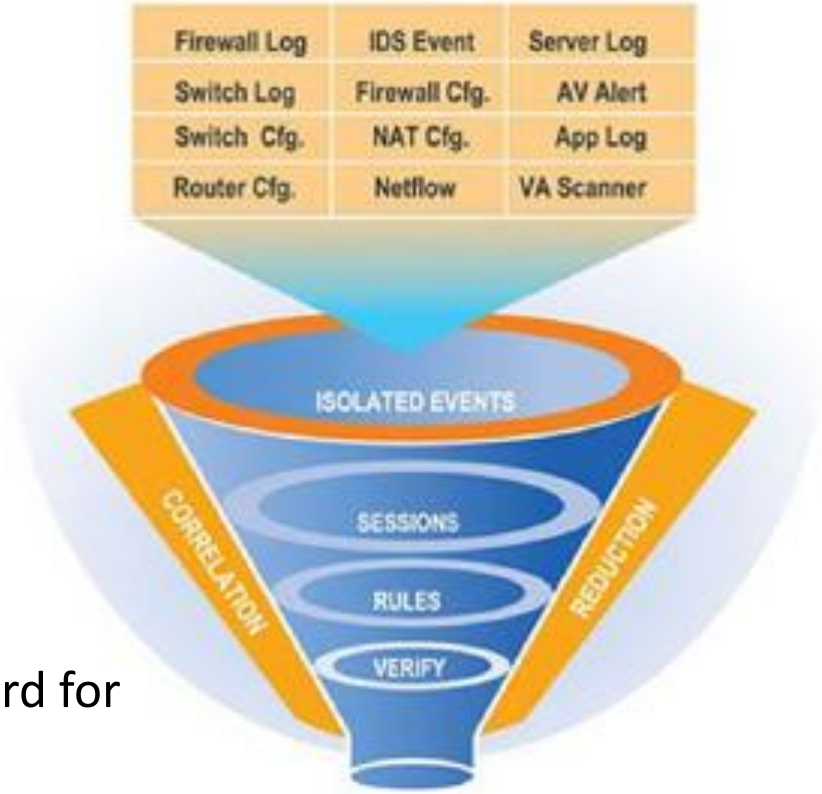
Security information and event management (SIEM) is a configurable security system of record that aggregates and analyzes security event data from on-premises and cloud environments.

SIEM assists with response actions to mitigate issues that cause harm to the organization and satisfies compliance and reporting requirements.

Gartner

Hype Cycle for IT Management Intelligence, 2023
Published 20 July 2023 • ID G00792530
By Cameron Haight

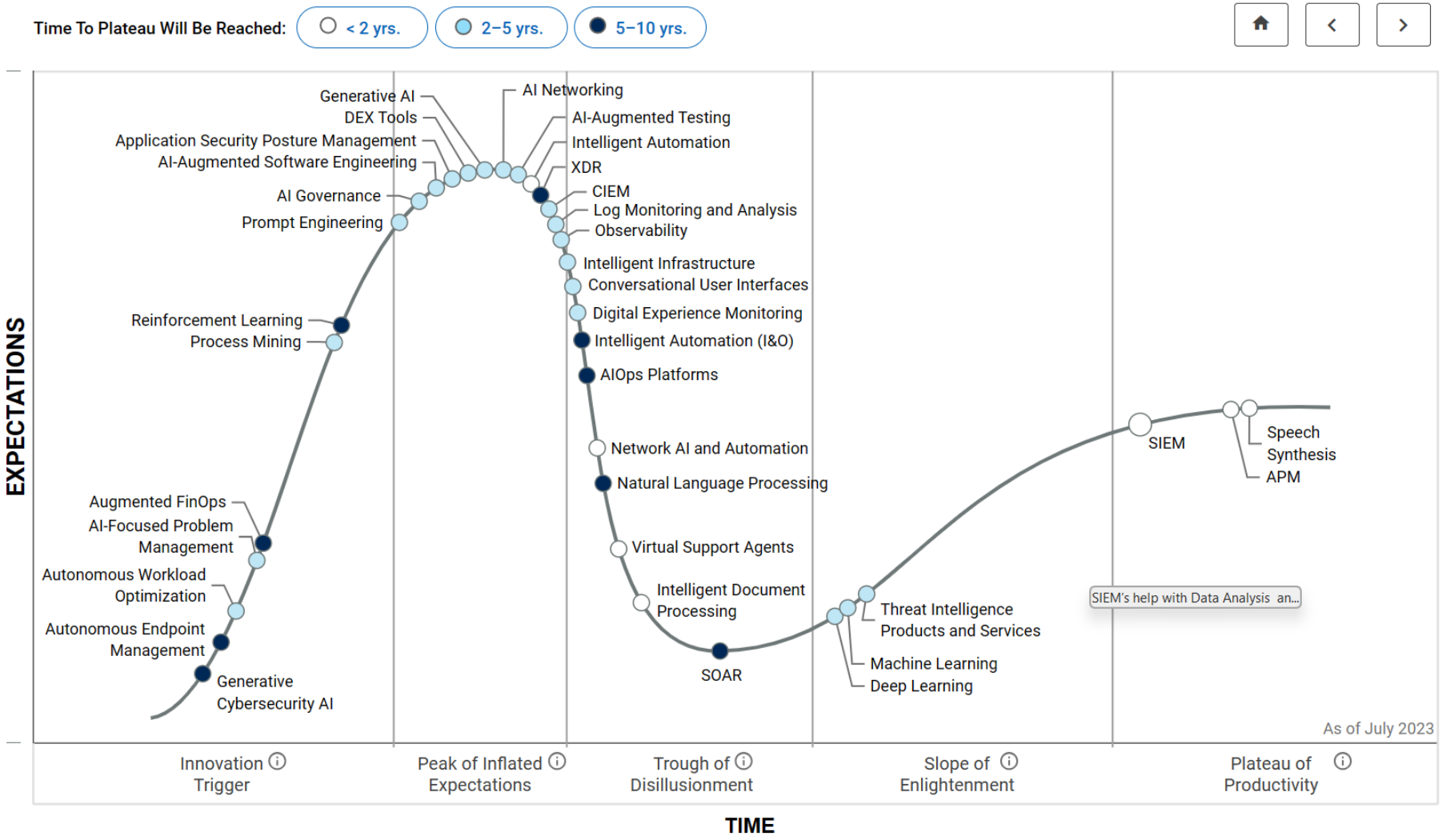
SIEM's help with Data Analysis and Correlation



- 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, for example:
  - ***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

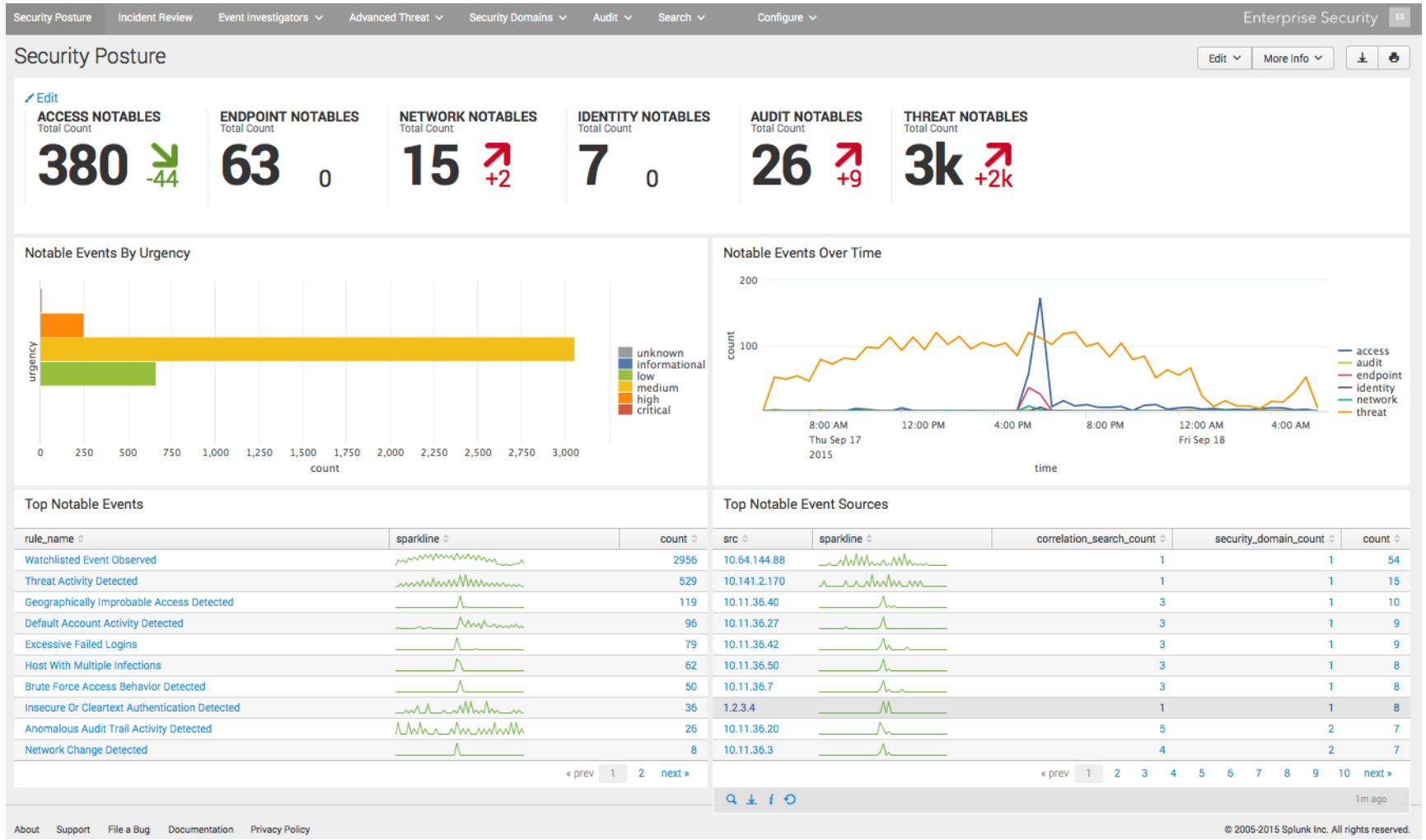
Hype Cycle for IT Management Intelligence, 2023

Published 20 July 2023 • ID G00792530
By Cameron Haight, Gartner

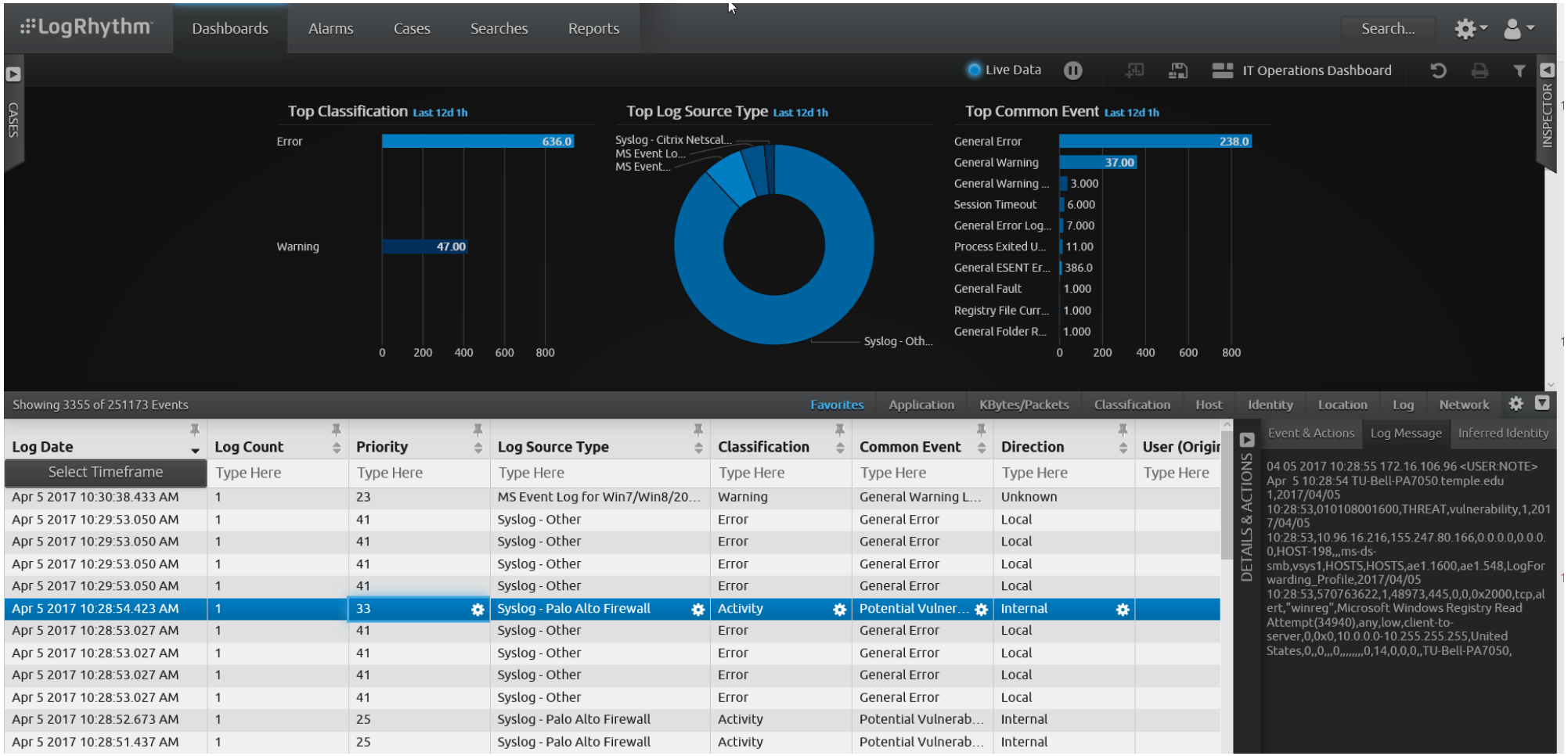


SIEM

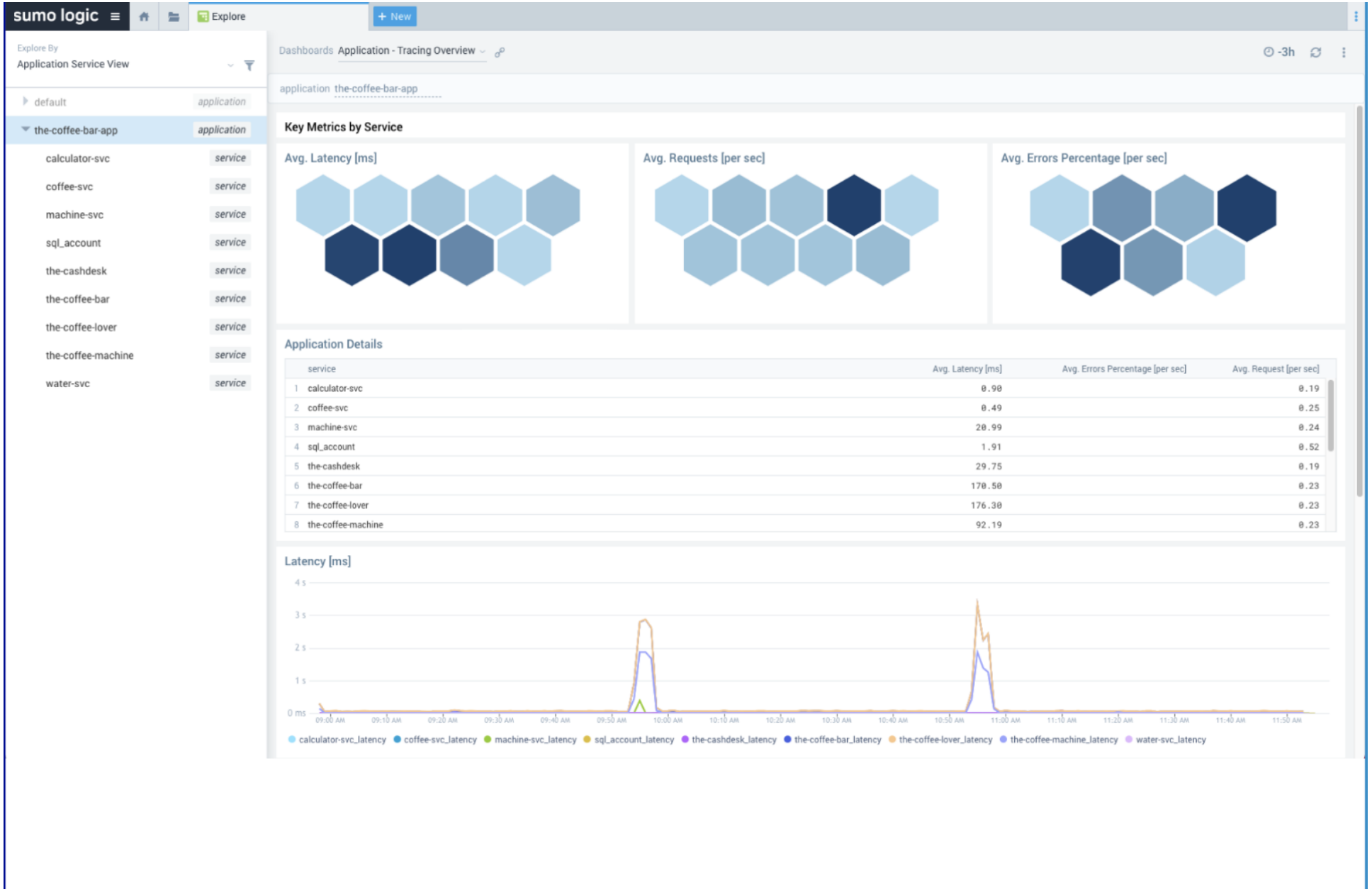
- ***Security Information and Event Management (SIEM)*** market is defined by the customer's need to analyze event data in real time
- Allows for the early detection of targeted attacks and data breaches
- Collect, store, investigate and report on log data for incident response, forensics and regulatory compliance.
- Aggregates event data (logs) produced by security devices, network infrastructure, systems and applications


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Security Posture
Edit
More Info
Edit
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
Notable Events By Urgency
urgency
unknown
informational
low
medium
high
critical
0
250
500
750
1,000
1,250
1,500
1,750
2,000
2,250
2,500
2,750
3,000
count
Notable Events Over Time
200
100
count
access
audit
endpoint
identity
network
threat
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
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
« prev 1 2 next »
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
« prev 1 2 3 4 5 6 7 8 9 10 next »
1m ago
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.

LogRhythm™

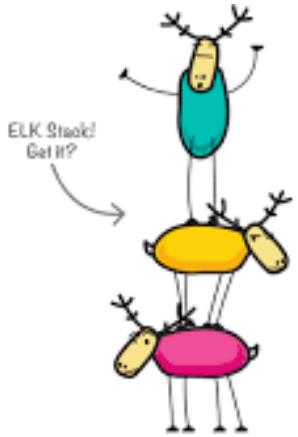

LogRhythm
Dashboards
Alarms
Cases
Searches
Reports
Search...
Live Data
IT Operations Dashboard
CASES
INSPECTOR
Top Classification Last 12d 1h
Error
636.0
Warning
47.00
0
200
400
600
800
Top Log Source Type Last 12d 1h
Syslog - Citrix Netscal...
MS Event Lo...
MS Event...
Syslog - Oth...
Top Common Event 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
Showing 3355 of 251173 Events
Favorites
Application
KBytes/Packets
Classification
Host
Identity
Location
Log
Network
Log Date
Log Count
Priority
Log Source Type
Classification
Common Event
Direction
User (Origi
Select Timeframe
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
DETAILS & ACTIONS
Event & Actions
Log Message
Inferred Identity
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,1,2017/04/05 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,LogForwarding_Profile,2017/04/05 10:28:53,570763622,1,48973,445,0,0,0x2000,tcp,alert,"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,

Sumologic


sumo logic
Explore
+ New
Explore By
Application Service View
default application
the-coffee-bar-app application
calculator-svc service
coffee-svc service
machine-svc service
sql_account service
the-cashdesk service
the-coffee-bar service
the-coffee-lover service
the-coffee-machine service
water-svc service
Dashboards Application - Tracing Overview
-3h
application the-coffee-bar-app
Key Metrics by Service
Avg. Latency [ms]
Avg. Requests [per sec]
Avg. Errors Percentage [per sec]
Application Details
service Avg. Latency [ms] Avg. Errors Percentage [per sec] Avg. Request [per sec]
1 calculator-svc 0.90 0.19
2 coffee-svc 0.49 0.25
3 machine-svc 20.99 0.24
4 sql_account 1.91 0.52
5 the-cashdesk 29.75 0.19
6 the-coffee-bar 170.50 0.23
7 the-coffee-lover 176.30 0.23
8 the-coffee-machine 92.19 0.23
Latency [ms]
4 s
3 s
2 s
1 s
0 ms
09:00 AM
09:10 AM
09:20 AM
09:30 AM
09:40 AM
09:50 AM
10:00 AM
10:10 AM
10:20 AM
10:30 AM
10:40 AM
10:50 AM
11:00 AM
11:10 AM
11:20 AM
11:30 AM
11:40 AM
11:50 AM
calculator-svc_latency
coffee-svc_latency
machine-svc_latency
sql_account_latency
the-cashdesk_latency
the-coffee-bar_latency
the-coffee-lover_latency
the-coffee-machine_latency
water-svc_latency

Hybrid – “ELK Stack”

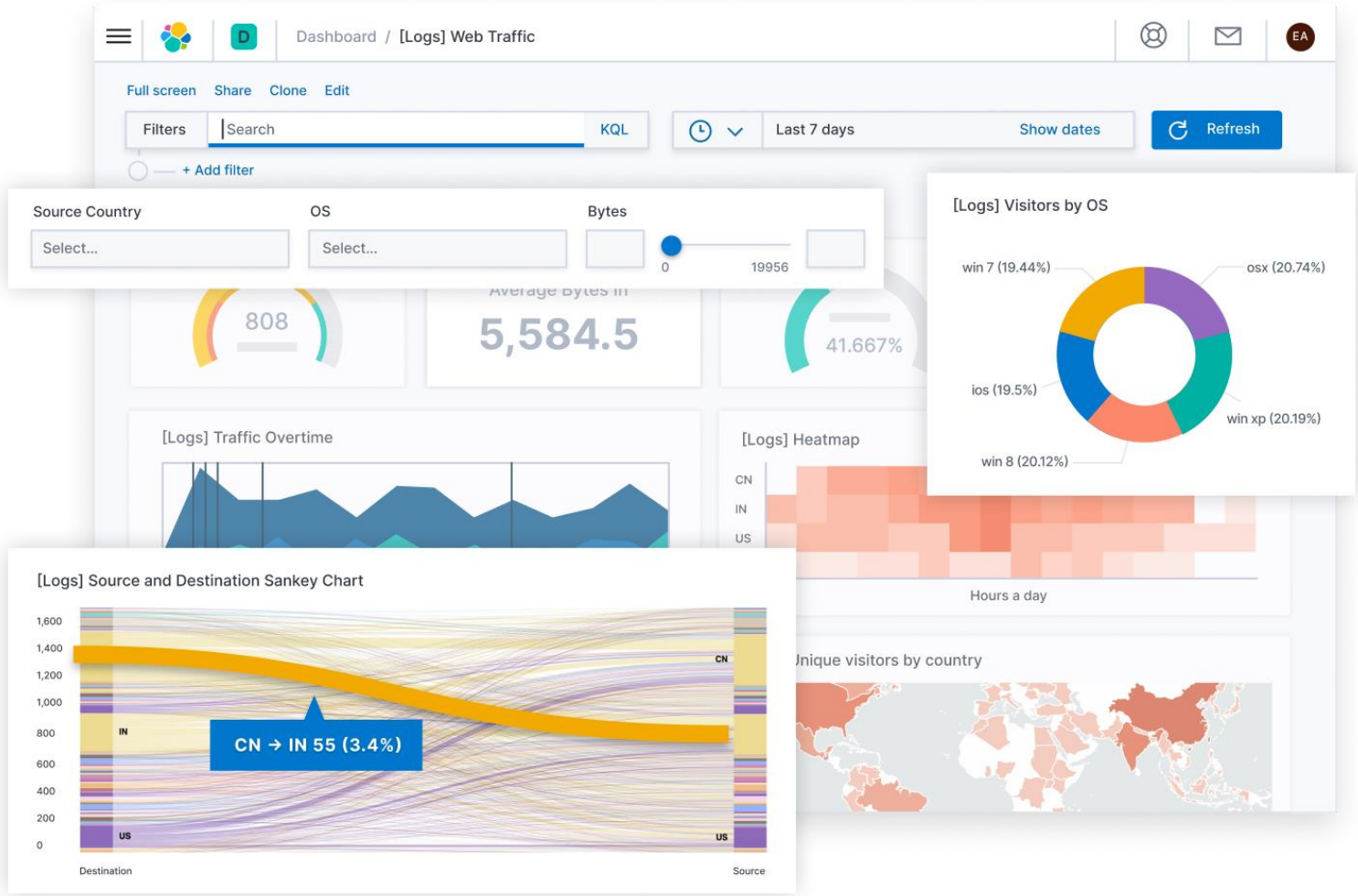
- On-Premises, or…
- Cloud (hosted)



E Elasticsearch

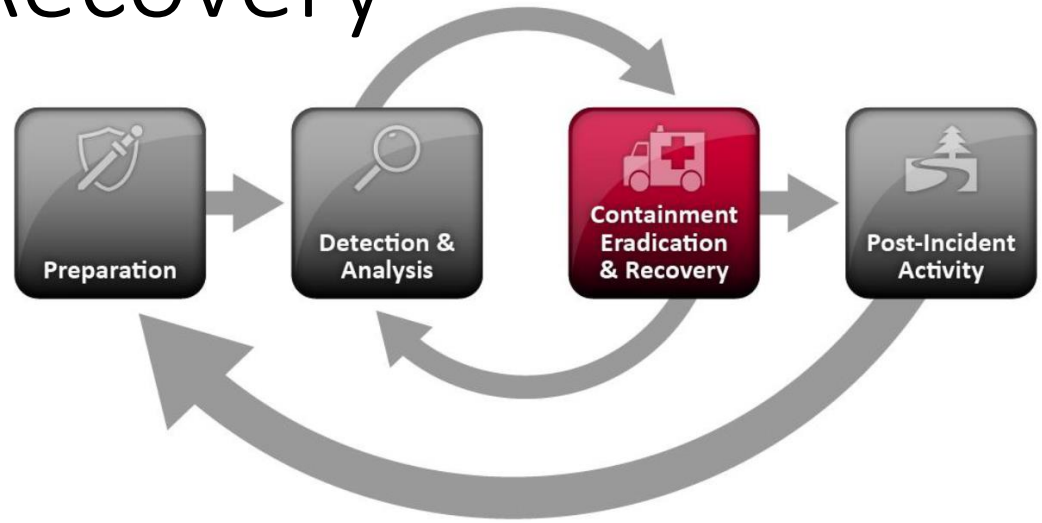
L Logstash

K Kibana



Note: Sankey charts are a type of flow diagram in which the width of the arrows is proportional to the flow rate

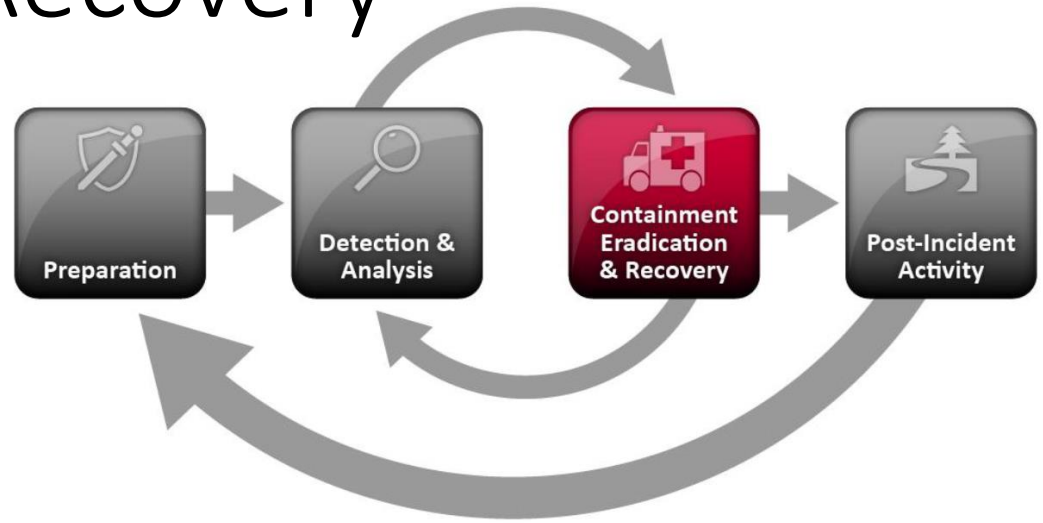
Containment, Eradication, and Recovery



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

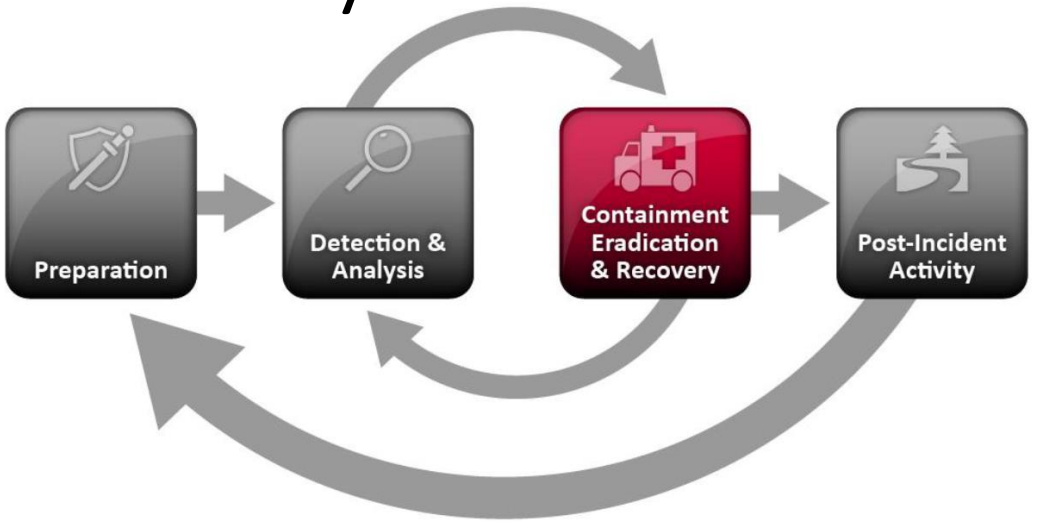


Eradication - After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as:

- 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

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:

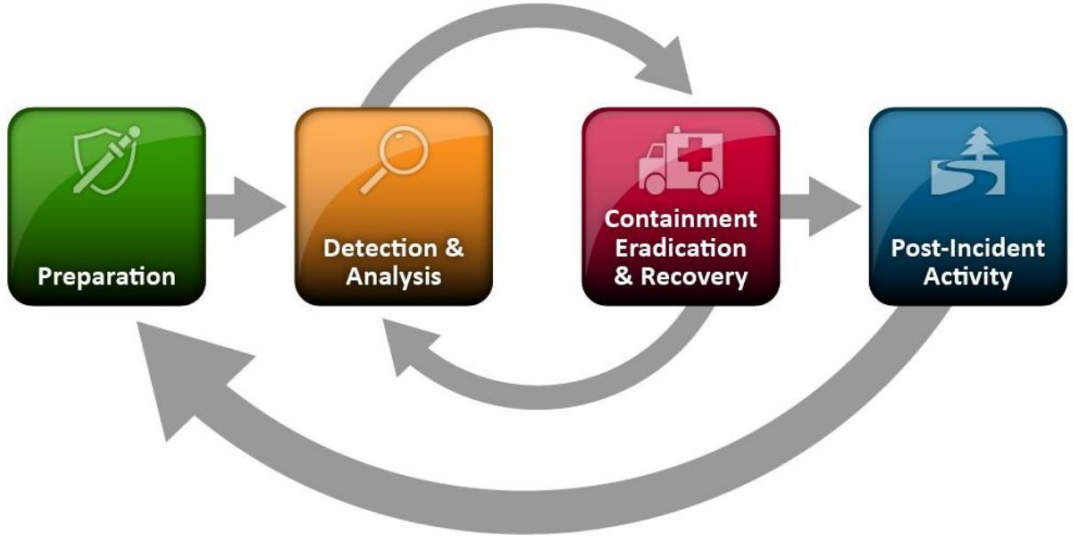
- Restoring systems from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tightening network perimeter security (e.g. firewall rules, boundary router access control lists, …)

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

- ✓Optional Labs 10 & 11
- ✓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