

MIS 4596

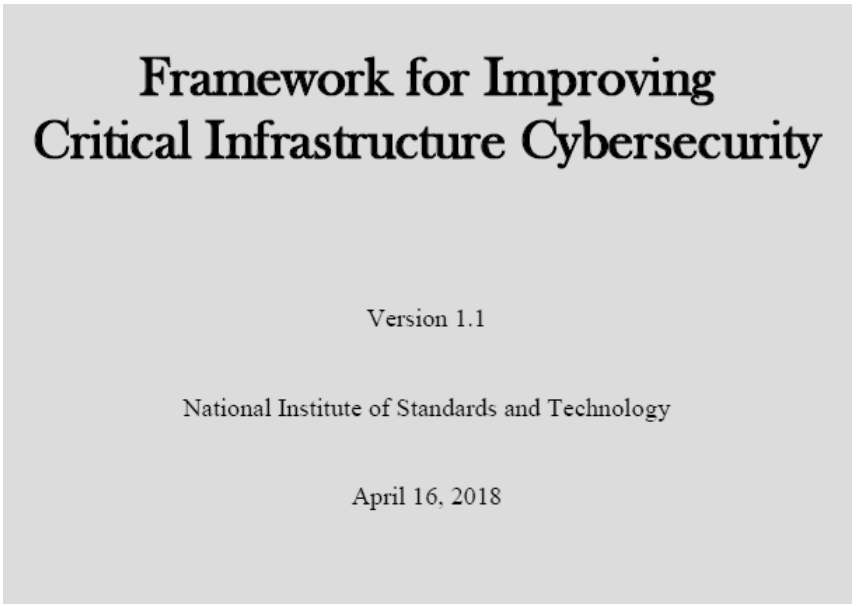
Unit#20

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

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?

| 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.

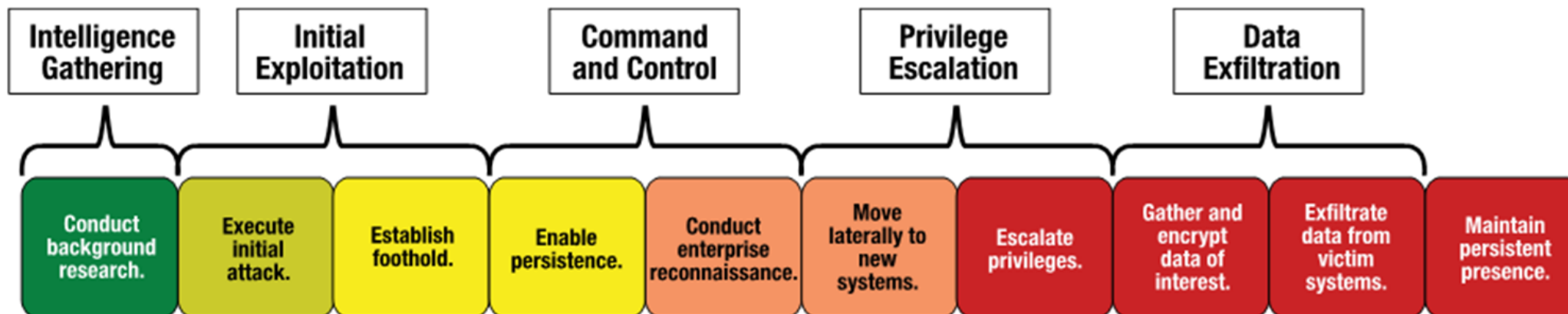
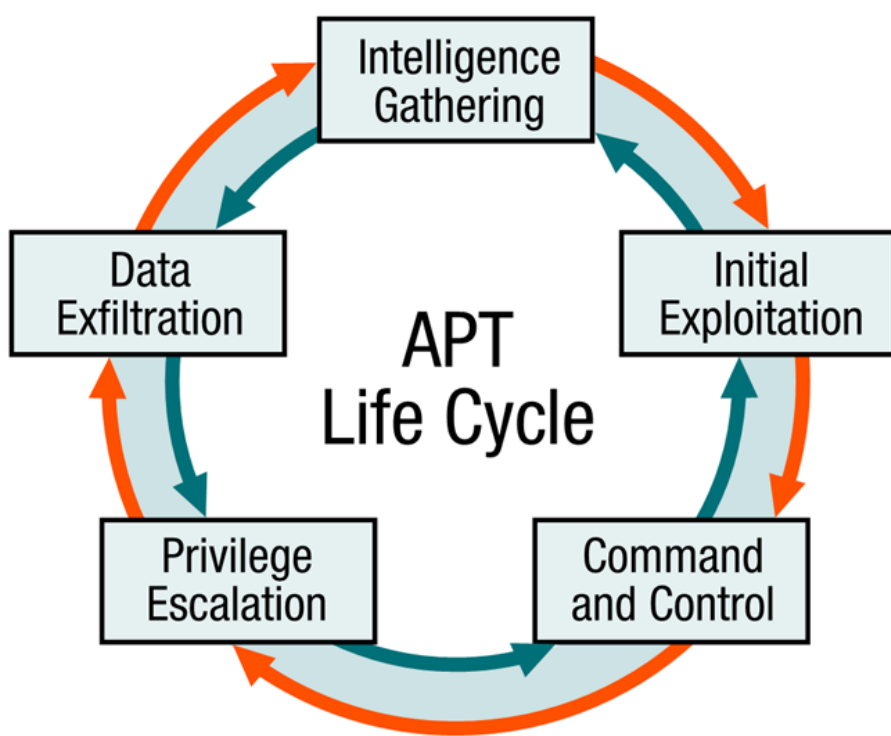
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization 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

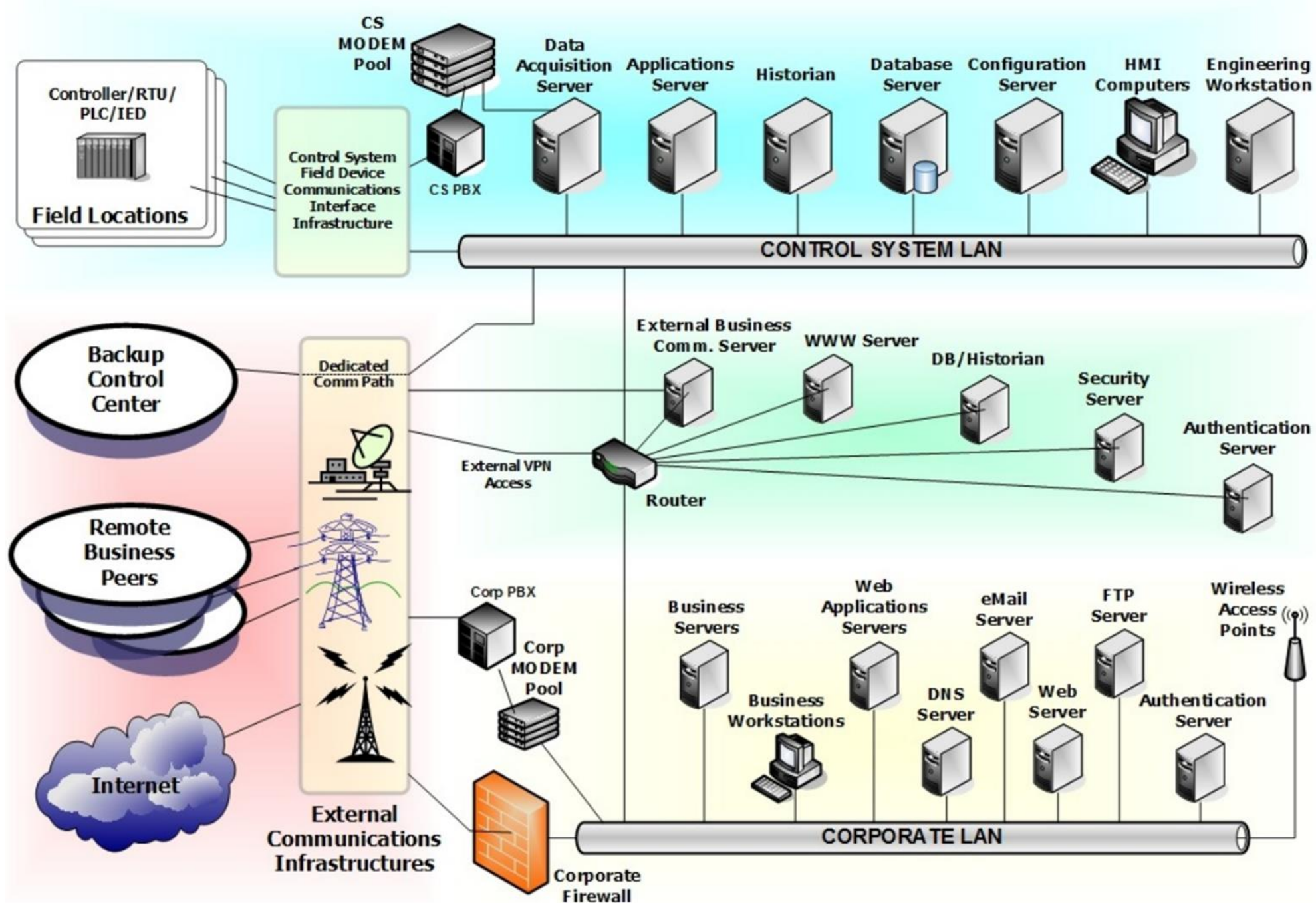
Is necessary because...

- 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

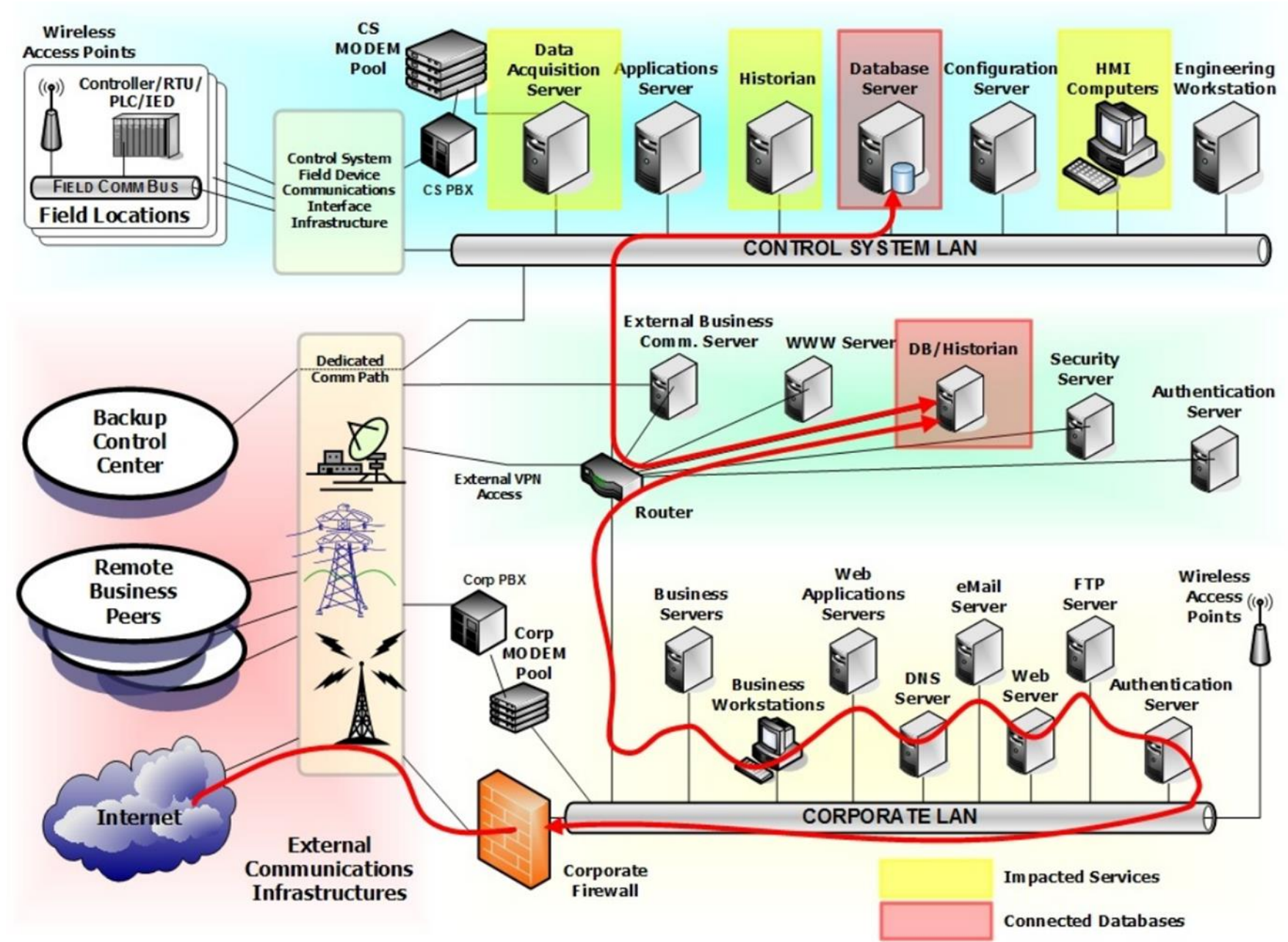


Example of a Network



Integrated networks

Example of Network Intrusion



Industry Targeting

“The top five most targeted industries in 2020 were:

- business and professional services,*
- retail and hospitality,*
- financial,*
- healthcare, and*
- high technology.*

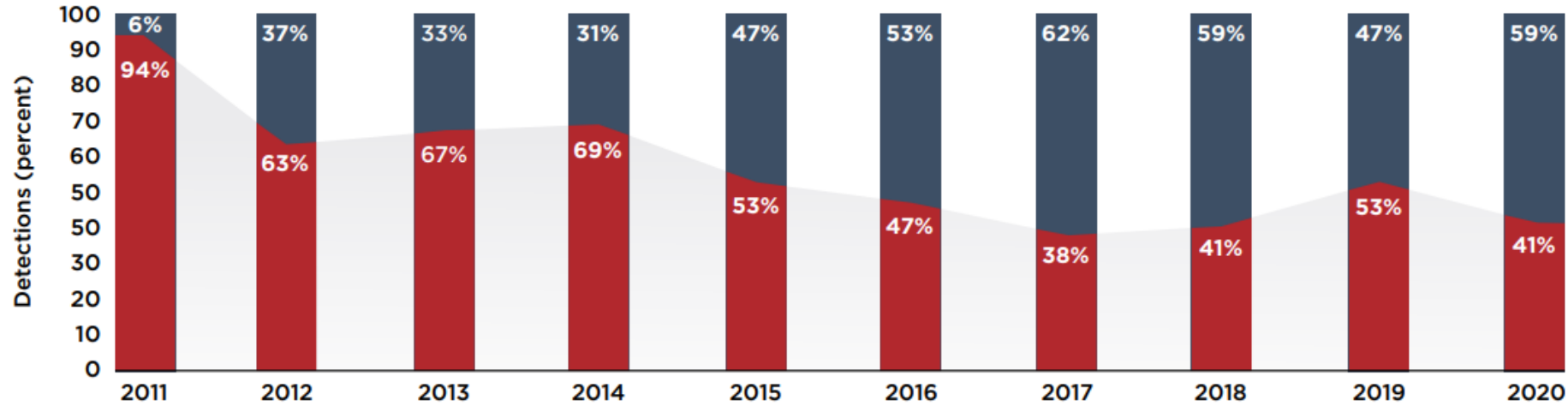
Over the past decade, business and professional services and financial have consistently placed in the top five most targeted industries.”

Page 17



| | | | |
|--|-----------|--|-----------|
| Ransomware | 36 | UNC2452 | 62 |
| Ransomware Evolves Into Multifaceted Extortion | 37 | Mapping UNC2452 Activity to the Targeted Attack Lifecycle Framework | 63 |
| Steps toward Proactive Hardening Against Ransomware in Multiple Environments | 41 | Case Studies | 72 |
| Recovery and Reconstitution Challenges in Post-Ransomware Scenarios | 45 | Insider Threat Risks to Flat Environments | 73 |
| Newly Named Threat Groups | 49 | Red Team Makes the Most of Social Engineering and System Misconfigurations | 76 |
| FIN11 | 50 | Conclusion | 80 |
| Pandemic-Related Threats | 56 | More Security Awareness to Build Best Practices | 81 |
| Threats Against Organizations Working with COVID-19 Information and Research | 57 | | |

Who is detecting intrusions by attackers?



Page 10

FIREEYE | MANDIANT



How long are attackers remaining in compromised systems?

| Compromise Notifications | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|--------------------------|------|------|------|------|------|------|------|------|------|------|
| All | 416 | 243 | 229 | 205 | 146 | 99 | 101 | 78 | 56 | 24 |
| External Notification | — | — | — | — | 320 | 107 | 186 | 184 | 141 | 73 |
| Internal Detection | — | — | — | — | 56 | 80 | 57.5 | 50.5 | 30 | 12 |

Median Dwell Time

416 > **24**
DAYS IN 2011 DAYS IN 2020

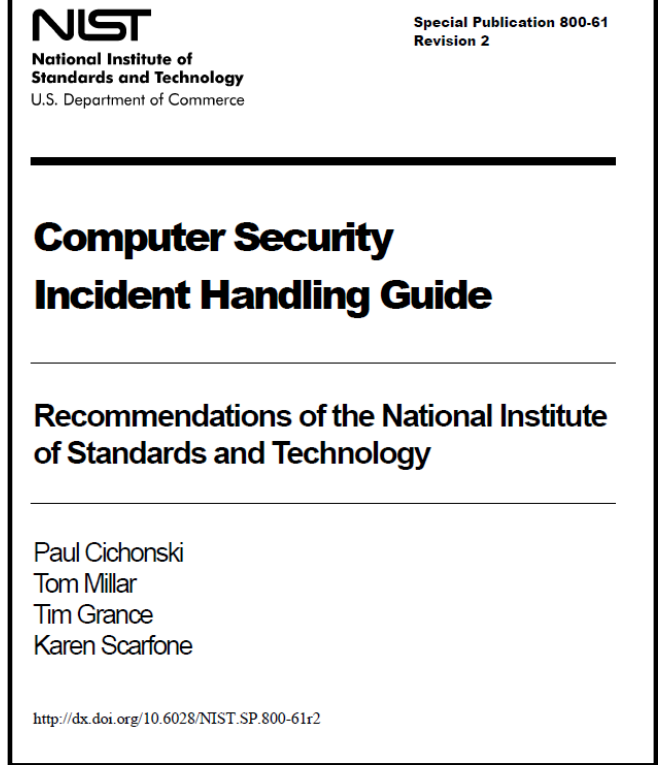
“Dwell time is calculated as the number of days an attacker is present in a victim environment before they are detected.”



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



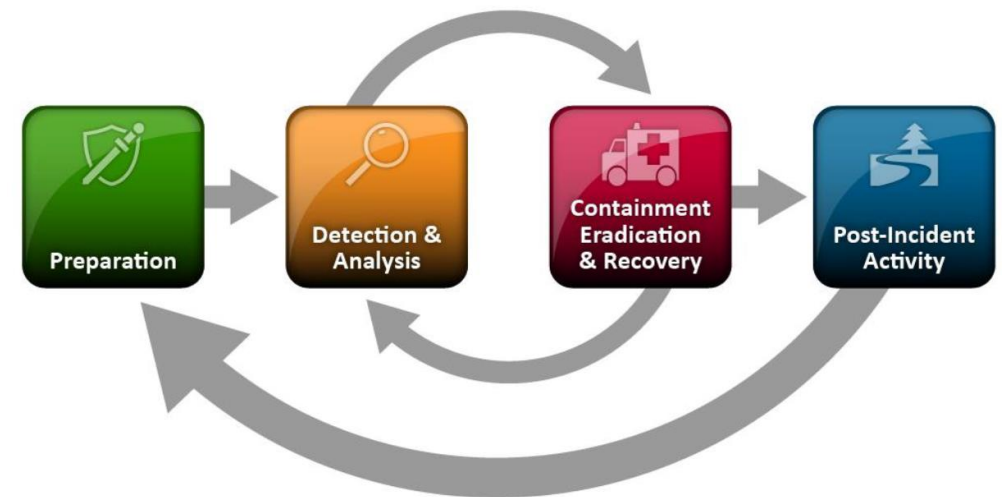
Handling an Incident - Preparation

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



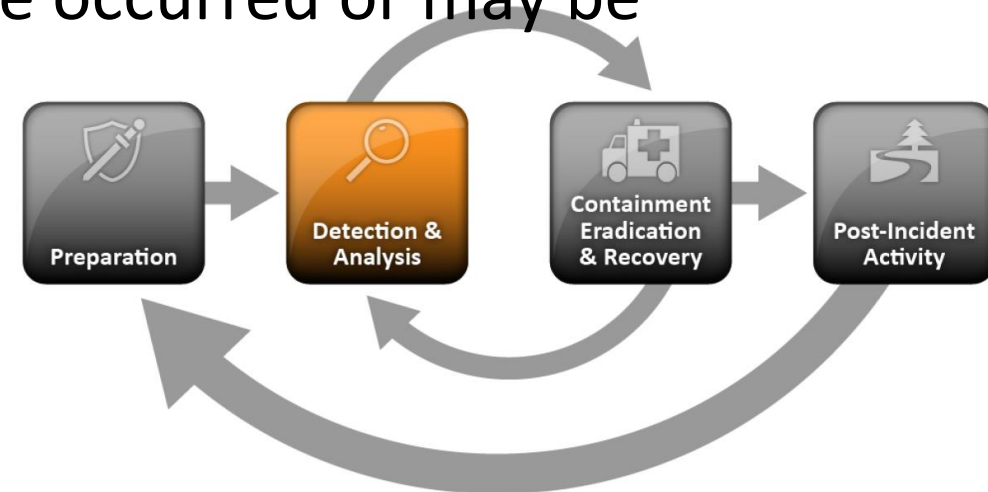
Handling an Incident – Detection and Analysis

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

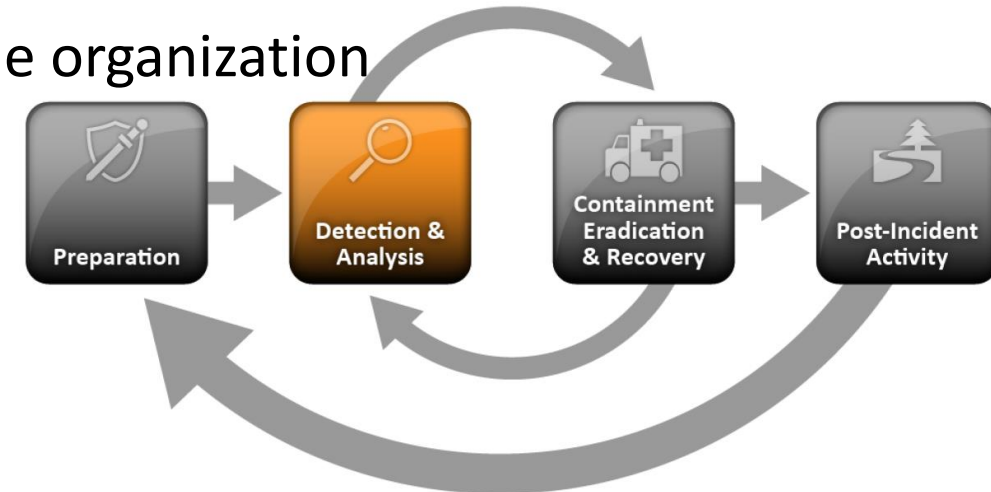


Handling an Incident – Detection and Analysis

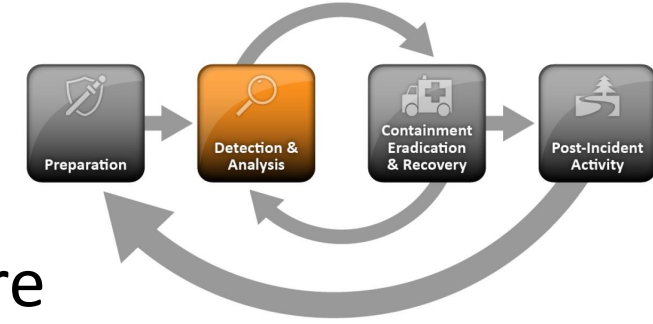
Precursors – While rare, if precursors are detected, the organization may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the organization could monitor activity involving the target more closely.

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

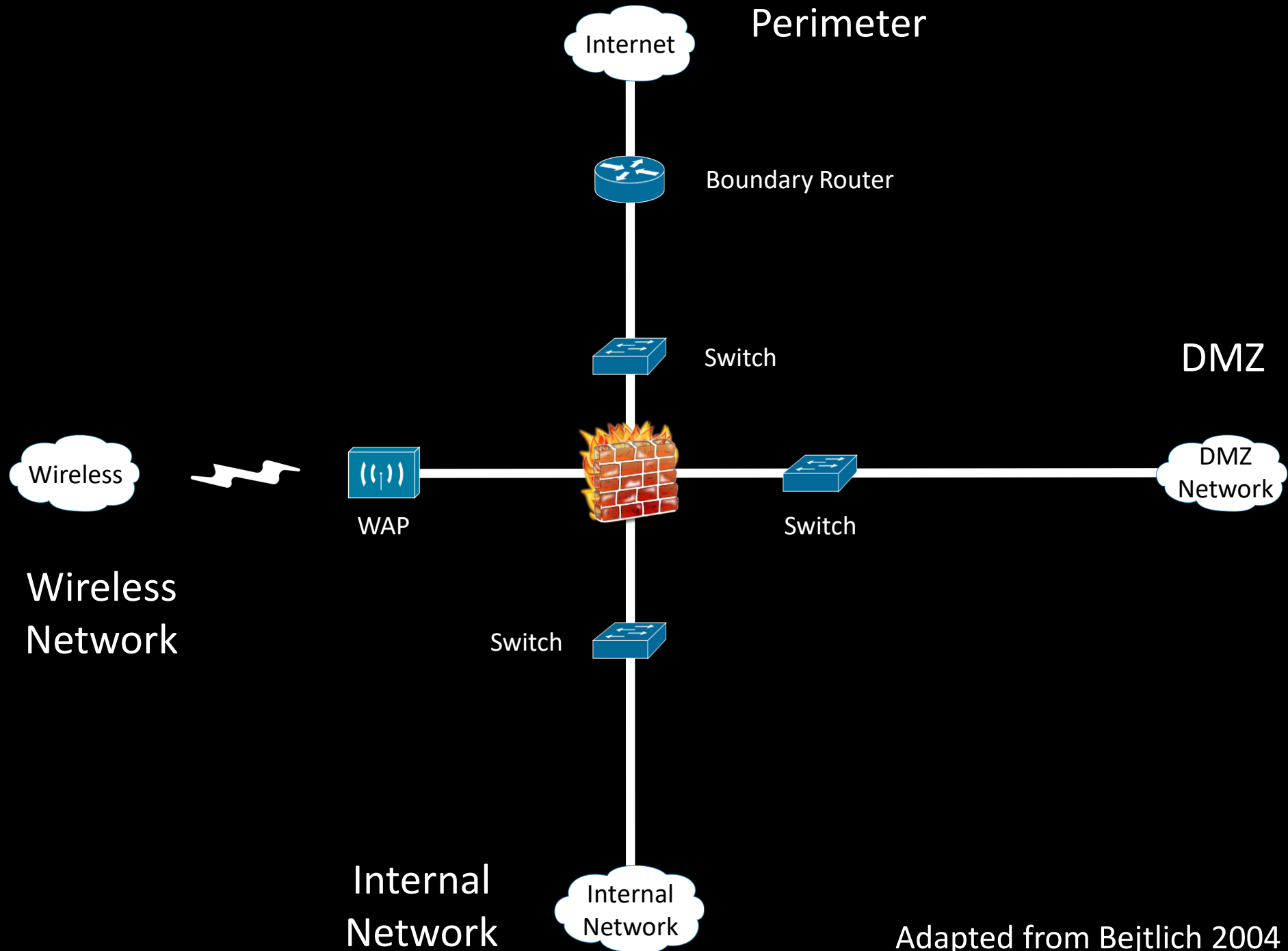


Detection and Analysis

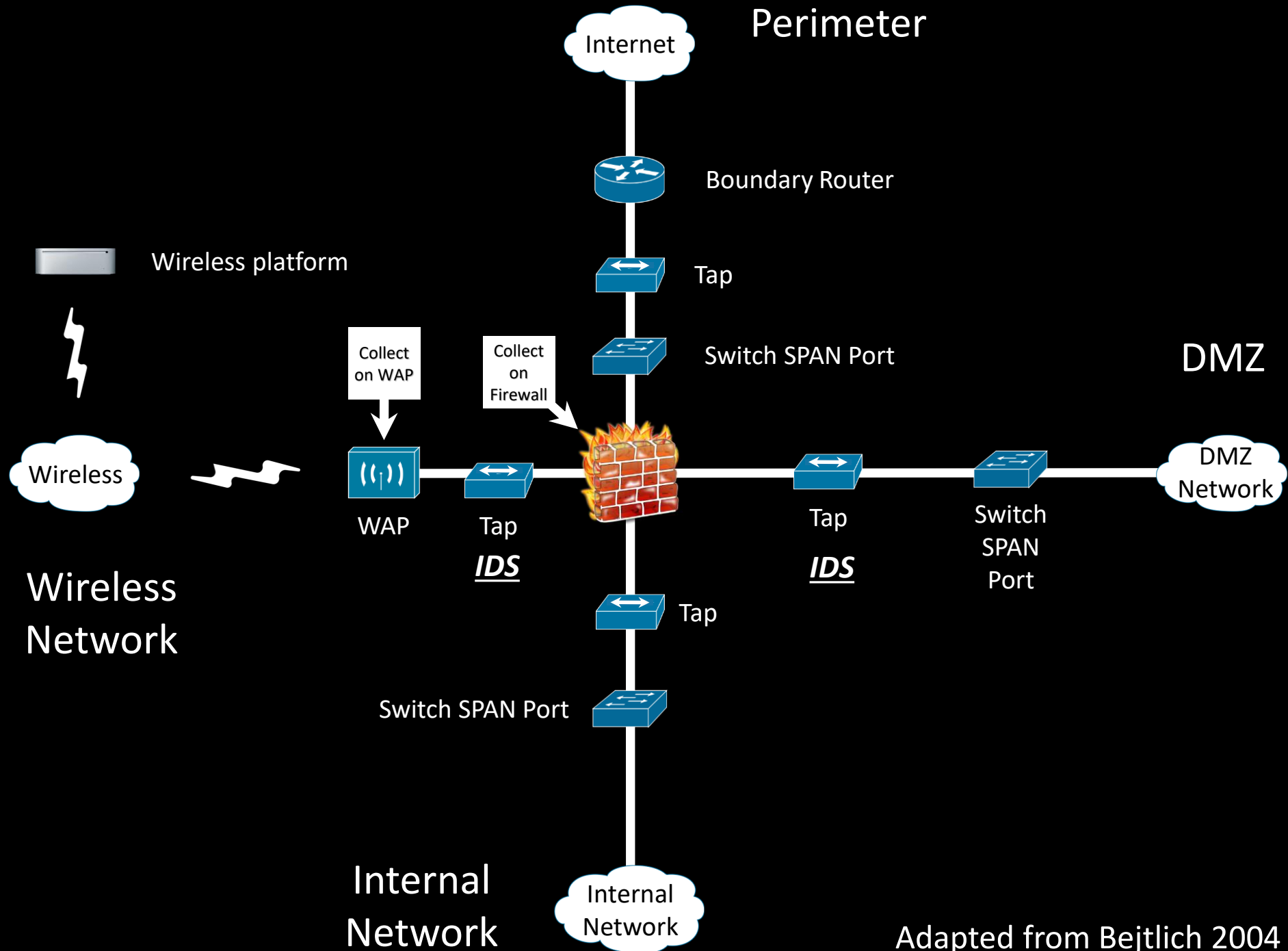


Indicators - While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to exhaustively list them, but some examples are listed below:

- 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



Adapted from Bejtlich 2004



Adapted from Bejtlich 2004

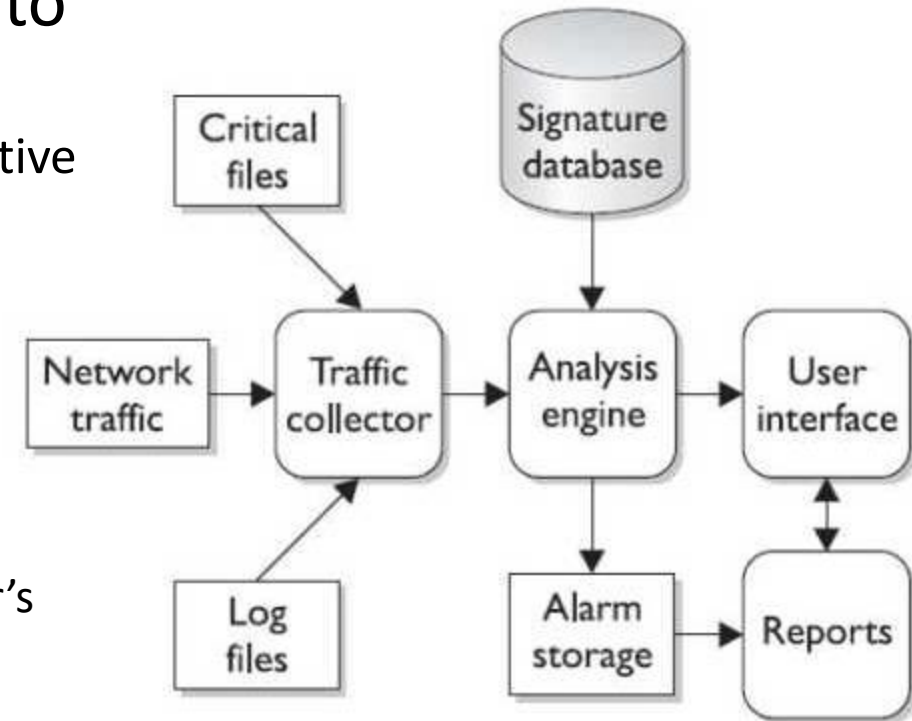
Intrusion Detection Systems (IDSs)

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



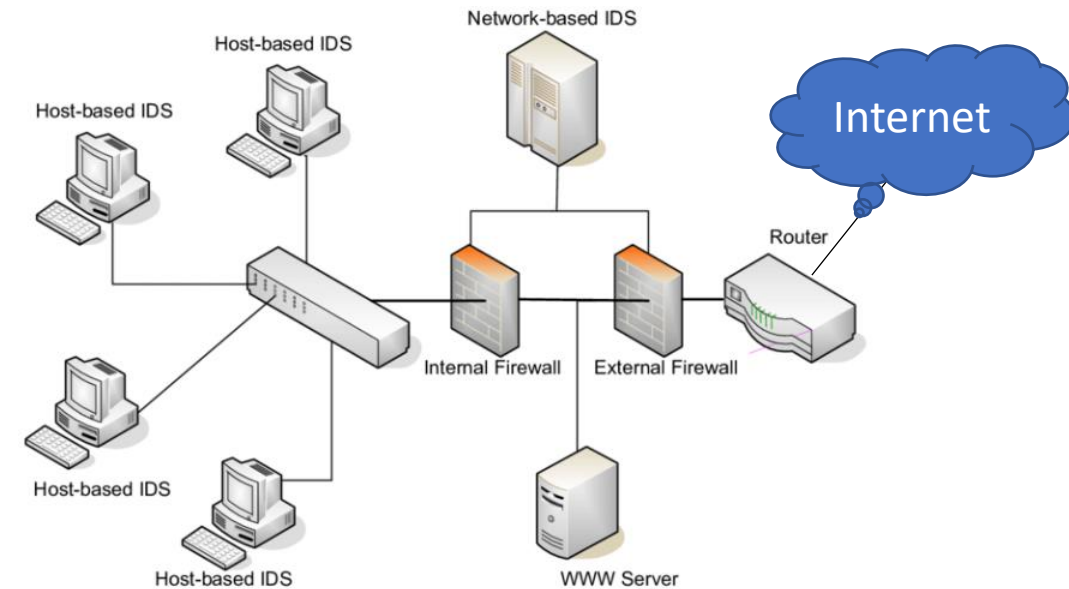
Intrusion Detection Systems (IDSs)

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

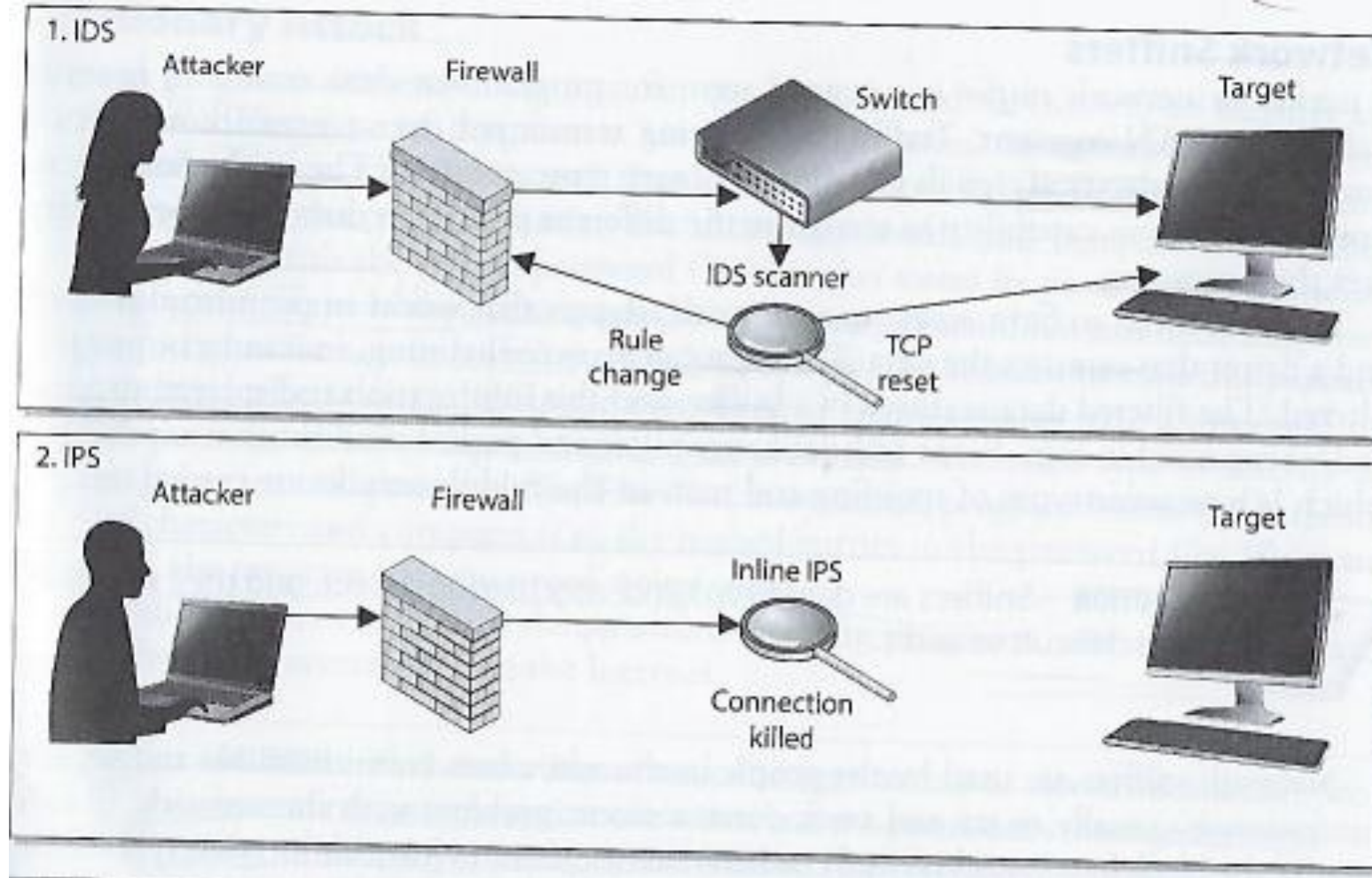
Detective and “after the fact” response

- 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*

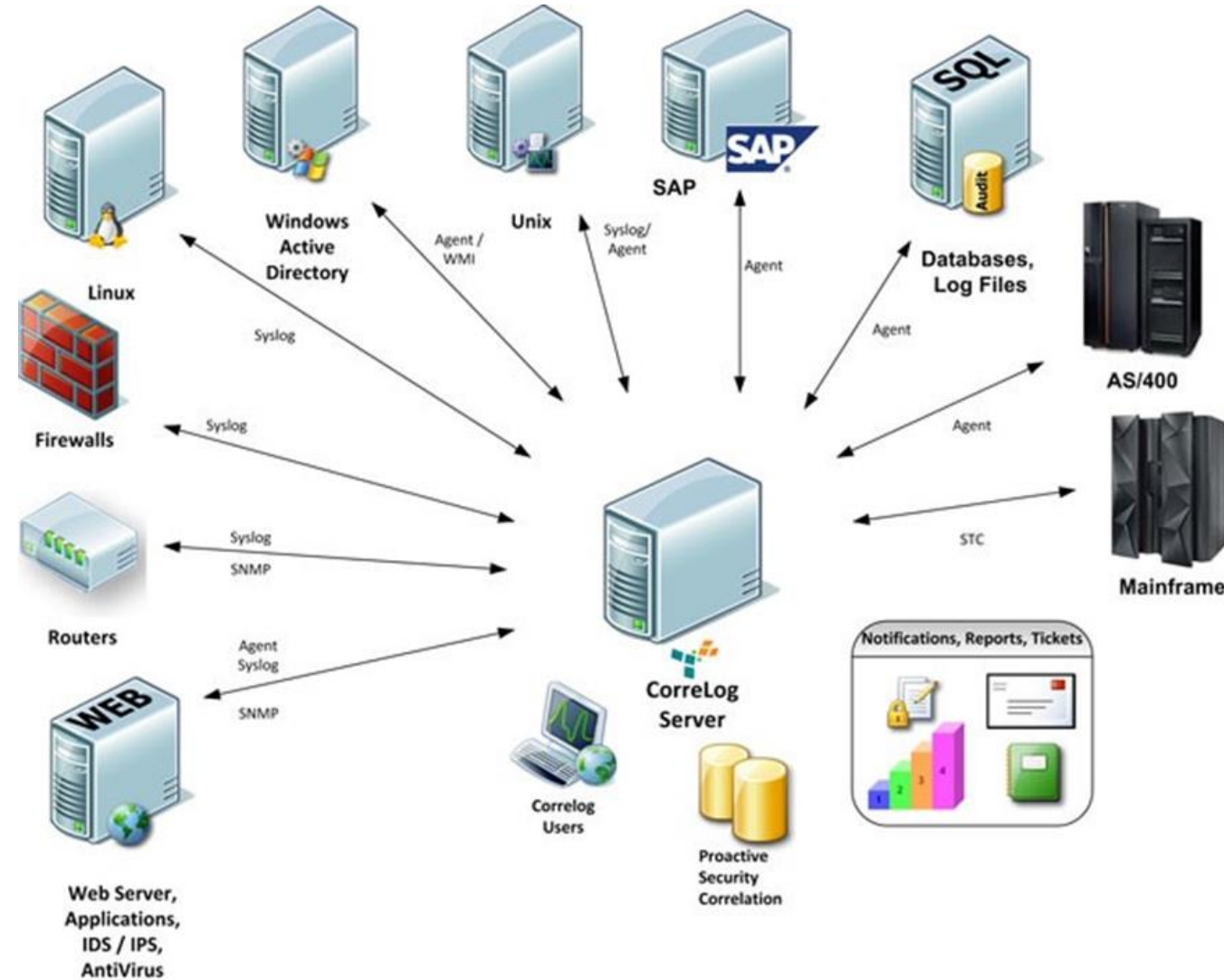
IDS versus IPS

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

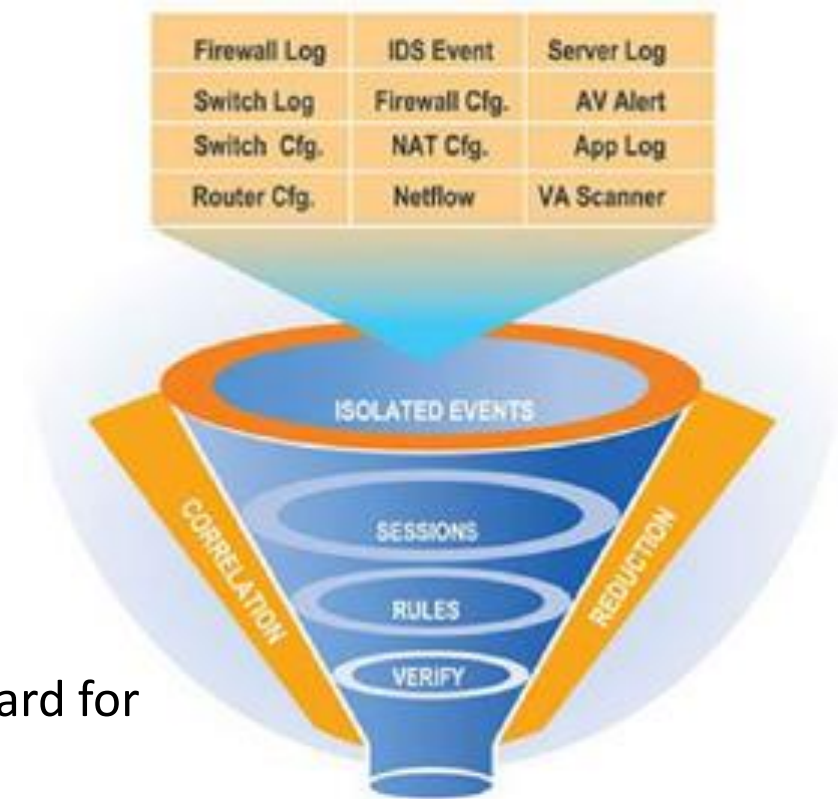


Continuous monitoring with a Security Information and Event Management (SIEM) system



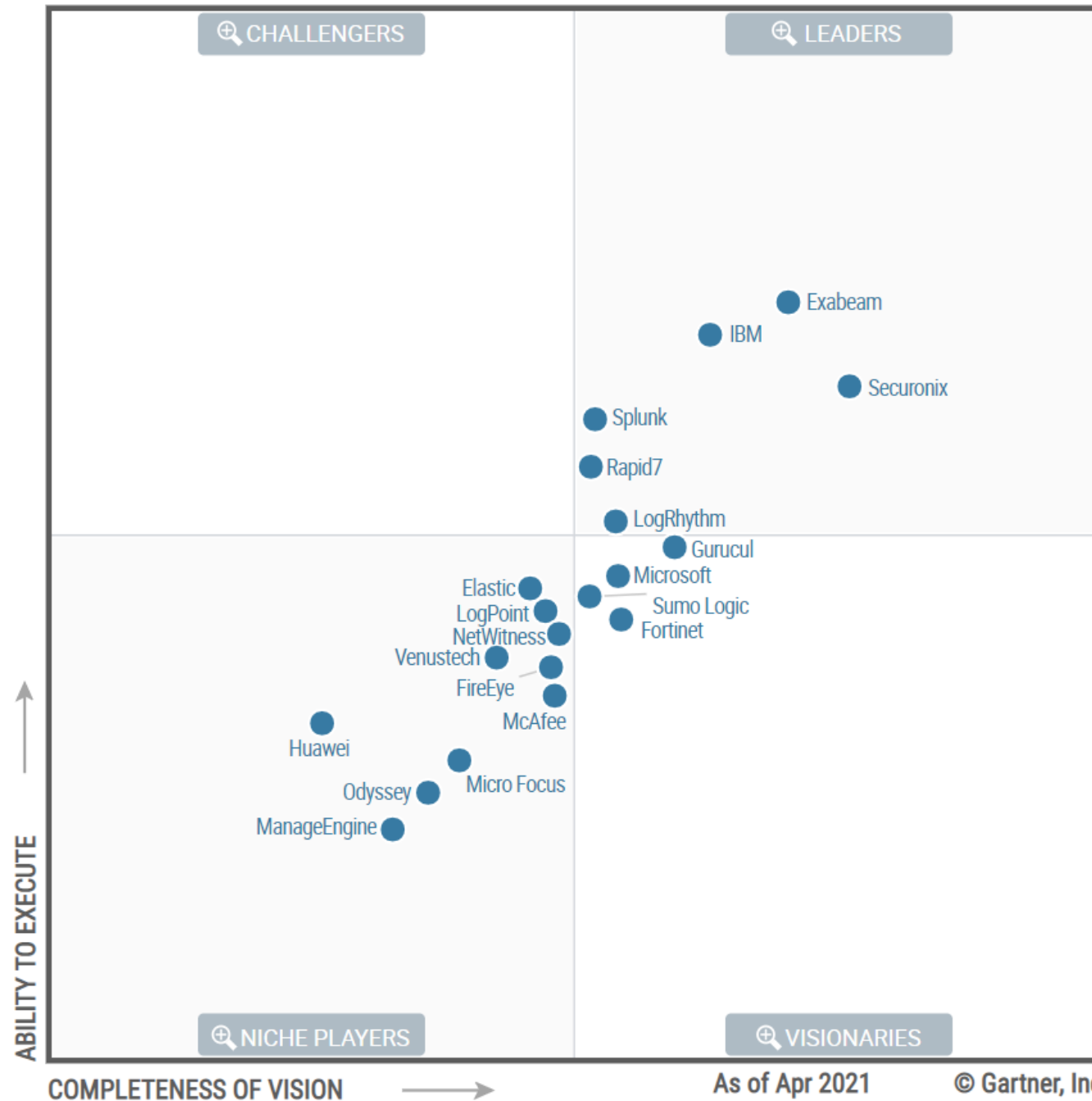
SIEM's help with Data Analysis and Correlation

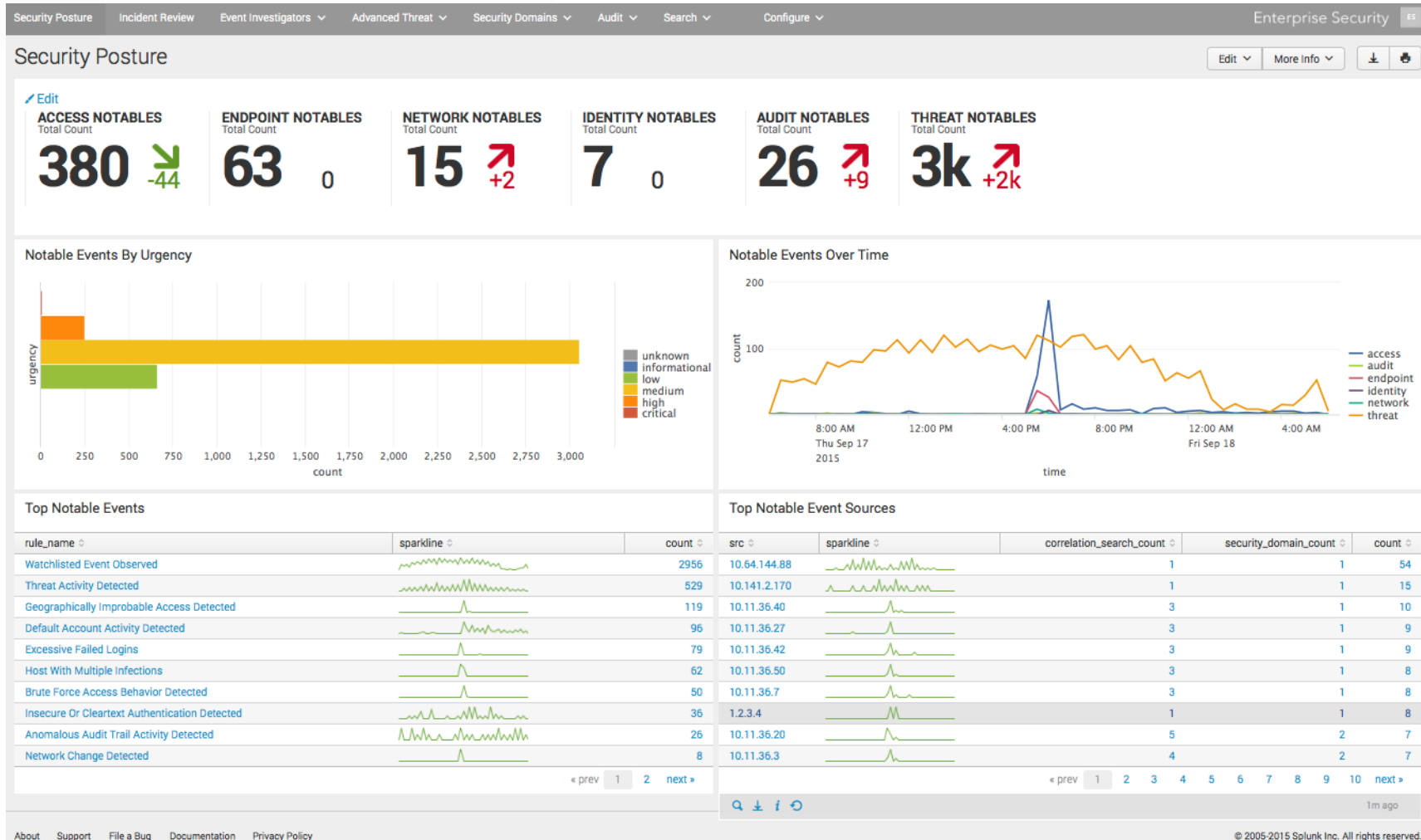
- Bring raw data events into one database
- Database software is programmed to look for “Notable events” or correlations
- Correlations will take seemingly isolated events and bring them forward for review/action:
 - **Windows Log:** Employee denied windows login (unknown user account)
 - **Identity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



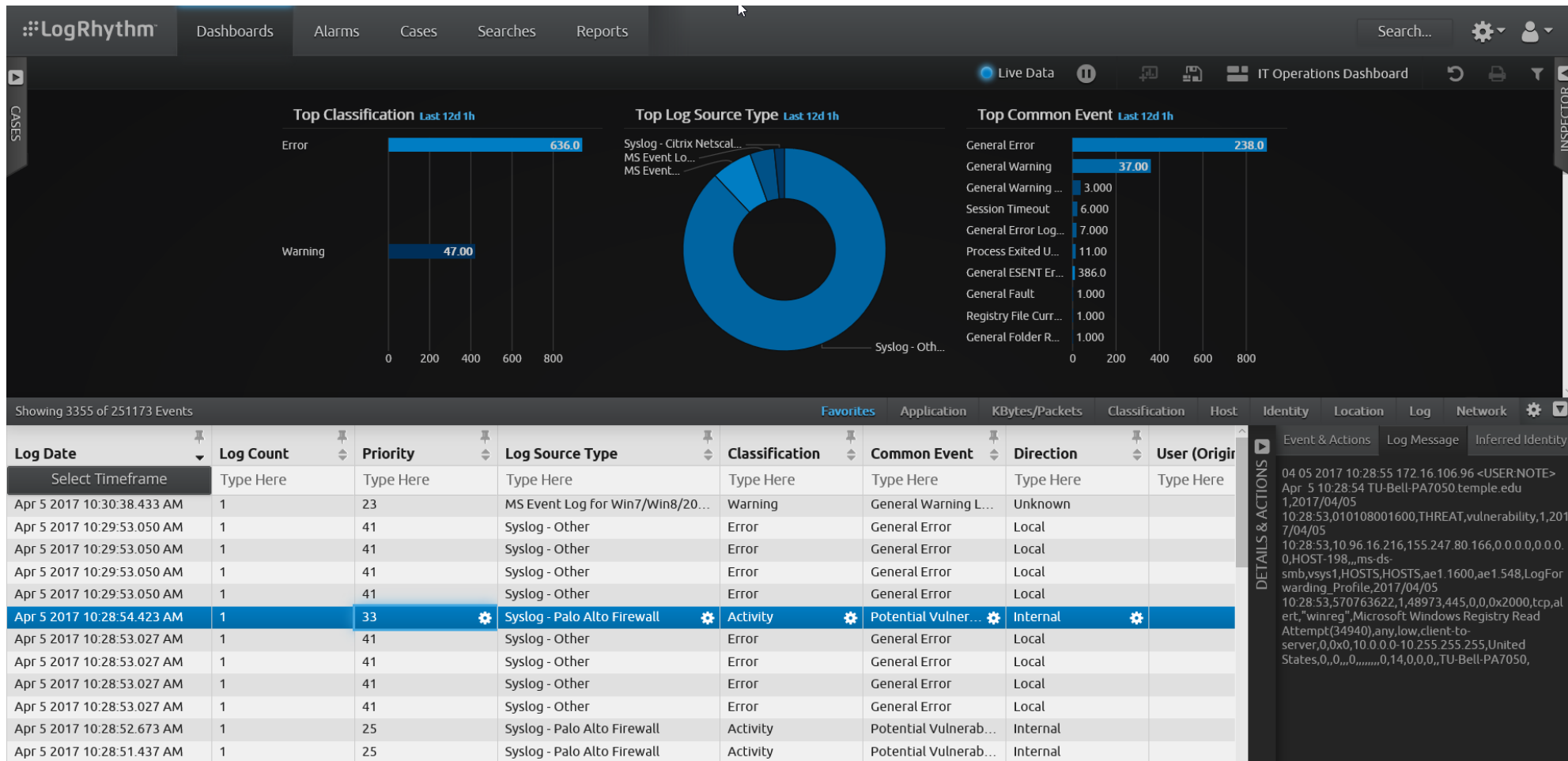
SIEM

- **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.





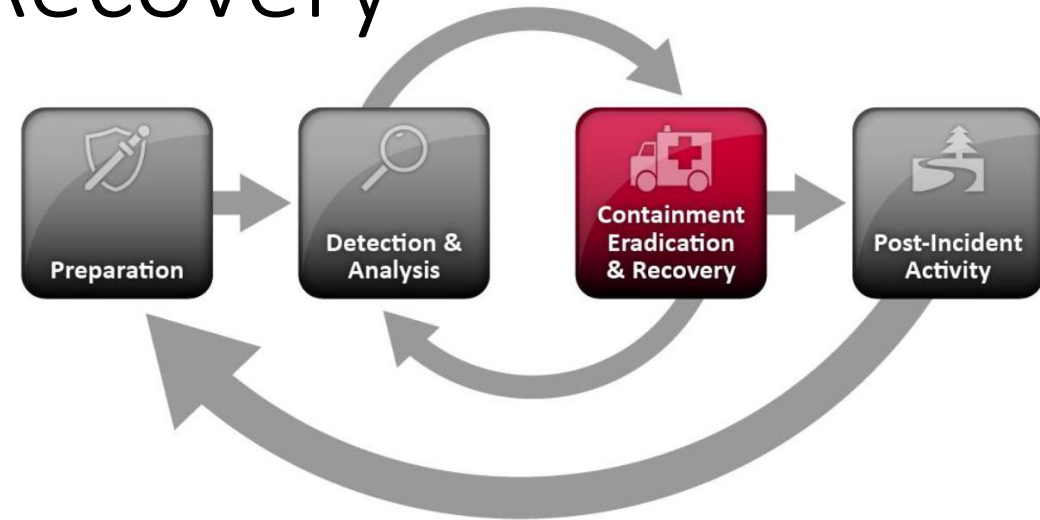
LogRhythm™



Containment, Eradication, and Recovery

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

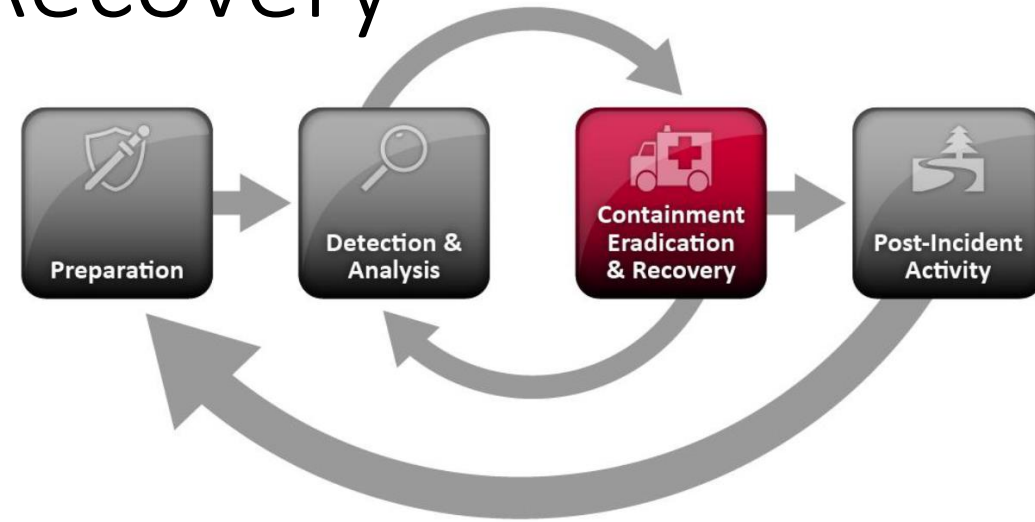
- Most incidents require containment, which provides time for developing a tailored remediation strategy
- An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions)
- Criteria for selecting among containment strategies are 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

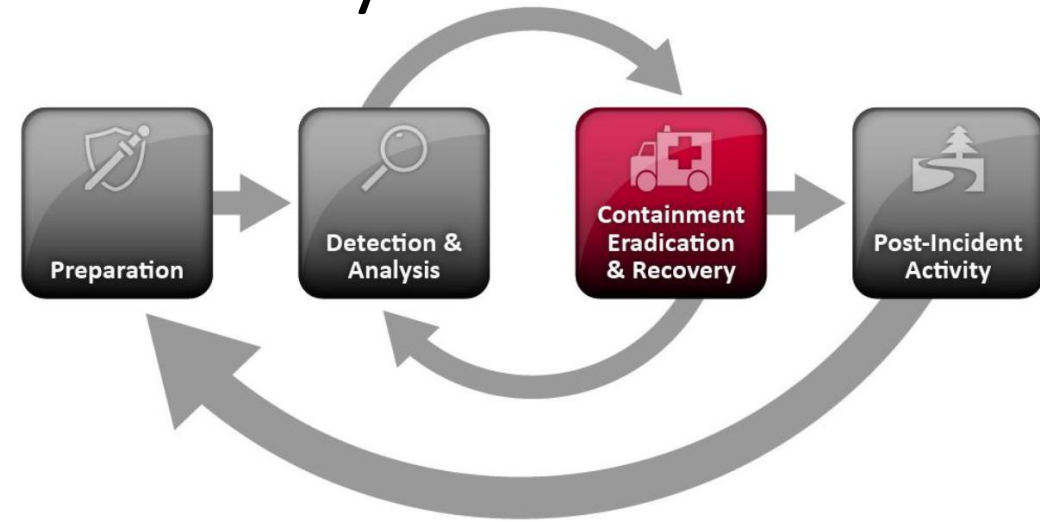
Recovery - In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents

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, ...)

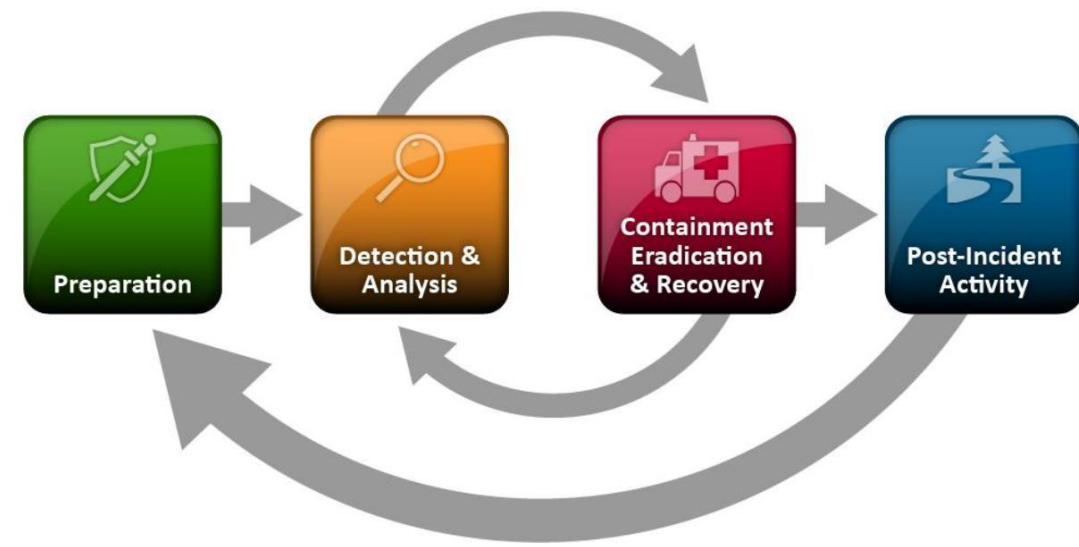
Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner

- 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

- ✓ 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