Computer Security Incident Handling
Detection and Analysis

Jeff Roth, CISSP-ISSEP, CISA, CGEIT

Senior IT Security Consultant

Coalfire

Agenda

- SECURITY INCIDENT CONTEXT
- TERMINOLOGY
- DETECTION AND ANALYSIS
  - ATTACK VECTORS
  - SIGNS OF AN INCIDENT
  - SOURCES OF PRECURSORS AND INDICATORS
  - INCIDENT ANALYSIS
  - INCIDENT DOCUMENTATION
  - INCIDENT PRIORITIZATION
  - INCIDENT NOTIFICATION
- EXAMPLE OF AN INCIDENT HANDLING CHECKLIST

Security Incident Context

- **Events verses Incidents[1]**
  - **Events**
    - An *event* is any observable occurrence in a system or network.
    - *Adverse events* are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

[1] National Institute of Science and Technology Special Publication 800-61 v2, COMPUTER SECURITY INCIDENT HANDLING GUIDE, August 2012

Coalfire

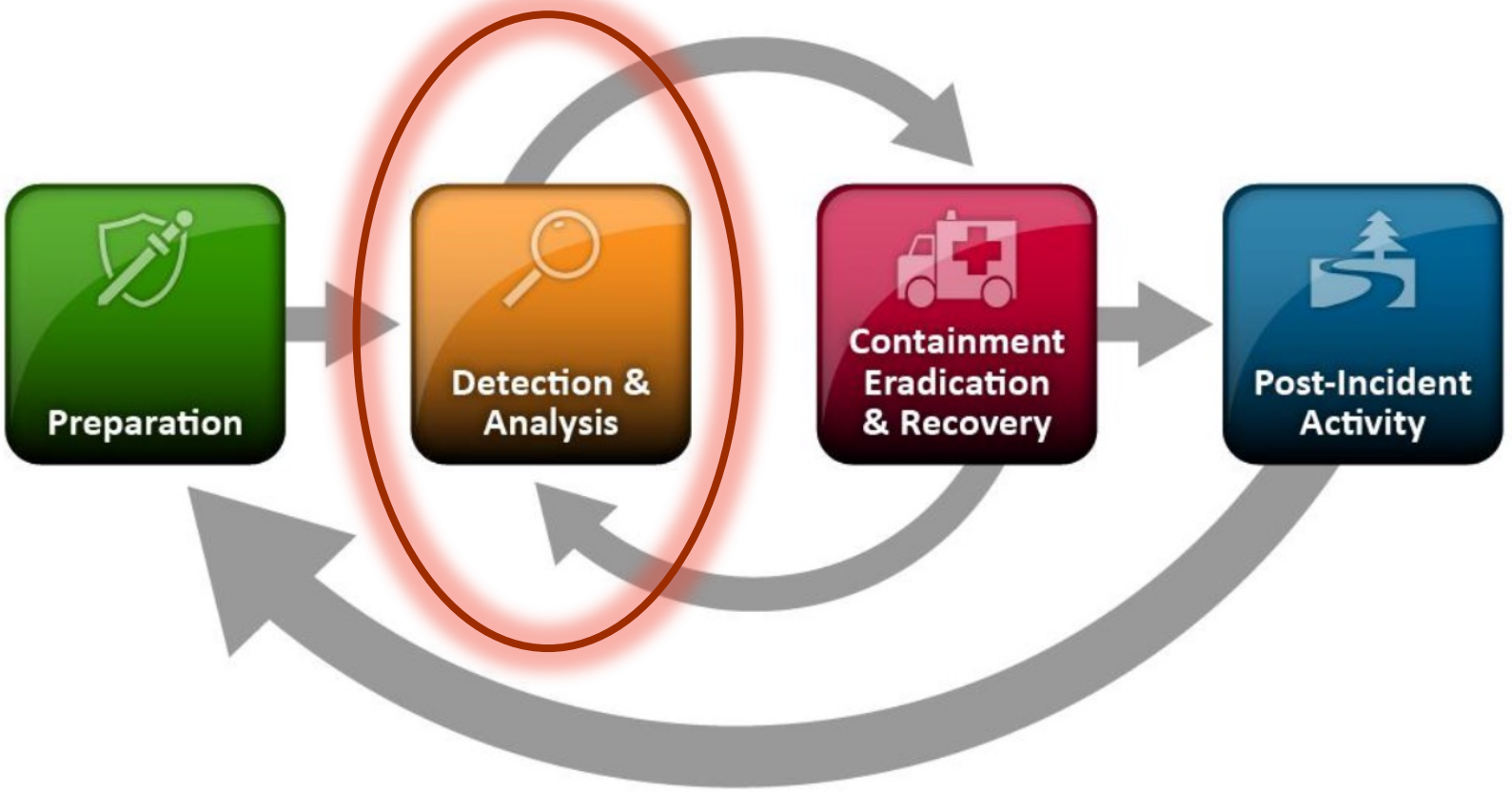
Incident Response Context

- **Events verses Incidents**[1]
  - **Incident -** A *computer security incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

[1] National Institute of Science and Technology Special Publication 800-61 v2, COMPUTER SECURITY INCIDENT HANDLING GUIDE, August 2012

Coalfire

Incident Response Context
Incident Response Life Cycle[1]



[1] National Institute of Science and Technology Special Publication 800-61 v2, COMPUTER SECURITY INCIDENT HANDLING GUIDE, August 2012

Coalfire

Security Incident Context

Organizational Structures

- **Incident Response Team Structure**
  - **Central Incident Response Team**. A single incident response team handles incidents throughout the organization (small organizations and for organizations with minimal geographic diversity)
  - **Distributed Incident Response Teams**-multiple incident response teams, each responsible for a particular logical or physical segment of the organization (large organizations and major computing resources at distant locations). **However, the teams should be part of a single coordinated entity**

Coalfire

Terminology

- **Threat**: The potential source of an adverse event. Common threat planes:
  - Human Interaction
    - Email (received and sent)
    - Web pages visited
    - Social sites
    - Blogs
  - Architectural
    - Network interfaces (External and internal)
    - Severs and running services and applications
- **Vulnerability**: A weakness in a system, application, or network that is subject to exploitation or misuse.

Terminology - Continued

- **Attack Vectors:** These are the means used by the attackers to exploit vulnerabilities. Examples are:
  - External/Removable Media
  - Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services
  - Web
  - Email
  - Social Engineering
  - Improper Usage
- **Precursor**: A sign that an attacker may be preparing to cause an incident.
- **Indicator**: A sign that an incident may have occurred or may be currently occurring.

Detection and Analysis

- First of all let's level set with the current state of Cyber attacks….
  - Many of the high profile attacks over the past few years are sophisticated in nature
  - The Threat actors are persistent and come from many areas of the world driven by a variety of motivations… Money and Data theft are primary goals
  - Neither of the above are uncommon nor can these be used as an excuse for inaction

Detection and Analysis - Signs of an Incident

- Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers.
- Manual means, such as problems reported by users (watch trouble ticket and work order systems).
- Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.

Detection and Analysis - Signs of an Incident

- We remember Signs of an incident come in two categories - precursors and indicators.
- Good News- If we detect precursors we have an opportunity to prevent the incident
- Bad News - Most attacks do not have any identifiable or detectable precursors

Detection and Analysis - Signs of an Incident

- So what detective and predictive controls should we have in place:
  - Profile Networks and Systems-measuring the characteristics of expected activity so that changes to it can be more easily identified
  - Understand Normal Behaviors. Incident response team members need to have system specific knowledge regarding networks, systems, and applications (normal behavior is readily known so that abnormal behavior is recognized quickly)

Detection and Analysis - Signs of an Incident

- So what detective and predictive controls should we have in place:
  - Create a Log Retention Policy (firewall, IDPS, OS and application logs). Remember that older log entries may show key clues such as
    - reconnaissance activity
    - previous instances of similar attacks
  - Remember many times the incident may not be discovered until days, weeks, or even months later – no log retention…no evidence

Detection and Analysis - Signs of an Incident

- So what detective and predictive controls should we have in place:
  - Protect the logs – All log need to write to a separate log server (write once only media preferred)
  - Perform Event Correlation.
    - Firewall log may have the source IP address
    - Application log may contain a username.
    - Network IDPS may detect that an attack was launched against a particular host

Detection and Analysis - Signs of an Incident

- So what detective and predictive controls should we have in place:
  - Keep All Host Clocks Synchronized from an authoritative NTP server
  - Use existing trouble ticket/work order systems along with incident knowledge base to better perform predictive analytics

Detection and Analysis - Incident Documentation

- **The issue tracking system should contain information on the following:**
  - The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
  - A summary of the incident
  - Indicators related to the incident
  - Other incidents related to this incident
  - Actions taken by all incident handlers on this incident
  - Chain of custody, if applicable

Detection and Analysis - Incident Documentation

- **The issue tracking system should contain information on the following: (continued)**
  - Impact assessments related to the incident
  - Contact information for other involved parties (e.g., system owners, system administrators)
  - A list of evidence gathered during the incident investigation
  - Comments from incident handlers
  - Next steps to be taken (e.g., rebuild the host, upgrade an application).

Incident Prioritization

Functional Impact Categories Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Prioritization of the Incident

Information Impact Categories Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII), Card Holder Data, electronic-Personal Health Information of customers, taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Proprietary information, such as protected critical infrastructure information (PCII), company formulas, plans, engineering data, etc. was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Prioritization of the Incident

Recoverability Effort Categories Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Detection and Analysis - Notification

- Once we have identified, analyzed and prioritized an incident, the incident response team will activate the notification processes based on the nature and severity of the incident
  - Call lists must be current, accurate and accessible by authorized personnel
  - Notification trees should be developed and clearly aligned with the documented escalation plan

Coalfire

Detection and Analysis - Notification

- **Non-IT Roles**
  - CEO, COO, CFO, CRO
  - Human resources
  - Public affairs
  - Legal department
  - Board of Directors
  - US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
  - Law enforcement (if appropriate)

Detection and Analysis - Notification

- **IT Specific Roles**
  - CIO
  - System owner
  - Head of information security
  - Local information security officer
  - Other incident response teams within the organization (includes subcontractors, service providers, business partners, etc.)
  - External incident response teams (if appropriate)

Detection and Analysis - Notification

- **Notification Effectiveness**
  - Based on prioritization, the notification call list will escalate based on:
    - Severity and size of the incident
    - Regulatory and contractual and functional impact
  - Notification can take the many forms concurrently to provide completeness, accuracy, speed and redundancy
  - For incidents involving regulatory and contractual impacts, both legal and public affairs will play a significant role as to incident investigation and information release respectively

Coalfire

Detection and Analysis – "Do Loop"

- **Based on the subsequent steps within the incident response process, the Detection and Analysis processes may be revisited until incident has been closed**
- **Why?**
  - During containment, eradication and recovery additional data is required
  - New attacks may continue as the containment and eradication corrective controls are in place. The detection and analysis will provide indicators that containment is successful

Detection and Analysis – "Do Loop"

- **Why? (Continued)**
  - Information from Detection and Analysis will be reviewed for the final incident report and lessons learned
  - Enters into the organization knowledge base and training of the incident response team members

Questions?

Thank you

For further information contact

Jeff.Roth@Coalfire.com
321-795-0391
Ron.Frechette@Coalfire.com
303-554-6333 x7826

Coalfire