
LouMUG
Louisville Microsoft Users Group
A Forum for Computer Professionals

Introduction to Incident Response

10/31/2025

Jordan Silva
Director of Managed Services

Jordan.silva@mirazon.com linkedin.com/in/jordansilva

Mirazon

Agenda

- What is Incident Response?
- The Incident Response Cycle
- IR Communication Tips
- Table-Top Exercise – Backdoors and Breaches

What is Incident Response

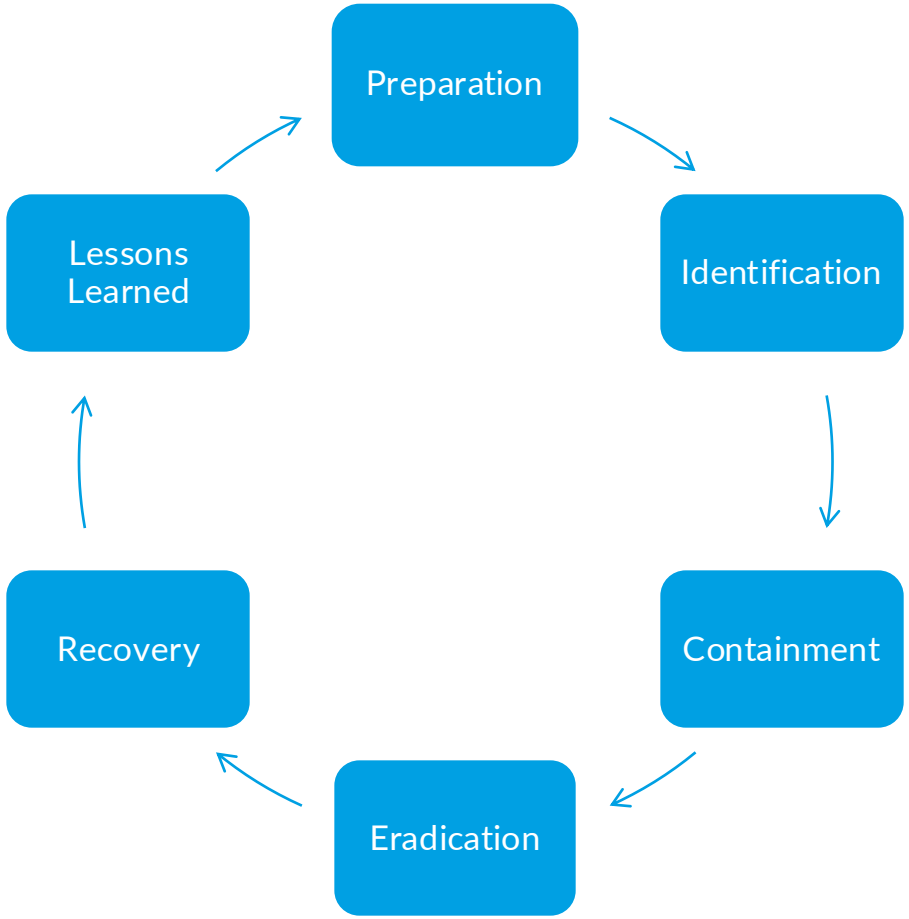
- **What is an Incident?** *A confirmed or highly confident probability of a non-authorized party successfully accessing a system or otherwise negatively impacting the Confidentiality, Integrity, or Availability of a system.*

- **What is Incident Response:** *The **coordinated** effort to investigate, respond to, and remediate an incident.*

Who participates in Incident Response

- **Incident Commander:** The person running the incident response.
  - Varies based on the size of the incident and maturity of the org. It could be an IT manager/director, a CISO, a dedicated IR team member, etc.
- **Infosec Team Members**
  - **SIEM Engineers:** The infosec team members who manage the logging and SIEM solutions
  - **SOC Analysts:** Analysts who are trained to locate and investigate IOCs
- **System Administrators:** The technical staff responsible for the infrastructure
- **Data Owners:** The team responsible for the impacted data.
- **3rd Party Incident Responders:** Hired 3rd parties to assist with specialty analysis.
  - Note: This is VERY common. Most large companies, including MSPs, use 3rd party IR for meaningful breaches.
- **Vendors:** Vendor support for impacted systems

The SANS Incident Response Cycle



Preparation

- **Training:** Formal, internal, etc.
- **Practicing:** Red Team exercises, Purple Team exercises, tabletop exercises, etc.
- **Tools Preparation:** Forensics kits, licensing checks, training, etc.
- **IR Planning:** Policies, Procedures, Role Assignments, Documentation

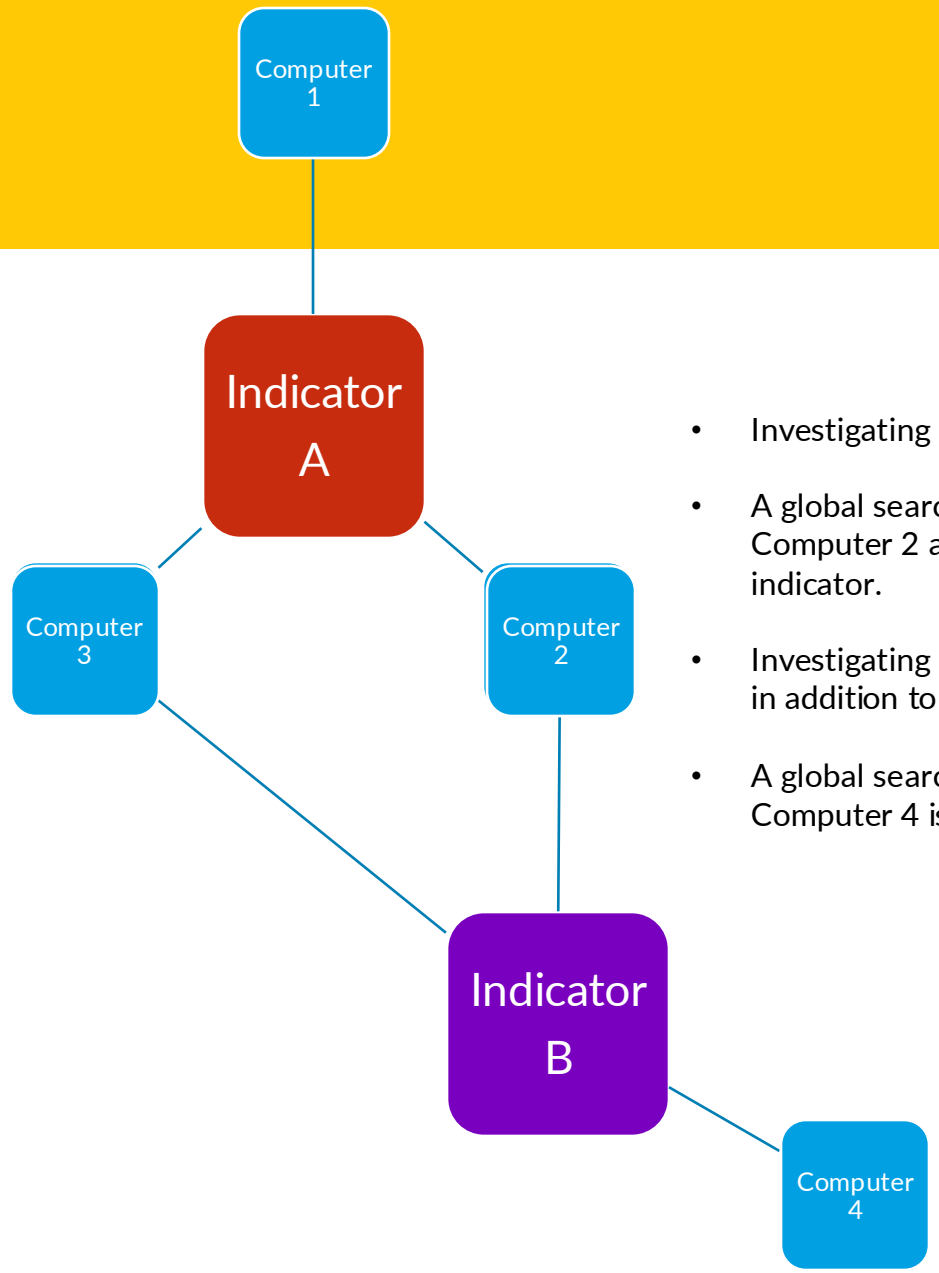
Identification

- **Reviewing Alarms \ Reported Activity**
  - Determining True \ False Positive
- **Starting the IR Process**
  - Setup Bridge
  - Incident Commander Assigned
  - IR Team comes online
- **Scoping the Incident**
  - What is impacted?
  - What is happening?
  - What is the overall impact?
- **Start Documenting**

More On Scoping:

Indicators of Compromise:

An artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.



- Investigating Computer 1 Finds Indicator A.
- A global search for Indicator A shows Computer 2 and 3 both have the same indicator.
- Investigating Computer 2 locates Indicator B in addition to Indicator A.
- A global search for Indicator B reveals Computer 4 is also impacted.

Identification Goals

Initial Access	• How did the attacker get in?
Persistence Methods	• How do the intend to stay connected?
Lateral Movement	• How did they move around the network?
Actions on Objectives	• What were they trying to accomplish?

Containment

- **Begin Isolation**
  - Isolate compromised systems
  - Limit connectivity between segments
- Take steps to **prevent further actions on objectives**
- Take forensic images

Eradication

- **Removing Malicious Software**
- **Cut off remote sessions if active**
- **Reset Passwords / Disable Credentials**
- **Begin Patching Flawed Systems**
- **Measure Twice, Cut Once**

Eradication – Why isn’t this step 1?

- If we don’t know how they got in, they can probably get back in.
- If the attacker believes we are aware, they may move faster or “scorch earth” and leave.
- We want to know the goal of the attack so we can prepare in the future.

Recovery

- Restore impacted systems to known good states or rebuild
- Recover data from backups
- Restore functionality of systems that were taken offline
- Validate resolutions of the incident are in place and working.

Lessons Learned

- Conduct a review of the incident
- What went well? What could be improved on? Where was their confusion?

Incident Response Communication Tips

Incident Response Communication Tip #1

Communicate Often:

The cadence of communication will vary per incident and will change as the incident progresses, generally with longer intervals as we progress into recovery and lessons learned.

The Incident Commander sets the cadence. Be clear on when communication should occur and how.

Incident Response Communication Tip #2

Communicate Precisely: Be clear about what you are communicating, provide the required context and explain the impact you believe it has.

Be clear if something is **DATA**, **ANALYSIS**, or a **QUESTION**

- **Data:** A factual piece of information, like an IP address, file name, etc.
- **Analysis:** A person's interpretation of data, often including hypotheses or conclusions.
- **Question:** A request for information

Incident Response Communication Tip #3

Out-of-Band Communication:

If primary communication methods (Email, Teams, etc.) are believed to be compromised, out-of-band communication plans will be used.

Note: This also impacts data sharing methods.

Thanks! Q&A

Jordan Silva – LinkedIn: https://www.linkedin.com/in/jordansilva

Lou MUG

Let’s Play

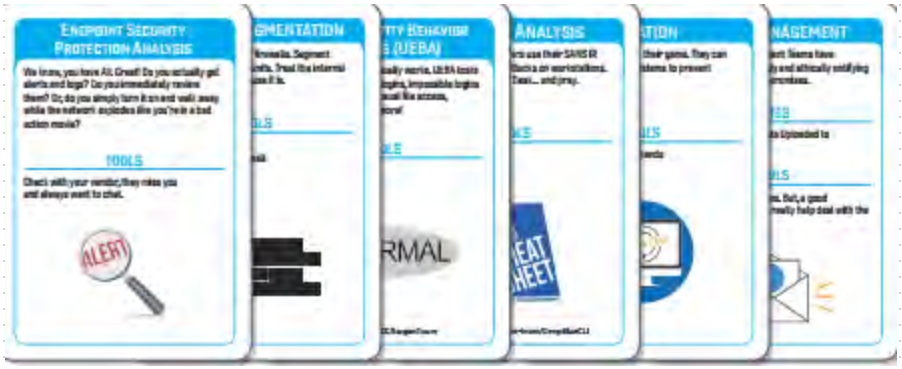
Special thanks to **Black Hills Information Security** for providing all decks for attendees today.

You are now a crack team of Cyber Security Incident Responders.

Your mission, should you choose to accept it, is to uncover the cyber mischief occurring in one of 3 scenarios we have setup around the office.

Uncover the Attack Chain

Use your Tools Wisely



How to Play

1. Your Incident Master will introduce you to the scenario.
2. You and the IR team will decide which of your procedure cards you would like to play to start the investigation.
3. Once selected, roll the dice. You need a 10 or higher to successfully execute your investigation step.
    - “Primary” procedures, get a +3 modifier, as you are more familiar with those tools.
4. If your roll is successful, and the procedure you selected is capable of detecting one of the attackers' actions, that card will be turned over.
5. You have 10 turns to successfully uncover all of parts of the attack.

A few notes:

- Not all tools can detect all kinds of attacks, so a successful roll does not guarantee a discovery. Think about the scenario and what tool matches what might be happening.

- Not all procedures help further an investigation at all, don’t get distracted.

- Only 1 Attack Chain card will be revealed per turn, so it may take multiple successful attempts to uncover all portions of the chain, even when using the same tool.