**Incident Response: Because “Oops” Is Not a Strategy**

**Meta:** Someone clicked the phishing link. Again. The ransomware note just popped up. Your CEO wants answers. Welcome to Incident Response, where every day is chaos management, and sleep is a myth.

A person sitting at a desk with several computers

AI-generated content may be incorrect.

Photo by [CDC](https://unsplash.com/@cdc?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

**1. What Is Incident Response (IR)?**

Incident Response is the cybersecurity version of emergency services. Think digital fire-fighters, but instead of flames, it’s “Why is our database speaking Russian?”

You’re the one who steps in when things have gone spectacularly wrong such as malware outbreak, data breach, rogue insider, or DarKVoicE from HR downloading “FreeGameCrackUltimate2023.exe.”

You investigate, contain, clean up, document everything, and hopefully prevent it from happening again. (***Spoiler***: It still will.)

**2. Types of Incidents That Will Ruin Your Day**

A screenshot of a computer

AI-generated content may be incorrect.

types of incidents

**3. The IR Process (“The Oh No” Workflow)**

A person in a suit and tie

AI-generated content may be incorrect.

Nope. Credit: GIPHY

**1. Preparation**

Before the digital house is on fire:

* Build an IR plan
* Define team roles
* Practice scenarios (tabletop exercises, not Monopoly)
* Know where your logs are (seriously)

**2. Detection & Analysis**

“Something weird is happening…”

* Alerts from SIEM
* Users screaming
* The server’s CPU is melting  
  Figure out: *What happened, how bad is it, and who messed up?*

**3. Containment**

Stop the bleeding.

* Isolate infected machines
* Kill malicious processes
* Pull the plug (*metaphorically*… or not)

**4. Eradication**

Get rid of the threat completely.

* Remove malware
* Patch vulnerabilities
* Change compromised credentials
* Purge shadow IT nonsense

**5. Recovery**

Turn stuff back on. Carefully.

* Restore from clean backups
* Monitor like a hawk
* Pray you don’t reinfect everything

**6. Lessons Learned**

Write reports. Blame nobody (publicly). Improve.

* Postmortem analysis
* Update playbooks
* Patch the human layer: training, awareness, “please stop clicking sketchy links” campaigns



Don't click, please. Credit: GIPHY

**4. The IR Mindset: Calm, Cool, Paranoid**

* **Don’t Panic.** Even if the server’s crying.
* **Assume Compromise.** Then prove it or disprove it.
* **Documentation is Holy.** If you didn’t write it down, you didn’t do it.
* **Think Adversarial.** “If I were the attacker, what would I do next?”
* **Know Your Environment.** If you don’t know what “***normal***” looks like, “***weird***” won’t stand out.

**5. Tools of the Incident Responder Trade**

A screenshot of a computer

AI-generated content may be incorrect.

Tools Essential

**Bonus tool:** A very large whiteboard and your third coffee of the day.

**6. Mistakes You Only Make Once (Hopefully)**



accidents? Credit: GIPHY

* Not having a plan
* Forgetting to unplug the infected printer (yes, printers get infected)
* Restoring from infected backups
* Not telling management until CNN calls
* Trusting “the intern said it was fixed”

**7. IR in Action: Mini Case Study**

A notebook and pencil on a table

AI-generated content may be incorrect.

Photo by [JESHOOTS.COM](https://unsplash.com/@jeshoots?utm_source=medium&utm_medium=referral) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

* **Alert:** Unusual outbound traffic to IP in North Korea.
* **Investigation:** Turns out finance installed a free VPN.
* **Containment:** Kill process, remove app, revoke credentials.
* **Eradication:** Delete persistence mechanisms, scan for more malware.
* **Recovery:** Restore finance’s machine from backup.
* **Lessons Learned:** Disable local admin access. Also, never trust anything with “Free” in the title.

**8. IR Roles & Titles (aka: Who Does the Stressing)**

A screenshot of a computer

AI-generated content may be incorrect.

Roles and possibly some estimates of salary (NOT ALL PLACES GIVE THE SAME, EVEN TO ME 🥲)

**9. How to Learn IR (Without Losing Your Mind)**

**Practice:**

* CyberDefenders, BlueTeamLabs, TryHackMe IR rooms
* Build your own DFIR lab with REMnux, Security Onion, and malware samples (carefully!)

**Read:**

* “The DFIR Report”
* “Incident Response & Computer Forensics” (Luttgens et al.)
* “Practical Malware Analysis”

**Watch:**

* 13Cubed, DFIR Diva, Forensic Focus on YouTube
* IR-focused talks at SANS, DEF CON, Black Hat

A cartoon penguin carrying a stack of books

AI-generated content may be incorrect.

Never Give Up. Credit: GIPHY

***Quiz Time***

1. **What’s the first step in incident response?**

a) Yell “we’re hacked!”  
b) Preparation  
c) Delete everything  
d) Tweet about it

**2. What tool is used for memory analysis?**

a) Wireshark  
b) Volatility  
c) Discord  
d) Ctrl+Alt+Delete

**3. Why do you contain before eradication?**

a) So the malware doesn’t spread  
b) To buy time for lunch  
c) To confuse attackers  
d) Because that’s what the flowchart says

*(Answers: 1b, 2b, 3a)*

**Enjoyed the read?**  
Smash the follow button, drop a comment, and share this with someone who still thinks “password” is a good password.