

Based on the sources, the roles explicitly identified as entry-level in the cybersecurity career progression are primarily engineering and technical support positions.

The designated **Entry-level** roles are:

- **Systems engineer**
- **Network engineer**
- **IT technician**

Additionally, while specific levels can vary, starting as a **SOC analyst** (Security Operations Center analyst) is noted as a strong way to gain experience if you are interested in blue team roles.

Other roles that are common in the field, but whose specific career level (entry, mid, or advanced) is not defined in the source, include:

- **Information security analyst**
- **Security engineer**
- **Network security engineer**

For comparison, roles such as security analyst, incident responder, and penetration tester are classified as mid-level.

The sources provide a detailed anatomy of a **fictional cyber attack**, which serves as an extensive case study or analysis resembling a major cybersecurity incident report, along with outlining the roles responsible for incident response and investigation.

The analysis details a completely fictional breach designed to highlight IAM (Identity and Access Management) pitfalls within an attack life cycle. The victim was a market-leading manufacturer with strong Intellectual Property (IP). The incident spanned a **two-year cycle**, from January 2014 through January 2016, demonstrating the patience of the attacker (a known organized crime syndicate).

The attack followed the classic phases of the **Cyber kill chain**—a framework that plots the paths typically seen through an attack cycle, used as an educational basis for defense. The phases of the attack were **reconnaissance, infiltration, exploitation and escalation, and then exfiltration and exit**.

#### 1. Reconnaissance and Infiltration

The reconnaissance phase, where detection is difficult, involved several steps:

- **Scanning:** External web and network scanning occurred, looking for direct attacks and externally facing vulnerabilities.
- **Research:** Extensive research was conducted on executives, employees, contractors, and suppliers (noting that the attack surface includes business partners who have access to systems).



FORTIFY THE FUTURE





[Skip to content](#)

**You said:**

incident respondern

**ChatGPT said:**

It sounds like you meant “incident responder.”

An incident responder is a cybersecurity professional (or emergency professional, depending on context) who reacts quickly to critical events—called *incidents*—to minimize damage, recover operations, and prevent future occurrences.

Here are the two main contexts where the term is used:



## Cybersecurity Incident Responder

Role: Detects, analyzes, and mitigates security breaches such as malware infections, ransomware, data theft, or unauthorized access.

Typical responsibilities:

- Monitor systems for suspicious activity (using SIEM tools like Splunk or Sentinel).
- Investigate alerts to determine scope and impact.
- Contain, eradicate, and recover from attacks.
- Conduct forensic analysis and write incident reports.
- Recommend improvements to prevent recurrence.

Common skills:

- Network and system administration
  - Malware analysis and threat hunting
  - Scripting (Python, PowerShell, Bash)
  - Familiarity with frameworks like NIST 800-61 or MITRE ATT&CK
- 



## Emergency or Disaster Incident Responder

Role: Reacts to physical emergencies (fires, accidents, natural disasters, etc.).

Responsibilities:

- Assess the situation and secure the area
  - Provide medical aid or rescue
  - Coordinate with police, firefighters, and EMS
  - Maintain readiness through drills and training
- 

Would you like me to explain how to become an incident responder (e.g., skills, certifications, and career path), or are you referring to a specific type of incident response (like cybersecurity or emergency response)?

Attach  
Search  
Study  
Voice

ChatGPT can make mistakes. Check important info.