Cybersecurity Incident Detection Methods - Summary

# Detection and Analysis Phase Overview

This phase focuses on discovering, validating, and investigating possible security incidents.  
- Detection = prompt discovery of suspicious activity  
- Analysis = validation and investigation of alerts

# Detection Tools

- Intrusion Detection Systems (IDS): Detects intrusions and sends alerts  
- SIEM (Security Information and Event Management): Collects and analyzes logs and security data  
Note: Tools only detect what they’re configured to—misconfigurations can leave gaps.

# 1. Threat Hunting

- Proactive and manual technique used by human analysts  
- Finds hidden threats missed by automated tools (e.g., fileless malware)  
- Involves researching threats, analyzing indicators, and using AI/ML for support  
- Threat Hunters: Specialists who look for vulnerabilities and unknown threats

# 2. Threat Intelligence

- Evidence-based data about known or emerging threats  
- Sources include:  
 - Industry reports  
 - Government advisories  
 - Threat data feeds (IPs, domains, hashes)  
- Managed using Threat Intelligence Platforms (TIPs) for context and prioritization  
Note: Threat feeds should supplement, not replace, detection.

# 3. Cyber Deception

- Involves tricking attackers to detect and analyze threats  
- Honeypots: Fake systems or files (e.g., “Client Credit Cards - 2022”) used to attract and monitor attackers

# Key Takeaways

- No single detection method is sufficient  
- Combine tools, intelligence, human analysis, and deception  
- Adapt strategies to evolving threats for stronger cybersecurity posture