Roles and Responsibilities

Incident Manager	Leads response efforts, making key decisions and ensuring coordination across the team	Tools	Project management software for task tracking (e.g., Asana, Jira)
Security Analysts	Conduct technical investigations and analyses using various tools	Tools	SIEM systems for monitoring and analysis (e.g., Splunk, LogRhythm), and forensics analysis tools for in-depth investigation (e.g., Encase, FTK)
Communications Officer	Manages all communications, ensuring clarity and timeliness	Tools	Secure communication platforms (e.g., Signal, Microsoft Teams for internal coordination)
IT Specialists	Implement technical fixes and restore systems	Tools	Endpoint detection and response (EDR) tools for mitigating threats (e.g., CrowdStrike Falcon, Microsoft Defender for Endpoint)
Legal and Compliance Officer	Provides legal guidance and ensures compliance with relevant laws and regulations	Tools	Compliance management software (e.g., LogicGate, NAVEX Global)

Incident Response Phases

Phase	Key Actions	Tools
Preparation	Establish an incident response policy, form a response team, and prepare incident response playbooks	Training platforms (e.g., Infosec IQ, CyberHoot)
Detection and Analysis	Monitor systems for signs of unauthorized activity, analyze alerts to confirm incidents	SIEM systems, intrusion detection systems (IDS) like Snort or Suricata
Containment	Isolate affected systems, apply short-term fixes	Network segmentation tools, firewall and intrusion prevention systems (IPS)
Eradication and Recovery	Remove malware, apply patches, and recover data from backups	Antivirus/malware removal tools, patch management software (e.g., ManageEngine Patch Manager Plus), backup and recovery solutions (e.g., Veeam, Acronis)
Post-Incident Evaluation	Document the incident, evaluate response effectiveness, update plans and defenses based on lessons learned	After-action review templates, lessons learned databases

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com