In incident response, there are various technologies that can assist security teams in effectively detecting and responding to security incidents. Here are some commonly used technologies:

1. **SIEM** (Security Information and Event Management):Data from various security tools and network devices is gathered and analysed by SIEM. By comparing and ranking security alerts, it lessens the deluge of notifications and aids incident response teams in identifying actual threats.
2. **SOAR** (Security Orchestration, Automation, and Response): Security teams can formalise workflows, referred to as playbooks, by using SOAR to coordinate various security operations and tools. It facilitates effective incident response and automates repetitive tasks.
3. **EDR** (Endpoint Detection and Response):EDR software offers ongoing endpoint monitoring and security for devices like computers and mobile phones. It analyses real-time data for suspicious activities, responds to advanced threats that may evade traditional antivirus software, and takes precautions to reduce risks.
4. **XDR** (Extended Detection and Response):In addition to endpoints, networks, and clouds, XDR integrates security tools, data sources, and analytics. Through the elimination of silos and the automation of response procedures, it establishes a centralised system for threat prevention, detection, and response.
5. **UEBA** (User and Entity Behavior Analytics):UEBA uses machine learning and behavioural analytics to find unusual user and device behaviours that might point to security risks. It is efficient at identifying malicious activities that imitate authorised network traffic as well as insider threats.
6. **ASM** (Attack Surface Management): The identification, evaluation, correction, and monitoring of vulnerabilities and potential attack vectors across the assets of an organisation are all automated by ASM solutions. It makes sure preventative security measures are in place and assists in locating weak spots in the attack surface.

Careers:

Forensic Analyst: Forensic analysts specialise in collecting, preserving, and analysing digital evidence related to security incidents. They use specialised tools and techniques to uncover the root causes of incidents, track the activities of threat actors, and support legal investigations.

Incident Response Manager: These professionals oversee and manage incident response operations. They develop incident response strategies, coordinate with internal teams and external stakeholders, and ensure effective incident handling and resolution. Incident response managers often have advanced technical skills and strong leadership capabilities.

Security Consultant: Security consultants provide advisory services to organisations regarding incident response strategies, processes, and technologies. They assess an

organisation's security posture, identify vulnerabilities, and make recommendations for improving incident response capabilities.

Resources:

- https://www.atlassian.com/incident-management/incident-response#assess-the-impact-and-apply-a-severity-level
- https://www.fortinet.com/resources/cyberglossary/incident-response
- https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan