Day 55

Exploitation Analyst

Incident Response and Automation with AI:

Incident Response and Automation with AI in cybersecurity is highly valuable because it enables organizations to detect, analyse, and respond to threats much faster and more effectively than manual methods. AI-powered systems can continuously monitor vast amounts of network traffic, user behaviour, and system logs to identify anomalies that may indicate potential attacks. By automating incident response, routine tasks such as isolating compromised systems, blocking malicious IP addresses, or applying patches can be executed instantly, reducing the time attackers have to cause damage. This not only minimizes the impact of breaches but also frees up cybersecurity teams to focus on more complex issues that require human expertise. Additionally, AI-driven automation improves consistency, reduces human error, and provides predictive insights, making organizations more resilient against evolving cyber threats.

Does this mean no human is needed now for this work?

No, AI doesn't replace humans—it supports them. AI automates routine tasks like detecting threats or isolating systems, but human expertise is still needed for complex decisions, analysis, and strategy. Together, they make cybersecurity faster and more effective.

Future in AI powered OT security:

The future of AI-powered OT (Operational Technology) security looks promising as industries increasingly connect critical systems like manufacturing, energy, and transportation to digital networks. AI will enhance OT security by providing real-time anomaly detection, predictive threat analysis, and automated incident response, reducing downtime and preventing large-scale disruptions. With the ability to learn from patterns and adapt to new attack techniques, AI will play a crucial role in safeguarding critical infrastructure while allowing human experts to focus on strategic decisions and complex threats.

Role of human expertise in AI driven OT Security:

Human expertise plays a critical role in AI-driven OT security because while AI can detect anomalies, automate responses, and predict potential threats, it cannot fully understand the operational context or business impact of every incident. Security professionals provide the judgment needed to validate AI alerts, distinguish between false positives and real threats, and decide the best course of action in complex or high-stakes situations. They also design, train, and fine-tune AI models to align with industry-specific OT environments, ensuring accuracy and reliability. Moreover, humans bring creativity, ethical reasoning, and strategic thinking—qualities that AI cannot replicate—making them essential partners in building resilient and trustworthy OT security systems.

--The End--