Day 48

Exploitation Analyst

OT Security and AI:

The evolving threat landscape in OT environments:

What is OT?

OT stands for Operational Technology. It refers to the hardware and software systems used to monitor and control physical processes, devices, and infrastructure like industrial machinery, power plants, pipelines, transportation, and building systems.

In short:

- IT (Information Technology) = data, networks, software.
- OT (Operational Technology) = machines, sensors, control systems (SCADA, ICS, PLCs).

Are they targeted?

The threat landscape in OT environments is evolving rapidly because industrial control systems (ICS), SCADA, and PLCs are increasingly connected to IT and internet networks. Traditionally, OT systems were isolated, but convergence has exposed them to modern cyber threats. Attackers now target OT for espionage, sabotage, and disruption of critical infrastructure.

Key evolving threats:

- Ransomware in OT: shutting down manufacturing or energy operations (e.g., Colonial Pipeline).
- Supply chain attacks: exploiting software updates to compromise OT.
- Nation-state APTs: targeting power grids, nuclear plants, or transport.
- Insider threats: employees misusing access to manipulate systems.
- Legacy vulnerabilities: OT often runs outdated, unpatched systems.

Introduction to AI:

What is AI?

AI (Artificial Intelligence) is the simulation of human intelligence in machines. It enables systems to learn, reason, and make decisions like humans. AI uses algorithms and data to perform tasks such as problem-solving, pattern recognition, natural language understanding, and automation.

AI’s potential in cybersecurity is huge because it can process massive amounts of data and detect patterns faster than humans.

- Threat detection → AI analyzes logs/traffic to spot anomalies or zero-day attacks.
- Malware analysis → ML models classify files as malicious/benign quickly.
- Automated response → AI can block malicious IPs or quarantine files in real-time.
- Phishing detection → Identifies suspicious emails/URLs.
- Behavioral analysis → Learns normal user behavior to flag insider threats.