# Day 49

# Exploitation Analyst

## OT Security and AI:

## AI in Endpoint Protection:

AI in endpoint protection helps secure devices like laptops, servers, and IoT systems by going beyond traditional signature-based antivirus.

- Behavior-based detection → AI monitors processes and flags unusual activity.
- Zero-day defense → ML models spot malware even without known signatures.
- Automated response → Suspicious files are quarantined instantly.
- Threat hunting → AI correlates endpoint data with global threat intel.

**What is Dwell time?**

Dwell time is the amount of time a cyber attacker remains undetected inside a network or system after breaching it.

- Starts: when the attacker first gains access.
- Ends: when the attack is detected and removed.

## AI in SIEM:

AI in SIEM (Security Information and Event Management) enhances how logs and alerts are processed.

- Noise reduction → AI filters false positives from millions of alerts.
- Anomaly detection → ML models spot unusual patterns in log data.
- Predictive analysis → Identifies potential threats before they escalate.
- Automated correlation → Connects events across systems to reveal hidden attacks.
- Faster response → AI can trigger playbooks for containment.

## AI in Network Security:

AI in network security strengthens defenses by making monitoring smarter and adaptive:

- Intrusion Detection & Prevention → AI models analyze traffic patterns to catch anomalies and zero-day attacks.
- Automated Threat Hunting → ML spots stealthy lateral movement or beaconing C2 traffic.
- Adaptive Firewalls → AI can dynamically adjust firewall rules based on evolving threats.
- DDoS Mitigation → Identifies abnormal spikes in traffic and blocks them in real time.
- Behavioral Analysis → Learns normal user/device behavior to detect insider threats.

## **AI in IDS/IPS:**

AI in IDS/IPS (Intrusion Detection & Prevention Systems) makes them far more effective than traditional signature-based ones:

- Anomaly Detection → ML learns normal network behavior and flags deviations (e.g., unusual port scans, lateral movement).
- Zero-Day Attack Detection → AI can spot unknown exploits by analyzing traffic features instead of relying only on known signatures.
- Reduced False Positives → AI refines detection by correlating events, so analysts aren't flooded with false alerts.
- Automated Response → In IPS, AI can block malicious traffic in real time (e.g., shutting down suspicious sessions).
- Threat Intelligence Integration → AI models enrich IDS/IPS with global threat feeds and adapt rules dynamically.

--The End--