AI Cyber Crisis Commander Workshop

Description:

This workshop introduces the fundamentals of cyber crisis management and demonstrates how artificial intelligence can support decision-making during security incidents. Participants learn how cyber crises occur when digital systems behave unexpectedly and teams must respond quickly with incomplete information. The workshop emphasizes that many real-world cyber failures are not caused by tools, but by incorrect decisions made under pressure.

Through practical activities, participants explore how early warning signals, such as abnormal login attempts, unusual network connections, or unexpected system processes can indicate potential cyber incidents. The workshop focuses on building systems that monitor these signals and assist teams in identifying, understanding, and responding to cyber threats effectively.

Objectives:

By the end of the workshop, participants will design and build a working prototype called the Crisis Commander Autopilot (CCA), a simplified Security Operations Center (SOC) system that can:

1. Collect signals from a target server (logs, system activity, network data, and files).
2. Learn the baseline of normal system behavior using machine learning.
3. Detect abnormal behavior through anomaly detection techniques.
4. Identify the likely type of incident using predefined rules.
5. Recommend response actions using automated playbooks.
6. Execute safe containment actions with human approval (human-in-the-loop).
7. Display system activity and alerts in a live monitoring dashboard.
8. Generate a professional incident report summarizing the detected event and response actions.

Workshop Agenda:

Day 1 – Foundations and System Setup

- Explain the cyber crisis mental model and introduce the Crisis Commander Autopilot (CCA).
- Introduce virtual machines (VM), create/verify the network, and configure snapshots.
- Set up the target environment (SSH access, users, logs).
- Configure telemetry collector to gather signals and create a baseline dataset.
- Train the Isolation Forest model, validate thresholds, and verify dashboard status

Day 2 – Crisis Simulation and AI Response

- Explain cyber attacks as behavioral patterns (brute force, scanning, suspicious processes).
- Run attack simulation (brute force) and observe AI-based detection.
- Add classification rules and map incident response playbooks.
- Enable human-in-the-loop response actions (approve block, lock, quarantine).
- Conduct a tiered autonomy challenge with scoring and leaderboard.

Day 3 – Evaluation and Reporting

- Review logs, analyze false positives and false negatives, and adjust thresholds.
- Improve response rules and playbooks and add rollback mechanisms.
- Generate the incident report and collect evidence.
- Perform final crisis demonstration (attack → detect → contain → recover).
- Conduct post-incident review and discuss decision outcomes and lessons learned.