■ SOC COMMAND CENTER (CENTER)

SOC Analyst — Jordan Fields Security Operations Center (Law Enforcement Cyber Division) SIEM Dashboard — Wazuh | Filebeat | Winlogbeat | Syslog 24/7 Monitoring — Police | 911 | Traffic | Utilities

■ POLICE HEADQUARTERS (TOP LEFT)

Police Records & Patrol Database (Winlogbeat — Windows Event Logs) Alert Type: Brute Force / Unauthorized Access

■ 911 DISPATCH / CAD SYSTEM (BOTTOM LEFT)

Emergency Response Network (Filebeat — Linux Logs) Alert Type: Service Downtime / System Error

■ TRAFFIC CONTROL CENTER (TOP RIGHT)

City Traffic Lights & IoT Sensors (Syslog / IoT Device Feed) Alert Type: Network Scanning / IoT Intrusion

■ CRITICAL INFRASTRUCTURE (BOTTOM RIGHT)

Fire / EMS / Utilities Monitoring Server (Log Source: Suricata IDS) Alert Type: Malware Infection / Ransomware

■ EVIDENCE HANDLING AREA (RIGHT SIDE)

Digital Evidence — Case #001 Collected By: Jordan Fields | SOC Analyst Hash Verification: SHA256: _____ Timestamp: _____ Chain-of-Custody Maintained for Court Integrity

■ INCIDENT RESPONSE PLAYBOOKS (OPTIONAL PANEL)

- Phishing Attempt - Malware Infection - Brute Force Attack - IoT Scan / Device Compromise

■ LEGEND BOX (BOTTOM CENTER)

Blue — Normal Log Flow Green — Healthy System Yellow — Warning / Suspicious Activity Red — Active Incident / Critical Alert

■ EVIDENCE TAGS (CUT APART)

Case #001 — Brute Force Case #002 — Malware Case #003 — IoT Intrusion Case #004 — 911 Service Lag

■ PROJECT REPOSITORY / QR CODE LABEL

SCAN TO VIEW PROJECT DOCUMENTATION GitHub: sitdownwithme/DAE-PROJECTS Final Report + Playbooks + SIEM Dashboards

■ MINI LABELS (CUT FOR CABLES/YARN)

Filebeat → 911 CAD Logs Winlogbeat → Police HQ Logs Syslog → pfSense Firewall Suricata → Network IDS