Job Title:

Security Operations Center (SOC) Analyst – Law Enforcement Division

---

Role Summary:

The SOC Analyst supports the police department's cybersecurity unit by detecting, analyzing, and responding to cyber threats targeting law enforcement systems and city infrastructure. This role ensures digital evidence integrity, protects public safety networks, and supports investigations with secure data handling and chain-of-custody compliance.

Key Responsibilities (5 Tasks/Duties):

1. **Monitor and analyze** live security event logs from police systems, public portals, and municipal infrastructure.

2. **Investigate alerts** for suspicious activity (phishing, brute-force attacks, malware infections, network intrusions).

3. **Execute incident response playbooks** and escalate confirmed incidents to digital forensics or investigative units.

4. **Document and preserve digital evidence** following chain-of-custody protocols for potential court use.

5. **Develop and maintain SIEM dashboards** for visibility into system health, user activity, and threat detection trends.

Required Skills / Tools (5 Core Skills):

1. **SIEM Platforms:** ELK Stack or Splunk for log analysis and visualization.

2. **Security Tools:** Nmap, Suricata, Hydra, Filebeat/Winlogbeat/Syslog for log forwarding and intrusion detection.

3. **Programming/Scripting:** Python and Bash for automation and custom log parsing.

4. **Incident Response:** Familiarity with NIST 800-61, playbook creation, and escalation workflows.

5. **Forensics & Evidence Handling:** Hash verification, case documentation, and digital chain of custody.

Sample Deliverables (5 Examples):

1. **SIEM Dashboards** tracking login anomalies, port scans, and suspicious network behavior.

2. **Incident Response Playbooks** detailing procedures for phishing, malware, and ransomware events.

3. **Chain-of-Custody Reports** documenting how digital evidence was collected, stored, and verified.

4. **Weekly Threat Analysis Reports** summarizing security posture across police and city networks.

5. **Critical Infrastructure Alerts** identifying and escalating risks to public safety systems (e.g., 911 CAD, traffic lights, patrol databases).

Work Environment / Department Type (2–3 Descriptions):

- Operates within the **Police Department's IT or Cybercrime Division**, collaborating with sworn officers, digital forensics teams, and public safety network engineers.

- Works in a **secure SOC environment**, with access-controlled facilities and 24/7 log monitoring.

- May coordinate with **city or state cybersecurity agencies** during major incidents or joint operations.

Work Rigor and Growth Style (2–3 Descriptions):

- **High accountability:** Every action and alert review impacts public safety and legal integrity.

- **Growth-focused:** Continuous training in forensics, network defense, and legal compliance for promotion to Senior SOC Analyst or Digital Forensic Examiner.

- **Collaborative and mission-driven:** Analysts contribute directly to protecting law enforcement operations, digital evidence, and community trust.