Security Analyst / SOC Analyst

Security | SMB | Enterprise

[Company Name] is seeking a Security Analyst to join our security operations team and serve as a front-line defender against cyber threats. You will monitor security alerts, investigate suspicious activity, lead incident response efforts, and continuously improve our detection capabilities. This role is essential to protecting our systems, data, and customers, and offers a fast-paced environment where you will develop deep expertise in threat detection and response.

Key Responsibilities

- Monitor security alerts from SIEM, EDR, and other detection tools, and triage them by severity and impact
- Investigate security incidents end-to-end including scoping, containment, eradication, and recovery
- Develop and tune detection rules, alerts, and dashboards to improve signal-to-noise ratio
- Perform log analysis and forensic investigation across network, endpoint, and cloud environments
- Document incidents, findings, and post-mortem analyses to improve future response
- Collaborate with IT, engineering, and compliance teams during incident response and security projects
- Contribute to threat intelligence gathering and proactive threat hunting activities

Required Skills & Experience

- 2+ years of experience in a security operations, SOC analyst, or incident response role
- Hands-on experience with SIEM platforms (Splunk, Microsoft Sentinel, Elastic Security, or Chronicle)
- Familiarity with EDR tools (CrowdStrike, SentinelOne, Carbon Black, or Microsoft Defender for Endpoint)
- Understanding of common attack techniques and the MITRE ATT&CK framework
- Experience with network traffic analysis and log analysis (firewall, proxy, DNS logs)
- Knowledge of operating system internals (Windows and Linux) for forensic investigation
- Strong analytical and communication skills for incident documentation and stakeholder reporting

Nice-to-Have

- Experience with SOAR platforms (Palo Alto XSOAR, Swimlane, or Tines) for automation
- Security certifications such as Security+, CySA+, GCIH, or GCFA
- Experience with cloud security monitoring (AWS CloudTrail, GCP Audit Logs, Azure Monitor)
- Scripting skills in Python, PowerShell, or Bash for automating investigation workflows
- Familiarity with digital forensics and malware analysis

Tech Stack

Splunk | CrowdStrike | Microsoft Sentinel | Elastic Security | MITRE ATT&CK | Wireshark | SOAR | Python | Jira | PagerDuty

What We Offer

- Competitive salary and equity package
- Flexible remote or hybrid work arrangement
- Health, dental, and vision insurance
- Annual learning and development budget
- Generous PTO policy

Interview Process

1. Recruiter phone screen (30 min)
2. Technical phone screen covering security fundamentals and incident response methodology (45 min)
3. Practical exercise: investigate a simulated security incident using logs and artifacts (60 min)
4. Team interview covering collaboration, communication, and on-call readiness (45 min)
5. Final conversation with the security team manager