Position Description

Position:	Security Analyst	**Date Created:**	August 13, 2026
Reports to:	SVP of Cybersecurity	**Date Revised:**	August 13, 2026

Overview

The Security Analyst supports 7 Layer Solutions' cybersecurity practice by monitoring, analyzing, and responding to security events, assisting with cyber posture and compliance activities, and contributing to client-facing security services. This role works under the direction of the SVP of Cybersecurity and collaborates with SOC, vCISO, and advisory resources to help protect client environments and deliver high-quality security outcomes.

Key Responsibilities

Security Monitoring & Incident Support

- Monitor and triage security alerts from SIEM, XDR/EDR, email security, identity, and related platforms in accordance with documented processes and SLAs
- Perform initial investigation and analysis of security events; escalate confirmed or complex incidents with clear findings and context
- Support incident response activities including evidence collection, timeline construction, and client communication under senior guidance
- Assist with threat hunting tasks, detection tuning recommendations, and playbook improvements
- Document all analysis and actions thoroughly in the ticketing / case management system

Cyber Posture, Compliance & Advisory Support

- Assist with cyber posture assessments, control gap reviews, and evidence collection for client engagements
- Support compliance-related activities (SOC 2, HIPAA, NIST CSF, CIS Controls, etc.) including documentation and control testing assistance
- Help prepare client-facing reports, summaries, and remediation tracking under the direction of senior consultants
- Contribute to policy, procedure, and standards development or updates as assigned

Continuous Improvement & Collaboration

- Stay current on common threats, attack techniques, and relevant security technologies
- Participate in knowledge sharing, runbook updates, and process improvement initiatives within the cybersecurity team
- Collaborate effectively with Managed Services, Advisory, and other internal teams on security-related escalations and client needs
- Other duties as assigned by the SVP of Cybersecurity or senior security leadership

Qualifications

To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed are representative of the knowledge, skill, and ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Education & Experience

- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or related field preferred (or equivalent practical experience)
- 2–5 years of experience in a security operations, security analyst, or related cybersecurity role (MSP, MSSP, or enterprise SOC experience a plus)
- Hands-on exposure to security monitoring tools (SIEM, EDR/XDR) and basic incident response processes
- Familiarity with common security frameworks (NIST CSF, CIS Controls, or similar) preferred

Technical Skills

- Working knowledge of Windows, networking fundamentals (TCP/IP, DNS, HTTP/S), and common attack patterns
- Experience reviewing security alerts, logs, and endpoint telemetry
- Familiarity with Microsoft security technologies (Defender, Sentinel, Entra ID security features) and/or other major XDR/SIEM platforms preferred
- Ability to follow structured investigation processes and produce clear written documentation
- Basic scripting (PowerShell or Python) for analysis or automation is a plus

Preferred Certifications

- CompTIA Security+, CySA+, or equivalent foundational security certification
- Microsoft SC-200 or similar vendor security certification (advantageous)
- Progress toward CISSP, CISM, or other advanced credentials viewed favorably

Soft Skills

- Strong analytical and problem-solving skills with attention to detail
- Clear written and verbal communication; ability to escalate with concise, actionable context
- Ability to work effectively both independently and as part of a team
- Professional client-facing demeanor and discretion with sensitive information
- Genuine interest in cybersecurity and continuous learning

Physical Demands

While performing the duties of this job, the employee is regularly required to talk, hear, and see. The employee is required to sit for long periods of time and will spend a significant portion of time on a computer. The employee will occasionally lift, push, or move up to 10 pounds.

Work Environment

The noise level in the work environment is usually moderate. Role may be hybrid or remote with flexibility as determined by the SVP of Cybersecurity; participation in on-call or shift coverage may be required depending on SOC support needs.

Reasoning Ability

Ability to apply structured analytical thinking to security events and investigations. Ability to distinguish normal from anomalous activity, prioritize effectively, and escalate appropriately when risk or complexity exceeds current scope.

Please note this job description is not designed to cover or contain a comprehensive listing of activities, duties, or responsibilities that are required of the employee for this job. Duties, responsibilities, and activities may change at any time with or without notice.

I acknowledge that I have read and understand the above job description in its entirety and am capable of performing all of the stated requirements.

Employee Signature: _____ Date: _____