IRFAN ALKAN

SOC Team Lead | Senior SOC Analyst | Incident Response | Security Operations

Istanbul, Türkiye | Open to Remote | irfanalkan@gmail.com | LinkedIn | GitHub

PROFESSIONAL SUMMARY

SOC Team Lead and Senior SOC Analyst with 4+ years of progressive security operations experience, advancing from SOC Analyst Intern to L1, L2, and Team Lead. **Hands-on with IBM QRadar, Splunk, and CrowdStrike Falcon across incident investigation, SIEM/EDR analysis, detection tuning, escalation support, and analyst mentoring.** Personally investigated approximately 300 SOC alerts/tickets and trained or mentored approximately 200 cybersecurity students and analysts across 20 cohorts.

CORE SKILLS

Security Operations: Incident Response | Alert Triage | Investigation Review | Escalation | Threat Investigation | Web Attack Analysis
SIEM / EDR: IBM QRadar | Splunk | CrowdStrike Falcon | AQL | SPL | Correlation Rules | Detection Tuning | IOC & Process-Tree Analysis
Network & Systems: Wireshark | TCP/IP | Sysmon | Active Directory | Windows/Linux | pfSense | Kali Linux | Jira

PROFESSIONAL EXPERIENCE

CYDEO - Remote **Mar 2022-Present**
SOC Team Lead & Cybersecurity Instructor | Jul 2025-Present
SOC Analyst L2 & Team Lead | Jul 2024-Jun 2025
SOC Analyst L1 & Cybersecurity Mentor | Jul 2022-Jun 2024
SOC Analyst Intern | Mar 2022-Jun 2022

- Progressed from SOC Analyst Intern to L1, L2, and Team Lead while remaining hands-on in monitoring, triage, incident investigation, escalation, containment support, and technical review of security cases.
- Investigated approximately 300 SOC alerts/tickets across web attacks, endpoint threats, malware, phishing, suspicious PowerShell, authentication attacks, ransomware, network scanning, and privilege escalation.
- Investigated approximately 200 IBM QRadar offenses using AQL and log analysis; worked with correlation rules, rule tuning, false-positive analysis, dashboards, and log-source troubleshooting.
- Conducted Splunk investigations using SPL, detection queries, alert analysis, field extraction, dashboards, and structured investigation workflows.
- Investigated approximately 70 CrowdStrike Falcon detections and approximately 80 process trees through IOC and process analysis, including limited endpoint containment and remediation support.
- Analyzed approximately 20 PCAPs with Wireshark and investigated web attacks including SQL injection, XSS, command injection, and remote code execution.
- Designed and implemented a standardized Jira SOC investigation template; trained or mentored approximately 200 cybersecurity students/analysts across 20 cohorts and reviewed investigation quality and technical reporting.

TECHNICAL PROJECTS

SOC Home Lab - Built and maintain a virtual SOC integrating pfSense, Windows Server/Active Directory, Sysmon, Splunk, and Kali Linux for attack simulation, telemetry ingestion, custom detections, validation, and investigation practice.
Security+ Test Engine - Built a Flutter/Firebase multi-platform practice application with a 1,107-question Security+ bank. secplus-test-engine.web.app

CERTIFICATIONS

RangeForce Security Engineer 1 Elite - Feb 2026-Feb 2030 | **CompTIA CySA+** - In Progress
CompTIA Security+ - Historical certification, earned 2022; expired Jun 2025

EDUCATION

M.A., International Relations - University of Oklahoma | **B.S., Electronics Engineering** - Turkish Air Force Academy