

Saafir Hale

Cybersecurity Analyst

SECURITY OPERATIONS · INCIDENT RESPONSE · THREAT DETECTION

Atlanta, GA (408) 337-7841 saafirhale@gmail.com saafirhale.com
linkedin.com/in/saafir-hale github.com/SaafirHale

SUMMARY

Security operations analyst with hands-on incident response across 300+ client organizations. Resolves high-impact incidents — business email compromise, account takeovers, malware, and phishing — in 1–3 minutes using SentinelOne, Wazuh, OpenCTI, and Microsoft Entra. Subject matter expert for security tooling across 50+ VIP clients, with strong Python and PowerShell scripting for detection, reporting, and automation. CompTIA A+ certified; Network+ in progress; B.S. in Cybersecurity underway.

TECHNICAL SKILLS

Security operations

Incident Response · Threat Detection & Triage · SIEM / EDR / XDR · SentinelOne · Wazuh · OpenCTI · Microsoft Defender · Mimecast

Identity & cloud security

Microsoft Entra / Azure AD · Microsoft 365 Security · Conditional Access · Intune · SSO

Threats handled

Business Email Compromise · Account Takeover · Malware · Phishing / Vishing · Browser Hijacking

Automation & scripting

PowerShell · Python · SQL · Security reporting · Compliance automation

Networking & infrastructure

802.1X / RADIUS / EAP-TLS · NAC · Cisco Meraki · Firewalls · VPNs · DNS

Tools & platforms

ServiceNow · NinjaOne · CloudRadial · Hudu · BackupRadar · Cisco OpenDNS

EXPERIENCE

Junior SecOps Analyst & Infrastructure Engineer

Nov 2024 – Present

Symphona · Smyrna, GA

Resolve 200+ security incidents — business email compromise, account takeovers, malware, phishing/vishing, and browser hijacking — across 300+ client organizations, averaging 1–3 minutes to full mitigation using SentinelOne, Wazuh, OpenCTI, Microsoft Entra, PowerShell, and Python.

Serve as CloudRadial Subject Matter Expert for 50+ VIP clients, maintaining SentinelOne, backup, and compliance reporting across each portal.

Built Python and PowerShell automation for an ITGlue-to-Hudu migration of 300+ client organizations and tens of thousands of assets — 95% first-pass success, with a reconciliation script recovering the remainder.

Led a 30-site 802.1X / EAP-TLS deployment with RADIUS/NPS on Microsoft Azure, enabling certificate-based network access control.

Recognized Subject Matter Expert for Hudu and NinjaOne; support 300+ client organizations.

IT Support Analyst — Intern

Aug 2024 – Nov 2024

Symphona · Smyrna, GA

Automated SentinelOne, BackupRadar, BrightGauge patch-compliance, and Cisco OpenDNS reporting for all VIP clients, cutting manual reporting effort by roughly 17.5%.

Performed daily backup-server verification for 50+ VIP clients to ensure recoverability.

Integrated Google Workspace SSO and authored 750+ knowledge-base articles spanning Microsoft, Google, and iManage platforms.

PROJECT HIGHLIGHT

Email Forensics Indexer (PowerShell)

Built a tool to index and parse .eml archives — MIME body extraction, keyword search, and progress tracking — for rapid investigation of phishing and BEC artifacts, with Excel-compatible output for reporting.

EDUCATION

B.S. Cybersecurity & Information Assurance

Anticipated Early 2027

Western Governors University

CERTIFICATIONS

CompTIA A+ · CompTIA

CompTIA Network+ (in progress) · CompTIA

Google Data Analytics Professional Certificate ↗ · Coursera

Sports Performance Analytics ↗ · University of Michigan

ServiceNow System Administrator ↗ · Udemy

ServiceNow Developer Course ↗ · Udemy

Kaggle

Python · Pandas · Intro to SQL · Advanced SQL · Data Cleaning · Data Visualization · Intro to Machine Learning · Intermediate Machine Learning