KYLE STANLEY

Cloud Security Analyst | Microsoft Sentinel | Azure Security | Detection Engineering

Bowie, MD | 301-520-0214 | kayjay18m@gmail.com

linkedin.com/in/ky-stanley | kyhomelab.github.io | github.com/kyhomelab

SUMMARY

Cloud Security Analyst specializing in Microsoft Sentinel, Azure security, and KQL detection engineering. Operate enterprise SIEM and Defender XDR monitoring for 3,000+ users, building custom KQL analytic rules mapped to MITRE ATT&CK, leading Azure security posture assessments aligned to NIST 800-53, and driving measurable vulnerability reduction. Built an Azure cloud-to-ground honeypot and a 15-tool containerized SOC lab. AZ-104 and Security+ certified; SC-200 in progress. Seeking Cloud Security Analyst or SOC Analyst II role in DC/MD/VA or remote.

TECHNICAL SKILLS

Cloud Security: Microsoft Sentinel, Microsoft Defender XDR, Defender for Cloud, Defender for Endpoint, Azure Security Center, Azure Log Analytics, Microsoft GCC High

Detection & SIEM: KQL (Kusto Query Language), Custom Analytics Rules, Threat Hunting, Detection Engineering, SIEM (Security Information and Event Management), Splunk, CrowdStrike Falcon EDR (Endpoint Detection and Response), Wazuh, Suricata IDS/IPS, Incident Response

Identity & Access: Microsoft Entra ID (Azure AD), Conditional Access, PIM, MFA, Active Directory, Okta, Privileged Access Reviews, Hybrid Identity (Azure AD Connect)

Endpoint & Email: Microsoft Intune, Windows Autopilot, SCCM, Device Compliance, PhishER, Avanan, Defender for Office 365

Automation & IaC: PowerShell, Python, Bicep, Docker, Proxmox, Shuffle SOAR, TheHive, Cortex, MISP

Frameworks: MITRE ATT&CK, NIST 800-53, NIST CSF, Zero Trust Architecture, Cyber Kill Chain

CERTIFICATIONS

- Microsoft Security Operations Analyst (**SC-200**) — In Progress
- Microsoft Azure Administrator Associate (**AZ-104**) — 2023
- **CompTIA Security+** — 2021
- **CompTIA A+** — 2021

PROFESSIONAL EXPERIENCE

Cloud Security / SOC Analyst — June 2025 – Present

Denpro Technology Solutions (Client: Archkey Solutions) | Bryans Rd, MD

- Architected and operationalized enterprise-wide Microsoft Sentinel and Defender XDR monitoring protecting 3,000+ users across 6 offices, multiple field sites, and hybrid cloud environments, with controls aligned to NIST 800-53
- Engineered 25+ custom KQL analytic rules and hunting queries in Azure Log Analytics detecting IOCs, lateral movement, privilege escalation, and cloud misconfigurations, each mapped to MITRE ATT&CK tactics and techniques
- Led enterprise Azure security posture assessment spanning tenant configuration, Entra ID, RBAC, and Conditional Access, delivering an executive remediation roadmap and POA&M prioritized against NIST 800-53
- Spearheaded vulnerability reduction program using Microsoft Defender Vulnerability Management, driving a 40%+ reduction in endpoints carrying 2+ critical CVEs through cross-team remediation coordination
- Uncovered and remediated high-risk identity exposures — shared credentials, rogue service accounts, and over-permissioned Entra ID roles — enforcing least-privilege and Zero Trust access patterns across the tenant
- Administer Entra ID identity lifecycle, Conditional Access, MFA enforcement, and PIM privileged access reviews; automate recurring Entra ID hygiene reporting and audit evidence collection using PowerShell and Microsoft Graph
- Engineered Sentinel Logic App playbooks orchestrating automatic user disablement, session revocation, and alert enrichment on high-severity identity events, accelerating containment MTTR
- Triage 15+ phishing submissions weekly via PhishER and Avanan, executing user isolation, mailbox purge, and endpoint investigation on confirmed compromises to contain threats rapidly
- Deliver client-facing incident response: contain compromised identities, conduct investigative user interviews, and coordinate onsite remediation for infected endpoints to restore operations

- Tuned Sentinel analytic rules and suppression logic to cut false-positive alert volume; expanded logging pipeline by onboarding new data connectors (Entra ID sign-ins, Defender for Cloud, Microsoft 365 audit, Defender for Endpoint) to close visibility gaps
- Hardened endpoint fleet through Intune compliance baselines, Conditional Access device-compliance gating, and Attack Surface Reduction (ASR) rules aligned to Microsoft secure-by-default guardrails
- Conducted threat hunts against Entra ID sign-in and Defender telemetry using MITRE ATT&CK-aligned hypotheses, converting validated findings into production analytic rules and recurring hunting queries

IT Specialist (Security Focus) **June 2024 – June 2025**

Smartlink Group LLC | Annapolis, MD

- Monitored CrowdStrike Falcon EDR logs, investigated security alerts, and led phishing incident response as primary IT contact for main office staff and C-suite executives
- Managed cloud identity security through Microsoft 365, implementing security policies and access controls
- Spearheaded Windows 10 to Windows 11 migration using Windows Autopilot for zero-touch deployment; conducted compatibility testing and established QA validation process
- Led cross-functional initiative redesigning HR-IT onboarding workflow, streamlining new hire account provisioning and improving first-day productivity
- Proposed, obtained approval for, and implemented Scribe documentation platform — achieved company-wide adoption for IT procedures and training
- Co-authored incident response playbooks and conducted new hire IT orientation ensuring security policy acknowledgment from day one

Senior IT Support Analyst **August 2023 – June 2024**

TEKsystems (Contracted to Venable LLP) | Washington, DC / Baltimore, MD (Hybrid)

- Delivered enterprise technical support to 800+ legal professionals across 15 nationwide office locations at major law firm with emphasis on security operations and identity management
- Implemented organization-wide multi-factor authentication deployment using Okta, strengthening identity security posture
- Monitored and analyzed security logs using Splunk SIEM for threat detection, security event analysis, and incident investigation
- Administered user accounts and permissions in Active Directory following principle of least privilege; managed enterprise software deployments via SCCM
- Maintained 90% SLA compliance on service request resolution, consistently meeting performance benchmarks

PORTFOLIO PROJECTS

Cloud-to-Ground Honeypot — Hybrid Azure Threat Intelligence Platform

Azure, Microsoft Sentinel, Bicep IaC, KQL, Shuffle SOAR, TheHive, MISP

- Designed hybrid cloud architecture connecting Azure-deployed honeypots with on-premises SOC; deployed via Bicep Infrastructure as Code templates for repeatable builds
- Built custom KQL detections for Microsoft Sentinel identifying RDP brute-force attack patterns; created Sentinel workbooks with global attack geolocation mapping
- Engineered SOAR automation: cloud alerts trigger local case creation, IOC extraction, and automated threat feed publication via GitHub API

Unified SOC Lab — Enterprise Security Operations Environment

Docker, Wazuh, Suricata, Velociraptor, TheHive, Cortex, Shuffle, MISP, Caldera, Arkime

- Architected containerized Security Operations Center with 15+ integrated tools enabling end-to-end security operations from detection through incident response; deployed Wazuh SIEM with Suricata IDS/IPS for network threat visibility
- Built SOAR workflows connecting detection platforms to TheHive case management and MISP threat intelligence; integrated Velociraptor endpoint forensics and Arkime full packet capture for deep-dive investigations
- Executed adversary simulations using MITRE Caldera with custom detections mapped to ATT&CK framework techniques

KQL Security Query Library — Open-source repository of security-focused KQL queries for threat detection, identity security monitoring, and compliance auditing in Microsoft environments. github.com/kyhomelab/kql-queries