David Sarkisyan

Brooklyn, NY 11214 | 917-755-2207 | Davidwsarkisyan@gmail.com | linkedin.com/in/srkyn | github.com/srkyn

CYBERSECURITY ANALYST

PROFESSIONAL SUMMARY

Cybersecurity Analyst with 3+ years of healthcare IT experience across Microsoft 365, Active Directory, Microsoft Entra ID, MFA, endpoints, access workflows, ticket documentation, and security communications. Focused on SOC workflows, Splunk investigation, IAM, endpoint security, vulnerability management, network defense, security monitoring, and clear security documentation. Hands-on portfolio includes Splunk detection content, Packet Tracer network-defense labs, an OPNsense/Proxmox security control plane, Active Directory cleanup, Entra ID stale-device review, browser extension permission review, scheduled-task review, and an authorized AI chatbot security assessment.

CORE SKILLS

Security Operations: alert triage, log review, incident notes, escalation, playbooks, threat monitoring concepts, remediation tracking

SIEM and Detection: Splunk SPL, Windows Security logs, Sysmon concepts, MITRE ATT&CK; mapping, false-positive review, investigation steps

Identity and Access: Microsoft Entra ID, Microsoft 365, MFA, Active Directory, onboarding/offboarding, group access, access review, privileged access concepts

Network Security: OPNsense, firewall rule intent, DNSSEC, DNS-over-TLS, DNS bypass prevention, CrowdSec, Proxmox/LXC visibility services

Monitoring and Assessment: VictoriaLogs, NetAlertX, OpenCanary, Uptime Kuma, Nuclei, Trivy, safe on-demand scanning, evidence review

Compliance and Documentation: HIPAA awareness, policy/procedure support, audit evidence notes, ServiceNow, Jira, stakeholder summaries

Languages: English; Russian, fluent speaking, reading, and writing

SELECTED SECURITY WORK

- Wrote Splunk SPL detections for Windows, Active Directory, Sysmon, and PowerShell activity with data assumptions, likely noise, ATT&CK; mapping, and analyst next steps.
- Completed Per Scholas Packet Tracer and security labs covering NAT, MAC/IP addressing, routed traffic flow, LAN setup, Telnet/SSH, FTP/web traffic, wireless hardening, ACLs, TACACS/RADIUS, DNS traffic, Linux authentication, server-log review, malware research, Windows registry/process review, PowerShell, file integrity, and encryption concepts.
- Created a stale-device review workflow for identity hygiene, checking old-looking device signals against ownership and usage context before recommending cleanup action.
- Documented Active Directory cleanup review notes for stale users/computers, group membership concerns, and review-before-action reporting.
- Built and documented an OPNsense/Proxmox security control plane covering firewall policy, DNSSEC, DNS-over-TLS, DNS bypass prevention, CrowdSec blocking, centralized logs, unknown-device awareness, canary alerts, and safe on-demand scanning.
- Performed an authorized AI/LMS security assessment from a standard-user session, producing a private 24-page report with 16 validated findings and sanitized public notes covering tool access, instruction hierarchy, LMS context exposure, retrieval boundaries, evidence handling, business impact, and remediation guidance.
- Developed defensive review tools for scheduled tasks and browser extension permissions to support endpoint risk review.

PROFESSIONAL EXPERIENCE

System Administrator

ALLCare Fertility, New York, NY | September 2022 - December 2025

- Resolved 10-25+ daily incidents and service requests across Windows, macOS, Microsoft 365, VPN, DNS, Wi-Fi, endpoints, printers, mapped drives, and login workflows.
- Supported identity and access operations for 100+ users through Active Directory and Microsoft Entra ID, including MFA support, password resets, group access, onboarding, offboarding, and account updates.
- Helped implement account lockout policy updates to strengthen identity security and reduce risk from repeated failed login attempts.
- Co-presented phishing awareness training with the cybersecurity team and helped employees identify suspicious emails, report threats, and follow safer account practices.
- Supported endpoint reliability by preparing devices, validating configurations, troubleshooting recurring issues, supporting compliance checks, and reimaging systems when needed.
- Improved documentation quality with clear troubleshooting steps, resolution notes, SLA updates, escalation details, ownership, and handoff-ready summaries in ServiceNow and Jira.
- Used PowerShell, PSADT, and batch scripting to reduce repetitive support work and standardize operational tasks.

Embryologist

Generation Next Fertility, New York, NY | April 2020 - September 2022

- Performed precise, time-sensitive laboratory work in high-stakes clinical workflows requiring documentation accuracy, quality control, escalation discipline, and calm decision-making.
- Handled sensitive patient records and biological sample data in compliance with HIPAA, preserving documentation accuracy, data integrity, and chain-of-custody practices.

PROFESSIONAL DEVELOPMENT

Cybersecurity Analyst Training and Portfolio Development

Per Scholas and Independent Security Projects, Brooklyn, NY | January 2026 - Present

- Enrolled in Per Scholas' intensive 15-week, 450+ hour Cybersecurity Analyst training program, scheduled for completion in July 2026, with hands-on work across security operations, network defense, endpoint protection, vulnerability management, incident response, Splunk, and technical documentation.
- Built practical SOC, IAM, and network-security judgment through Packet Tracer labs, Wireshark traffic analysis, Linux authentication and CLI work, Windows PowerShell practice, server-log review, wireless/security hardening labs, access-control exercises, Splunk searches/dashboards/alerts, vulnerability scanning, centralized logging, and incident documentation.

EDUCATION

Western Governors University | B.S., Cybersecurity and Information Assurance, in progress | August 2025 - December 2027

Per Scholas | Cybersecurity Analyst Training | April 2026 - July 2026

CERTIFICATIONS

CompTIA CySA+

Splunk Core Certified User

CompTIA A+ ce

Google Cybersecurity Professional Certificate

Fortinet Certified Fundamentals Cybersecurity

Cisco Endpoint Security