Aaron Kulczyk

(717) 882-6741 | aaron@kulczyk.tech | www.kulczyk.tech | www.rvits.net
Active TS/SCI Eligible Clearance | CompTIA Security+

SUMMARY

IT Specialist (GS-11) and Air Force Cyber Systems Operations professional with hands-on experience defending, monitoring, and administering DoD enterprise networks. Works daily with Tenable SecurityCenter, Trellix Endpoint Security, Forcepoint NGFW, Kiwi Syslog Server, and SolarWinds to find vulnerabilities, review host, firewall, and network logs for anomalous activity, and carry fixes through to remediation. Experienced with RHEL clustering on CEPH storage, VMware virtualization, network-based Windows deployment, and kiosk hardening, and builds PowerShell and Node.js tools that automate administration. Security+ certified under DoDM 8140.03 with an active TS/SCI elligible clearance.

SKILLS

- **Cyber Defense:** Tenable SecurityCenter, Trellix ePO (Threat Prevention, Firewall, DLP), Forcepoint NGFW, IDS/IPS, HIPS/HIDS, DISA STIG compliance, BitLocker, firewall ACL policy
- **Log and Network Monitoring:** Kiwi Syslog Server log aggregation, SolarWinds, WhatsUp Gold, Wireshark
- **Systems:** Windows Server, Windows 10/11, RHEL/Linux, Active Directory, Group Policy, DNS, DHCP, WSUS, SCCM, Office 365
- **Infrastructure:** VMware vSphere (vMotion, HA), RHEL clustering, CEPH, Hyper-V, Dell/Cisco routing and switching, TCP/IP, VLANs, VPN, backup and disaster recovery
- **Deployment:** WDS, PXE, UEFI HTTP boot, Windows image customization, kiosk configuration and hardening
- **Scripting and Development:** PowerShell (including Windows Forms), Bash, Node.js, JavaScript, SQL, web design

EXPERIENCE

IT Specialist, GS-11 **Feb 2025 – Present**
Department of the Air Force, Annville, PA

- **Vulnerability Management:** Scan enterprise systems with Tenable SecurityCenter, prioritize findings, and track remediation through to closure.
- **Endpoint and Perimeter Defense:** Maintain the Trellix Endpoint Security suite (ePolicy Orchestrator, Threat Prevention, Firewall, DLP) and Forcepoint NGFW; review endpoint, firewall, and DLP events for threats and policy violations and support containment.
- **Log Analysis:** Aggregate syslog data from network devices, firewalls, and servers in Kiwi Syslog Server and review it alongside SolarWinds and WhatsUp Gold monitoring to spot anomalous activity and isolate root causes.
- **Incident Triage:** Determine the scope, urgency, and impact of system and network issues across Windows, RHEL, DNS, DHCP, and Dell/Cisco environments; recommend and carry out remediation and document findings for leadership.
- **Clustering and Virtualization:** Build and maintain RHEL clusters backed by CEPH distributed storage alongside VMware vSphere clusters.
- **Network Imaging:** Run PXE deployments with WDS and UEFI HTTP boot to image systems with customized Windows 11 builds, including in offline environments.
- **Kiosk Development:** Create and harden kiosk systems, including a PowerShell Windows Forms kiosk application with admin tools restricted by Active Directory authentication and security-group membership.
- **Systems Administration:** Administer Active Directory and Group Policy; apply security baselines and WSUS patching to reduce the attack surface; perform backups and maintain disaster recovery plans.

Cyber Systems Operations **Jul 2022 – Present**
United States Air Force, Annville, PA

- Apply DISA STIG configurations to mitigate vulnerabilities and implement BitLocker encryption to protect data at rest.
- Configure firewall ACLs to allow only required inter-VM traffic on the domain network while monitoring IP traffic.

- Implement and monitor firewalls, antivirus, intrusion detection systems, and host-based intrusion prevention (HIPS/HIDS).
- Use PowerShell and the Linux terminal across virtualized environments to configure network settings and enforce security settings.
- Manage servers for high availability, configure routers, switches, and access points, reimage and domain-join systems, and resolve end-user issues.

Information Technology Manager **May 2016 – Jul 2022**

Lake Tobias Wildlife Park, Halifax, PA

- Planned and built network infrastructure, including Cat5e, Cat6, and fiber runs, and expanded the network with proper subnetting.
- Configured and deployed new systems and applications; performed network maintenance and upgrades with minimal downtime.
- Supported end users with hardware, software, and email issues and coordinated team efforts to resolve problems.
- Project managed IOT infrastructure with point of sale (POS), IP cameras, Access Point management, LOS point-to-points, and wireless mesh systems.

PROJECTS

- **Knowledge Base:** Building a self-hosted documentation platform (Node.js) for system administrators, with Active Directory sign-in and role-based access mapped from AD groups.
- **Self-Hosted Applications:** Develop and host several Node.js web applications on personal infrastructure, including a dashboard and inventory-tracking tools that use NFC tags.
- **River Valley IT Solutions LLC:** Owner of an IT services business providing website design, business email setup and hosting, Starlink rentals, and ongoing hosting and maintenance.

CERTIFICATIONS AND TRAINING

- CompTIA Security+ (DoDM 8140.03 compliant)
- Theater Deployable Communications Operations, 152 hours: rebuilt, reconfigured, and deployed a vSphere platform (vMotion, HA) with firewall, proxy, SolarWinds, redundant domain controllers, HIPS, and backup servers, focused on security and vulnerability management
- Cyberspace Fundamentals, 160 hours
- System Operations Apprentice, 400 hours

EDUCATION

- Harrisburg Area Community College: 3 years of Computer Science coursework, including Computer Science I–III, Network Communication Technology I, and Web Exploration and Design
- Air Force standardized cyber and IT fundamentals training