SAMSON SCHMIDT

CYBERSECURITY | SECURITY OPERATIONS | IAM | ENDPOINT SECURITY

651-707-7679 | samsonschmidt1@gmail.com | linkedin.com/in/samson-schmidt | samsonschmidt.com

PROFESSIONAL SUMMARY

Cybersecurity and IT professional with 3+ years of experience and hands-on enterprise security responsibilities across security operations, IAM, endpoint security, vulnerability management, and compliance. Support access reviews, incident investigation and response, security control validation, and NIST/CMMC/SOX requirements. CompTIA Security+ and CySA+ certified, with experience using Active Directory, Okta, CrowdStrike Falcon, Microsoft 365, SIEM, EDR, and vulnerability management workflows.

CERTIFICATIONS

CompTIA Security+ | CompTIA CySA+ | Cisco CCNA (In Progress)

TECHNICAL SKILLS

Security Operations: SOC monitoring, Wazuh SIEM, Elastic Security, CrowdStrike Falcon, EDR, alert triage, log analysis, incident response support, threat intelligence, Tenable Nessus, vulnerability management, FIM, MITRE ATT&CK

Identity & Access: Active Directory, Okta, Microsoft 365, IAM, MFA/SSO, YubiKey, RBAC, least privilege, privileged/generic accounts, access reviews, Group Policy

Endpoint & Infrastructure: Tanium, Zscaler, Varonis, BitLocker, vSEC:CMS, Windows, Linux, macOS, network segmentation, VLANs, DNS, DHCP

Governance & Compliance: NIST, CMMC, SOX, security control validation, access audits, audit evidence, compliance remediation

PROFESSIONAL EXPERIENCE

Ducommun Inc. | **IT Technician**

St. Croix Falls, WI | Nov 2025 - Present

- Support enterprise identity, endpoint security, infrastructure, and day-to-day security operations for 70+ users and hundreds of endpoints as the primary site IT contact.
- Administer identity lifecycle and access controls across Active Directory, Okta, and Microsoft 365, including provisioning, privileged/generic accounts, MFA/YubiKey authentication, and least-privilege access.
- Conduct monthly SOX access audits across 80+ user, service, and generic accounts; reconcile HR access records against Active Directory, maintain audit evidence, remediate discrepancies, and support NIST/CMMC assessment readiness.
- Support endpoint security monitoring and incident investigations using CrowdStrike Falcon, Tanium, Zscaler, and Varonis; validate device posture and BitLocker protection and remediate security or access findings.

North House | **IT Manager**

Minneapolis, MN | Oct 2023 - Oct 2025

- Managed user onboarding/offboarding, account setup, SaaS access, and Windows/macOS endpoint deployment across business operations.
- Administered user accounts, endpoints, collaboration systems, and business applications while resolving identity, access, hardware, and software issues and delivering end-user training.

CYBERSECURITY PROJECTS

- **Wazuh SIEM Lab:** Deployed a VMware-based Wazuh environment monitoring Windows/Linux endpoints; generated brute-force and privilege-escalation test activity to validate detections; triaged security alerts/logs, FIM changes, and vulnerability findings and mapped activity to MITRE ATT&CK.
- **Nessus Vulnerability Management Lab:** Performed credentialed vulnerability scans against two Windows 11 endpoints; reviewed findings by severity and affected system and prioritized remediation based on risk.
- **Active Directory Lab:** Built a Windows Server 2025 domain with two Windows clients; configured DNS, domain authentication, user/group administration, Group Policy, and role-based access controls (RBAC).
- **TryHackMe SOC & Blue Team Training:** Completed guided SOC L1 labs covering alert triage, reporting/escalation, SIEM, EDR, threat intelligence, DFIR, and IOC prioritization using the Pyramid of Pain.

EDUCATION

North Central University | **Bachelor of Science, Information Science**

Minneapolis, MN | May 2023

Information Science Student of the Year Award (2022-2023)