Michael Swain

IT & Cybersecurity · SOC Lead / Security Engineer

linkedin.com/in/michael-swain · ~6 yrs cybersecurity · 8 yrs IT · team of 8 · 20K+ endpoints · 10+ clients

SOC Lead with roughly 6 years in cybersecurity and 8 in IT, grown through one organization from network engineering to the SOC floor. I lead a team of 8 analysts protecting 20,000+ endpoints across 10+ clients in multiple industries — driving detection engineering and threat hunting, owning high-severity incident response, and mentoring analysts while keeping response fast and evidence-based.

EXPERIENCE

SOC Lead
2025 – Present

Managed IT & Security Services Provider

- Lead a team of 8 SOC analysts protecting 20,000+ endpoints across 10+ clients in multiple industries — owning triage quality, escalation, and shift handoffs.
- Drive detection engineering in Elastic SIEM: build and tune detections, map coverage to MITRE ATT&CK, and cut false positives on the highest-volume alert sources.
- Lead incident response for high-severity cases end to end — scoping, containment, and post-incident reporting.
- Run proactive threat hunts across client environments and convert hunt findings into durable new detections.
- Mentor L1/L2 analysts and standardize playbooks, documentation, and escalation paths.

SOC Analyst · L1 → L2
2020 – 2025

Managed IT & Security Services Provider

- Monitored and triaged alerts across Elastic SIEM, CrowdStrike EDR/XDR, and SentinelOne, determining severity and business impact.
- Investigated suspicious activity using logs, threat intelligence, and forensic data; documented findings, actions, and remediation.
- Executed and refined incident-response playbooks; used CrowdStrike RTR and PowerShell for live response and evidence collection.

L2 Service Desk Administrator · Staff Augmentation
2019 – 2020

Managed IT & Security Services Provider

- Resolved escalated technical issues via ScreenConnect, minimizing downtime and holding SLA compliance across queues.
- Led RingCentral softphone support for the City of Phoenix's COVID-19 vaccination registration effort.
- Managed Active Directory — account creation, password resets, and group policy — and adapted across diverse client environments.

Network Technician & Engineer
2018 – 2019

Managed IT & Security Services Provider · Integration Division

- Configured switches, routers, and wireless access points; installed and troubleshot equipment across multiple sites.
- Ran physical and wireless site surveys; designed and remediated WLANs with Ekahau Pro.
- Traveled nationally for deployments and network upgrades.

TECHNICAL SKILLS

SIEM & Detection	Elastic SIEM, Detection tuning, MITRE ATT&CK, Log & forensic analysis
EDR / XDR	CrowdStrike EDR/XDR, CrowdStrike RTR, SentinelOne, Cortex XDR · XQL
IR & Threat	Incident triage, Escalation, Threat intelligence, IR playbooks, NIST-aligned response
Scripting	PowerShell, XQL, CrowdStrike RTR
Networking & Systems	TCP/IP · DNS · DHCP, Subnetting, Air-gapped networks, Ekahau Pro, Windows · Linux · macOS, Active Directory

CERTIFICATIONS & TRAINING

CompTIA Security+ Certified
Google IT Support Professional Coursera · Certified
CompTIA CySA+ In progress
CompTIA PenTest+ In progress

PluralSight SOC Analyst 1 & 2 — hands-on labs
Udemy CySA+, PenTest+ & CCNA coursework
Coursera Google IT Support Professional