MICHAEL FUENTES

Cybersecurity Leader | CISSP

mikevfuentes@gmail.com | linkedin.com/in/michael-fuentes | cybersecurity.heyitsmikefuentes.com

SUMMARY

Cybersecurity leader with 9+ years building and scaling managed security services. Currently a security architecture and engineering team lead, helping transform a reactive SOC into a proactive MDR practice while supporting service design and profitability. Proven record of mentoring engineers, launching revenue-generating services, and partnering across sales, operations, and executive leadership to strengthen security posture and operational efficiency. Pairs hands-on, AI-assisted development with secure-by-design practices to rapidly prototype and deploy internal tooling.

EXPERIENCE

Security Architecture & Engineering Team Lead

Oct 2024 - Present

All Covered · Konica Minolta

- Lead the design and deployment of SOAR across managed security services, building cross-team automations that lowered operational costs.
- Launched a new Dark Web Monitoring service at a 60% profit margin, surfacing stolen credentials before they were exploited in the wild.
- Merged siloed SIEM and managed EDR into a unified MDR offering, advancing the SOC from reactive to proactive.
- Owned vendor evaluation and requirements for new managed security services, reducing cost while protecting profitability.
- Defined the go-to-market process for new security services, partnering with sales, operations, development, marketing, and executive leadership.
- Mentored and coached SOC team members on technical growth and career advancement.

Senior Cybersecurity Engineer

Aug 2022 - Oct 2024

All Covered · Konica Minolta

- Led deployment, support, and maturation of managed endpoint security services for 400+ clients, tailoring solutions to each client's business needs and risk profile.
- Served as senior escalation point for lower-level analysts, providing expert guidance on cybersecurity incident review and response.
- Mentored team members on security best practices, processes, and incident response.
- Built data-driven business cases for new hires, supporting team expansion through demonstrated service growth and client demand.
- Developed SOAR and Python automation scripts, reducing manual data analysis time by 50%.
- Used SentinelOne for threat triage, improving accuracy between true and false positives and increasing response efficiency.
- Partnered with IT, business, and executive teams to drive successful solution adoption and high customer satisfaction.

Incident Response Consultant

Sep 2021 - Aug 2022

ConnectWise, LLC

- Served as Incident Commander for partner-facing incidents, coordinating subject matter experts and external partners to ensure rapid environment recovery.
- Cut partner downtime by 50% through incident response process improvements.
- Led a cross-functional team to develop incident response playbooks and guidelines, shortening response times by 35%.
- Used EDR, SIEM, and ad-hoc tooling to detect, investigate, and contextualize malicious activity across global time zones.
- Analyzed client logs and artifacts with IOC and open-source tooling to determine root cause, TTPs, and threat intelligence.
- Architected AWS infrastructure for incident response, decreasing data ingestion and processing time by 75%.
- Advised SMB and enterprise partners on containment, eradication, and risk reduction via incident-centric gap analysis.

Information Security Engineer

May 2018 - Sep 2021

ConnectWise, LLC

- Reduced enterprise partner risk through a Vendor Risk Management Program, surfacing new revenue opportunities from risk data.
- Built NIST Cybersecurity Framework-compliant product assessments and vendor remediation plans.
- Automated routine vendor management processes in Python; built a separate automation tool that cut manual workload by 30%.
- Architected multi-node, multi-cloud data discovery and classification in AWS for data loss prevention (DLP).
- Designed and tested system and application hardening guidelines based on CIS Benchmarks.
- Planned and built CTFs for customer enablement and educated MSPs and small businesses on the adversary mindset.

Managed Data Security Analyst

Jan 2017 - May 2018

Sienna Group, LLC

- Maintained customer-managed data security infrastructure and software.
- Resolved helpdesk tickets and remediated DLP configuration and installation issues for managed service customers.
- Validated data classification effectiveness by creating and testing data against the DLP engine.

TECHNICAL PROFICIENCIES

Security Operations: MDR, SOAR, threat correlation, incident response, SOC maturation

Endpoint & EDR: SentinelOne, Bitdefender

Cloud & Virtualization: AWS, Vultr, Cloudflare, Docker & Docker Compose, VMware

Development: Python (FastAPI), React / Next.js, TypeScript, REST APIs, PostgreSQL, Git

AI-Assisted Development: Building and deploying full-stack apps with Claude/LLMs and local models (Ollama), applying secure-by-design practices (JWT auth, password hashing, rate limiting)

Infrastructure & Self-Hosting: Linux server administration, reverse proxies (Caddy, Nginx), Tailscale, UniFi networking, Home Assistant

Data Protection: DLP, data classification (TITUS)

Frameworks: NIST Cybersecurity Framework, CIS Benchmarks

Operating Systems: Windows, Linux, macOS

EDUCATION & CERTIFICATIONS

B.S., Computer Science · University of South Florida May 2018

Certified Information Systems Security Professional (CISSP) · ISC2 Aug 2024