

Noah Cook

Bellevue, WA | cook.nnoah@gmail.com | [linkedin.com/in/noahcook001](https://www.linkedin.com/in/noahcook001) | github.com/cooknoah | noahcook.dev

PROFESSIONAL SUMMARY

Security engineer at a managed security provider, automating security reporting from Tenable, SentinelOne, Red Canary, Okta, and other platforms for 60+ client organizations and 2,100+ endpoints on AWS Lambda and S3. Previously at Medco Tool, automated CrowdStrike and Mimecast reporting in Python and rolled out KnowBe4 to 270+ users. CompTIA Security+ and AWS Cloud Practitioner certified.

TECHNICAL SKILLS

Security Automation: Python API integrations, scheduled reporting pipelines, Power BI dashboards

Endpoint and Network Security: CrowdStrike EDR, SentinelOne, Red Canary, Tenable, NinjaOne, Check Point, Cloudflare

Security Monitoring: Alert triage, log analysis, threat escalation, documentation

Security Awareness: KnowBe4 LMS, phishing simulations, user training

Cloud and Identity: AWS (Lambda, EventBridge, S3), Azure, M365, Okta, Obsidian Security, Active Directory

Email Security: Mimecast administration, phishing analysis, domain blocklisting

SIEM and Logging: Splunk, log aggregation, event correlation, dashboard monitoring

Compliance and Documentation: HIPAA/HITECH, ISO 27001, SOC 2, PCI-DSS (conceptual), SOPs, runbooks

EXPERIENCE

Junior Security Engineer | Cyvatar • Remote

Aug 2026 - Present

- Generated security reports for 60+ client organizations and 2,100+ endpoints from Tenable, SentinelOne, Red Canary, Cloudflare, Check Point, NinjaOne, Obsidian Security, Okta, and Vonahi.
- Ran the reporting pipeline in AWS, using Lambda functions on an EventBridge Scheduler to pull vendor metrics into S3 as JSON.

Security Analyst | Medco Tool • Remote

Oct 2025 - Jul 2026

- Automated monthly security reporting in Power BI with Python scripts pulling CrowdStrike, Mimecast, and KnowBe4 API data.
- Monitored 300+ endpoints via CrowdStrike EDR, triaging alerts and escalating confirmed threats with documentation.
- Reviewed 5,000+ suspicious emails via Mimecast, blocking 200+ malicious domains across the organization.
- Coordinated TLS certificate renewal with DigiCert, managing the end-to-end lifecycle without service interruption.

Security Analyst Intern | Medco Tool • Remote

Feb 2025 - Oct 2025

- Triaged suspicious emails via Mimecast and monitored endpoints via CrowdStrike EDR, escalating confirmed threats.
- Administered KnowBe4 for 270+ users, managing phishing simulations and training completion tracking.

EDUCATION

Bachelor of Science in Information Technology

Florida International University, Miami, FL

April 2026

Relevant Coursework: Network Security, Cybersecurity Principles, IT Infrastructure, Systems Administration

CERTIFICATIONS

CompTIA Security+

April 2026

AWS Certified Cloud Practitioner

July 2026

PROJECTS

MAAT - Malware Analysis Automation Tool

Python, oletools, pefile, VirusTotal API

- Built a Python CLI tool for automated static malware analysis of Office documents, PE binaries, and PDF files.
- Implemented VirusTotal API hash lookups with caching and a 0-10 risk scoring engine, generating HTML/JSON reports via Jinja2.