Sunny Nguyen

thesunnynguyen@gmail.com | linkedin.com/in/thesunnynguyen | portfolio.sunnyitsolutions.com

EDUCATION

Master of Science, Cybersecurity Management GPA: 4.0 | Expected Apr. 2027

University of Utah — David Eccles School of Business

Courses: Networking & Servers, Cybersecurity Management, Web-Based Applications **Incoming S26:** Secure Network Operations, Vulnerability Management, Cloud Computing

Bachelor of Science, Information Systems — Management Minor Apr. 2025

University of Utah — David Eccles School of Business

Courses: Data Structures & Algorithms, Programming with Python, Accelerated OOP, Systems Design & Analysis, Database Fundamentals

CERTIFICATIONS

CompTIA Security+ | CompTIA Network+ | Google Cybersecurity Professional | NIST RMF | PCEP — Python **In Progress:** CompTIA CySA+ | AWS Solutions Architect Associate

TECHNICAL SKILLS

Security:	Incident Response | Digital Forensics | Threat Detection | Vulnerability Assessment | Network Security | Log Analysis | SIEM (Splunk, Microsoft Sentinel) | MITRE ATT&CK; | NIST RMF
Application Security:	RBAC Design | Authentication & Authorization | Session Management | Secure API Design | Audit Logging | Threat Modeling
Development:	Python | TypeScript | Next.js | SQL (PostgreSQL) | REST APIs | Git/GitHub | Linux | Bash
AI & Cloud:	Claude API | Ollama | AWS | n8n
Tools:	Wireshark | Nmap | Burp Suite | Kali Linux | Active Directory | Windows Event Viewer | Supabase | Stripe | Twilio

WORK EXPERIENCE

IT Security Consultant & Software Developer Sep. 2025 – Present

Sunny IT Solutions, Salt Lake City, UT

- Conducted network assessments and vulnerability scans for small business clients — identified misconfigurations, unpatched systems, and authentication weaknesses; delivered remediation reports and implemented fixes
- Designed and deployed secure internal web applications with production-grade controls: RBAC, SMS-based 2FA with device trust, bcrypt hashing, OTP rate limiting, account lockout, tamper-evident audit logging, and payment webhook signature verification
- Built custom internal tooling replacing manual workflows — inventory tracking, sales analytics, order management, and business reporting — deployed as live operational systems
- Hardened client endpoints and configured network security controls; advised on data protection policies aligned with each client's compliance requirements

Digital Forensics / Incident Response Mentorship (Remote) Mar. 2025 – Aug. 2025

Ensign Services, Inc

- Completed structured, weekly mentorship with the security department — developing practical understanding of malware analysis, digital forensic methodology, and incident escalation protocols
- Applied MITRE ATT&CK and NIST frameworks across real incident scenarios; contributed to threat intelligence enrichment workflows

Help Desk Analyst (Hybrid) Jan. 2025 – Aug. 2025

Ensign Services, Inc

- Investigated and resolved escalated network and endpoint security incidents in a HIPAA-regulated enterprise environment
- Supported enforcement of data protection policies and risk mitigation efforts across clinical systems

Software Engineer Intern Nov. 2023 – Apr. 2024

Tongues Language Games, Salt Lake City, UT

- Built and maintained Python backend systems; implemented AI prompting techniques to enhance user-facing product features

PROJECTS

Secure Internal Operations Platform (Confidential Client) 2025 – Present

Next.js 15, TypeScript, Supabase/PostgreSQL, Stripe, Twilio Verify, AWS

- Architected a multi-role internal business platform with production-grade security: RBAC enforced at middleware and API route level, JWT session management, SMS 2FA with device trust, bcrypt hashing, OTP rate limiting, account lockout, and immutable audit logging
- Built full analytics suite (sales trends, peak-hour analysis, inventory tracking), staff management with temporary password provisioning, and TCPA-compliant SMS notification flows

AI-Powered Healthcare Request System 2025 — Hackathon, Intermountain Health

React, Tailwind CSS, Claude API

- Designed and built a full-stack AI intake and triage system modeled on a real healthcare department workflow — replaced a manual Microsoft Form → email → spreadsheet process with automated AI classification and an admin management dashboard
- Architecture scoped directly from real Intermountain Health operational requirements and validated with department stakeholders during the event

AI SOC Agent & AI Triage / Threat-Hunt Companion 2026

Python, n8n, Claude API, MCP, Wazuh/OpenSearch

- Built AI agents that triage security alerts, query logs, enrich with threat intelligence, and output analyst-ready summaries — using MCP, Notion runbooks, and persistent agent memory across investigation sessions
- Implemented human-AI partnership model: read-only investigation with staged, analyst-approved response actions

ElderShield — AI Scam Detection Platform 2025

Python, Ollama, Web

- Built a privacy-preserving scam detection platform for elderly users using a locally-hosted AI model — no data transmitted externally
- Three-role system (elder, caregiver, admin) with scam likelihood scoring, manipulation tactic identification, plain-language guidance, and caregiver alert notifications

Enterprise Security Homelab 2025 – Present

- Simulated multi-stage attacks and detections across VMs; hands-on experience with incident detection, threat hunting, log analysis, and system hardening across enterprise-grade tooling

DoD Cyber Sentinel Skills Challenge Jun. 2025

- Competed in real-world CTF challenges across forensics, OSINT, web security, malware analysis, and networking using CyberChef, Burp Suite, Wireshark, Nmap, and Python

ACTIVITIES

BSidesSLC 2026 — AI-driven security agent workshops (MCP, n8n, Wazuh, Claude Code)

TryHackMe | HackTheBox — Active practitioner