AUSTIN H. KEENAN

SENIOR SECURITY ENGINEER | SECURITY OPERATIONS, DETECTION & INCIDENT RESPONSE

Reading, PA
201-519-5181 ▪ austin@keenan.life
linkedin.com/in/austinkeenan

STRENGTHENING THREAT DETECTION, INSIDER RISK DEFENSE & SECURITY AUTOMATION

Cybersecurity engineer with 8 years across security operations, incident response, and detection engineering in financial services, manufacturing, and critical infrastructure. Founded an enterprise insider-threat program that surfaced 12+ active data-exfiltration cases and authored 100+ Splunk detections under a bi-weekly sprint cadence. Core strengths span SIEM/SOAR operations, security automation, and NIST-aligned program governance.

CORE COMPETENCIES

Security Operations (SecOps) ▪ Incident Response & Investigation ▪ Detection Engineering ▪ SIEM & SOAR (Splunk ES, Resilient) ▪ Insider Threat & Data Loss Prevention ▪ Threat Detection & Monitoring ▪ Security Automation & AI Enablement ▪ Vulnerability Management ▪ Risk Assessment & Third-Party Risk ▪ NIST CSF / 800-53 · FISMA · PCI · GDPR ▪ Cloud Security (AWS, Azure / Entra) ▪ MITRE ATT&CK

Technologies: Splunk ES ▪ Resilient ▪ CrowdStrike ▪ Varonis ▪ Nessus Tenable ▪ KnowBe4/AIDA ▪ Keeper ▪ McAfee ePO/Trellix ▪ Microsoft Defender ▪ Sentinel ▪ Purview ▪ Intune ▪ Entra / Active Directory ▪ Exchange ▪ Azure ▪ AWS ▪ ServiceNow ▪ JIRA / Confluence ▪ PowerShell

PROFESSIONAL EXPERIENCE

Flagger Force – Hummelstown, PA — Mar 2025 – Present

VC-backed national traffic-control and work-zone safety provider; roughly 200 employees.

Senior Systems Security Engineer

Sole senior security engineer for the enterprise, owning the security program end to end against a roughly $60K annual tooling budget following a Blue Sea Capital investment.

- Built the enterprise information-security program from zero, spanning policy set, alert triage and incident response on the Microsoft Defender and Sentinel stack, and authentication hardening; presented the six-month build to the board, which increased its investment in the company.
- Cut user phishing click rate from **15%** to **3%** by rebuilding awareness training on KnowBe4/AIDA with machine-learning-tiered difficulty and per-user paths and trimmed administrative license cost roughly **33%** through a utilization audit.
- Hardened enterprise authentication through a companywide uplift, deploying Windows Hello for Business on a hybrid Entra / on-premise Active Directory model alongside Keeper credential management with biometric MFA and Intune-based managed-device assurance.
- Consolidated a fragmented OneDrive/NAS/USB/SharePoint estate onto a controlled, ticketed Confluence/Jira system with granular access, and began rolling out Microsoft Purview data-sensitivity labeling across files, email, and messages.
- Instituted an automated security-metrics framework of KPIs and KRIs measuring behavioral change and advises executive leadership on cyber-insurance strategy and enterprise risk posture.

Santander US – Wyomissing, PA — Sep 2021 – Mar 2025

U.S. arm of a global banking group; financial services SecOps under federal regulatory oversight.

Associate, Information Security

Member of the bank's Cyber Threat Detection Management function, covering detection engineering, DLP, and SecOps metrics across testing and development teams.

- Automated all daily, weekly, and monthly SecOps metrics reporting, reclaiming **30+** hours per week (near a full FTE) and seeding a formal security-automation request pipeline that compounded the savings.
- Engineered **100+** custom Splunk detections per year under a bi-weekly sprint process for development, tuning, and production deployment, weighted toward insider-threat and DLP use cases.
- Raised FISMA maturity from **Level 2/3** (Defined/Implemented) to **Level 4** (Managed and Measurable) by reengineering DLP rules across every data domain and building evidence-backed Splunk KRIs and KPIs around them.
- Formalized the Detection Assurance Forum, a quarterly governance review of detection coverage, and authored the observations reporting that drove follow-up engineering and workshop scheduling.

AUSTIN H. KEENAN 201-519-5181 | austin@keenan.life

Lutron Electronics – Coopersburg, PA Oct 2020 – Sep 2021

Privately held lighting-control manufacturer with a CUI government services division.

Security Technician

Second security hire reporting to the Director of Information Security; built operational security for the enterprise and its regulated government services division.

- Established security operations from the ground up, covering authentication hardening, 2FA/MFA, alert monitoring, incident response, reporting automation, and a dozen-plus policies drafted and approved.
- Administered hardware MFA (DUO/YubiKey) for the CUI government services division, handling hundreds of access requests per week.
- Assumed end-to-end ownership of the Arctic Wolf MSSP relationship, validating or rejecting findings and reducing retainer reliance through in-house automation and SecOps coverage.

Customers Bank – Phoenixville, PA Feb 2020 – Sep 2020

Mid-Atlantic commercial bank and financial services provider.

Junior Cyber Risk Specialist

- Introduced an InfoSec approval gate requiring vendors to submit security documentation and environment proof before onboarding, inserting security into a previously unvetted procurement flow.
- Reviewed roughly **two dozen** vendors per month (**3–7** per week) against the new third-party-risk standard despite initial organizational resistance.

EARLY CAREER

Santander US – Holmdel, NJ Mar 2019 – Aug 2019

Junior Cybersecurity Analyst

- Launched Santander US's **first** insider-threat program alongside DLP monitoring in the Cybersecurity Fusion Center, running Splunk ES investigations that surfaced **12+** employees and contractors exfiltrating regulated data, several leading to termination.
- Applied project-management discipline to security-engineering intake, onboarding hundreds of terabytes of new log sources and configuring **3** enterprise DLP tools for active triage.

QMA / Prudential – Newark, NJ Jul 2018 – Mar 2019

Information Security Analyst (Internship)

- Deployed Nessus Tenable and built 30/60/90-day identify-classify-remediate procedures on a direct CISO mandate, driving dozens of vulnerabilities patched on predictable monthly timetables.
- Operationalized a dormant Varonis instance with firm data-sensitivity classifiers for proprietary model data, triaging **2,000–5,000** DLP alerts per month as the precursor to a full monitoring capability.

EDUCATION & CERTIFICATIONS

Bachelor of Professional Studies (BPS), Cyber Security – Saint Peter's University ▪ GPA **4.0/4.0**

Coursework: Secure Software Engineering ▪ Cryptography (graduate level) ▪ Network Monitoring ▪ Digital Forensics & Penetration Testing (Wireshark, Nmap, Kali, Metasploit, Autopsy, FTK Imager)

Certifications: AWS Certified Cloud Practitioner ▪ CCAK (Certificate of Cloud Auditing Knowledge) – in progress ▪ CISSP – in view

Honors: James J. Damiano '53 Award for Leadership and Academic Excellence ▪ Alpha Sigma Lambda National Honor Society ▪ Gold Medal for Academic Excellence (2018, 2019)