ANDREW J. HANNAFORD

New York, NY | (612) 715-1375 | AndrewJ.Hannaford@gmail.com | linkedin.com/in/andrew-hannaford

PROFESSIONAL SUMMARY

Security platform architect specializing in detection engineering and AI security infrastructure. Led zero-downtime SOAR migration serving 50+ analysts, reduced alert fatigue by 40%, and architected detection-as-code pipelines in Go/Python across multi-cloud environments (AWS, GCP, Azure, Kubernetes). Currently modernizing enterprise AI security — implementing controls for agentic workflows and MCP traffic visibility across corporate endpoints. Holds 10 GIAC/SANS certifications and a SANS MS in Information Security Engineering.

TECHNICAL SKILLS

Detection & Response: Detection-as-Code (Go, Python), Splunk SIEM, Sumo Logic, Cortex XSOAR/XSIAM, ThreatConnect SOAR/TIP, CrowdStrike EDR, SentinelOne, Security Onion, Sigma Rules, YARA

Cloud & AppSec: AWS, GCP, Azure, Kubernetes, Docker, Terraform, Buildkite, Flux, Prisma Cloud/CSPM, CI/CD Security, CodeQL, Semgrep, SAST/DAST, SSO/SAML

Threat Hunting & Forensics: Elastic Stack/ELK, Snort, Suricata, Zeek, Volatility, KAPE, Plaso, Network Traffic Analysis

Languages & Tools: Python, Go, JavaScript, Bash, PowerShell, SQL, Java, C#, NoSQL/MongoDB, PostgreSQL, Git, ServiceNow, Atlassian Suite

AI Security: Onyx, Surepath, Island, Wiz, MCP Security, Agentic Workflow Controls, LLM/Claude Automation, AI Endpoint Visibility, DLP, Browser Isolation

PROFESSIONAL EXPERIENCE

BREX

Dec 2025 – Present

Senior Security Engineer

New York, NY

- Own the detection engineering program across corporate, SaaS, and multi-cloud environments (AWS/GCP/Azure/Kubernetes); design 30+ detection-as-code rules in Go/Python, cutting MTTR by 35% and false positives by 45% in Q1.
- Lead incident response and vulnerability management end-to-end—triage, forensics, containment, remediation, and post-incident reviews; standardize 12 runbooks and run quarterly tabletop exercises to strengthen SLA adherence across 3 teams.
- Led AI security infrastructure modernization — implemented controls for agentic workflows (OpenClaw) integrating Onyx, Surepath, Island, and Wiz to enforce DLP, browser isolation, and cloud security posture; extended visibility to MCP (Model Context Protocol) traffic and AI tool usage on corporate endpoints, establishing inspection, logging, and policy enforcement at the host layer.
- Architected a fully automated SOC workflow using Claude-powered plugins integrated with Sumo Logic SIEM and additional data sources — enabling end-to-end ticket triage, runbook-driven investigation, and batch case resolution with minimal analyst intervention; developed the runbook library and batch case-working framework now used as the standard response operating procedure.

ROCKSTAR GAMES / TAKE-TWO INTERACTIVE

Jun 2023 – Sep 2025

Lead Security Operations Engineer (Jun 2025 – Sep 2025)

Senior SOAR Engineer (Jun 2023 – Jun 2025)

New York, NY

- Owned the Cortex XSOAR platform across 4 business units (Rockstar, 2K, Zynga, Gearbox) serving 50+ SOC analysts; set multi-year platform roadmap, defined program KPIs, and delivered 200+ automation workflows slashing alert handling time by 60%.
- Orchestrated the XSOAR-to-XSIAM migration across 4 business units: defined 10-week plan, coordinated 8 stakeholder teams, migrated all automation playbooks and integrations, and executed cutover with zero downtime—presented outcomes to security leadership.
- Refactored 80+ Splunk SIEM detection rules and alert ingestion pipelines, cutting false positive volume by 40% (~3,000 fewer false alerts/month) and improving SOC triage accuracy to 92%.
- Engineered 15+ cross-platform integrations between ServiceNow CMDB, EDR, SIEM, and SOAR, automating enrichment workflows and eliminating ~20 hours/week of manual analyst handoffs.

- Deployed SAST pipelines (CodeQL, Semgrep) scanning 50+ repositories per commit and Prisma Cloud (CSPM) across 300+ workloads; mentored 3 junior engineers on security tooling and established review practices adopted org-wide.

NBCUNIVERSAL Mar 2022 – Feb 2023
Senior Security Automation Engineer Denver, CO / Remote

- Owned the enterprise SOAR platform (Cortex XSOAR) for 40 SOC analysts, engineering 60+ automation playbooks in Python that cut manual triage effort by 70% and enabled the team to absorb 30% more alert volume.
- Developed integrations with ThreatConnect SOAR/TIP to ingest, classify, and correlate 15+ threat intelligence feeds, slashing threat intel processing time by 55%.
- Implemented Splunk SIEM common data model and alert classification for 80+ custom detection rules, standardizing alert taxonomy across the enterprise.
- Partnered with SOC analysts on 50+ high-priority incidents, driving cross-functional triage and response; refined the IR handbook (30+ procedures) and reduced mean resolution time by 35% through targeted automation.

RAYTHEON INTELLIGENCE & SPACE Oct 2019 – Mar 2022
Development Manager (May 2021 – Mar 2022) Washington DC Area
Security Engineer II (Feb 2021 – May 2021)
Security Engineer (Oct 2019 – Feb 2021)

- Managed delivery of 5+ technical projects across a 12-person multidisciplinary team: built program roadmaps, ran requirements gathering with federal stakeholders, and maintained 95% on-time delivery.
- Conducted 10+ offensive security penetration tests for DHS and CISA clients, identifying 40+ critical and high-severity findings and delivering remediation roadmaps that improved agency security posture.
- Designed and shipped the Headless Hunter threat hunting platform (Python, MongoDB, Elastic Stack), processing 50K+ threat signals/week across 3 federal programs.
- Developed an automated threat intelligence platform (Python, PostgreSQL) aggregating 10+ feeds into a unified store, cutting analyst lookup time by 50% and ensuring up-to-date threat context for active investigations.

EARLIER EXPERIENCE

Avtex Solutions – Associate Consultant – Bloomington, MN Jun – Oct 2019
Western State Bank – IT Security Intern – Fargo, ND Dec 2018 – May 2019
Stoneridge Software – Development Intern – Barnesville, MN May – Dec 2018
Cable ONE – Field Technician – Fargo, ND May 2015 – May 2018

OPEN SOURCE & COMMUNITY

GIAC Advisory Board — Active Member
Review and refine GIAC certification exams, contribute to curriculum development, and advise on security education standards with SANS faculty.

Cloud Security Alliance (CSA) — Active Member
Participate in working groups focused on cloud security best practices, Zero Trust architecture, and AI security standards.

EDUCATION

Master of Science, Information Security Engineering – Cloud Security
SANS Technology Institute, Bethesda, MD

Bachelor of Arts, Computer Science
North Dakota State University, Fargo, ND

CERTIFICATIONS & HONORS

GIAC Advisory Board Member | **10 Active GIAC/SANS Certifications**
GSEC (Security Essentials) • GCIH (Incident Handler) • GCIA (Intrusion Analyst) • GDSA (Defensible Security Architecture) • GWEB (Web Application Defender) • GCSA (Cloud Security Automation) • GCPN (Cloud Penetration Tester) • GCPM (Certified Project Manager) • GSTRT (Strategic Planning, Policy & Leadership) • SSAP (Security Awareness Professional)
Other: ITIL 4 • CSM • English (Native) • Spanish (Full Professional)
CTF: 2024 NCL Team 8/386 (Top 2%) • 2024 NCL Individual 24/526 (Top 4%) • 2021 NCL Team 36/3,917 (Top 0.9%)