Griffin Dutka

SECURITY OPERATIONS ENGINEER

griffindutka0@gmail.com · 815.600.6581 · Chicago, IL · linkedin.com/in/griffindutka

SUMMARY

Security Operations Engineer with deep expertise in DLP incident response, endpoint security architecture, and AI-driven automation. Built AI-powered investigation and reporting workflows that cut report drafting time from 90 minutes to under 10 minutes across 200+ incident reports. Engineered a multi-layer offboarding security system with zero unauthorized post-termination device access across 1,000+ terminations. Combines hands-on detection engineering with direct stakeholder communication up to the executive level.

EXPERIENCE

Security Operations Engineer
Beyond Finance
July 2025 – Present
Chicago, IL (Remote)

- Leads daily DLP incident response as primary analyst — coordinates 20+ analyst triage reviews across CyberHaven, Teramind, Datadog, Google Admin, Absolute, CrowdStrike, CyberArk, and Abnormal; direct escalation contact for HR, Legal, and executive leadership
- Cut report drafting from 60–90 minutes to under 10 minutes by automating end-to-end DLP report generation via Claude and Gemini — **200+ reports at 0% failure rate**, recovering an estimated **150–200+ analyst hours per month**
- Engineered DLP-specific Gemini prompts for real-time CyberHaven user activity queries; built Data Dawg, a browser-based investigation skill that self-improves from each output and compacts context every 5th cycle for sustained accuracy
- Eliminated unauthorized post-termination device access across **685 terminations** by architecting the Dead Man Switch (DMS) — a multi-layer offboarding lockdown system presented to and approved by the CEO
  - Layer 1: Absolute OS freeze — auto-bricks offline devices after 30 days via embedded offline timer; no internet required
  - Layer 2: Cached credential clearing via NinjaOne and JumpCloud MDM heartbeat scripts on devices inactive 3–5 days
  - Automated 7-day and 24-hour device warning emails; ServiceNow unlock form for IT false-positive recovery
- Owns High Risk User Monitoring (HRUM) — monitors employees on PIPs, suspected IP theft, disgruntled employees, and anomalous behavior; conducts entry and exit reviews with sustained cross-platform behavioral analysis spanning weeks to months
- Automated the full HRUM lifecycle using Torq, Datadog, and AWS S3 — replaced manual spreadsheet tracking with a **100% accuracy** workflow across all sensitive employee transitions
- Surfaced **80,000+ GB of stale data risk** across **4,500+ devices** by deploying custom Mac and Windows discovery scripts fleet-wide; scoped tiered auto-deletion by business unit (Sales 30d / Corporate 90d / IT 180d)
- Authored official P0, P1, and P2 incident playbooks now in active use across the security team — covering identification, war room mobilization, containment, scoping, reporting, and remediation
- Reduced DLP exposure surface by implementing 4 CyberHaven hard-block policies (copy/paste, screenshots, printing, removable media) and 3 Datadog detection monitors for anomalous login activity
- Standardized security request intake by replacing ad hoc HR channels with a Slack-based workflow enforcing scope selection, business justification, and SLA accountability
- Serves as data custodian for legal and HR — e-discovery exports via Google Vault and Looker; compliance alignment with NIST CSF, ISO 27001, NERC CIP, GDPR, PCI-DSS, HIPAA, SOX, and SOC 2
- Deployed Absolute EDD to 150+ test users for PII, financial record, and GDPR-sensitive field scanning

Cybersecurity Analyst

Exelon Corporation

2023 – 2025
Chicago, IL

- Investigated security incidents using Splunk, CyberArk, and Carbon Black for threat detection, log analysis, and incident response; documented and escalated findings to senior analysts and stakeholders
- Assisted in deploying security tooling to **1,000+ endpoints** across Linux RHEL 7/8, Windows Server 2016–22, and EMS environments — including on-prem deployments of CyberArk, Splunk, Carbon Black, and Aruba ClearPass
- Developed Splunk SPL queries and dashboards for real-time endpoint activity and network traffic monitoring; optimized Carbon Black endpoint detection policies to reduce false positives
- Managed privileged access via CyberArk and identity-based network access control via Aruba ClearPass; ensured compliance with NERC CIP and additional regulatory frameworks
- Authored SOPs, incident handling workflows, and troubleshooting guides for cross-team knowledge sharing and audit readiness

TECHNICAL SKILLS

DLP & Monitoring
CyberHaven · Teramind · Datadog · Google Admin · CrowdStrike · Abnormal · CyberArk

Endpoint & MDM
Absolute · JumpCloud · NinjaOne · ServiceNow · Carbon Black

SIEM & Detection
Splunk (SPL) · Datadog · CyberArk

Automation & Cloud
Torq · Tray.io · AWS S3 · PowerShell · LaunchD · Task Scheduler · Windows Storage Sense

AI & Prompt Engineering
Claude · Gemini · Google Drive AI Projects · Ask Gemini (browser)

Data & E-Discovery
Google Vault · Looker · Absolute EDD

Network & Identity
Aruba ClearPass · Cisco · Checkpoint

Compliance Frameworks
NIST CSF · ISO 27001 · NERC CIP · GDPR · PCI-DSS · HIPAA · SOX · SOC 2 · FISMA · OWASP

EDUCATION

B.S. Cybersecurity
Bellevue University
GPA: 4.0 · 2023
Intrusion Detection · Incident Response · Digital Forensics · Web App Security · Access Controls · Cryptography · Compliance Frameworks

A.S. Cybersecurity
Joliet Junior College
2021
Networking · OSINT · Log Analysis · Network Traffic Analysis · Penetration Testing · Forensics

Certificate of Achievement, Cybersecurity
Joliet Junior College
Issued May 2021 · Valid through 2033

ALSO NOTABLE

150–200+ analyst hours recovered monthly from AI pipeline

2,700+ devices covered by data discovery scripts

20+ security controls implemented post-P0 incident

<2.5% human correction rate on AI-generated reports