Griffin Dutka

SECURITY OPERATIONS ENGINEER

CONTACT

EMAIL
griffindutka0@gmail.com
LINKEDIN
linkedin.com/in/griffindutka
SITE
griffty.com
LOCATION
Chicago, IL

IMPACT

1,500+
Terminations secured · zero unauthorized access

300+
AI-generated DLP reports · <10 min each

80,000+ GB
Stale data risk surfaced across 4,500+ devices

150–200+
Analyst hours recovered per month

TECHNICAL SKILLS

DLP & Monitoring
Enterprise DLP · UAM · SIEM · workspace admin · EDR · email security · PAM

Endpoint & MDM
Endpoint resilience · MDM · RMM · ITSM · Carbon Black

SIEM & Detection
Splunk (SPL) · cloud SIEM · detection engineering

Automation & Cloud
SOAR · iPaaS automation · cloud storage · PowerShell · LaunchD · Task Scheduler

AI & Prompt Engineering
LLM agents · AI agent workspaces · prompt engineering · agentic workflows

Data & E-Discovery
Enterprise vault · BI analytics · legal review · endpoint data discovery

Network & Identity
Aruba ClearPass · Cisco · Checkpoint

EDUCATION

B.S. Cybersecurity
Bellevue University
GPA 4.0 · 2023 · NSA-Recognized

A.S. Cybersecurity
Joliet Junior College
2021

Cert. of Achievement
Joliet Junior College
2021 · valid through 2033

COMPLIANCE

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

SUMMARY

Security Operations Engineer with deep expertise in DLP, AI-driven security automation, SOC agentics, endpoint security, and incident response across large-scale enterprise environments. Experienced operating across on-prem and cloud/SaaS platforms, with a track record of designing and implementing security programs that reduce risk, improve response times, and scale across the organization.

EXPERIENCE

Security Operations Engineer

Beyond Finance · Chicago, IL (Remote) · July 2025 – Present

- Leads daily DLP incident response as primary analyst — coordinates 25+ daily analyst triage reviews across DLP, UAM, SIEM, EDR, PAM, email security, and endpoint resilience platforms; direct escalation contact for HR, Legal, and executive leadership
- Engineered an agentic SOC/DLP pipeline — AI agents that triage alerts, review user activity, correlate logs, and draft executive-ready incident reports — recovering **150–200+ analyst hours per month**
- Engineered DLP-specific prompts for real-time user-activity queries and automated log analysis using browser-based investigation ./skill workflows that self-improve from each output and compact context every 5th cycle for sustained accuracy
- Built the **Analyst Action Hub** in an AI agent workspace — a daily dashboard the team works from to track review tasks, pull ticket requests, and log completions; serves as a live monitor for the entire DLP program, providing visibility to VPs and executives
- Eliminated unauthorized post-termination device access in a cloud-based environment across **1,500+ terminations** by architecting a Dead Man Switch (DMS) — a multi-layer offboarding lockdown system
  - **Layer 1:** Firmware-level OS freeze — auto-bricks offline devices after 30 days via embedded offline timer; no internet required
  - **Layer 2:** Cached credential clearing via RMM and MDM heartbeat scripts on devices inactive 3–5 days depending on job title
  - **Layer 3:** 20+ blocking controls and monitors across DLP, UAM, and SIEM platforms to detect any post-termination activity on high-turnover users
  - Automated 7-day and 24-hour device warning emails; ITSM unlock form for IT false-positive recovery
- 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
- Standardized security request intake by replacing ad hoc Slack channels with an ITSM-based workflow enforcing scope selection, business justification, and SLA accountability

Cybersecurity Analyst

Exelon Corporation · Chicago, IL · 2023 – 2025

- 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 **1,500+ 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