Erik Lindgren

Cybersecurity Analyst

erik.lindgren@example.com linkedin.com/in/eriklindgren (555) 493-2276 Arlington, VA

SUMMARY

Security analyst with seven years in SOC operations and threat detection for finance and federal-sector clients. Tuned a Splunk deployment that cut false positives 44%, led containment on 60+ confirmed incidents, and keeps median alert-to-verdict time at 12 minutes on a 150-alert daily queue.

EXPERIENCE

Cybersecurity Analyst — Meridian Vale Financial

2021 – Present

- Triage 150+ SIEM alerts a day in Splunk Enterprise Security; median time to verdict down from 45 minutes to 12
- Tuned 80 detection rules against MITRE ATT&CK, cutting false positives 44% while widening technique coverage across 12 tactics
- Led containment on 60+ confirmed incidents, including a phishing campaign that touched 900 mailboxes and zero executive accounts

SOC Analyst — Argus Sentinel Group

2019 – 2021

- Monitored 12 client environments on a 24x7 SOC rotation; escalation accuracy held above 96% across 18 months
- Wrote 30 Cortex XSOAR playbooks automating enrichment for a tier-1 queue that processes 2,000 alerts a week

IT Support Specialist — Chesapeake Freight Lines

2018 – 2019

- Administered Active Directory, group-policy baselines, and endpoint protection for 400 users across 3 distribution sites and a headquarters
- Rolled out MFA to 100% of staff within four months, blocking 300+ credential-stuffing attempts the first year

EDUCATION

B.S. Information Systems — University of Maryland 2018

SKILLS

Detection	Splunk · Microsoft Sentinel · CrowdStrike Falcon · Wireshark · Zeek
Frameworks	MITRE ATT&CK · NIST 800-53 · PCI DSS · CIS Controls
Practices	Incident response · Threat hunting · Vulnerability management · Phishing analysis

CERTIFICATIONS

CompTIA Security+

CompTIA CySA+