

CP

Carolyn Parker

Cyber Security Analyst

SOC manager with 12 years in security operations, including 5 years running 24/7 teams. Built two SOC's from a handful of analysts to follow-the-sun coverage. Focus on detection engineering discipline, analyst retention, and honest metrics reported to executives.

Location

Alpharetta, GA

Phone

(770) 555-0104

Email

damon.ackerley@example.com

Education

M.S. Information Security, Georgia Institute of Technology, 2016

B.S. Computer Engineering, Auburn University, 2013

GIAC Security Essentials, Certified Information Systems Security Professional

Key Skills

- SOC operations leadership (Tier 1 through detection engineering)
- Log platform strategy across Splunk, Sentinel, and Chronicle
- Detection engineering programs and Sigma governance
- Incident response leadership and executive communication
- Adversary technique coverage assessment
- Budget ownership and vendor negotiation
- Hiring, mentoring, and analyst career pathing
- Purple team program design
- Regulatory reporting on card-data controls, New York

Professional Experience

SOC Manager, Cardinal Ridge Insurance, Alpharetta, GA

2021 - Present

- Lead a 19-person SOC (Tier 1, Tier 2, detection engineering, threat intel) covering a US and European footprint of roughly 42,000 users across life and P&C business lines.
- Cut mean time to contain from 4.2 hours to 51 minutes over 18 months by rebuilding the on-call rotation, standing up a detection-engineering pod, and killing 200+ legacy Splunk rules with no true-positive history in 12 months.
- Own the SOC's operating budget of \$6.8M, including log platform licensing renegotiation that reduced ingestion cost per gigabyte by roughly a third after moving high-volume firewall logs to a cheaper tier.
- Report monthly to the security chief and quarterly to the audit committee on detection coverage against the adversary technique framework, staffing ratios, and top unresolved risks.
- Kept voluntary attrition on the team under 8% in a market where the benchmark ran closer to 20%, through a rotation program that moves analysts between hunt, detection, and incident response every 9 months.

SOC Team Lead, Beacon Harbor Logistics, Marietta, GA

2018 - 2021

- Managed a 9-analyst team responsible for a fleet-tracking platform, electronic data interchange environment, and 5,000 warehouse endpoints.
- Led the response effort during a supply chain intrusion via a compromised managed service provider; scoped 41 affected hosts, coordinated with the federal field office in Atlanta, and delivered the postmortem to the CEO.
- Rebuilt the alert intake process so every SOC ticket carried adversary technique tagging, which later fed the first coverage heat map the security org had produced.
- Ran hiring for 11 SOC roles over three years, standardizing a practical interview using a redacted Splunk investigation.

Senior Cybersecurity Analyst, Fairhollow Payments, Atlanta, GA

2015 - 2018

- Senior response analyst on a card-data payments environment; handled 60+ confirmed incidents including card-skimmer JavaScript and mail-order and telephone-order fraud rings.
- Built the first purple team program between SOC and offensive security, running quarterly exercises against payment authorization flows.
- Authored the company's ransomware playbook, later reused during two live incidents in 2017.
- Mentored 4 Tier 1 analysts, three of whom promoted to Tier 2 within 18 months.

Cybersecurity Analyst, Fairhollow Payments, Atlanta, GA

2013 - 2015

- Monitored ArcSight and later Splunk for the payments SOC on rotating shifts.
- Handled day-to-day phishing and malware triage across 8,000 endpoints.

financial rules, and state breach notification

- Board and audit committee reporting

- Wrote the first internal wiki entries for common incident types, which became the seed of the team's runbook library.
- Selected for the response on-call rotation within 14 months, ahead of the usual timeline.