John Schoonover

Director of Engineering

Minnesota, USA

912-414-4180
johnmschoonover@gmail.com
https://www.linkedin.com/in/johnmschoonover/

—

Professional Summary

Visionary Director of Engineering and named inventor on two in-flight patents with 8+ years in cybersecurity and 4+ years leading high-performing engineering teams across enterprise-scale environments. Recognized for designing scalable architectural patterns that support rapid adaptation in fast-evolving threat landscapes. Adept at aligning security engineering initiatives with organizational detection, response, and risk reduction objectives. Proven track record of building resilient platforms, empowering talent, and evolving infrastructure to accelerate cyber agility and operational excellence across the Cyber Fusion Center (CFC).

Experience

Target / Director of Engineering - Cybersecurity - SIEM

AUGUST 2018 - PRESENT, MINNEAPOLIS, MN

- Lead a multidisciplinary engineering team responsible for the core security telemetry platform, encompassing **data ingestion, enrichment, storage, and access across full-stack layers** — from backend log pipelines to UI integration frameworks.
- Built scalable design patterns and architecture to support **rapid adaptability** across a constantly evolving threat landscape, ensuring the platform can pivot quickly to meet new detection, response, and intel needs.
- Partner closely with incident response, detection engineering, and threat intel teams to build integrated tooling, some of which intersects with SOAR platforms — enabling **reduction of effort for workflows** across triage, enrichment, and investigation.
- Collaborate with product management and senior leadership across organizational levels to align technology investments with **risk reduction and threat visibility objectives**, ensuring shared priorities across business and technical domains.
- Enabled integration of frontend components (React/Node) into platform workstreams, offering design-level guidance while delegating hands-on development to specialized engineers.
- Supported infrastructure modernization efforts, managing cloud and on-prem deployments, and coordinating closely with hardware teams.
- Led migration efforts from commercial SIEM platforms to a **custom-built, modular security data ecosystem**, dramatically improving cost efficiency and increasing flexibility to ingest and query diverse security telemetry.
- Advocated for sustainable team practices by mentoring engineers, scaling ownership, and reducing single points of failure — creating **repeatable success patterns** across ingestion, alerting, and response mechanisms.
- Designed and implemented real-time observability and latency detection patterns that surpassed capabilities found in most commercial SIEM platforms — enabling proactive mitigation of ingestion issues and increasing overall platform resilience and response effectiveness.

Best Buy / Senior Information Security Analyst

MAY 2016 - AUGUST 2018, RICHFIELD, MN

- Architected platform migration strategy from ArcSight to Elasticsearch, enabling seamless warm cutover and improved ingest reliability.
- Mentored engineers on visibility and asset monitoring, resulting in a 40% increase in security tooling coverage in less than six months.
- Developed dynamic ingestion, parsing, and visualization layers using Machine Learning, Logstash, and scripted solutions.
- Built host inventory monitoring solutions to drive informed coverage and risk assessments across the SOC.

Patents

- **Process for Real-Time Validation of Comprehensive Visibility for "perfect feeds" (Patent Pending)**
  System to validate end-to-end visibility for high-value telemetry ("perfect feeds") enabling proactive detection of blind spots, ingestion & parsing gaps, and rules efficacy impacts.

- **Criticality-Aware Drop Control for High-Throughput SIEM Pipelines *(Patent In-Flight)***
  Context-aware pattern for feed volume mitigation while maintaining propagation of rare events for security use cases.

Education

2023 - Western Governors University / MBA

2020 - Western Governors University / B.S., Cybersecurity

2011 - Thomas Nelson Community College / A.S., Physics (Honors)

2012 - University of Virginia / Studies in Physics & Mathematics

Skills

Security Engineering & Architecture: SIEM (Elastic, ArcSight), Log Pipeline Design, Scalable Ingestion Patterns, SOAR collaboration & scoping

Cloud & Infrastructure: Scalable Deployment Patterns, On-Prem Systems, Infrastructure Integration, Hardware-Aware Engineering, Workload Virtualization

Tooling & Scripting: Python, Go, Bash, REST API integration, GitOps workflows, parallel processing

Team & Strategy: Multi-team & Full-Stack Team Leadership, Engineering Roadmaps, Technical Mentorship, Cross-Org Collaboration, Agile Practices, Performance Coaching.