Sean Cullen

Security Engineer | Security Architect - Detection Engineering | Cloud & Hybrid-Identity Security | Incident Response

sean@secop.dev | Arkansas, USA | U.S. Citizen | sean.secop.dev | LinkedIn: www.linkedin.com/in/secopdev/ | GitHub: github.com/secopdotdev

PROFESSIONAL SUMMARY

Hands-on security engineer and architect with 5+ years architecting, operating, and continuously improving enterprise-scale detection and response programs across Fortune 200 environments spanning 11,000+ endpoints and 25,000+ users. Deep technical expertise in SIEM/SOAR engineering, EDR/XDR, detection content development, threat hunting, and DFIR, paired with secure-by-design cloud and hybrid-identity architecture across Microsoft Azure, Entra ID, Entra Connect, and on-premises Active Directory. Long-standing partner to the CISO and CIO on Zero Trust roadmaps and board-level risk reduction, with growing depth in DevSecOps and cloud-native security - containers, infrastructure-as-code, CI/CD, and supply-chain hardening. Passionate about driving down MTTD and MTTR through automation, high-fidelity/low-volume telemetry, and ATT&CK-aligned analytics that prevent material cyber loss.

CORE COMPETENCIES

Detection & Response: Detection Engineering, Threat Hunting, MITRE ATT&CK, Incident Response (IR/DFIR), Purple Teaming, Behavioral Threat Analytics, Breach & Attack Simulation (BAS), Data Loss Prevention (DLP), Alert Triage, Playbook Development

SIEM / SOAR: Microsoft Sentinel, CrowdStrike NGSIEM, Azure Logic Apps, KQL (Kusto Query Language), Analytic Rule Tuning, Log Source Onboarding, Detection-as-Code

EDR / XDR / MDR: CrowdStrike Falcon, Microsoft Defender for Endpoint, Microsoft Defender XDR, Microsoft Defender for Cloud, Endpoint Hardening

Cloud & Identity: Microsoft Azure, Entra ID (Azure AD), Hybrid Identity (Entra Connect), On-Prem Active Directory Integration, Directory Synchronization, Intune, Purview, IAM / PAM / PIM, Just-in-Time (JIT) Access, Conditional Access, MFA / SSO, Zero Trust Architecture

DevSecOps & Cloud-Native Security: Docker, Kubernetes (K3s / K8s), Container Hardening, Infrastructure-as-Code Security (OpenTofu / Terraform, Ansible), Kustomize / Helm, CI/CD Security, Supply-Chain Security (SCA), Vulnerability / CVE Management, Image Scanning (Trivy / hadolint), Zero Trust Network Access (ZTNA)

Vulnerability & Attack Surface: Qualys, Defender for Vulnerability Management, External Attack Surface Management (EASM), Cloud Security Posture Management (CSPM), Threat Modeling, Risk Assessment

Programming & Automation: Python, KQL, PowerShell, Bash, Go, Rust, Infrastructure-as-Code (OpenTofu / Terraform, Ansible), REST APIs, JSON / YAML, Git, CI/CD Pipelines, DAST

Offensive & Forensics Tooling: Burp Suite, Nmap, Wireshark, Kali Linux, Active Directory, Group Policy

Frameworks & Compliance: NIST CSF, NIST 800-53, ISO 27001, SOC 2, PCI-DSS, HIPAA, GDPR

PROFESSIONAL EXPERIENCE

Security Analyst II - Novolex 2026 - Present

Charlotte, NC | $9B+ revenue | Fortune 200 | scope exceeds title

Acting as lead architect/engineer for a full greenfield enterprise security stack - SIEM, SOAR, EDR, and internal MSSP-style multi-tenant operations. Official title Security Analyst II; ownership and scope are at the architecture-lead level.

- Architecting a multi-tenant Microsoft Sentinel SIEM (delegated workspace model) with tenant isolation, cross-tenant detection federation, and RBAC governance - centralizing operations across independently governed business units.
- Engineering Detection-as-Code pipelines (IaC/GitOps) to version, test, and promote analytic rules, hunt queries, and watchlists across tenants - cutting content-promotion cycle time from days to minutes.
- Designing multi-tenant log ingestion (DCR normalization, per-tenant enrichment, ingestion-tier cost controls) standardizing onboarding and optimizing platform spend.
- Building an internal MSSP-style operating model - standardized tenant onboarding, detection baselines, and SOAR playbooks delivered as repeatable, auditable units.

Security Analyst II (Acting Director of Security Operations) - Novolex 2025 - 2026

Charlotte, NC | $9B+ revenue | post-merger integration of 15 entities

Engineered and scaled an enterprise SIEM/SOAR platform integrating 40+ log sources with normalization, enrichment, and Logic Apps automation, reducing MTTD/MTTR by 60% and SOC operating costs by 20%. Designed end-to-end security architecture for a multi-tenant cloud environment; serve as incident response lead, validating controls through adversary emulation and driving operational readiness across all acquired business units.

- Directed rapid EDR/MDR deployment - integrating 60+ security technologies and rolling out CrowdStrike Falcon and Microsoft Defender for Endpoint across 11,000 assets in under 100 days, establishing a hardened endpoint baseline in a greenfield environment.
- Architected secure-by-design controls (least-privilege IAM, compliance-aligned guardrails, resilient telemetry, AI/ML detection pipelines), reducing aggregate enterprise risk exposure by 90%.
- Directed end-to-end incident response across identity, network, endpoint, and business teams, reducing potential incident impact by $5M+ annually.
- Unified SOC operations across 15 acquired businesses by standardizing SIEM/SOAR platforms, detection content, and IR playbooks, delivering centralized visibility and consistent enterprise-wide threat coverage.
- Partner directly with the CISO and CIO on cybersecurity strategy, board-level reporting, and Zero Trust roadmap execution across all business units.
- Designed an incident response tabletop exercise (TTX), streamlining the hiring process and capability validation for Security Analysts.

Security Analyst II - Pactiv Evergreen 2023 - 2025

Lake Forest, IL | Fortune 200 | $5B+ revenue | 13,000 identities | 8,000 endpoints

Promoted from analyst into a full-time engineering role as the organization's first dedicated cybersecurity engineer. Managed SIEM and SOAR platforms, developing behavioral threat analytics, designing automated response workflows, and building threat-hunting dashboards. Partnered directly with the CISO to stand up the security organization from the ground up.

- Optimized detection and response by re-engineering SIEM pipelines and tuning analytic logic - cutting SIEM ingestion costs 40%, accelerating MTTR 2.5x, and cutting false-positive volume 3x.
- Engineered and scaled SOAR automation across 11,000 endpoints and 25,000 identities using KQL and conditional Azure Logic Apps workflows, driving 22,000+ automated incident resolutions and 12,000+ response actions.
- Built and maintained a MITRE ATT&CK-mapped detection content library - analytic rules, hunt queries, and watchlists - expanding technique coverage and accelerating proactive threat hunting.
- Authored a 92-page situational Incident Response Plan and accompanying automated playbooks, aligning orchestration with human decision points, regulatory obligations, and enterprise risk objectives.
- Strengthened identity security with JIT access via Azure PIM, risk-based Conditional Access through Entra ID Protection, and removal of local admin rights, reducing identity attack surface by 45%.
- Performed systemic threat modeling and attack-surface assessments across Active Directory, EASM inventories, internet-facing applications, and executive impersonation vectors, reducing exploitable risk by 60%.
- Mentored junior analysts and engineers, established SOC standard operating procedures, and represented security in change-advisory boards, vendor evaluations, and architecture reviews alongside CIO leadership.

Security Analyst - Pactiv Evergreen 2021 - 2023

Lake Forest, IL | Fortune 200 | $5B+ revenue | 13,000 identities | 8,000 endpoints

Served as a frontline, advanced SOC analyst specializing in deep forensic investigations, threat hunting, and high-fidelity incident response across cloud, identity, and endpoint domains. Played a key role in maturing detection capabilities by reducing false positives, operationalizing threat intelligence, and establishing repeatable investigative standards.

- Performed advanced forensic analysis across endpoint (EDR), identity (Azure AD/Entra ID), and cloud telemetry to reconstruct attack timelines, identify root cause, and scope enterprise-wide impact.
- Executed hypothesis-driven threat hunting aligned to adversary TTPs (MITRE ATT&CK), uncovering previously undetected persistence mechanisms and lateral movement activity.
- Led hands-on incident response for high-severity events (phishing, credential compromise, malware, privilege escalation), coordinating containment, eradication, and recovery actions.
- Developed and standardized SOC SOPs and designed comprehensive investigative dashboards (Sentinel Workbooks).
- Integrated and operationalized external threat intelligence feeds into SIEM workflows, enriching detections and enabling proactive identification of emerging threats.
- Tuned SIEM detection logic and correlation rules to significantly reduce false positives while increasing detection fidelity and signal-to-noise ratio.
- Collaborated with engineering teams to translate investigative findings into durable detection improvements and automated response enhancements.

Integration Technician - Business IT Source 2015 - 2017

Vernon Hills, IL

Leveraged a mechanical engineering background, technical writing, and Six Sigma methodology to optimize IT workflows while integrating hardware with existing infrastructure across 6+ Fortune 500 organizations. Provided on-site integration and process consulting, delivering reliable system implementations in enterprise environments.

- Seamless integration of commercial compute resources into enterprise technology infrastructure.
- On-site engineering and customer management.

KEY PROJECTS

Endpoint Detection & Response

- Microsoft Defender, CrowdStrike, and DLP agent configuration for 11,000 endpoints.
- Consistent detection, prevention, and response capabilities.
- Enhanced threat visibility and strengthened endpoint protection.

Microsoft Sentinel - Multi-Tenant Architecture

- Centralized security monitoring and detection across distributed cloud and on-premises environments.
- Scalable log ingestion, cross-tenant data integration, and detection engineering workflows supporting unified threat visibility.
- Automated response ensuring consistent security governance across the enterprise.

MDR Architecture

- Threat detection in depth - 2,000 unique MITRE ATT&CK TTP-based alerts.
- MTTR reduction - 50%.
- Enterprise visibility - single pane of glass for query and remediation spanning 12+ SaaS solutions.
- Automated response across endpoints, identities, and cloud environments.

Cloud-Native Security & DevSecOps (Self-Directed)

- Ship services as digest-pinned, non-root, read-only-rootfs containers with all Linux capabilities dropped and no-new-privileges enforced, meeting a restricted container-security baseline.
- Gate every image build on hadolint linting and Trivy vulnerability scanning (fail-on-Critical), backed by an automated CVE-tracking workflow that watches upstream base images and proposes digest bumps.
- Provision and operate hybrid-cloud infrastructure as code (OpenTofu, Ansible, Kustomize/Helm) on K3s/Kubernetes and Docker, with Cloudflare Zero Trust Network Access (ZTNA) tunnels replacing inbound exposure.
- Integrate hybrid identity - Microsoft Entra ID with on-premises Active Directory via Entra Connect - for unified authentication across cloud and self-hosted services.

EDUCATION

B.B.A., NSA-Certified Cyber Security Program - University of Texas at San Antonio 2018 - 2021

Focus: Business Management, Operating System Hardening, Malware Analysis, Python Scripting

PROFESSIONAL DEVELOPMENT & TRAINING

Completed training, exam-preparation coursework, and certificates of completion across cloud security, security operations, and offensive disciplines. These reflect continuing professional development and self-directed study - not held certifications. Certificates of completion for individual courses are available on request.

- AZ-500 Azure Security Engineer - Microsoft (coursework)
- SC-200 Security Operations Analyst - Microsoft (coursework)
- SC-100 Cybersecurity Architect - Microsoft (coursework)
- Cybersecurity Analyst (CySA+) - CompTIA (coursework)
- PenTest+ (V11 & V12) - CompTIA (coursework)
- Certified Ethical Hacker (CEH) - EC-Council (coursework)
- Computer Hacking Forensic Investigator (CHFI) - EC-Council (coursework)
- Security Essentials (GSEC) - GIAC (coursework)
- Incident Response for Management - Mandiant
- Creative Red Teaming - Mandiant
- ITIL 4 Leader: Digital & IT Strategy - Axelos
- APIs & API Design with Python