Keith M. Soncrant

DFW, TX
linkedin.com/in/keith-soncrant
github.com/soncsec

Strategic cybersecurity leader with 20+ years of experience partnering with executives to build, scale, and transform security organizations across Fortune 500, federal, and DoD environments. Built and led security programs ranging from three-person specialist teams to enterprise organizations of more than 200 personnel, creating operating models, capabilities, and investment strategies aligned with business needs and risk tolerance. Proven track record driving enterprise security strategy, organizational design, operational excellence, and cross-functional execution across people, process, and technology. Transformed reactive security operations into intelligence-driven Detection & Response programs, increasing detection coverage 3,000% and reducing mean time to respond 92% at Zscaler. Combines deep expertise in threat intelligence, threat hunting, incident response, malware analysis, cloud security, and security operations with executive communication, Board reporting, strategic planning, budget and vendor management, and strong business acumen.

EXPERIENCE

Zscaler Dec 2022 – Present
Director of Detection and Response • Remote

- Partner closely with the CISO to drive strategic initiatives, organizational planning, and operational execution across Corporate Security and Product Security functions.
- Build and lead a global Detection & Response organization protecting over 100,000 endpoints and 200,000 cloud assets across multi-cloud and on-premises environments.
- Develop and execute multi-year security strategy and operating plans, increasing detection coverage by 3,000% while reducing mean time to respond by 92%.
- Lead organizational design, mission definition, staffing strategy, and operational readiness assessments supporting the expansion of Corporate Security and Product Security capabilities.
- Manage planning and execution of the CISO organization's operational budget, ensuring strategic investment alignment and effective resource allocation.
- Lead the development of agentic triage platform to automatically perform 70% of analysis for all incidents as well as review analyst output to ensure consistent quality analysis and provide real-time situational awareness for leadership and all analysts.
- Oversee strategic vendor relationships, contract evaluations, and technology partnerships to maximize security capabilities and organizational value.
- Coordinate cross-functional strategic planning initiatives for the CISO organization, aligning security priorities with business objectives and executive leadership expectations.
- Prepare executive-level presentations, board materials, and customer-facing briefings communicating security strategy, Detection & Response capabilities, and organizational maturity.
- Report enterprise security posture, operational readiness, and strategic risk initiatives to executive leadership and the Board of Directors on a quarterly basis.
- Lead technical due diligence and capability assessments supporting Corporate Security acquisitions and strategic integration efforts.
- Establish governance frameworks aligning detection and response capabilities with MITRE ATT&CK, CIS, and internal security standards while driving measurable operational improvements.
- Transform the Security Operations Center operating model from an outsourced MSSP to a globally distributed 24x7 organization with standardized processes and consistent service delivery.
- Drive operational excellence through automation, AI-enabled workflows, and Agile-inspired execution models, reducing analyst workload by 35%, accelerating detection engineering by 90%, and increasing detection output by 400% year over year.
- Serve as executive incident commander for major cybersecurity events, coordinating cross-functional crisis response efforts and executive decision-making across the organization.
- Lead annual executive tabletop exercises and crisis simulations to strengthen enterprise resilience and executive preparedness for cyber incidents.
- Worked closely with product managers to drive Zscaler product development to better support SecOps use cases. Heavily involved in the development of the Agentic SOC (ASOC) product development and release.

Equifax Aug 2018 – Dec 2022
Cyber Operations Transformation Lead (VP Level) • Remote

- Led team development, collaboration, training, process improvement and Intelligence Driven Defense fusion for 130+ analysts across 8 functional areas.
- Led activities to push maturity of the overall cybersecurity program forward through development of people, process and technology — overseeing a NIST CSF increase from 1.4 to 3.6.

• Reduced response efforts by 50% while increasing capabilities through improved intelligence collection and analysis automation which expanded capabilities to identify and address threats specific to Equifax and similar financial institutions.

• Standardized analysis techniques and quality evaluations to improve analytical methods ensuring quality analysis for every investigation — improving evaluation scores from an average of 6.5 to 9.9/10.

• Transformed and integrated vulnerability assessment, penetration testing, intelligence processing, mitigation development and incident response processes to be threat-focused and measurable.

• Led skill assessments and training program creation to build new and expand existing talent within the organization — resulting in the creation of 2 new functional areas and increasing program headcount by 450%.

Revolutionary Security June 2017 – Aug 2018
Senior Security Consultant • Remote

• Transformed reactive SOCs into proactive, intelligence-driven Security Intelligence Centers (SICs).

• Evaluated and improved security postures for international corporations using the NIST Framework, providing short and long-term recommendations across all security facets.

Lockheed Martin / Leidos Cyber Jan 2004 – June 2017
Cyber Intelligence Analyst Staff • Ft. Worth, TX / Remote

• Progressed through four roles over 13 years, from founding member of the LM CIRT team to Staff-level Cyber Intelligence Analyst supporting enterprise and customer-facing operations.

• Architected and delivered a comprehensive Enterprise Security program from the ground up, spanning 12+ functional domains including policy governance, security architecture, IAM, vulnerability management, TPRM, SAST/DAST, and wireless security — establishing control standardization, secure coding standards, and security technology selection criteria adopted enterprise-wide.

• Served as technical lead throughout, partnering with customer success teams to ensure operational readiness and long-term program sustainability across enterprise and customer-facing environments.

• Led the LM Aeronautics Malware program performing static and dynamic analysis of APT specimens and delivering company-wide mitigation indicators.

• Collaborated with CISOs and CIOs at major organizations to assess security capabilities, develop maturity roadmaps, and lead on-site incident response for APT intrusions.

• Designed and delivered custom training programs in incident response, intelligence management, malware analysis, signature development, and endpoint forensics.

• Led red team penetration testing against critical systems using known APT techniques, and developed system/network integrity tooling for malware detection.

• Built Intelligence Driven Defense principles into all IT security aspects throughout Lockheed Martin.

TECHNICAL PROFICIENCIES

Frameworks & Methodologies	MITRE ATT&CK, Intelligence Driven Defense (IDD), NIST CSF, CIS Controls, Kill Chain Analysis
Security Operations	SOC/SIC Design, Threat Hunting, Incident Response, Detection Engineer, Intelligence Management, Attack Emulation, Forensics, Malware Analysis, Reverse Engineering, Penetration Testing, Threat Research
Tools & Platforms	SIEM (Splunk, Chronicle, ELK), SOAR (XSOAR, Chronicle, ServiceNow SecOps), EDR, Cloud Security Platforms
Cloud & Infrastructure	AWS, GCP, Azure, Private Cloud, On-prem, Federal/DoD Infrastructure
Programming Languages	C/C++, Java/JavaScript, Python/PHP, SQL, HTML/CSS, Bash, VB
Leadership & Process	Security Program Transformation, Mentorship, Agile-lite, Tabletop Exercise Facilitation, Analyst Training & Development

CERTIFICATIONS

CISSP • CEH

EDUCATION

Texas A&M University — College Station, TX Jan 2002 – Dec 2002
Master of Computer Science • Emphasis in Network Security and Distributed Computing

Texas A&M University — College Station, TX Sep 1998 – Dec 2001
Bachelor of Science, Computer Science • Minor in Business – Emerging Technologies