REDEYE

CYBERSECURITY · ENGINEERED

CAPABILITIES STATEMENT 2026

SIEM Engineering | AI-Augmented Security Operations | ICS / OT Specialty

Matt Lucas, CEO and Owner
matt@redeyesecurity.com
629-249-5437 · redeyesecurity.com
7115 Southpoint Pkwy Ste 5, Brentwood, TN 37024

UEI	CAGE	PRIMARY NAICS	SAM.GOV	BUSINESS SIZE
CYYLN9Z8NUP9	21QF9	541512	Active registration	Small business

COMPANY OVERVIEW

RedEye Security is a Tennessee cybersecurity firm built on 15 years of enterprise SIEM architecture and security operations at Raytheon, Securonix and GuidePoint Security. Its flagship product, Caver, is a production-grade log analytics engine organizations self-host without per-seat licensing or vendor lock-in, and it ships with Carbide, RedEye's own EDR.

RedEye layers AI-augmented operations on top: automated alert triage, LLM-assisted detection authoring and agentic response pipelines that multiply analyst capacity. As a niche specialty it extends the same SIEM and detection-engineering depth into ICS and OT environments, including water utilities, energy and critical infrastructure, where its own scanner and industrial-protocol expertise produce current, local exposure intelligence. It also monitors the radio layer of a control environment: the SCADA radio links that sit before the firewall and outside every network segment, a plane no IP-based OT tool or SIEM can see.

CORE CAPABILITIES

SIEM architecture and engineering. Design, implementation and optimization of Splunk, Microsoft Sentinel, Securonix, QRadar, Elastic and Devo environments. ATT&CK-driven data-source gap analysis, detection-as-code pipelines and measurable reductions in alert fatigue.

Security data-platform engineering. OCSF-normalized security data lakes, federated search via Caver, detection-as-code with backtesting, and cloud-native log pipeline architecture on AWS, Azure and GCP. Detection-content migration from Sigma, Splunk, Elastic, Sentinel, QRadar and Defender into Caver, with a coverage report on what did and did not carry.

AI-augmented security operations. LLM-assisted detection authoring, automated alert triage, incident summarization and analyst force-multiplication through Etairos, RedEye's AI and automation division. RAG-enabled threat-hunt workflows and agentic response runbooks.

vCISO and cybersecurity program management. NIST CSF 2.0 program leadership, risk register, governance cadence and executive reporting. Annual risk assessments, tabletop exercises, phishing simulation and workforce training aligned to compliance requirements.

Vulnerability assessment and penetration testing. IT network, application and cloud-infrastructure testing with exploitability-weighted, prioritized remediation. Zero Trust architecture review and DevSecOps integration.

Threat intelligence and research. Continuous collection on exposed attack surfaces and active campaigns. CVE and CISA KEV correlation against client-specific environments, adversary profiling and ATT&CK-mapped coverage-gap analysis. RedEye is a CVE Numbering Authority.

ICS / OT security, the niche specialty. Active and passive scanning and decoded-protocol monitoring for Modbus, DNP3, EtherNet/IP, OPC UA, BACnet, S7comm, IEC-104, IEC 61850 (GOOSE/MMS) and PROFINET. CISA KEV correlation for industrial assets, IEC 62443 architecture, and engagement models aligned to federal grant programs (CWSRF, DWSRF, FEMA HSGP) for water and energy utilities.

RF-layer OT monitoring. Rural and remote OT sites report over unlicensed SCADA radio, a link that is before the firewall, outside every network segment and never on the internet. RedEye senses that spectrum with a receive-only sensor that never transmits, decodes the traffic (with the customer's own radio key where a link is encrypted) and correlates it with network and log telemetry on one timeline. Delivered today as an OT radio assessment; continuous in-platform monitoring is in development.

Telecommunications security and AI voice. Security architecture for VoIP, SIP and WebRTC infrastructure. AI-powered call handling, natural-language IVR and real-time transcription through CallingEdge.

Continuous monitoring and incident response. OCSF-normalized telemetry ingestion, asset-aware enrichment and SOC-workflow integration. Managed detection and response with Carbide EDR. Incident response planning, tabletop exercises and signed-PDF regulatory reporting (EPA, AWIA, NJCCIC).

DEVELOPED TECHNOLOGIES

Caver 4.36. Self-hosted log analytics: five query languages (SPL, SQL, KQL, ES|QL, LSQL) plus Sigma, 5,000+ detection rules and 430+ vendor content packs, detection-as-code and federated search. OCSF Parquet on S3-compatible storage at a measured 48:1 against raw ingest. Flat per-deployment license, no per-GB ingest charge.

Carbide EDR. Included with Caver and RedEye MDR at no extra cost. No kernel driver: user-mode ETW on Windows, eBPF CO-RE on Linux, macOS in development. OCSF into the same lake; kill, isolate and quarantine over a separate authenticated response channel.

Caver Industrial and Clinical. Add-ons on the same engine. Industrial: ATT&CK for ICS, Purdue-zone rollup and device-identity decode for Modbus, DNP3, EtherNet/IP, S7comm, BACnet and IEC 104. Clinical: PHI access review, patient journey and controlled-substance reconciliation.

Etairos.ai and CallingEdge. Etairos is RedEye's AI business-services platform: multi-tenant agentic workflows, LLM orchestration and CRM integration, in production across several verticals. CallingEdge is its AI voice platform on WebRTC and production VoIP.

PAST PERFORMANCE

SECTOR	STATUS	SCOPE
Federal civilian agency	Active	Cybersecurity and Splunk SIEM engineering support for agency infrastructure, as a subcontractor to a large IT prime.
Commercial IT services	2022 to 2025	Cybersecurity and security-engineering services under a services agreement. RedEye's largest engagement by value.
Commercial advertising	Active, 2022 to present	Managed security services: security monitoring, incident response and endpoint protection under a managed-services agreement.
Commercial IT services	Complete, 2024	Cybersecurity and security-engineering services under purchase order.

Customer names, contract values and reference contacts are released to primes and contracting officers on request, subject to RedEye's customer-reference release. Partners: BlastWave, Johnson Controls, telemetri.ai.

Principal background, individual rather than corporate: Raytheon (RTX) SIEM architecture and detection engineering for defense programs; Securonix platform engineering across financial services, healthcare and federal; GuidePoint Security consulting for commercial and government clients; Auto-Owners Insurance SIEM architecture and AI implementation; InvestCloud SIEM engineering and team management. Currently CEO and owner of RedEye Security.

WHY REDEYE

We build the tools we deploy.
Caver, its collector and Caver Industrial are production systems RedEye builds, not vendor configurations. Clients get no per-seat licensing and a team that understands the stack from the bit to the dashboard.

We see the radio layer.
OT security tools watch network traffic and SIEMs watch logs. Neither senses the SCADA radio link an attacker can read from the fence line with an inexpensive receiver. RedEye senses that spectrum, receive-only, and correlates it with the network and the logs on one timeline.

ICS / OT fluency is native.
Modbus, DNP3, EtherNet/IP, OPC UA, IEC-104, IEC 61850, PROFINET and IEC 62443 are core competencies. Caver's agent workforce needs no language model, so it runs in an isolated environment and can be assessed as controls rather than taken on faith.

Grant-aligned from day one.
Pricing and program structures align with CWSRF, DWSRF, FEMA HSGP and IIJA funding. RedEye helps clients apply for the grants that pay for the work, not just respond after funding is secured.

ENTITY INFORMATION

LEGAL NAME RedEye Security LLC	ENTITY TYPE Tennessee LLC, small business	PRINCIPAL Matt Lucas, CEO and Owner
UEI CYYLN9Z8NUP9	CAGE 21QF9	SAM.GOV Active registration
PRIMARY NAICS 541512, Computer Systems Design	ADDITIONAL NAICS 541519, 541690, 561621	PSC CODES D310, D307, DA10, R425
SOCIOECONOMIC Small business; not SDVOSB, HUBZone, 8(a) or WOSB	CVE PROGRAM CVE Numbering Authority (CNA), RES	TAUD Associate Member (FY 2026-2027)

COMPLIANCE POSTURE, STATED PLAINLY

- Cleared vSOC staff. No facility clearance.
- No FedRAMP authorization, no ATO, no IL listing.
- No CMMC certification and no completed SOC 2 audit; practices only.
- No GSA MAS or OASIS+ vehicle held.
- Caver self-classified ECCN 5D002, License Exception ENC; standard published cryptography only, no ITAR content.
- Anthropic Cyber Verification Program participant, Defense Access.

FRAMEWORKS AND STANDARDS

NIST CSF 2.0 | NIST SP 800-82 | IEC 62443 | MITRE ATT&CK | ATT&CK for ICS | OCSF | Zero Trust | AWIA / EPA | NERC CIP | PCI-DSS | CMMC 2.0 practices