REDEYE
CYBERSECURITY · ENGINEERED

CAPABILITIES ONE-PAGER 2026

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

Matt Lucas, CEO and Owner
matt@redeyesecurity.com
629-249-5437 · redeyesecurity.com
Brentwood, TN 37024

UEI	CAGE	NAICS	PSC	ENTITY
CYYLN9Z8NUP9	21QF9	541512, 541519, 541690, 561621	D310, D307, DA10, R425	RedEye Security LLC, Tennessee LLC

BUSINESS SIZE	SOCIOECONOMIC	SAM.GOV	CVE PROGRAM	TAUD
Small business	None held: not SDVOSB, HUBZone, 8(a) or WOSB	Active registration	CVE Numbering Authority (CNA), RES	Associate Member, TAUD (FY 2026-2027)

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 and extends the same detection-engineering depth into ICS and OT, including the SCADA radio layer that sits before the firewall and outside every network segment.

CORE CAPABILITIES

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

Security data-platform engineering. OCSF-normalized security data lakes, federated search via Caver, detection-content migration from Sigma, Splunk, Elastic, Sentinel, QRadar and Defender with a coverage report on what did and did not carry.

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

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 and PROFINET. CISA KEV correlation for industrial assets. IEC 62443 architecture.

RF-layer OT monitoring. A receive-only sensor that never transmits, decoding unlicensed SCADA radio traffic and correlating it with network and log telemetry on one timeline. Delivered today as an OT radio assessment; continuous in-platform monitoring is in development.

vCISO, assessment and response. NIST CSF 2.0 program leadership, risk register and executive reporting; network, application and cloud penetration testing with exploitability-weighted remediation; continuous monitoring, IR planning and tabletop exercises.

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. 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: ATT&CK for ICS, Purdue-zone rollup and device-identity decode for Modbus, DNP3, EtherNet/IP, S7comm, BACnet and IEC 104; PHI access review and controlled-substance reconciliation.

Etairos and CallingEdge. Etairos is RedEye's AI and automation division, agentic workflows and LLM orchestration in production; CallingEdge is its AI voice platform.

PAST PERFORMANCE AND REFERENCES

RedEye holds corporate past performance as a company, including active federal work performed as a subcontractor to a large IT prime, plus commercial managed-security, insurance and IT-services engagements. Customer names, values and reference contacts are released on request, subject to RedEye's own 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; InvestCloud SIEM engineering and team management in fintech. Currently CEO and owner of RedEye Security.

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.

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