REDEYE
CYBERSECURITY · ENGINEERED

CAPABILITIES ONE-PAGER 2026 · TEAMING WITH SIEMTUNE (CSITCO LLC)

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

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

UEI	CAGE	NAICS	PSC
CYYLN9Z8NUP9	21QF9	541512, 541519, 541690, 561621	D310, D307, DA10, R425

ENTITY	BUSINESS SIZE	SOCIOECONOMIC	SAM.GOV
RedEye Security LLC, Tennessee LLC	Small business	None held: not SDVOSB, HUBZone, 8(a) or WOSB	Active registration

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 Splunk-compatible log analytics engine organizations self-host without per-seat licensing or vendor lock-in. 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, Splunk-compatible 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 2.5. Self-hosted, Splunk-compatible log analytics engine. Full SPL plus four transpiled query languages, detection content across 185 vendor packs, OCSF-normalized data lake, federated search, and an agent workforce of 36 named workers, none requiring a language model. Flat per-deployment license, no per-GB ingest charge.

Caver Industrial and Clinical. Two add-ons on the same engine. Industrial carries the ATT&CK for ICS matrix, Purdue-zone rollup and nine decoded industrial protocols. Clinical carries PHI access review, patient journey and controlled-substance reconciliation.

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

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.

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; current Sr. SIEM Engineer and team manager at InvestCloud.

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.

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

HOW REDEYE AND SIEMTUNE COME TO A PRIME

Two subcontractors to one prime, each in its own lane, neither working through the other. SIEMtune (CSITCO LLC d/b/a SIEMtune) is an SBA-certified SDVOSB and HUBZone small business, both certified 07/08/2026, and carries a Top Secret cleared principal. RedEye carries corporate past performance and a fielded SIEM platform. The pairing answers the two questions a prime asks a new sub: the socioeconomic credit its subcontracting plan needs, and a delivery record behind it. Neither company holds a facility clearance, so FCL-required work is out of scope for the pairing.