Matt Lucas

Cybersecurity Leader, SIEM Architect, AI Engineer

(540) 257-3635 Matt@RedEyeSecurity.com linkedin.com/in/mattlucas719 Nashville, TN

SUMMARY

Senior cybersecurity and AI engineering leader with 15+ years building enterprise SIEM platforms, AI-driven security operations, and autonomous AI systems. Deep expertise spanning SIEM engineering, cloud security architecture, AI/ML operations, and critical infrastructure protection.

TECHNICAL SKILLS

AI & MACHINE LEARNING

LLM tool use & function calling, prompt engineering & caching, MCP server development, autonomous AI agent orchestration, retrieval-augmented generation (RAG), pgvector embeddings, natural language processing (NLP), predictive analytics, AI cost optimization

SIEM & SECURITY

Splunk Enterprise/ES, Securonix, Azure Sentinel, SOAR, ICS/SCADA (Modbus, DNP3, EtherNet/IP, OPC UA), PCI/PHI compliance, NIST CSF, IEC 62443, threat detection, incident response

CLOUD & INFRASTRUCTURE

AWS (EC2, S3, VPC, GovCloud), Azure, Terraform, Ansible, Docker, Cloudflare, Vercel, CI/CD (Jenkins, GitLab, GitHub Actions), Kubernetes

DEVELOPMENT

Python, Bash, TypeScript, Next.js, React, Node.js, PostgreSQL, Supabase, REST APIs, WebSocket, GraphQL

AUTOMATION & ORCHESTRATION

n8n, Salt, Chef, Puppet, Ansible, LDAP, Nagios, custom AI dispatch frameworks

COMMUNICATION PLATFORMS

Twilio (WhatsApp, SMS), Telegram Bot API, Bland.ai (AI voice), ElevenLabs TTS, WebRTC, SIP/RTP, VoIP/IVR

INDUSTRIES

Government & Defense | Financial Services | Healthcare | Critical Infrastructure | Telecommunications | SaaS / Enterprise Software

PROFESSIONAL EXPERIENCE

AI Engineer (Independent Projects)

Independent / Nashville, TN

- Lead end-to-end AI integration strategy for SMBs, designing and deploying LLM-powered solutions that automate operations across sales, customer service, scheduling, and internal workflows
- Architected and built a multi-tenant AI platform (Next.js 14, Supabase, LLM APIs) serving multiple business verticals with per-client AI agents, knowledge bases, and tool integrations
- Engineered 50+ custom AI tool functions enabling LLM agents to interact with Google Workspace, Microsoft Graph, HubSpot CRM, CompanyCam, and other business APIs
- Implemented prompt caching strategies reducing AI API costs by 60-80% on input tokens
- Built multi-channel AI communication layer spanning web chat, Telegram, WhatsApp, SMS, and AI voice (Bland.ai + ElevenLabs TTS)
- Designed and deployed per-customer AI agent infrastructure on AWS (Terraform, Packer, Ansible)
- Built an AI dispatch framework using n8n for zero-lock-in agent orchestration: GitHub issues as work orders, Telegram approval gates, AI coding agents for execution
- Developed passive OT network monitoring solutions with protocol-aware threat detection across Modbus, DNP3, EtherNet/IP, S7comm, OPC UA, and BACnet
- Designed ICS/SCADA assessment methodology aligned with NIST CSF, IEC 62443, and AWWA cybersecurity guidance

---

Sr. SIEM Engineer / Team Manager

InvestCloud / West Hollywood, CA / August 2022 – Present CURRENT

- Lead AI-driven automation initiatives integrating LLM capabilities with Splunk workflows to accelerate threat detection, triage, and response
- Design and implement CI/CD pipelines for all Splunk code using Git, Jenkins, and Ansible, enabling repeatable deployments across global infrastructure
- Architect multi-layered, scalable Splunk Enterprise deployments in public cloud across multiple countries, navigating complex data sovereignty and access regulations
- Build and maintain disaster recovery with high availability across VPC regions leveraging SHC, SmartStore, and indexer clustering
- Manage PCI and PHI datasets with granular role-based access controls and compliance auditing
- Lead team operations following Agile methodology with sprint planning, scrum ceremonies, and backlog orchestration
- Develop automation to reduce manual SIEM operations, improving team efficiency and reducing mean time to detection
- Lead zero-downtime upgrade processes for production Splunk architecture systems

Sr. Splunk Engineer

World Wide Technologies (WWT) / St. Louis, MO / March 2023 – September 2023 CONTRACT

- Designed and implemented automation for upgrading multiple large-scale Splunk cluster environments (200+ TB daily ingestion each) with zero downtime
- Engineered custom SHC Deployer mechanisms with error detection and logic validation, fully integrated with CI/CD via Git
- Built a Splunk Deployment Server cluster with configuration replication sourced from Jenkins and Ansible through Git
- Performed full risk assessments across all Splunk components
- Created centralized dashboards leveraging REST APIs to monitor and manage application loads on Splunk DS forwarder deployments

---

Sr. SIEM Engineer / Team Manager

Securonix / Nashville, TN / February 2022 – August 2022

- Managed and grew a cybersecurity team delivering SIEM solutions (Splunk, Securonix, Sentinel), automation, and cloud architecture (AWS/Azure)
- Provided full architectural assessment of forwarding architecture, design topology, and data routing strategies across on-premise and cloud environments
- Drove complex advances in Securonix, working directly with customers to solve unique security use cases
- Served as Securonix SME for technical questions, escalations, and multi-tenant deployment architecture
- Engineered DevOps automation for Securonix deployment, monitoring, health status, and QA processes
- Delivered SIEM solutions architecture with focus on scalable growth, performance tuning, and expanded analytics capabilities

---

Team Manager, SIEM Cyber Defense SME

Raytheon / Dulles, VA / October 2018 – February 2022

- Led and scaled the VSOC team, driving profitability and operational effectiveness
- Set team goals, performed quarterly evaluations, and coordinated cross-team resource sharing across VSOC, ProServ, Analysts, and Threat Hunters
- Managed hiring pipeline, conducting technical interviews for Splunk engineering roles
- Supported and maintained SIEM deployments with focus on optimization, usability, and environment visibility
- Developed and maintained practice documentation including methodologies, SOPs, reporting templates, and sales collateral
- Integrated new architectural features into existing infrastructures and provided analysis of cybersecurity trends for future needs
- Reviewed SIEM configurations for compliance with RCS and industry best practices

Sr. Splunk Engineer & Sr. Cloud Architect

GuidePoint Security / Reston, VA / February 2018 – October 2018 CONTRACT

- Built cloud automation leveraging Terraform, Ansible, and Demisto to manage and deploy scalable AWS environments
- Established GitLab-based workflows for standardized automation across multiple client environments
- Served as SME on Splunk and various security technologies, guiding the company on emerging security strategies
- Integrated enterprise toolsets to improve team productivity and customer response time (PagerDuty, Demisto, Splunk, AWS, Slack)

Sr. Splunk Engineer

Securities Exchange Commission / Washington, DC / August 2017 – February 2018 CONTRACT

- Implemented and administered Splunk and Splunk Enterprise Security Suite for federal regulatory operations
- Designed data ingestion pipelines and security visualizations for the Enterprise Security Suite
- Built and integrated contextual data into notable events and workflow automation within Splunk ES
- Designed hybrid cloud architecture for source flexibility and scalability
- Established GitLab-based automation procedures for full environment management

CONCURRENT CONTRACT ENGAGEMENTS

Independent Consultant / Contract Engineer

October 2011 – October 2018 CONTRACT

Sr. Splunk Engineer - Adobe (via Defense Point Security)

Alexandria, VA / October 2016 – August 2017

- Designed and built Splunk environments spanning hybrid internal and Azure/AWS deployments across every cloud region and multiple geographic data centers
- Automated all infrastructure provisioning using Salt and Git
- Led migration from QRadar to Splunk with 100% data migration at 10+ TB/day indexing rate
- Designed peer review code deployment workflows compliant with PCI and HIPAA guidelines
- Mentored employees on enterprise Splunk usage and developed repeatable deployment scripts

Splunk Engineer - General Electric

Glen Allen, VA / March 2015 – October 2016

- Enhanced and verified Splunk Enterprise Security implementations
- Designed hybrid cloud solutions across Verizon, Azure, and Amazon environments
- Built Chef-based automation for server deployment across local and cloud infrastructure
- Managed DNS and F5 BIG-IP/HAProxy for high-volume traffic distribution across continents
- Maintained and upgraded large clustered environments with hundreds of real-time users

Splunk Developer - TIAA-CREF

Charlotte, NC / March 2014 – February 2015

- Architected Splunk solutions for auditing production platforms at enterprise scale
- Designed high-availability clustered environments with performance-optimized configurations
- Created complex dashboards for diverse end-user needs across the organization

Sr. Voice Engineer - City of Houston

Houston, TX / March 2014 – April 2017

- Provided recommendations and direction for city-wide VoIP solutions
- Served as SME and primary point of contact for enterprise-level VoIP architecture
- Built and trained a support team for long-term city infrastructure maintenance

Sr. VoIP & Ops Engineer - Computer Sciences Corporation (CSC)

Chantilly, VA / October 2011 – October 2018

- Designed and implemented redundant international VoIP solutions for the Department of State
- Designed and managed Splunk for large-scale data management, alerting, and dashboards
- Served as SME for enterprise Splunk deployment strategies including peering replication
- Managed large CentOS server clusters with high-availability using Chef, Ansible, and custom automation
- Led migration from on-premise to AWS hybrid deployments

Support Engineer Supervisor, Tier 2

Voxeo / Orlando, FL / October 2010 – October 2011

- Supervised support operations for customers with on-premise VoIP and IVR solutions
- Trained Tier 1 personnel on technologies, customer interaction, and escalation procedures
- Designed and deployed Nagios monitoring across 8 data centers and cloud environments
- Served as Splunk SME, designing dashboards and migrating customer data from multiple sources
- Designed cloud migration strategies from physical data center servers to AWS