Garrett Spear

AI-READY CYBERSECURITY ENGINEER PRINCIPAL

Bossier City, LA
garrett.spear@outlook.com
(318) 663-8900
LinkedIn • @ garrettdspear
GitHub • @ garrettds11
Website • www.garrettspear.info

Lead IC specializing in detection engineering, SOC automation, and AI-ready security workflows in multi-tenant managed security environments, with an MBA-driven focus on business impact, service design, and operational efficiency.

HIGHLIGHTS

2 Degrees

5 Active Organizations

9 Certifications

9 Years in Cybersecurity

19 Years in the workforce

KEY FOCUS AREAS

Detection Engineering
Security Automation
Threat Intel Enrichment
Agentic AI Foundations
Vulnerability Assessment
MSSP Operations
Web Design
Cloud-native Microservices
AI Ops Integration

CORE TOOLS

Splunk Enterprise Security
Qualys
AWS
GCP
Generative AI Tooling

SUMMARY

Principal-level cybersecurity engineer with nearly 9 years in MSSP/SOC environments (all at GDIT), specializing in detection engineering, analytic operations, security automation, and threat intelligence enrichment. Designs and operates SIEM workflows, enrichment pipelines, adaptive response actions, and orchestration patterns that prepare organizations to integrate LLMs and agentic AI into threat detection, investigation, and vulnerability-aware defense. Combines deep technical execution with MBA-level business acumen, aligning security engineering, automation, and platform design with service strategy, operational efficiency, and customer value.

PROFESSIONAL EXPERIENCE

(SMB) Director — Technology & Market Strategy Oct 2025 – Present

Revelation Escapes Ministry • 501(c)(3) Nonprofit Organization

Business Operations | Market Analysis | Process Optimization | Service Design

- Direct operational strategy and internal processes for a nonprofit entertainment and community-oriented venue, emphasizing customer experience quality, service flow optimization, and operational reliability.
- Conduct structured market analysis to identify local demand, competitive positioning, pricing strategies, and opportunities for differentiated service offerings aligned with the organization's mission.
- Evaluate throughput, capacity planning, and staffing models to support peak-hour scheduling, resource utilization, and operational efficiency.
- Guide the improvement of customer-facing digital experiences, including website structure, reservation flows, and SEO-aligned enhancements.
- Support financial decision-making by analyzing revenue patterns, cost structures, and operational data to recommend improvements aligned with nonprofit stewardship principles.
- Identify opportunities for workflow automation, data-informed decision support, and streamlined management practices based on MBA coursework and service design strategy.

(SMB) Solution Architect/Engineer — Platform R&D May 2025 – Present

VulnServer Labs LLC (owner)

AI-Ready | Automation | Business & Strategy | Cloud | DevOps | Market Analysis | Security | Service Design | Web App

- Architect and engineer a cloud-native cybersecurity lab and ethical hacking platform focused on automation, multi-tenant workloads, frontend and backend development, and an AI-assistant service.
- Designed an event-driven orchestration system using AWS Amplify, Lambda, API Gateway, EC2/ECS, DynamoDB, S3, CloudFront, and SES to manage provisioning, lifecycle control, and environment teardown.
- Developed structured YAML API specifications aligned with OpenAPI-style contract principles to standardize service interactions and ensure reliable frontend–backend integration.

PROFESSIONAL CERTIFICATIONS

AWS Certified AI Practitioner (in progress)
Splunk Enterprise Security Certified Admin
Splunk Core Certified Advanced Power User
Splunk Certified Cyber Security Defense Analyst (CDA)
CrowdStrike Falcon Administrator

Vendor-neutral
ISC2 CISSP (in progress)
CompTIA CySA+ CE
CompTIA Network+ CE
CompTIA Security+ CE
CompTIA CASP+ CE (expired)
ITIL 4 Foundations
NSA CNSSI Certificate of Senior Systems Manager

EDUCATION

Master of Business Administration
Louisiana State University Shreveport
Class of 2026 – Present

B.S., Computer Networking & Cybersecurity
University of Maryland Global Campus
Class of 2021 – Graduate

A.A.S., Network Security
Bossier Parish Community College
Class of 2017 – Graduate

TECHNICAL SKILL AREAS

Security & Automation
Splunk ES, Splunk SOAR, correlation searches, risk-based alerting, IOC enrichment, adaptive response actions, workflow actions, cyber threat intel integration/automation, detection tuning, Swagger OpenAPIv3.1, Stainless MCP

Languages & Platforms
SPL (Splunk), RegEx, JSON, YAML, Terraform, Git, HTML/CSS, JavaScript/Node, Python, PowerShell, Bash, Linux, Windows, Docker, GitHub, HTTP/REST APIs, Google Cloud (GCP), Amazon Web Services (AWS), Terraform

- Built Terraform-based infrastructure-as-code modules to automate deployment, ephemeral lab environment creation, key management, and destruction of short-lived workloads.
- Implemented a secure magic-link authentication workflow using signed tokens, session fingerprints, and cookie-bound controls to prevent unauthorized access and link sharing.
- Integrated Stripe checkout with backend automation to generate session metadata, trigger lab provisioning events, and enforce time-bound (8-hour) environment lifecycles.
- Developed backend structures to support future LLM-assisted evaluation, including scoring rubrics, model-selection logic, and structured data pipelines for AI-driven feedback.
- Created vulnerable applications and simulated exploitation paths (SQLi, authentication flaws, chained attack vectors) to support detection engineering and analyst training.
- Built a secure full-stack web interface for lab access and control, implementing modular TypeScript/JavaScript UI components, authentication flows, interactive dashboards, and real-time status polling.
- Implemented CI/CD pipelines using GitHub Actions for automated testing, build generation, artifact packaging, S3/CloudFront deployments, versioning, and cache invalidation to support rapid iteration.
- Defined service positioning, pricing concepts, and academic/enterprise integration scenarios, using MBA coursework and market analysis to align platform capabilities with target customer segments and sustainable operations.

(Enterprise) Cybersecurity Engineer Principal
Sep 2024 – Present

General Dynamics Information Technology • Principal Detection Engineer (Lead IC)

AI-Ready | Automation | Cloud | Customer Outcomes | Security | Service Strategy | Splunk

- Lead analytic engineering for a multi-tenant Splunk ES deployment, including correlation searches, data models, and risk logic for managed security customers.
- Built API-driven enrichment workflows integrating AbuseIPDB, VirusTotal, and other OSINT sources for search-time and alert-time enrichment.
- Developed workflow actions and adaptive response actions in Splunk ES and custom apps to automate enrichment and hand-off to SOAR pipelines.
- Developed API-driven enrichment and automation patterns, integrating external threat intelligence sources and Splunk ES adaptive response actions into SOC workflows.
- Designed foundations for agentic, AI-assisted SOC workflows, including orchestration patterns and session-based enrichment structures to support future LLM integration.
- Created dashboards and operational reports that expose coverage, alert quality, and threat trends for MSSP customers, supporting leadership decision-making and service improvement.
- Led high-risk triage, guided incident response, and supported threat hunting across multi-tenant environments.
- Contributed to technical solution design and strategic modernization proposals for cyber operations and automation initiatives, aligning engineering efforts with business goals and customer expectations.

(Enterprise) Cybersecurity Analyst Advisor (Content Engineer)

Sep 2023 – Sep 2024

General Dynamics Information Technology

Automation | Customer Outcomes | Incident Response | Security | SOC Leadership | Splunk | Threat Intel

- Served as lead IC for Splunk ES analytic operations and incident response for the TSS managed security platform.
- Developed detections for exploitation attempts, threat behaviors, and high-fidelity correlation searches.
- Operationalized threat intelligence by integrating IOC sources and aligning detection logic to observed adversary tactics.
- Designed and delivered tabletop and micro-tabletop exercises to build SOC analyst skills and response muscle memory.
- Performed lead incident response duties, including triage, scoping, and threat hunting.

(Enterprise) Security Operations at GDIT/CSRA

Feb 2017 – Sep 2023

USGovSOC, Cloud Services, Technology Shared Services

- Shortened for brevity; additional experience available upon request.
- Developed the TSS Computer Security Incident Response Plan.
- Served in SOC Tier I, II, and III roles in managed security services operations since CSRA.

PROJECTS & TECHNICAL LEADERSHIP

Kalico — AI Command Line Utility for Debian

2025

AI-Ready | Dev | CLI Tooling | Linux

- Designed a modular AI-assisted command line utility for Debian-based systems to streamline security, research, and automation workflows from the terminal.
- Implemented a core orchestration layer with pluggable subcommands, shared configuration, and reusable prompt/response handling across local and remote LLM backends.
- Integrated support for local LLM runtimes and HTTP-based remote models using structured YAML configuration, enabling environment-specific behavior without code changes.
- Established patterns for command “contracts” (status, help, config, run) to keep behavior predictable, testable, and easy to extend as new AI-powered workflows are added.

SecureTTS — Text-to-Speech Web App

2025

Cloud | Web App | APIs | Security | AI-Ready

- Designed a secure text-to-speech system using AWS Lambda, API Gateway, DynamoDB, and event-driven pipelines.
- Implemented authentication, key-scoped API access, and secure token workflows for private audio generation.
- Built the UI and API for generating, storing, and retrieving audio files within controlled access boundaries.

GeoVive — Geospatial Charting Web App

2025

Cloud | Web App | Geospatial | Data Pipelines | AI-Ready

- Created a map-based intelligence platform for event tracking, entity mapping, and data enrichment workflows.
- Built ingestion pipelines, schema designs, and UI prototypes for geospatial overlays and multi-source data fusion.
- Developed backend logic to support structured event metadata (who/what/where/when) for analytical workflows.

(SMB) Faith & Fire — E-Commerce Website

2024–Present

Web | E-Commerce | Brand & Sales | UX

- Developed an e-commerce presence for handcrafted seasonings and grilling products.
- Built interactive product pages, automated invoicing flows, and order-tracking integration.
- Optimized digital branding, page structure, and mobile responsiveness for online sales.

TimeLogr — Timesheet Management System

2025

Web App | Business Logic

- Designed a multi-role time tracking system supporting employees, managers, and admins with audit logging.
- Implemented workflow logic for draft → submitted → approved → reopened states with justification enforcement.
- Built structured logging models capturing actions, reasons, IP address, and client fingerprinting.

(SMB) CPBC Web Services — Digital Infrastructure Lead and Finance Team Member

2023–Present

Web | Content Ops | Streaming | Ops Support

- Built and maintained a church website, digital content workflows, and live service streaming architecture.
- Developed automation for schedule updates, event posting, and content publishing driven by structured data.
- Improved SEO, accessibility, and site reliability through continuous refinement and monitoring.

ScrapeWeb — Electron/Puppeteer Blog Metadata Scraper for Desktop

2024 – 2025

Automation | Desktop App | Web Extraction | Security-Oriented Tooling

- Developed a cross-platform Electron desktop application using Puppeteer to extract structured metadata from blog articles and documentation pages.
- Designed a scraping pipeline to capture titles, authors, descriptions, canonical URLs, update timestamps, and other meta-tag fields, with fallbacks for inconsistent site structures.
- Implemented JSON and Markdown export options with timestamped filenames, a directory picker, and a modular renderer for future output types.
- Integrated a modern UI with improved button styling, hover transitions, window resizing behavior, and embedded branding assets.

- Added auto-update functionality using electron-updater, including progress events, restart prompts, and GitHub release integration.