

James Morton

Senior Security Engineer, Threat Detection

☎ (512) 555-6842 ✉ james.morton@example.com
🌐 linkedin.com/example/jamesmorton 📍 Austin, TX 78704

STRENGTHS

- 🎯 **Detection lifecycle ownership**
Led hypotheses from data validation through deployment, tuning, measurement, and retirement. Investigators gained cleaner signals and clearer decisions.
- 📊 **Security data analysis**
Used Python and SQL on large datasets to find behavior that routine alert review missed. Those findings shaped useful hunts.
- 🔧 **Reliable delivery**
Introduced Git review, automated testing, CI/CD, and observability. Releases became easier to trust, even during busy response periods.
- 👥 **Practical collaboration**
Worked beside Security Operations during incidents, exercises, and code pairing. Shared context early, which made hard decisions easier.
- ♥️ **Responsible AI evaluation**
Tested LLM, agentic, and MCP workflows with attention to permissions and failure modes. Risk stayed visible before automation moved forward.

SKILLS

Threat detection MITRE ATT&CK
Detection as code Python SQL
SIEM Git CI/CD AWS Linux
Containers EDR Airflow
Terraform Anomaly detection

LANGUAGES

English Native

SUMMARY

Senior **threat detection** and security engineer with 10 years of experience building signals, telemetry pipelines, **detection content**, and security automation across cloud, endpoint, identity, email, and application environments. Advanced Python and SQL practitioner, using large security datasets for baselining, validation, behavioral analytics, anomaly detection, and retrospective threat hunting. Leads **MITRE ATT&CK** aligned detection lifecycles from hypothesis through deployment, tuning, measurement, and retirement, with clear **false positive thresholds**. Builds detection as code through Git, peer review, automated testing, CI/CD, observability, and reliable production workflows. Partners with Security Operations on investigations, incidents, tabletop exercises, attack simulation, and code pairing. Communicates technical decisions through RFCs, documentation, presentations, and practical risk analysis.

EXPERIENCE

Senior Threat Detection Engineer

Ironwood Cloud Systems 📅 March 2023 - Present 📍 Austin, TX

Leads detection engineering across cloud, endpoint, identity, email, and application telemetry. Owns production content, pipeline reliability, AI assisted security evaluation, and partnerships with Security Operations.

- Built ATT&CK aligned detections across five telemetry domains, reducing noisy alerts through measured thresholds.
- Applied Python and SQL baselines across large datasets, exposing subtle behavioral signals for **retrospective scans**.
- Moved **detection as code** through Git review, automated tests, CI/CD, and safer production releases.
- Improved AWS, EDR, identity, and **application pipelines** with enrichment and observability, revealing coverage gaps.
- Evaluated LLM, agentic, and secure MCP workflows, documenting permissions, exposure, limitations, and failure modes.
- Supported investigations, incidents, **tabletop exercises**, attack simulations, code pairing, and detection maintenance with **Security Operations**.

Security Detection Engineer

Mesa Digital Infrastructure 📅 January 2020 - February 2023 📍 Denver, CO

Developed detection content and telemetry integrations for distributed infrastructure. Guided hypothesis testing, threat intelligence enrichment, alert tuning, and operational handoff across security engineering and response teams.

- Converted **threat intelligence** into ATT&CK detections and retrospective scans, giving investigators clearer hunting paths.
- Used Python and SQL behavioral analysis to baseline identities, endpoints, and **cloud** workloads before deployment.
- Created Git workflows with **peer review** and automated validation, shortening safe detection release cycles.
- Integrated AWS, EDR, and application telemetry with enrichment logic, improving visibility across investigations.
- Applied **anomaly detection** and **feature engineering** to separate unusual activity from expected business behavior.
- Partnered with Security Operations during incidents, exercises, attack simulations, and **detection lifecycle** reviews.

Security Engineer

Lone Star Software Services 📅 June 2017 - December 2019 📍 Dallas, TX

MY CAREER



- Senior Threat Detection Engineer at Ironwood Cloud Systems (3.5 Years)
- Security Detection Engineer at Mesa Digital Infrastructure (3.1 Years)
- Security Engineer at Lone Star Software Services (2.5 Years)
- Security Analyst, Detection and Response at Frontier Commerce Technologies (7 Months)

- Built foundational security engineering capabilities across cloud and enterprise environments. Delivered **detection content**, **data onboarding**, automation, and incident support while documenting architecture decisions and operational tradeoffs.
- Built cloud and endpoint detections from threat hypotheses, validating data quality before production rollout.
 - Queried large security datasets with Python and SQL, turning behavioral findings into actionable detection logic.
 - Introduced Git based content review and **automated testing**, improving confidence in deployment changes.
 - Expanded **telemetry ingestion** across AWS, Linux, containers, identity, and email sources for broader coverage.
 - Documented detection architecture through RFCs, presentations, and operational guides for engineering partners.
 - Supported malware analysis, **digital forensics**, incident investigations, and **response automation** during security events.

Security Analyst, Detection and Response

Frontier Commerce Technologies 📅 October 2016 - May 2017 📍 San Antonio, TX

Supported detection and response operations through alert analysis, threat hunting, **data validation**, and incident documentation. Worked with senior engineers to improve signal quality and investigation speed.

- Validated **endpoint**, **identity**, and email telemetry against threat hypotheses, improving investigation context.
- Used SQL and Python for alert analysis, surfacing recurring behavior that informed new detections.
- Maintained SIEM dashboards and **advanced queries**, helping analysts prioritize actionable security **signals**.
- Assisted retrospective hunts across cloud and application data, connecting threat intelligence with observed activity.
- Documented incident findings, **tuning** decisions, and response steps for repeatable Security Operations workflows.
- Joined tabletop exercises and attack simulations, recording detection gaps for later engineering work.

PROJECTS

AI Assisted Detection Evaluation 📅 2025

Tested LLM, agentic framework, and secure MCP workflows for detection support. Documented permissions, data exposure, model evaluation, failure modes, and safe response automation decisions.

Detection as Code Reliability Program 📅 2024

Built a practical Git, peer review, automated testing, CI/CD, and observability workflow for detection content. Improved release confidence while preserving clear tuning and retirement decisions.

Behavioral Threat Hunting Pipeline 📅 2022

Combined Python, SQL, Airflow, anomaly detection, and feature engineering for repeatable retrospective scans across large security datasets and enriched telemetry.

LEADERSHIP & AWARDS

- GIAC Certified Incident Handler recognized for incident response depth and practical investigation leadership.
- Security Detection Engineering Award for advancing reliable ATT&CK aligned content and production validation.
- Technical Leadership Recognition for clear RFCs, code pairing, mentoring, and cross team delivery.

EDUCATION

Bachelor of Science in Computer Science

Texas State University 🎓 GPA: 0 📅 2016 📍 San Marcos, TX

Coursework: *Operating systems, databases, network security, software engineering*

CERTIFICATIONS

- GIAC Certified Incident Handler (GCIH) 📅 2019
- AWS Certified Security - Specialty 📅 2022

TECHNICAL SKILLS

- **Programming and Querying:** Python, SQL, Go
- **Detection Engineering:** MITRE ATT&CK, detection as code, false positive tuning
- **Source Control and Delivery:** Git, CI/CD, peer review
- **Cloud Security:** AWS, IAM, CloudTrail
- **Operating Systems:** Linux, Windows, shell scripting
- **Containers and Infrastructure:** Docker, Kubernetes, Terraform
- **Security Analytics:** SIEM, dashboards, advanced queries
- **Endpoint Security:** EDR, endpoint telemetry, response automation
- **Data Pipelines:** Airflow, Databricks, telemetry ingestion
- **AI Security:** LLMs, agentic frameworks, MCP
- **Threat Analysis:** threat intelligence, threat hunting, attack simulation
- **Behavioral Analytics:** anomaly detection, feature engineering, model evaluation

PROFESSIONAL AFFILIATIONS

- Active security engineering contributor focused on detection quality, threat hunting, and practical automation.
- Professional participant in incident response, cloud security, and threat intelligence communities.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST