Kingston Mcguire

Senior Incident Response Analyst

(512) 555-0184 | kingston.mcguire@example.com | linkedin.com/example/kingstonmcguire | Austin, TX 78701

STRENGTHS

Incident leadership
During ransomware matters, kept counsel, analysts, and client IT aligned; calm updates helped teams make timely decisions.

Forensic reasoning
When evidence conflicted, compared host, memory, and network clues until timelines separated confirmed compromise from suspicion.

Client communication
Translated technical findings for executives and counsel, giving stressed stakeholders clear choices and practical next steps.

Analyst mentoring
Coached four analysts through command-line triage and evidence handling; peers gained a reliable resource for difficult investigations.

Operational improvement
Turned recurring investigation lessons into hunting queries and playbooks, helping responders work with greater consistency.

SKILLS

Incident response | Digital forensics | Host forensics | Network forensics | Cloud incident response | Ransomware | Business email compromise | Funds transfer fraud | APT analysis | EDR | Threat hunting | Network protocols | Packet analysis | Remediation planning | Client communication

SUMMARY

Senior **incident response** analyst with five years of cybersecurity experience across SOC operations, **digital forensics**, cloud investigations, and client-facing DFIR consulting. Leads investigations across Windows, macOS, Linux, AWS, Azure, and GCP environments, connecting technical evidence with practical containment and recovery decisions. Handles ransomware, **business email compromise**, **funds transfer fraud**, APT activity, EDR telemetry, network logs, and large-scale indicator hunting. Clear reports and briefings help executives, counsel, and IT teams act during high-pressure incidents. Mentors analysts, improves playbooks, manages concurrent client matters, and contributes to knowledge sharing through workshops and technical presentations. Ready to help a collaborative incident response team protect clients, guide sound decisions, and improve resilience before, during, and after security events.

EXPERIENCE

Senior Incident Response Analyst

Redwood Shield Advisory | January 2025 - Present | Austin, TX

Leads concurrent DFIR engagements for ransomware, BEC, and targeted intrusion matters. Coordinates analysts, outside counsel, client IT teams, and cloud evidence workflows across a remote matrixed consulting model. Guides investigation quality, remediation planning, reporting, mentoring, and internal knowledge development.

- Led **ransomware** investigations through executive readouts, aligning analysts, counsel, and **client IT** teams.
- Collected host and network evidence across **Windows**, **macOS**, Linux, AWS, Azure, and GCP environments.
- Built **remediation plans** from **EDR**, authentication, firewall, and cloud audit evidence for client recovery.
- Translated forensic findings into concise reports and briefings that supported decisions during urgent incidents.
- Mentored four analysts on command-line triage, evidence handling, indicator development, and quality reviews.
- Created hunting queries and playbook content that improved consistency across large, urgent investigations.

Incident Response Analyst

Blue Mesa Digital Defense | January 2023 - December 2024 | Dallas, TX

Managed client investigation workstreams for mid-market organizations, from prospective scoping through containment decisions and after-action reporting. Applied forensic analysis across endpoint, memory, disk, network, identity, and cloud evidence while coordinating ticket queues, project plans, client updates, and **escalation** decisions.

- Scoped prospective engagements by documenting affected users, hosts, accounts, and cloud resources before containment.
- Examined disk images, memory captures, endpoint telemetry, and **network logs** to establish intrusion timelines.
- Investigated **ransomware** precursors, credential misuse, **funds transfer fraud**, and mailbox compromise for client teams.
- Used EDR analytics, **PowerShell**, DNS, proxy data, and **packet analysis** to identify attacker activity.
- Produced findings and remediation recommendations that connected technical evidence with business risk and operational priorities.
- Maintained ticket queues and project plans while meeting client updates and evidence milestones during stressful matters.

Security Operations Analyst

Cypress Ridge Security Operations | September 2021 - December 2022 | Plano, TX

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Senior Incident Response Analyst at Redwood Shield Advisory (1.7 Years)
- Incident Response Analyst at Blue Mesa Digital Defense (1.9 Years)
- Security Operations Analyst at Cypress Ridge Security Operations (1.2 Years)

Supported distributed customers through SOC monitoring, first-line incident triage, evidence preservation, and escalation package development. Used EDR, SIEM, email security, Windows logs, Linux command-line tools, DNS records, and network telemetry to separate routine activity from credible threats.

- Monitored EDR, **SIEM**, email security, and network alerts for distributed customer environments.
- Triaged suspicious authentication, endpoint, and email events using **Windows** logs and **Linux** command-line tools.
- Built escalation packages with timelines, affected assets, observables, and recommended containment steps for responders.
- Preserved evidence and performed basic forensic review for phishing, **BEC**, malware, and unauthorized access cases.
- Created detection tuning recommendations from recurring false positives and emerging attack patterns for SOC analysts.
- Presented incident patterns during team reviews and updated response runbooks and knowledge base content.

PROJECTS

Cloud Incident Response Playbook 2025

Turned recurring AWS, Azure, and GCP investigation lessons into practical triage paths, evidence checklists, escalation points, and client-ready recommendations for cloud incidents.

Large-Scale Indicator Hunt 2024

Built a repeatable hunt using EDR telemetry, DNS records, authentication events, and network logs to connect suspicious activity across client environments.

LEADERSHIP & AWARDS

- Cybersecurity Program Excellence Award, University of North Texas, 2021
- National Cyber League Individual Scouting Report, Gold Tier, 2021
- Dean's List, University of North Texas, Fall 2020 and Spring 2021

EDUCATION

Bachelor's Degree in Cybersecurity

University of North Texas GPA: 3.8 2021 Denton, TX

Coursework: *Digital Forensics, Network Security, Incident Response, Cloud Security*

CERTIFICATIONS

- GIAC Certified Incident Handler (GCIH) 2024
- Microsoft Certified: Security, Compliance, and Identity Fundamentals 2022

TECHNICAL SKILLS

- **Incident Response:** DFIR, ransomware response, BEC investigations
- **Digital Forensics:** Disk imaging, memory analysis, evidence handling
- **Endpoint Detection:** EDR telemetry, endpoint analytics, detection review
- **Security Monitoring:** SIEM, email security, alert triage
- **Network Analysis:** Wireshark, packet analysis, network logs
- **Cloud Security:** AWS, Azure, GCP
- **Operating Systems:** Windows, macOS, Linux
- **Command Line:** PowerShell, Bash, command-line investigation
- **Threat Hunting:** Indicator development, hunting queries, IOC analysis
- **Identity Analysis:** Authentication events, credential misuse, mailbox compromise
- **Network Protocols:** DNS, HTTP, TCP/IP
- **Reporting Tools:** Technical reports, executive briefings, after-action summaries

PROFESSIONAL AFFILIATIONS

- DFIR Study Group Mentor, Austin Security Professionals Association, 2025 - Present
- Volunteer Incident Response Workshop Presenter, Central Texas Cyber Alliance, 2024 - Present

- Cybersecurity Club Case Competition Team, University of North Texas, 2019 - 2021

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST