Mila Aguirre

Incident Response Analyst

(312) 555-0186 mila.aguirre@protonmail.com
linkedin.com/example/milaaguirre Chicago, IL 60614

STRENGTHS

Evidence-Based Analysis
During ransomware reviews, tied conclusions to artifacts and timelines so incident leaders could act with confidence.

Clear Technical Writing
Converted complex findings into concise explanations and playbooks; reviewers relied on wording during high-pressure cases.

Detection Judgment
Challenged noisy SIEM logic with controlled scenarios, helping teams see missing steps and practical escalation points.

Practical Automation
Built small Python and PowerShell utilities for repetitive artifact work; analysts gained more consistent investigation results.

Collaborative Response
Briefed engineers, customers, and commanders in shared reviews, keeping evidence quality and remediation priorities visible.

SKILLS

Incident Response | Digital Forensics | Threat Intelligence | Detection Engineering | Threat Analysis | Vulnerability Assessment | Penetration Testing | Red Teaming | Malware Analysis | MITRE ATT&CK | Technical Writing | AI Content Evaluation | Analytical Skills | Security Coding | English Fluency

SUMMARY

Incident Response Analyst with more than five years of hands-on cybersecurity experience across detection engineering, incident response, digital forensics, threat intelligence, and adversary emulation. Evaluates **AI-generated security content** with evidence-based judgment, testing **threat analysis**, **vulnerability assessments**, **offensive security techniques**, and defensive recommendations against realistic investigations. Uses Python, PowerShell, SQL, Splunk, Microsoft Sentinel, Velociraptor, Wireshark, Sigma, and MITRE ATT&CK to build repeatable scenarios, validate detection logic, and explain technical findings clearly. Leads investigations across endpoint, identity, cloud, and network telemetry, then turns evidence into practical remediation guidance for engineers, incident commanders, customers, and reviewers. GCIH-certified with a bachelor's degree and native-level English communication. Ready to help Canyon Ridge AI produce more accurate, reliable cybersecurity reasoning through careful analysis, clear writing, and practical security experience.

EXPERIENCE

Senior Incident Response Analyst

Red Harbor Cyber January 2025 - Present Chicago, IL

Leads incident-response investigations across endpoint, identity, cloud, and **network telemetry** while creating AI evaluation scenarios, forensic utilities, detection tests, and concise technical critiques for security leaders.

- Built adversary-emulation prompts that tested AI security reasoning across **ransomware** and credential-abuse scenarios.
- Created **Python** utilities that normalized forensic artifacts and produced repeatable detection-validation cases for reviewers.
- Challenged Splunk and **Microsoft Sentinel** detections against **MITRE ATT&CK**, exposing gaps and false positives.
- Critiqued **vulnerability assessments** and offensive-security recommendations, separating exploitable findings from unsupported assumptions.
- Briefed incident commanders on evidence quality, escalation conditions, and remediation priorities during high-pressure reviews.

Incident Response Analyst

Northstar SOC Services May 2023 - December 2024 Evanston, IL

Investigated managed-services alerts across endpoint, email, and identity systems, combining DFIR collection, **threat intelligence**, detection development, customer writing, and repeatable analysis exercises.

- Correlated SIEM events, EDR telemetry, and authentication records to resolve endpoint and identity alerts.
- Used **Velociraptor** and Wireshark to reconstruct attack timelines and preserve artifacts for **DFIR** review.
- Developed Sigma rules and **Splunk** searches that tested phishing, **PowerShell** abuse, and persistence coverage.
- Mapped threat-intelligence indicators to **MITRE ATT&CK** before recommending containment actions for customer investigations.
- Authored incident summaries and playbooks that translated technical evidence into usable customer guidance.
- Created Python parsers for logs and packet captures, reducing repetitive analysis across investigation exercises.

Cybersecurity Analyst

Meridian Digital Forensics May 2021 - April 2023 Oak Park, IL

LANGUAGES

English — Native

Spanish — Proficient

MY CAREER

- Senior Incident Response Analyst at Red Harbor Cyber (1.7 Years)
- Incident Response Analyst at Northstar SOC Services (1.6 Years)
- Cybersecurity Analyst at Meridian Digital Forensics (1.9 Years)

Supported **incident triage** and forensic examinations for small and mid-sized organizations, validating alerts, reviewing vulnerabilities, documenting evidence, and presenting findings to security stakeholders.

- Reviewed **endpoint** images, **cloud** audit records, and suspicious email artifacts during supervised response cases.
- Applied structured methods to identify initial access, execution, persistence, and lateral movement activity.
- Queried **Microsoft Sentinel** and Splunk data to validate alert logic and prepare senior escalations.
- Performed **Nmap** and **Burp Suite** reviews that separated confirmed vulnerabilities from unverified risk hypotheses.
- Wrote evidence timelines and remediation notes that helped client teams reproduce investigation findings.
- Presented threat-intelligence summaries and post-incident lessons learned to distributed security response teams.

PROJECTS

AI Security Reasoning Evaluation Library 2025

Created reproducible adversary-emulation and incident-analysis scenarios for testing AI-generated threat analysis, defensive reasoning, vulnerability claims, and investigative completeness.

Detection Validation Exercise Framework 2024

Combined Sigma, Splunk, Microsoft Sentinel, Python, and MITRE ATT&CK methods into repeatable exercises for measuring detection quality.

Forensic Artifact Analysis Toolkit 2023

Built parsing workflows for endpoint artifacts, packet captures, and authentication records, producing clear timelines and evidence-based response notes.

LEADERSHIP & AWARDS

- Cyber Defense Club Outstanding Case Analysis Award, 2021
- Northeastern Illinois University Dean's List, 2020
- Cybersecurity Capstone Showcase Finalist, 2021

EDUCATION

Bachelor's Degree in Cybersecurity

Northeastern Illinois University GPA: 3.8 2021 Chicago, IL

Coursework: *Incident response, digital forensics, network security, ethical hacking, malware analysis*

CERTIFICATIONS

- GIAC Certified Incident Handler (GCIH) 2024
- CompTIA CySA+ 2022

TECHNICAL SKILLS

- **Programming Languages:** Python, PowerShell, SQL
- **SIEM Platforms:** Splunk, Microsoft Sentinel, SIEM
- **Digital Forensics:** Velociraptor, Windows artifacts, Cloud audit records
- **Network Analysis:** Wireshark, Packet captures, Network telemetry
- **Detection Engineering:** Sigma, Splunk searches, Alert validation
- **Threat Frameworks:** MITRE ATT&CK, Adversary emulation, Threat intelligence
- **Security Testing:** Nmap, Burp Suite, Vulnerability assessment
- **Incident Response:** Incident triage, Containment, Escalation
- **Offensive Security:** Penetration testing, Red teaming, Offensive techniques
- **Endpoint Security:** EDR telemetry, Endpoint images, Windows tools
- **AI Security Evaluation:** AI-generated content, Model reasoning, Technical feedback

PROFESSIONAL AFFILIATIONS

- Cyber Defense Club, Incident Response Workshop Coordinator, 2020 - 2021
- University Cyber Range, Peer Lab Mentor, 2020 - 2021
- Chicago Cybersecurity Meetup, Volunteer Technical Presenter, 2023 - Present

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST