Benjamin Frisanco

Green Bay, WI
+1-906-284-0875
iambenfrisanco@gmail.com
Linkedin.com/in/frisanco/

Incident Response Analyst | Threat Hunter | DFIR Specialist
Experienced in enterprise incident response, threat hunting, and forensic analysis

---

Skills

Incident Response & Threat Detection:
Incident Response, Threat Hunting, DFIR, Malware Analysis, Log Analysis, Cyber Threat Intelligence

SIEM & Detection:
IBM QRadar, Splunk, Elastic, SIEM Use Case Development, MITRE ATT&CK, Detection Tuning, Alert Triage

Tools & Technologies:
Wireshark, Endpoint Detection & Response (EDR), Volatility, API Security, OWASP Top 10

Programming:
Python, SQL, Bash, PowerShell

Systems & Networking:
Network Security, TCP/IP, Active Directory, AWS, Azure

Education

BS Computer Science | *Information Technology Minor*
Michigan State University, East Lansing, MI

Professional Experience

Professional Development — Independent DFIR | Green Bay, WI **07/2025 — Present**

- Conducted simulated incident response investigations across endpoint and memory artifacts, performing threat hunting, malware analysis, and forensic triage in lab environments.
- Performed memory forensics and malware analysis to identify persistence mechanisms, lateral movement, and indicators of compromise.

Salt Security | San Diego, CA & Green Bay, WI **12/2022 — 07/2025**

Senior Cyber Operations Analyst

- Managed large-scale incident response investigations across 100+ enterprise environments, including detection, triage, containment, and remediation.
- Conducted threat hunting and investigative analysis of OWASP API Top 10 attack techniques, identifying malicious behavior, validating impact, and informing response actions.
- Developed Python and MySQL automation to accelerate incident response workflows, forensic data analysis, and investigative triage, reducing analyst effort by 35%.
- Designed automated investigative reporting solutions to deliver clear, client-ready incident findings and prioritized security improvement recommendations, reducing reporting effort by 50%.

Cybersecurity Analyst

- Conducted host- and network-based investigations to triage alerts, analyze suspicious activity, and support containment and remediation.
- Built automated incident triage and forensic enrichment workflows using Python and MySQL, reducing manual investigative effort by 40%.

Professional Development — Career Break | San Diego, CA **06/2022 — 12/2022**

Freelance InfoSec Specialist

- Built and maintained hands-on DFIR labs leveraging Python, Bash, and PowerShell to simulate investigations, analyze malicious behavior, and refine incident response workflows.
- Achieved Top 2% global ranking on TryHackMe (Cyber Defense / Blue Team learning paths).

Dow, Inc. | Midland, MI **01/2020 — 01/2022**

Security Operations Center Analyst

- Conducted enterprise incident response and threat investigations across hybrid IT/OT environments, analyzing endpoint, network, and SIEM telemetry to identify malicious activity and support containment efforts.
- Designed and implemented SIEM detection use cases aligned to the MITRE ATT&CK framework, improving visibility into attacker behavior and enterprise threats.
- Investigated phishing campaigns and social engineering activity, enhancing detection workflows and response procedures across corporate environments.

Project Experience

Malware Research & Threat Intelligence Home Lab

- Architected and maintained a dedicated malware research and threat analysis lab to support hands-on investigation of malicious files, attacker behavior, and post-exploitation techniques.
- Performed static, dynamic, and memory-based malware analysis to identify execution flow, persistence mechanisms, and indicators of compromise
- Documented findings to inform detection logic, threat intelligence reporting, and investigative methodology improvements.

SIEM Tuning and Use Case Development — SASE

- Designed, tested, and tuned SIEM detection use cases for SASE environments, integrating Zscaler telemetry into QRadar to improve visibility into network-based threats.
- Mapped detections to the MITRE ATT&CK framework to enhance investigative context and response prioritization.

Certifications

Cisco CCNA | Cisco CCNA Cybersecurity | AWS Cloud Practitioner | Azure Fundamentals