Kieren Gregory

Crestview, FL

630-828-4926|kgregory1197@aol.com| www.linkedin.com/in/kierengregory|github.com/kgregory2023

SUMMARY: Cybersecurity Master's student with hands-on experience in threat intelligence, penetration testing, and secure software development. Skilled in OSINT, MITRE ATT&CK mapping, and incident triage through red and blue team cyber operations. Security+ certified with proven success in real-world security projects, attack surface analysis, threat analysis and AI-based detection systems. Strong communicator with a passion for translating technical findings into actionable security insights and reports.

EDUCATION

Masters in Cyber Security at The University of West Florida May 2027

Bachelors in Cyber Security with Honors at The University of West Florida May 2025

- Minor in Computer Science
- Cumulative GPA: 3.75/4.0

Associates in Education with Highest Honors at Northwest Florida State College May 2022

- Cumulative GPA: 3.93/4.0: Presidents List in General Education

SKILLS

Cybersecurity Domain Expertise: Threat Detection & Analysis, Pen Testing, Threat Analysis, Vulnerability Assessments, Network Security, Machine Learning ,OSINT
Threat Intelligence & OSINT Tools: BBOT,, WHOIS, Google Dorking, HaveIBeenPwned
Threat Intelligence Frameworks: MITRE ATT&CK Framework, CVE/CWE correlation,log analysis (Kibana, Security Onion)
Platforms: Kali Linux, Metasploit, Wireshark, Burpsuite, Nmap, Scapy, Microsoft 365,Docker, Git, Github,
Security Framework Knowledge: NIST CSF, OWASP Top 10, ISO 27001, PCI DSS
Soft Skills: Leadership, Adaptability, Problem-Solving, Team Collaboration, Analytical Thinking, Attention to Detail
Programming Languages: JavaScript, Python, SQL, Java, C++, Bash Scripting, CSS, Powershell

CERTIFICATIONS

CompTIA Security+ April 2025
Comptia CySA+ (In Progress)

THREAT RESPONSE, OSINT and CYBER EXPERIENCE

Red Team & Blue Team Cyber War Gaming January 2025 - May 2025

- Mapped attacker behavior using t**he MITRE ATT&CK framework (T1046, T1078, T1569.002**) to simulate real-world adversary campaigns.
- Conducted Red Team operations **using Scapy, Nmap, and Burp Suite**; Blue Team response included log analysis, packet inspection, and s**ystem hardening with Suricata**
- Triaged simulated intrusions and **mapped alerts to ATT&CK tactics**, enabling better understanding of ransomware kill chains and lateral movement indicators.
- Documented findings in structured reports for both offensive and defensive exercises, improving incident response accuracy by **30%.**

Open Source Intelligence (OSINT) & Attack Surface Analysis Black Lantern Security Volunteer April 2025

- Conducted real-world OSINT reconnaissance **using BBOT, Nuclei, and Censys** to uncover exposed domains, open ports, and impersonation risks for mock targets.
- Discovered **over 40+ assets using subdomain enumeration**, certificate transparency logs, and historical DNS records.
- Mapped **external attack surface exposure to known CVEs** and correlated potential threats to underground forums and threat actor behaviors.
- Generated actionable intelligence summaries to inform defensive security posture and phishing risk reduction.
- Monitored **leak sites and threat actor forums** to simulate dark web alerting and credential exposure workflows

OSINT Labs TryHackMe **June 2025**
- Completed advanced IMINT and GEOINT challenges using image recognition, reverse search, and open-source platforms.
- Demonstrated investigative techniques across labs like Searchlight IMINT and Sakura Room.

Hack The Box Academy SOC Analyst Labs May 2025 - Present
- Completed hands-on SOC analyst training, simulating live incident triage and real-time threat monitoring using SIEM tools.
- Conducted log analysis and incident response drills using ELK Stack and Splunk to detect and investigate simulated intrusions.
- Monitored and triaged simulated SOC alerts, escalating threats based on structured playbooks to emulate real-world workflows.
- Applied MITRE ATT&CK framework to map attacker behaviors; trained extensively with Splunk, ELK Stack, and Windows Event Logs.

Penetration Testing Report (Kali Linux, Metasploit, Wireshark, Nmap, SMB, Meterpreter) January 2024 - May 2024
- Authored **a 10-page technical report** detailing vulnerabilities, CVEs, and exploit attempts, aligned mitigation strategies to **NIST CSF and OWASP Top 10**, reducing risk exposure by an estimated **70%**
- Mapped a **5-host subnet**, uncovered **16 unique** attack vectors across **12+** services, 4 exploit attempts, executed RCE via EternalBlue
- Discovered and **exploited 2** flaws, **SQL Injection** and **XSS**, exposing risks to authentication bypass and client-side compromise
- Identified exploitable services and **mapped findings to MITRE ATT&CK TTPs** to assess adversary emulation potential.

CYBERSECURITY PROJECTS

DeepCam: Real-Time Deepfake Webcam Defense Monitoring Project (Python, AI Security, ML) May 2025 - Present
- Project demonstrates **practical defense strategies** against deepfake identity spoofing and biometric fraud
- Interfaced with DeepFaceLive to **simulate face swap attacks** for testing detection effectiveness
- Integrating **MediaPipe** Face Mesh to **track eye landmarks and compute** Eye Aspect Ratio (EAR) for liveness validation

Capstone Security Lead Web App Development (JavaScript, Node.js, JWT, CSS) January 2025 - May 2025
- **Led security** design for a networking platform used by **4+ test users**, implementing **JWT** authentication and encrypted session handling
- Designated RBAC logic to **control access** across **2 user tiers**, mitigating unauthorized data exposure in application routes
- Managed a **4 person team** to integrate secure backend logic with frontend usability, ensuring seamless **user experience** and **security alignment**

Secure Software Abuse Case Analysis – Exoskeleton Navigator Aug 2024 - Nov 2024
- **Conducted** threat modeling **using use and abuse cases** to evaluate system safety for wearable navigation systems.
- **Identified 10+ potential attack vectors** including GPS spoofing, firmware tampering, and data theft; proposed **technical** and **policy-based** countermeasures.
- **Drafted** security recommendations **aligned with NIST and OWASP standards**, including MFA, AES encryption, and audit controls for risk mitigation and system integrity.