CHRISTIAN DENIS

📞 (305) 607-7196 | ✉️ Crisden14@gmail.com | 🔗 linkedin.com/in/christian-denis-4a2495195 | Clearance: Top Secret / SCI | Location: Miami/FL | Open to relocation | Remote & On-site

CYBERSECURITY ANALYST | INTELLIGENCE PROFESSIONAL

Motivated cybersecurity student and experienced Intelligence Analyst with 4 years of analytical and security-focused work in the U.S. Coast Guard. Proven ability to assess threats, manage sensitive information, and deliver actionable insights. Currently pursuing a B.S. in Cybersecurity and GIAC certifications to build on a foundation of secure systems, network defense, and cyber threat analysis.

KEY SKILLS

• Incident Response Lifecycle: Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned
• Log Analysis | SIEM Tools | Event Correlation
• Threat Hunting | Triage | Alert Analysis
• Root Cause Analysis | Forensics | Memory & Disk Imaging
• Malware Analysis (basic) | Indicators of Compromise (IoCs)
• Network Security | Firewalls | IDS/IPS
• Windows & Linux Security | Command Line Proficiency
• Ticketing Systems | Escalation Procedures | Reporting
• Analytical Thinking | Problem-Solving | Cross-Team Collaboration

CERTIFICATIONS

• GIAC GCIH – Certified Incident Handler
• GIAC GSEC – Security Essentials Certification
• GIAC GFACT – Foundational Cybersecurity Technologies
• Top Secret / SCI Clearance (Active)

EDUCATION

SANS Technology Institute— B.S. in Cybersecurity
August 2024 – Present | GPA: 3.0

Southern New Hampshire University — Cybersecurity Studies
February 2022 – July 2024 | GPA: 3.78 | Dean's List & Honor Roll

Miami Dade College — Business Administration
August 2014 – January 2016 | GPA: 2.8

CYBER PROJECTS & ENGAGEMENT

- Hack The Box –

    - Conducted network forensic investigation using a provided PCAP file to trace initial attacker IP, identify malicious payload via SHA256 hash matched in VirusTotal (family: Pikabot), and analyze self-signed TLS certificate metadata (ports, timestamp, localityName). Reconstructed breach timeline, identified data exfiltration indicators, and documented findings using Wireshark and Network Miner.

    - Simulated a SOC Tier 1 investigation of suspicious logon activity and malicious PowerShell execution. Correlated authentication logs, security alerts, and PowerShell transcripts to identify persistence mechanisms, initial access vectors, and attacker IP. Strengthened triage workflow and familiarity with Windows event artifacts.

PROFESSIONAL EXPERIENCE

United States Coast Guard — Intelligence Analyst
February 2021 – February 2025
- Analyzed cyber and physical threat data to support risk assessments, incident response planning, and mission-critical decision-making.
- Transformed raw intelligence into actionable insights to identify patterns, detect emerging threats, and strengthen security posture.
- Ensured the protection of sensitive systems and information through adherence to confidentiality, integrity, and availability (CIA) principles.
- Collaborated with interagency partners and cybersecurity teams to share intelligence, reduce risk exposure, and support proactive defense strategies.

Motor Yacht Industry — Captain / First Mate
November 2017 – February 2021
- Managed navigation, safety, and compliance with maritime laws.
- Oversaw vessel systems, technical maintenance, and crew operations.
- Delivered personalized service to high-net-worth individuals, ensuring privacy and discretion.

Coya Miami — Server
January 2015 – October 2017
- Delivered exceptional customer service in a high-paced environment.
- Honed interpersonal and multitasking skills critical to client-facing roles.