Mihai Ionut Botos

SOC Analyst | Threat Detection | Incident Response

Cluj-Napoca, Romania | harciogul-tehnic@tuta.com | linkedin.com/in/mihai-botos/

PROFILE SUMMARY

SOC Analyst supporting a 23,900-user, 41,000-device enterprise environment — triaging 500+ alerts weekly and managing CVE/vulnerability remediation. Built a SOC-wide phishing-IOC automation that cut triage time ~85% (20-30 min to 2-5 min) across 1,000+ reports/week. Certified in CompTIA Security+ and HTB CDSA (both first-attempt); production experience with Microsoft Sentinel, Defender XDR, KQL, Splunk, and XSOAR. Currently building detection engineering depth (Sigma/YARA, Centri CDEA, Level Effect CDETH) in a self-hosted lab. Marine Corps veteran with an active security clearance.

CORE TECHNICAL SKILLS

SIEM & SOAR: Microsoft Sentinel, Microsoft Defender XDR, Splunk, XSOAR, Kibana, KQL

Network & Endpoint: Suricata, Wireshark, Palo Alto Panorama, Sysinternals Suite

Cloud & Identity: Azure, Sentinel Playbooks, Entra ID, Active Directory Security, Windows Event Analysis

Security Operations: Threat Detection, Incident Response, Phishing Analysis, Vulnerability Assessment & CVE Remediation, Digital Forensics, Malware Triage

Platforms & Tools: Linux (scripting / host triage), Windows, macOS, Git

CERTIFICATIONS

- HTB Certified Security Defense Analyst (CDSA) — June 2024
- CompTIA Security+ (first attempt) — September 2023
- Transmission Systems Supervisor — August 2023
- NGT Cyber Security Associate — July 2023

CURRENTLY DEVELOPING

Building detection engineering depth through a self-hosted home lab (Sigma and YARA rule writing, Snort/Zeek network detection), while pursuing Centri's Certified Detection Engineer (CDEA) and Level Effect's CDETH (Detection Engineering & Threat Hunting: Windows).

PROFESSIONAL EXPERIENCE

Security Operations Center Analyst | SIG Group **March 2025 – Present**

- Triage 500+ security alerts weekly across phishing, endpoint, identity, and cloud sources in a 23,900-user / 41,000-device environment using Microsoft Sentinel, Defender XDR, and Azure telemetry.
- Review automated vulnerability scan findings, apply policy against CVE identifiers, and raise remediation tickets for confirmed exposures.
- Designed and deployed an automated email-IOC workflow, adopted SOC-wide, that extracts and enriches indicators from 1,000+ phishing reports/week, cutting median triage time from 20-30 minutes to 2-5 minutes (~85% faster).
- Built and maintain Sentinel identity-containment playbooks covering all 23,900 users, auto-triggered on every high-severity Microsoft-detected credential-phishing incident.

Security Operations Center Analyst | Betfair Development Romania **March 2024 – March 2025**

- Investigated SIEM/SOAR alerts (Splunk, XSOAR) across a broader, faster-moving threat landscape spanning multiple dedicated security teams, escalating confirmed threats with supporting evidence and remediation guidance.
- Analyzed suspicious network and host activity using Suricata, Palo Alto Panorama, and Active Directory / endpoint telemetry.
- Reviewed phishing reports, documented findings, and coordinated response actions with cross-team security stakeholders; contributed to detection and incident response process improvements.

Team Leader | U.S. Marine Corps **April 2018 – March 2023**

- Led and mentored personnel while maintaining operational readiness, accountability, and mission effectiveness in high-tempo environments; trained 15 personnel and supervised 4, providing hands-on mentorship and performance oversight.
- Planned and implemented secure communication systems supporting military operations, including secure comms support for artillery exercises in the Pacific region; received an excellence award for communication support.
- Improved contingency and emergency response procedures for field communications, and maintained an active security clearance while enforcing disciplined handling of sensitive operational information.

EDUCATION

Southern New Hampshire University (SNHU) — Bachelor's Degree in Cyber Security

GPA: 3.27

NGT Academy — Full Stack Network Associate and Cyber Security Accelerator

Completed 2023