ILYES HAMDI

Ben Arous, Tunisia Ilyes.hamdi@istic.ucar.tn +216-21797806 in/ilyeshamdi github.com/ilyesHamdiii

SUMMARY

Junior blue-team analyst focused on SIEM investigation, Windows/Sysmon log analysis, incident reporting, and CTI-to-detection workflows. Hands-on practice with Elastic/Kibana, Splunk, Wazuh, MITRE ATTACK;, Sigma/YARA, PCAP analysis, and structured SOC case reporting through HTB CDSA labs, internship work, and personal blue-team projects.

SKILLS

Alert triage, IOC analysis, incident timelines, root-cause analysis, escalation notes, remediation reporting

Elastic/KQL, Splunk/SPL, Wazuh, Sigma, YARA, MITRE ATTACK; mapping

Windows Event Logs, Sysmon, PowerShell artifacts, Linux logs, process and network telemetry

PCAP analysis, DNS/HTTP anomalies, C2 detection, Suricata/Snort/Zeek basics

Python, FastAPI, Streamlit, PostgreSQL, Docker, Git, MISP, STIX 2.1

EXPERIENCE

Cybersecurity / CTI Intern

Forvis Mazars Group **June 2026 - July 2026, Tunisia**

- Developing a CTI-to-detection engineering platform that ingests MISP indicators, normalizes IOCs, maps activity to MITRE ATT&CK and produces SOC-ready detection use cases.
- Built analyst workflow for IOC provenance, telemetry readiness, detection gap tracking, and report export.
- Generated Sigma/KQL/SPL-style detection templates for validation in SIEM workflows.
- Documented detection logic, evidence requirements, and analyst handoff notes.

Practical SOC Training

Hack The Box Academy **November 2025 - April 2026, Remote**

- Investigated simulated SOC cases in Splunk and Elastic by correlating Windows Event Logs, Sysmon process activity, network indicators, commandline artifacts, and user/host context.
- Reconstructed attack timelines for phishing, suspicious PowerShell execution, C2 traffic, privilege escalation, and Active Directory-related activity.
- Performed alert triage, IOC extraction, root-cause analysis, MITRE ATTACK; mapping, and incident reporting.
- Wrote detection logic and translated indicators into Sigma/YARA and SIEM queries for review.
- Utilized EDR platforms (CrowdStrike, Microsoft Defender) over 3-month capstone project to analyze endpoint telemetry, identify lateral movement patterns in weekly exercises.
- Monitored IPS alerts and analyzed network intrusion attempts during 12 weekly simulated SOC scenarios using Suricata and Snort to enhance detection accuracy and incident response effectiveness.

PROJECT

GrantScope — Entra ID OAuth & Service Principal Risk Investigator

Personal project · github.com/ilyesHamdiii/GrantScope/tree/public-demo · July 2026 - July 2026

- Built a cloud identity investigation tool to analyze OAuth applications, service principals, permission grants, app credentials, privileged app-role assignments, owners, sign-in activity, and directory audit events.
- Designed correlation logic to identify risky tenant-wide grants, stale or newly added credentials, missing owners, privileged service principals, suspicious consent activity, and unusual app usage patterns.
- Generated analyst-ready case packets with affected users/apps, evidence timeline, risk rationale, remediation steps, and investigation notes for SOC/cloudsecurity handoff.
- Implemented import workflows for evidence bundles and structured findings into cases, suppressions, and reviewable security observations.

Blue-Team Incident Reports

Hack the Box · github.com/ilyesHamdiii/blue-team-portfolio/tree/main/incident-reports

- Produced incident reports covering executive summary, technical timeline, affected assets, evidence, IOCs, ATT&CK; mapping, impact, and remediation.
- Correlated endpoint, authentication, process, network, and IDS evidence to explain attacker behavior and escalation path.

EDUCATION

Bachelor's Degree in Network & Systems

Higher Institute of Information Technologies and Communication · Tunisia · 2024

- Relevant Coursework: Network Security, Operating Systems, TCP/IP, Linux Administration
- Focus Areas: Cybersecurity, System Administration, Network Infrastructure

CERTIFICATIONS

Certified Defensive Security Analyst

Hack the Box · 2026

- Practical certification covering SIEM analysis, alert triage, incident investigation, threat detection, and security reporting.