Panagiotis Kavakopoulos

Greece | +30 6971945096 | panoskava2006@gmail.com
linkedin | github | panoskava.dev

Computer Science undergraduate pursuing opportunities in Security Operations and SOC Analysis. Experience includes investigating over **14 Blue Team Labs Online** scenarios, completing Hack The Box SOC Analyst training, and maintaining a secured Linux homelab environment. Languages: Native Greek, C2 English

Education and Certifications

B.Sc. Computer Science, University of Western Macedonia. 2024 - present.

Blue Team Level 1 (BTL1): Certification coursework finished, examination scheduled for October 2026.

- Completed theoretical preparation and hands-on training modules, with the practical certification exam planned for mid - late October 2026.

Other Certifications:

- **SOC Analyst Path** (Hack The Box, Aug 2025) - SIEM, alert monitoring, log analysis, incident response.
- **Cyber Security 101** Certificate (TryHackMe, Aug 2025)
- **Java Course** (Codecademy, Apr 2026)
- **Learn SQL** (Boot.dev, May 2026)

Activities:

- **IEEE Student Branch, Treasurer (2024-2026)**: Oversaw branch financial ledgers, organized events, and maintained structured documentation while facilitating internal team communication.

Projects

Blue Team Labs Online (BTLO) Investigations : Successfully solved over 14 Security Operations Center scenarios.

- **Executed practical SOC exercises** encompassing alert triage, artifact analysis, timeline creation, and detailed incident reporting within time constraints.
- **Analyzed Windows and Linux telemetry data**, focusing on noise reduction and structured documentation of security findings. Some of the labs include:
  - **SIEM and Threat Hunting (BOTS v1, Splunk It, Drilldown):** Analyzed Splunk telemetry spanning Sysmon, Windows Event Logs, Suricata, and FortiGate feeds to detect brute-force attacks, web shell deployments, persistent threats, and unauthorized credential extraction.
  - **Cloud Incident Response (Spilled Bucket, Print, Blocker):** Evaluated AWS CloudTrail records alongside VPC Flow Logs to trace key leakage and privileged IAM misuse, while investigating host-based logs for exploitation vectors.
  - **DFIR, Phishing, and Network Analysis (Deep Phish, Vortex, Sticky Situation)**:Examined raw PCAPs, SMTP headers, web artifacts, USB forensic evidence, and registry entries to extract actionable indicators of compromise.

Cybersecurity Portfolio (panoskava.dev):

- Developed a public platform to host security investigation write-ups from BTLO investigations, detailing tools, methodologies, and actionable findings to showcase real-world SOC capabilities.
- Published comprehensive incident response documentation and investigative workflows to supplement formal coursework.

Homelab Security Operations (Proxmox, TrueNAS, Docker):

- Architected a secured Linux infrastructure implementing least-privilege access, ZFS integrity verification, and containerized service deployment.
- Hardened Traefik reverse proxy using TLS encryption, security headers, IP restriction policies, and automated patch management via Watchtower.
- Deployed self-hosted Vaultwarden instance with disabled user registration and strict privilege boundaries to safeguard credential stores.
- Configured automated disaster recovery pipelines featuring TrueNAS network storage, scheduled database dumps, and synchronized offsite backups.

Production Salon Booking Platform (komihairsalon.gr): Engineered a web application utilizing Next.js, SQL, and Docker containerization, emphasizing access control mechanisms, data privacy, and server hardening.

Technologies and Languages

- **Security operations:** SOC workflows, alert monitoring, alert triage, incident response, cybersecurity, analytical skills
- **SIEM & endpoint:** Splunk, Search Processing Language (SPL), Elasticsearch, Sysmon, Windows Event Logs
- **Network & threat analysis:** Wireshark, TCP/IP, DNS, HTTP, SMTP, CyberChef, VirusTotal, AbuseIPDB, MITRE ATT&CK
- **DFIR & cloud:** Autopsy, FTK Imager, Windows Registry artifact analysis, AWS CloudTrail, VPC Flow Logs
- **Systems & scripting:** Windows, Linux, Docker, Proxmox, TrueNAS, Traefik, Python, Bash, SQL, Java, C++