YOUSSEF OURGOUS

Cybersecurity & Systems Engineer

youssef.ourgous@gmail.com | +212 6 91 58 95 06 | Casablanca, Morocco | linkedin.com/in/youssef-ourgous

PROFESSIONAL SUMMARY

Cybersecurity Engineer with 4+ years of hands-on experience in systems administration, security operations, threat detection, and network security. Experienced in designing and operating end-to-end SOC and SIEM environments using Wazuh, Suricata, and the ELK Stack, as well as implementing identity and access management solutions and secure, automated IT infrastructures. Skilled in security monitoring, incident detection and response, network hardening, penetration testing, and cybersecurity operations across Linux and Windows environments. CCNA and CCNA Security certified, Master's degree in Systems Engineering and Cybersecurity. Trilingual in Arabic, French, and English, with a strong focus on operational cybersecurity and threat detection.

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer & IT Systems Administrator · Higher School of Technology – Hassan II University of Casablanca

September 2021 – Present | Casablanca, Morocco

- Built and operate a full SOC: multi-node Elasticsearch cluster (elkmaster), Logstash pipelines for firewall/auth/syslog events, Kibana dashboards, and Wazuh SIEM with active response and UEBA analytics.
- Deployed honeypot infrastructure (SSH, HTTP, FTP decoys) to capture real-world attacker TTPs and feed live threat intelligence into SIEM detection rules.
- Automated security monitoring with Fail2ban, custom firewall log pipelines, and webhook alerting to reduce mean time to detect (MTTD).
- Administer Linux (Ubuntu Server, CentOS, Debian) and Windows Server; manage VMware ESXi, Proxmox, and Docker container deployments.
- Configure pfSense firewalls, OpenVPN gateways, VLAN segmentation, IDS/IPS, and FreeIPA IAM (LDAP, Kerberos SSO, RBAC) for network security and access control.
- Conduct penetration tests and vulnerability assessments using Nmap, Wireshark, Burp Suite, and Metasploit; produce actionable remediation reports.
- Lead cybersecurity awareness workshops and phishing simulation campaigns for faculty and staff.

Network Security Technician – Internship · Africa verify

July 2021 – August 2021 | Casablanca, Morocco

- Designed and deployed a fully segmented cybersecurity lab with 6 isolated network segments, a pfSense firewall/IDS, and a vulnerable Active Directory environment, implementing a multi-layer detection stack consisting of Wazuh EDR, Splunk SIEM, and Snort IDS to simulate and detect real-world attacks mapped to the MITRE ATT&CK framework.
- Executed and validated 10+ attack scenarios, including brute-force attacks, Kerberoasting, Pass-the-Hash, NTDS hash extraction, and Active Directory enumeration, validating detection capabilities across the SIEM/EDR/IDS stack.
- Developed "Guardian AI," a 5-agent autonomous SOC using Python, FastAPI, Redis Streams, and LLMs to detect, correlate, and automatically respond to security threats through IP blocking on pfSense, while generating incident reports through a React-based dashboard — achieving end-to-end detection and response in under one second.

KEY PROJECTS

- **SOC Infrastructure – ELK Stack & Wazuh SIEM** *Full SOC Build · Ongoing*
  - Deployed multi-node Elasticsearch cluster across dual networks (192.168.2.x / 10.10.18.x); built Logstash pipelines normalizing logs from firewalls, Linux/Windows hosts, and web servers.
  - Integrated Wazuh agents on all endpoints with UEBA baselines, active response, and compliance dashboards (PCI-DSS, GDPR).
  - Built Kibana dashboards: geo-attack maps, brute-force heatmaps, IOC timelines, and anomaly detection views with automated webhook alerting.
- **Personal Homelab — High-Availability Infrastructure*Deception*** *Infrastructure · Active*
  - Designed low-interaction honeypot emulating SSH, HTTP, and FTP services; captured attacker TTPs including credential stuffing, brute-force tools, and web exploits.
  - Correlated honeypot telemetry with SIEM to enrich threat intelligence, update IDS signatures, and refine Fail2ban and firewall blocking policies.
  - Generated threat intelligence reports: attacker geolocations, tool signatures, campaign timelines, and recurring malicious IP ranges.
- **Kubernetes Security Lab** *Academic · MUS-SAISN Program*
  - Deployed a 3-node Kubernetes cluster running Ubuntu 24.04 with Calico CNI, implementing RBAC, NetworkPolicies, and Prometheus/Grafana monitoring through Helm.
  - Aligned the environment with COBIT IT governance controls and security best practices

TECHNICAL SKILLS

SOC & SIEM: ELK Stack (Elasticsearch, Logstash, Kibana, Filebeat), Wazuh, Splunk, UEBA, Alert Triage, Threat Hunting, IOC Analysis, Threat Intelligence, Automated Alerting, Security Monitoring, Log Analysis
Threat Detection & IR: Honeypot Design & Deployment, Snort, Suricata, IDS/IPS, Incident Response, Forensic Log Analysis, Fail2ban, Firewall Log Pipelines, MTTD Reduction, MITRE ATT&CK
Penetration Testing: Nmap, Wireshark, Burp Suite, Metasploit, Kali Linux, Vulnerability Assessment, Web App Testing (SQLi, XSS, RCE)
Network Security: pfSense, FortiGate, OpenVPN, VLAN Segmentation, VTP, Firewall Policy, ACLs, IDS/IPS, Traffic Analysis, TCP/IP, DNS, DHCP, HTTP/S, Cisco IOS, Static & Dynamic Routing (OSPF, RIP)
Systems & Virtualisation: Linux (Ubuntu/CentOS/Debian), Windows Server, Active Directory, VMware ESXi, Proxmox, High-Availability Clustering, NAS/NFS Storage, Kubernetes, Docker, System Hardening, Patch Management
IAM & Access Control: Active Directory, FreeIPA, LDAP, Kerberos SSO, RBAC, Sudo Policies, Host-Based Access Control (HBAC)
Scripting & DevSecOps: Bash, Python, PowerShell, CI/CD Security Integration, Security Automation, DevSecOps Practices
Platforms & Tools: Hadoop, Django/Wagtail, Apache/Nginx, Zabbix, Apogée, Git

EDUCATION

Master's Degree – Systems Engineering & Cybersecurity – EST Casablanca, Université Hassan II *2025 – 2027*
Bachelor's – Cybersecurity & Intelligent Systems Engineering – EST Casablanca, Université Hassan II *2024 – 2025*
Professional Bachelor's – System Administration & Cybersecurity – EST Casablanca, Université Hassan II *2023 – 2024*

LANGUAGES & CERTIFICATIONS

Languages: French (Native) · English (Professional) · Arabic – Darija (Native)
Certifications: CCNA Security · CISSP (In Progress) · PMP (In Progress)

CERTIFICATIONS

Professional Certifications

- Cisco Certified Network Associate (CCNA)
- CCNA: Enterprise Networking, Security & Automation
- CCNA: Switching, Routing, and Wireless Essentials (SRWE)
- Cisco Certified Network Associate Security (CCNA Security)
- Python Essentials 1
- ITIL 4 Foundation *(In Progress)*

Training & Conference Certificates

- Data Analysis and Visualization with R — European Union Conference
- Introduction to ESP32 — European Union Conference

ACTIVITIES & INTERESTS

– Member of the **Institutional Council of the Higher School of Technology of Casablanca (University Hassan II).**
– Active LinkedIn content creator sharing cybersecurity insights, SOC architecture tips, and network security tutorials for the Moroccan and African tech community.
– Continuous self-development in threat hunting, SIEM engineering, and blue team techniques through personal lab environments and online cybersecurity platforms.
– Passionate about mentoring students and peers in cybersecurity fundamentals and best practices within the academic environment at EST Casablanca.