DANIEL DAYAN

Junior SOC Analyst | Cybersecurity & IT Support

Israel | 054-912-0911 | danieldayan2512@gmail.com | LinkedIn

PROFESSIONAL SUMMARY

Cybersecurity graduate of a hands-on 650-hour program sponsored by the Israel Ministry of Defense (Cisco & Fortinet specialization), with ongoing hands-on practice through Hack The Box Academy and a self-built home lab. Hands-on across enterprise networking, Windows Server/AD, Linux, FortiGate NGFW and SIEM/SOC workflows (Splunk, IBM QRadar). Experienced in alert triage, log investigation, structured troubleshooting and clear documentation; service-oriented, with military SAP/CRM ticketing experience under time pressure.

PRACTICAL TRAINING & LAB EXPERIENCE

Cyber Security Bootcamp — ITQ

2024 – 2025

650 hands-on hours — Cisco & Fortinet specialization, Israel Ministry of Defense discharged-soldier track

- Enterprise networking on Israel's largest Cisco training lab (Cisco IOS XE): TCP/IP, IPv4/IPv6 addressing, ICMP, DNS, DHCP, HTTP/S, VLANs, OSPF, STP, EtherChannel, NAT & port-forwarding, ACLs, VPN, IPsec/GRE and structured troubleshooting.
- Windows Server 2022: deployment, server roles, Active Directory, Group Policy, remote access, storage technologies, server maintenance, hardening and performance monitoring; Linux administration (LPI track): CLI, permissions, users/groups, package management, regular expressions, Bash scripting.
- Cisco Layer-2 security, secured routing and VRF; site-to-site VPNs with IPsec IKE phases and GRE tunnels secured by crypto maps/profiles; FortiGate NGFW: security policies, stateful inspection, deep packet inspection, IPS, DLP, WIPS wireless threat mitigation, user authentication, logging/monitoring and segmentation.
- SOC workflows: first-level alert triage, log investigation and the incident response lifecycle, with hands-on IBM QRadar SIEM and Splunk SOAR.

Hack The Box Academy & Personal Home Lab

2025 – Present

Continuous self-directed training — offensive security modules, guided paths and live practice targets

- Hands-on offensive security: Nmap enumeration and footprinting, Burp Suite / OWASP ZAP, SQL injection and SQLMap, file inclusion and upload attacks, XSS, command injection, server-side attacks (SSRF, SSTI, SSI), fuzzing (ffuf), Metasploit, password attacks (Hashcat, Hydra), shells & payloads, OWASP Top 10.
- Completed full methodology modules: Penetration Testing Process, Vulnerability Assessment and Bug Bounty Hunting Process — scoping, reporting and professional communication of findings.
- Built and maintain a personal home lab: Windows Server with Active Directory, Linux and Kali machines on a virtualized network; practice service configuration, connectivity checks and hardening.
- Use the lab for log review, Wireshark traffic analysis and evidence collection; practice authorized workflows end to end — scope, enumerate, assess, validate, document.

MILITARY SERVICE

Service Coordinator — Soldier Benefits, Israel Defense Forces

2022 – 2025

- Managed soldier benefits and entitlements with accuracy, confidentiality and service orientation, using SAP to search records and process requests.
- Logged, prioritized and tracked cases to closure in CRM and ticketing workflows; handled sensitive requests under time pressure with soldiers, commanders and external agencies.

EDUCATION

High School Computer Science — 10 Units

2020 – 2022

Final project: Android application in Java for cryptocurrency price tracking and currency conversion (USD/EUR/ILS); web development with HTML/CSS.

TECHNICAL SKILLS

Security / SOC	Splunk, Splunk SOAR, IBM QRadar SIEM, alert triage, log investigation, incident response lifecycle, vulnerability assessment and management, documentation and escalation.
Security Tools	Nmap, Wireshark, Burp Suite, OWASP ZAP, ffuf, SQLMap, Metasploit, Hashcat, Hydra.
Networking	TCP/IP, IPv4/IPv6, ICMP, DNS, DHCP, HTTP/S, SMB, FTP, SSH, VLANs, OSPF, VPN, IPsec/GRE, IKE, ACLs, NAT, basic routing; Cisco & FortiGate; IPS, DLP, WIPS; cloud-managed security concepts.
Systems & Labs	Windows, Windows Server 2022 (Active Directory, Group Policy), Linux, Kali Linux, Ubuntu; virtualized home-lab environments.
IT Support & Service	Structured troubleshooting, ticketing and CRM workflows, SAP record search and processing, remote access, user-support mindset, Windows support fundamentals.
Scripting & Dev	Python, Bash, PowerShell, Java, SQL, HTML/CSS.

PROFESSIONAL READINESS

- Ready for first-level investigation from day one: alerts, related logs, affected services, user reports and basic network indicators before escalating.
- Clear documentation of findings for technical and non-technical readers; military-honed patience, confidentiality and follow-up.

LANGUAGES

Hebrew — Native | English — Very Good (technical reading and communication)