Giagkidis Dimitrios

DIMITRIOS GIAGKIDIS

System & Network Administrator | SOC Analyst & Incident Response

Thessaloniki, Greece (EU – 100% Remote Ready)

[dgiagkidiss@gmail.com] | [+306973186136] | [http://www.linkedin.com/in/dimitrios-giagkidis-9267857b] | [https://dimis-gkds-sec.pages.dev/]

Professional Summary

IT Operations and Infrastructure specialist with over 10 years of progressive experience—advancing from Help Desk and Operational Support to System and Network Administration across enterprise environments. Over the past 3 years, my primary focus has shifted solidly toward Defensive Cybersecurity, Threat Detection, and Incident Response.

Years of administering Windows Server, Active Directory, Exchange, and cloud infrastructure provide a deep understanding of baseline enterprise behavior. That operational foundation drives my security analysis—allowing me not just to triage an alert, but to evaluate whether the underlying activity makes sense in context and separate true positives from operational noise.

To sharpen my defensive and offensive capabilities, I completed the **Hack The Box CDSA** and **CPTS** training paths, conducting hands-on lab investigations covering SIEM log analysis, threat hunting, DFIR, and malware analysis, which I document on my personal Hugo-based technical portfolio. In daily investigations, I rely on **Splunk (SPL)**, **Microsoft Sentinel (KQL)**, **Microsoft Defender XDR**, Wireshark, Sysinternals, Volatility, and Eric Zimmerman tools.

Technical Skills

- **SIEM, Threat Detection & SecOps:** Splunk (SPL, Alert Triage, Log Correlation, Dashboarding), Microsoft Sentinel (KQL), Microsoft Defender XDR, SIEM/SOAR Operations, Threat Hunting, Incident Response, Use Case Testing.
- **Digital Forensics & Analysis (DFIR):** Wireshark (PCAP Analysis), Volatility 3, Eric Zimmerman Tools, Sysinternals Suite, Windows Event & Sysmon Log

Analysis.

- **Infrastructure & Virtualization:** Windows Server Administration (2012–2022), Hyper-V, VMware, Backup & Recovery Systems, Vulnerability Management.
- **Cloud & Identity:** Microsoft Azure / Entra ID, Microsoft 365 Administration, Intune, SCCM, Active Directory, Microsoft Exchange.
- **Networking & Security:** Cisco Routing & Switching, LAN/WAN, Firewall Security, Network Traffic Monitoring, Advanced Troubleshooting.
- **Security Tooling & Validation:** ELK Stack, Security Onion, Burp Suite, Nmap, BloodHound, Metasploit.

Cybersecurity Projects & Hands-on Training

Hack The Box – Certified Defensive Security Analyst (CDSA Path) *(Completed Path)*

- Performed end-to-end SIEM alert investigations, log correlation, and threat hunting using **Splunk (SPL)** and ELK Stack across simulated enterprise attack scenarios.
- Analyzed network captures (PCAPs), Windows Event Logs, Sysmon telemetry, and endpoint artifacts to reconstruct attack timelines and identify Indicators of Compromise (IoCs).
- Trained in detection engineering principles, security monitoring workflows, and structured incident reporting.
- *Verification:* CDSA Path Achievement | Sherlock/Lab Badge

Hack The Box – Certified Penetration Testing Specialist (CPTS Path) *(Completed Path)*

- Executed structured vulnerability assessments, Active Directory attack path analysis, web application testing, and Windows/Linux privilege escalation labs—leveraging offensive methodologies to strengthen defensive detection logic.
- *Verification:* CPTS Path Achievement | Badge 1 | Badge 2 | Badge 3

Professional Experience

System and Network Administrator | DEMO Pharmaceuticals S.A.

Thessaloniki, Greece | Jun 2022 – Present

- Lead administrator for server and network infrastructure supporting 130+ corporate and laboratory users in a high-compliance pharmaceutical environment.
- Collaborated with external SOC operations on security alert triage, log investigation, ticket handling, and incident containment across endpoints and network infrastructure.
- Executed ongoing Vulnerability Management tasks, patch remediation, and network security hardening protocols.
- Implemented and monitored enterprise Backup & Recovery systems to ensure data integrity and business continuity.

IT Operational Support Specialist | MYTILINEOS S.A.

Thessaloniki, Greece | Feb 2020 – May 2022

- Provided global-scale technical support for 5,000+ end-users via enterprise ticketing systems, maintaining strict SLA and incident resolution standards.
- Administered core Microsoft & Cloud infrastructure, including Microsoft 365, Azure, Entra ID, Intune, SCCM, Active Directory, and Exchange.
- Supported Cisco networking hardware and LAN/WAN routing across distributed operational environments.
- Applied structured root-cause analysis to diagnose complex system/network anomalies and collaborated with senior engineering teams to improve operational security workflows.

System Administrator | Ellinair S.A.

Thessaloniki, Greece | Apr 2016 – Feb 2020

- Managed Microsoft Exchange Server operations, Elastix Voice Center, and enterprise server virtualization environments.
- Monitored network security, system health, and corporate infrastructure availability, performing rapid troubleshooting and incident recovery.
- Deployed, configured, and hardened Windows/Linux operating systems, hardware, and core business applications.

Earlier Experience:

- **IT System Administrator** | Municipality of Lagadas *(2015)*
- **Service Desk Manager** | OTE (Hellenic Telecommunications Organization) *(2014)*

Education & Certifications

Education

- **Vocational Training Diploma (EQF Level 5)** – Computer Systems, Networking and Telecommunications | SAEK (IEK) Lagadas

Certifications & Completed Paths

- **HTB Certified Defensive Security Analyst (CDSA)** – Completed Path *(Exam in progress)*
- **HTB Certified Penetration Testing Specialist (CPTS)** – Completed Path
- **CCNA Routing and Switching** – INFOLAB Enterprise Training
- **Google Cybersecurity Certificate** – Coursera / Google
- **Automating Real-World Tasks with Python** – Coursera / Google
- **ECDL (ACTA) Computer Science** – Aristotle University of Thessaloniki (AUTH)