Nadim Al-Saliby

Security Engineer | DevSecOps

Address: Beirut, Lebanon

Email: nadimjsaliby@outlook.com

Portfolio: https://nadimjsaliby.com **|** **Blog:** https://blog.nadimjsaliby.com

Summary

Cybersecurity, cloud, and threat intelligence professional with 8+ years of IT experience across Linux administration, cloud infrastructure, automation, and security operations. In parallel with my engineering work, I design and build OSINT and dark web intelligence capabilities, including DarkHuginn, a platform focused on threat monitoring, digital investigations, blockchain analysis, and intelligence enrichment that was acquired by WhoMeta. I combine hands-on technical depth with a strong security mindset to build resilient systems, automate operations, and support cyber threat detection and investigation.

Experience

Chief Security Officer — 05/2025 – Present
WhoMeta, Remote

Lead the design and implementation of security architecture, threat intelligence infrastructure, and monitoring platforms supporting cybercrime investigations and intelligence analysis.

- Designed and implemented cloud infrastructure using Terraform Infrastructure-as-Code, enabling reproducible and secure deployments.
- Architected and deployed Azure Kubernetes Service (AKS) and RKE2 airgapped environments running security and intelligence microservices.
- Built a security monitoring and threat intelligence platform integrating Wazuh, TheHive, Trivy, renovate, Bandit, MISP, etc…
- Integrated the DarkHuginn OSINT platform with WhoMeta investigative workflows to enrich intelligence with dark web, cryptocurrency, and identity data.
- Implemented real-time alerting pipelines to Microsoft Teams to support rapid incident response and operational awareness.
- Designed observability and monitoring stack using Prometheus and Grafana for infrastructure and security telemetry.
- Implemented GitOps workflows and CI/CD pipelines to automate infrastructure and platform deployments.
- Developed automation pipelines connecting intelligence collection, SIEM detection, and investigation platforms.

Founder & Threat Intelligence Engineer — 02/2024 to 05/2025
DarkHuginn, Lebanon

- Designed & built a threat intelligence platform that discovers and analyzes onion services and extracts indicators such as emails, cryptocurrency wallets, & infrastructure metadata.
- Developed automated dark web crawling pipelines using Python, Tor, and asynchronous scraping frameworks.
- Built blockchain intelligence workflows to analyze cryptocurrency transactions, wallet balances, and relationships between wallets used in illicit activity.
- Implemented OSINT enrichment pipelines linking collected emails to social media accounts and other open-source intelligence sources.
- Designed scalable data processing architecture using message queues and distributed workers for large-scale intelligence collection.

Linux & Cloud Engineer – 03/2023 to 03/2025
Carma, Lebanon

- Supervise distributed systems and networks in data centers and AWS Cloud, ensuring optimal functionality and reliability.
- Establish robust backup strategies that substantially decrease downtime and strengthen data protection.
- Create and maintain comprehensive monitoring systems using influxdb, Grafana, Icinga2, and Kibana to enable proactive issue resolution.
- Spearhead automation initiatives with Ansible to optimize processes and enhance configuration management efficiency in Linux environments.
- Design and deploy load balancing and failover strategies to ensure system uptime and resilience against high traffic or server failure.
- Conduct regular performance assessments and optimize Linux and cloud services, leveraging monitoring data to identify and resolve bottlenecks.
- Develop and test disaster recovery procedures for cloud and on-premises infrastructure to ensure rapid recovery and minimal data loss in case of system failures.
- Implement security best practices on Linux servers and AWS resources.

IT Engineer – 03/2022 to 03/2023
4T, Lebanon

- Set up and resolved issues with Windows Server 2019, improving system reliability and uptime.
- Oversaw Cisco Meraki switches and firewalls to maintain secure and efficient network operations.
- Managed Microsoft 365 Defender, bolstering organizational cybersecurity efforts.
- Implemented Zabbix Monitoring for both on-premises and cloud servers, enhancing performance tracking capabilities.
- Configured and supervised Veeam for backup and replication, ensuring the safeguarding of critical data.project, the "Let's Join" Pavilion, fostering teamwork and enhancing design execution skills.

System Administrator – 09/2021 to 03/2022
Smart Solution & E-Consultancy, Lebanon

- Administered Windows Server 2012 networks, including domains, Active Directory (AD), DNS, and DHCP, to ensure seamless operational continuity.
- Configured and managed backup and restore protocols, significantly enhancing data security and reliability.
- Diagnosed and reported issues related to server performance, networking, and infrastructure, leading to improved system uptime and operational efficiency.
- Configured VLANs, trunking, SNMP groups, and access control lists on Cisco ASA switches to optimize overall network performance and security.

System Administrator - 07/2018 to 06/2021
Universant, Lebanon

- Oversaw and resolved issues for both Windows and Linux servers, ensuring peak performance and reliability.
- Developed and implemented disaster recovery plans to enhance system uptime and resilience.
- Assessed network vulnerabilities and applied necessary patches, significantly mitigating security risks.
- Configured and upgraded servers to uphold system integrity and optimize performance.
- Diagnosed and resolved network performance issues, resulting in measurable enhancements in speed and reliability.

Education

Bachelor's Degree in ICT with Emphasis on Digital Forensics – 07/2023
AUST, Lebanon

Certifications

- **PWK 200** - Offensive Security
- **RHCSA (Red Hat Certified System Administrator)** - Linux Academy
- **MCSE (Microsoft Certified System Engineer)** - Microsoft
- **MCSA (Microsoft Certified System Administrator)** - Microsoft
- **CCNA (Routing and Switching)** - Cisco

Skills & Expertise

- Windows Administration
- Linux Administration
- Cisco ASA
- Cisco Meraki
- Python Programming
- ELK Stack
- Icinga2 Monitoring
- Grafana Dashboards
- Prometheus Monitoring
- Memory Forensics
- OWASP Principles
- Ansible & Puppet
- WAZUH SIEM & Threat Intel
- AWS IAM Role & Lambda
- Azure Administration
- Office 365
- AWS Technologies
- PAM Solutions
- PowerShell & Bash Scripting
- Windows Forensics
- Burp Suite
- Nmap Scanning
- Nessus Vulnerability
- Wireshark Analysis
- OSINT Techniques
- Immunity Debugger
- Nikto
- SQLmap

Languages

Arabic: Native| **English:** Fluent | **French:** Fluent | **German:** Basic (A1, in progress)