GHAZI BELGUITH

Cybersecurity Consultant

+216 24 339 774 ghazi.belguith.work@gmail.com Tunisia,TN ghazibelguith

Summary

Cybersecurity consultant with over 8 years of experience in the banking and financial sector, combining technical expertise and leadership in SOC operations. Skilled in risk analysis, incident response, and security governance, with a proven track record in developing security standards, managing SOC teams, and leading forensic investigations.Known for analytical rigor, adaptability, and teamwork under pressure.

Skills

- **Security Platforms:** SIEM (Splunk, ELK, Graylog, LogRhythm, Wazuh, Microsoft Sentinel), SOAR (Cortex XSOAR, Shuffle), EDR/XDR (CrowdStrike, SentinelOne, Sekoia, Sophos, Cortex XDR, TrendMicro), Amazon GuardDuty, AWS CloudTrail.
- **ISO/Frameworks:** MITRE ATTACK, NIST, ISO 27001, OWASP, GDPR, Cyber Kill Chain

Professional Experience

Cybersecurity Consultant, *Banking and Financial Council (CBF) - Independent* **Tunis** *02/2023 - Present*

- **Member of the Tunisian FinancialCERT**
- Lead and manage the SOC team (Level 1 to Level 3): recruitment, training, skill development, and performance evaluation.
- Supervise detection, triage, and incident response activities.
- Define and maintain SOC operational processes (playbooks, escalation paths, and communication workflows).
- Drive the implementation and continuous improvement of SOC tools (SIEM, SOAR, EDR, XDR, Threat Intelligence platforms).
- Coordinate actions with CERT, IT, and Risk Management teams during major security incidents.
- Produce and present security reports (KPIs, trends, major incidents) to clients.
- Conduct continuous technological and operational monitoring of threats, vulnerabilities, and best practices.
- Assist in developping processes and procedures for clients.
- Ensure compliance with security frameworks and standards (ISO 27001, NIST, MITTRE ATTACK, etc.).

Technical Environment: EDR: TrendMicro, Cortex XDR - SIEM: ELK, Qradar, LogRhythm, Wazuh, Microsoft Sentinel SOAR: Shuffle - Threat Intelligence: MISP, OpenCTI - GitLAB - TheHive.

SOC Analyst L2, *INTRINSEC - Independent* **Tunis** *02/2022 - 08/2023*

- Investigated and analyzed security incidents escalated by Level 1 analysts.
- Supported clients in incident response and remediation processes.
- Monitored and qualified alerts from EDR,XDR,SIEM tools (CrowdStrike, SentinelOne, HarfangLab, SEKOIA, SPLUNK).
- Correlate between different sensors and sources to help in decision making.
- Produced investigation reports and attack visualizations.
- Contributed to threat intelligence and reduced false positives through process optimization.

Technical Environment: EDR: SentinelOne, CrowdStrike, HarfangLab - SIEM: Splunk - SOAR: Cortex XSOAR - Vulnerability Management: Qualys - Threat Intelligence: MISP, Sekoia XDR.

Cybersecurity Analyst, *Banking and Financial Council (CBF) - Full-time* **Tunis** *02/2019 - 02/2022*

- **Member of the Tunisian FinancialCERT**
- Led the implementation of security policies, audits, and ISO 27001 readiness.
- Monitored infrastructure availability, backups, and access management (IAM).
- Investigated and responded to cybersecurity incidents reported by member banks.
- Produced detailed incident reports with impact analysis and remediation recommendations.
- Deployed and managed open-source tools for incident management and threat intelligence (MISP, TheHive, Cortex, SIEM).

Technical Environment: MISP, TheHive, Cortex, GLPI, OpenVAS, Nagios, Centreon, Zabbix, SIEM (ELK, Graylog, SIEMonster), XDR (Sophos Intercept X), Windows (Active Directory, WSUS, Office 365).

Cybersecurity Consultant, *KEYSTONE - Full-time* **Tunis** *02/2018 - 02/2019*

- Identify potential threats.
- Conduct joint research to study risks and threats.
- Act as a communication hub for the entire sector, especially during crisis periods.
- Send information bulletins to members following attacks to strengthen security and prevent similar incidents.
- Send alerts to banks informing them of updates to apply in order to mitigate recent vulnerabilities.

Technical Environment: Sandbox, Kali Linux, Metasploit, Nmap, Burp Suite, SQLmap, Wireshark, John the Ripper.

Certifications

- ISO 27001 Lead Auditor
- ISO 27001 Lead Implementer
- Blue Team Level 1
- SC-200: Microsoft Security Operations Analyst
- (ISC)² Certified in Cybersecurity (CC)
- Splunk Core Certified User
- Sekoia Security Analyst
- Blockchain and Financial Services Training
- FIRST CVSSv3 Certificate
- CCNA Security

Education

National Engineering Degree in Telecommunications **SFAX, TN** *2018*
International Institute of Technology (IIT)
Specialization: Systems and Network Administration and Security.

Applied Bachelor's Degree in Network Administration and Security **SFAX, TN** *2015*
National School of Electronics and Telecommunications (ENET'COM)

Baccalaureate in Computer Science **SFAX, TN** *2010*
Mahmoud Megdiche High School

Languages

- **Arabic** [Native]
- **French** [C1]
- **English** [B2]