ISMAEL BELEM

North Bergen, NJ
929-326-8527
belem2010@hotmail.fr
https://www.ismaelbelem.com
linkedin.com/in/ismael-belem-95bb08173
github.com/Ibelem1

PROFESSIONAL SUMMARY

Results-driven Cybersecurity Analyst with 4+ years in blue team operations, incident response, and digital forensics. Experienced in leveraging SIEM (Microsoft Sentinel, Wazuh, Splunk) and EDR (CrowdStrike Falcon, Microsoft Defender) to protect 400+ endpoints across public cloud (Azure, AWS, GCP), hybrid, and on-prem environments. Proven track record in reducing false-positive alerts by 25%, leading SOC teams, and conducting comprehensive security gap assessments. Skilled in developing SOPs, performing threat hunting, analyzing adversary TTPs and IOCs, and delivering executive-level security briefings to technical and non-technical stakeholders.

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst II | **Dataprise (MSSP)** Sep 2023 – Present
North Bergen, NJ

- Designed and deployed enterprise detection and telemetry dashboards in CrowdStrike LogScale and Microsoft Sentinel (KQL), improving SOC visibility across managed environments.
- Implemented automated host containment workflows (Attack Disruption) using CrowdStrike Fusion SOAR to isolate compromised systems based on vetted detection alerts.
- Served as the highest technical escalation point for SOC investigations, supporting incident response engagements involving advanced threat actors and enterprise breaches.
- Conducted proactive threat hunting and adversary infrastructure analysis using telemetry, OSINT sources, adversary TTPs, and emerging intelligence feeds.
- Monitored and investigated security alerts across CrowdStrike Falcon and Microsoft Sentinel, analyzing host telemetry and log data to identify IOCs, IOAs, and potential compromise.
- Conducted incident investigations including malware detections, account compromise, and unauthorized activity across managed environments.
- Managed over 400 endpoints using CrowdStrike: enforced EDR policies, coordinated sensor deployments, and developed detection workflows and automated playbooks using PowerShell and Python.
- Security awareness training (KnowBe4, PII-Protect "Breach Secure Now"): oversaw 200 accounts, created automated training programs, phishing simulations, and monthly newsletters.
- Appointed by Cyber Department President to lead vendor evaluation project assessing cybersecurity awareness tools measuring efficiency, scalability, and AI capabilities.
- Led creation of incident response SOPs and playbooks; trained Tier 1 SOC analysts and delivered monthly client briefings including vulnerability and remediation reports.
- Provided ongoing intelligence briefings on emerging threats, adversary TTPs, cybercrime trends, and new IOCs to SOC analysts and client stakeholders.

Cybersecurity Engineer | **Cohere Cyber Secure (MSSP)** Sep 2022 – Sep 2023
Manhattan, NY

- Provided overall security posture assessments in After-Action Reports covering penetration testing scope, risk management, mitigation strategies, and lessons learned.
- Triaged security incidents including ransomware, following the Incident Response Framework and performing host- and network-based forensics to determine root cause and preserve evidence.
- Configured policies in CrowdStrike Falcon to harden environments and prevent attacker lateral movement.
- Monitored, created detection rules, and onboarded clients to SIEM (Wazuh), developing custom rules and parsers using regex and threshold tuning to improve alert fidelity.
- Developed Incident Response, ransomware, phishing, and Wazuh deployment SOPs and playbooks to standardize response and onboarding procedures.
- Conducted quarterly Vulnerability Assessments using Nessus and CrowdStrike; applied CVSS scoring, communicated findings to clients, and coordinated remediation planning.
- Monitored and analyzed Linux operating systems for security threats and vulnerabilities, implementing timely remediation.

Operations Manager | **Bocaphe** Jan 2020 – Sep 2022
Manhattan, NY

- Conducted recruitment, training, and scheduling of new employees.
- Provided support for all internal POS systems and utilized AnyDesk/TeamViewer for tablet-based computer troubleshooting.
- Facilitated software setup for new technological products and internal systems.

Freelance IT Technician Jan 2013 – Sep 2021

Ouagadougou, Burkina Faso & Manhattan, NY

- Provided maintenance and hardware upgrades for PCs and laptops.
- Installed and configured operating systems, VMware, Wireshark, antivirus, Office 365, Azure, and Linux.
- Delivered IT support assistance to third-party clients.

EDUCATION

Master of Science | ***Digital Forensics and Cybersecurity*** May 2022
John Jay College of Criminal Justice (CUNY) New York, NY

Advanced Certificate | ***Applied Digital Forensics (A.C. P.B.)*** May 2022
John Jay College of Criminal Justice (CUNY) New York, NY

Bachelor of Science | ***Computer Science and Information Security*** Dec 2020
John Jay College of Criminal Justice (CUNY) New York, NY

Associate of Science | ***Computer Network Technology*** May 2019
Borough of Manhattan Community College (CUNY) New York, NY

CERTIFICATIONS

CrowdStrike Certified Falcon Administrator – CCFA-200

Microsoft Certified: Security Operations Analyst Associate – SC-200

Microsoft Certified: Azure Administrator Associate – AZ-104

Microsoft Certified: Security, Compliance, and Identity Fundamentals – SC-900

CompTIA Security+ – SY0-601

TECHNICAL SKILLS

SIEM & EDR: Microsoft Sentinel, Splunk, Wazuh, CrowdStrike Falcon, Microsoft Defender for Endpoint, CrowdStrike LogScale, KQL

Threat Hunting & IR: Threat Hunting, Incident Investigation, Adversary Infrastructure Analysis, Detection Engineering, IR Lifecycle, MITRE ATT&CK, TTPs, IOC/IOA Analysis, Playbook Development, SOAR

Detection & Platform Engineering: CrowdStrike LogScale, Microsoft Sentinel (KQL), Detection Rule Development, Security Telemetry Engineering, Automation Workflows

Threat Intelligence & OSINT: MISP, AbuseIPDB, Abuse.ch, Shodan, Maltiverse, Lumu, SpiderFoot, Maltego, Recon-ng, IOC Analysis, IOA Analysis

Vulnerability Management: Nessus, Greenbone, Cavelo, CVSS, Vulnerability Assessment, Remediation Tracking, Risk Assessment

Digital Forensics: Autopsy, FTK Imager, Sleuth Kit, Wireshark, HxD Hex Editor, Jump List Analysis, Prefetch Analysis, USB Forensic Tracker, HashMyFiles

Security Workflow & Automation: PowerShell, Python, Bash Scripting, n8n, CrowdStrike Fusion, SOAR, Playbook Development

Cloud & Identity Management: Microsoft Azure, Microsoft Intune, Active Directory, Google Cloud Platform (GCP), AWS

Frameworks & Methodology: NIST CSF, MITRE ATT&CK, Zero Trust, Defense in Depth, Incident Response Framework, Kill Chain

Networking: TCP/IP, OSI Model, VLANs, Network Traffic Analysis, Cisco Packet Tracer

Virtualization & Labs: VMware, VirtualBox, Proxmox Virtual Environment, FLARE VM, Docker

Operating Systems: Windows, Windows Server, Linux, Ubuntu, Kali Linux, Parrot OS, macOS

Languages: English (Fluent), French (Fluent – Professional Proficiency)

PROJECTS

Threat Intelligence & SIEM Integration | ***Proxmox VE, Wazuh, MISP, Ubuntu, Sysmon, Python Scripting*** Fall 2024
Home Lab

- Built and managed a cybersecurity homelab using Proxmox VE, Wazuh, and MISP to simulate an enterprise SOC environment.
- Deployed and configured Ubuntu-based virtual machines on Proxmox, including Wazuh Manager and MISP servers.
- Integrated Wazuh with the MISP API to enable automated threat intelligence correlation for Indicators of Compromise (IoCs) such as malicious IPs, domains, and file hashes.
- Installed and monitored Wazuh agents and Sysmon on Windows endpoints to collect endpoint telemetry, analyze security events, and validate real-time detection and alerting workflows.

Cyber Risk Assessment & Management | ***NIST CSF, MITRE ATT&CK*** Spring 2023
John Jay College of Criminal Justice

- Developed a comprehensive Information Security and Privacy Program incorporating Zero Trust, Defense in Depth, and Agile Security frameworks.
- Applied cyber risk mitigation strategies and threat modeling techniques; built a risk mitigation plan addressing high-risk threats to support long-term cyber maturity.

Azure Sentinel SIEM – Live Cyber Attack Map | ***PowerShell, KQL*** Fall 2022
John Jay College of Criminal Justice

- Used a custom PowerShell script to extract metadata from Windows Event Viewer and forward it to a third-party geolocation API.
- Configured Microsoft Sentinel workbook to display global RDP brute-force attack data on a world map, visualizing attack origin and magnitude in real time.

Digital Forensic Investigation | ***Autopsy, FTK Imager, Prefetch, Jump List, HashMyFiles*** Spring 2022
John Jay College of Criminal Justice

- Served as Forensic Investigator, collecting and preserving digital evidence from forensic images across multiple case scenarios involving data theft and unauthorized intrusion.
- Maintained Chain of Custody documentation and produced comprehensive investigative reports for each case.

Raspberry Pi SOC & Pentesting Homelab | ***OpenSSH, Kali Linux, Docker, Raspberry Pi, Portainer*** Fall 2021
Home Lab

- Built a portable cybersecurity homelab on Raspberry Pi using Docker and Portainer to simulate a secure virtualized security testing environment.
- Installed and configured Docker containers through Portainer's web interface to deploy and manage cybersecurity tools, including Kali Linux and Metasploitable.
- Created isolated containerized lab environments for penetration testing, vulnerability assessment, attack simulation, and network security practice without exposing the home network.
- Configured remote administration and monitoring using SSH, Docker networking, and Portainer stack deployments to streamline container orchestration and security lab management.