ISAAC FERNANDES

Fortaleza - Ceará +55 (85) 9.

eyezuhk.com.br linkedin.com/in/isaacfn/ isaacfn95@gmail.com

CAREER OBJECTIVE

- Information Security Analyst | CTI | Detecting Engineer | SOC | SIEM | THREAT HUNTING | DFIR | CSIRT

PROFESSIONAL EXPERIENCE

CAPGEMINI

Job Title: Security Consultant V | SOC Detection Engineer (03/2023 - Now)
Responsibilities: Detection Engineering, Threat Hunting, Digital Forensics and Incident Response, Qradar Management, Splunk, Elastic, Azure Sentinel, Crowdstrike, Sentinel, Jira, Gitlab Management, Detection as code, OpenCti, Anomaly, Resilient, Detect Mitre, Confluence, Playbook Creation, Purple Team exercises with Caldera and Atomic Red team, Tanium.
Key Achievements: Significant progress in detection maturity for a leading multinational automotive manufacturer, reducing false positives by 90%, while strengthening overall security operations and incident response capabilities.

ISH TECNOLOGIA

Job Title: Cyber Defense | Threat Hunter | Detection Engineer | SOC L3 | SIEM (05/2022 - 03/2023)
Responsibilities: Threat Hunting, Digital Forensics and Incident Response, RSA Netwitness Management, Securonix SNYPR, Kape, Volatility, Dettect, Mitre, D3fend, TaHiTI, MAGMA, NIST, ServiceNow, Reporting, Documentation Creation, Daily Client Meetings.
Key Achievements: Evolution in Information Security Maturity of Large Brazilian Companies

MORPHUS SEGURANÇA DA INFORMAÇÃO

Job Title: Information Security Analyst Jr | Blue Team | SOC L1/L2| SIEM (06/2021 - 05/2022)
Responsibilities: SIEM and Threat Intelligence alert triage, Threat Hunting, Incident Response, LogRhythm and Qradar management, Resilient SOAR, Azure Sentinel, Splunk, Nessus, Darktrace, Proofpoint, Zabbix, Fortinet, Kaspersky Security Center, BAS, OSINT, MITRE ATT&CK, Lockheed Martin Cyber Kill Chain, Diamond Model, OWASP, NIST compliance, OTRS ticket handling with vendors, Reporting, Daily checklists, Documentation creation.
Key Achievements: Maintained security for multiple large companies in Latin America.

ENERGY TELECOM

Job Title: Support Technician - Monitoring (07/2018 - 05/2021)
Responsibilities: Management of PRTG Network Monitor, Centreon, Icinga, Troubleshooting Sonicwall, Sophos, Routing, Switching, DHCP, DNS, NAT, Service Desk Telephone and Qualitor, Documentation of routine checklists for Bacula, Veeam, vSphere Data Protection, and Backup Exec backups.
Key Achievements: Ensured availability of critical assets for important companies in Brazil.

PHOTONICS LABORATORY

Position: Undergraduate Researcher (05/2016 - 12/2016)
Responsibilities: Research in Photonics, Numerical Simulations, Optical Communication Systems, Article Writing, Support for the Annual Iecom Meeting on Communications, Networks, and Cryptography..
Key Achievements: Fundamental scientific contribution in the field of optical computing.

LANGUAGE SKILLS, COURSES, AND SKILLS

Portuguese: Native **English:** Advanced | Fluent **Spanish**: Basic

---

CCD | BTL 1 | CISCO CyberOps Associate | GHSOC - Security Operation Center | | IBM QRadar SIEM Foundation | TCM - Practical Ethical Hacker | TCM - Practical Windows Forensics | TCM - Practical Malware Analysis | TCM - Detection engineering for beginners | TCM - Practical API hacking| | TCM - Practical phishing campaigns | NSE 1,2 and 3

Office Tools: Advanced in Microsoft Office Suite | Advanced in Excel
Programming Languages: Python, powershell, shell, C, MATLAB;

ACADEMIC BACKGROUND

- Bachelor's Degree in Telecommunications Engineering - Federal Institute of Ceará (2021)

VOLUNTEER WORK

- **Computer Teacher (01/2017 - 06/2017)**
- **Coordinator at the Telecommunications Engineering Academic Center (01/2015 - 01/2017)**