Joao Marcelo Miranda

Rio de Janeiro, Brazil (UTC-3) | +1 (954) 569-8583 | joao.miranda423@gmail.com
linkedin.com/in/joaomarcelo-miranda | github.com/jo-marcelo | jomiranda.com

PROFESSIONAL SUMMARY

Security analyst with hands-on experience in Microsoft Sentinel and Defender XDR, writing KQL to investigate endpoint, identity, and network telemetry and mapping findings to MITRE ATT&CK. B.S. Computer Science, CompTIA CySA+. Dual US and Brazilian national in Rio de Janeiro: full US Eastern hours overlap, no sponsorship required, native English and fluent Portuguese.

CERTIFICATIONS

CompTIA CySA+ | ISC2 Certified in Cybersecurity (CC) | ITIL Foundation

TECHNICAL SKILLS

Security Tools: Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Endpoint (MDE), Sysmon, Tenable Nessus, Wireshark, Nmap
Query and Scripting: KQL (Kusto Query Language), PowerShell, Python, Bash, SQL
Platforms: Microsoft Azure, Active Directory, Windows Server, Linux
Focus Areas: Threat hunting, incident response, detection engineering, vulnerability management, log analysis, system hardening
Frameworks: MITRE ATT&CK, DISA STIG

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer (Intern) | LOG(N) Pacific | Remote | June 2026 to August 2026

- Ran proactive threat hunts across endpoint and network telemetry using Microsoft Sentinel and Microsoft Defender for Endpoint.
- Authored KQL queries against DeviceNetworkEvents and DeviceProcessEvents to isolate suspicious activity, including a living-off-the-land PowerShell port scan traced through 100+ failed internal connection attempts.
- Mapped process execution and network telemetry to MITRE ATT&CK techniques to support root-cause analysis.
- Audited and remediated Windows systems against DISA STIG controls, implementing 10+ hardening tasks across account policy, credential settings, and administrative restrictions.

SECURITY PROJECTS

DFIR Case Study: Azure Control-Plane Domain Compromise | Sentinel, Defender XDR, KQL | github.com/jo-marcelo/sentinel-mde-dfir-domain-compromise

- Reconstructed a simulated 17-hour domain compromise across three hosts using 28 documented KQL queries against Sentinel (ASIM, Sysmon, Windows Event Log) and Defender XDR; delivered a 20-page incident report.
- Established Azure Run Command abuse (T1651) as the initial access vector: an administrator password reset executed as SYSTEM, used five times across two hosts, bypassing OS privilege escalation entirely.
- Identified an AdminSDHolder ACL backdoor (T1222.001) granting a service account GenericAll, re-propagating domain-admin rights hourly and surviving password resets and host rebuilds.
- Statically analyzed five artifacts on an isolated REMnux VM, identifying RemCom and matching its named pipes to Sysmon telemetry.
- Authored and validated two Sentinel detection rules for techniques that produced no alert; corrected a KQL tokenization defect matching 1 of 7 events, surfacing a second attacker session missed in the original analysis.

Azure Brute-Force Threat Hunt | Defender for Endpoint, KQL | github.com/jo-marcelo/azure-threat-hunting-kql

- Investigated an Azure VM misconfigured with a public IP exposing internal infrastructure services (DNS, DHCP, domain services) to the internet.
- Built a five-stage KQL hunt: confirmed exposure via DeviceInfo, ranked the top 20 attacking source IPs by failed-logon volume, then joined failed against successful authentication to rule out a stealthy compromise.
- Confirmed zero unauthorized access despite sustained credential guessing (T1110.001); documented hardening steps including Azure Bastion or just-in-time access instead of public IPs.

Vulnerability Management Lab | Tenable Nessus | github.com/jo-marcelo/tenable-vulnerability-management-lab

- Ran authenticated Nessus scans against a Windows lab environment, triaged 24 findings by severity and exploitability, and drove them to 4 through targeted remediation, an 83% reduction.
- Identified removal of an end-of-life Wireshark install as the highest-yield single action, clearing 17 of the 20 resolved findings.

Windows STIG Hardening Automation | PowerShell | github.com/jo-marcelo/stig-hardening-monorepo

- Wrote paired PowerShell remediation and rollback scripts for ten DISA STIG controls covering password history, minimum password age, and lock-screen policy.
- Included deliberate misconfiguration scripts to verify audit tooling detects drift.

EDUCATION

B.S. Computer Science | Western Governors University | July 2025