Joao Marcelo Miranda

Rio de Janeiro, RJ | +55 21 97507-7948 | joao.miranda423@gmail.com
linkedin.com/in/joaomarcelo-miranda | github.com/jo-marcelo | jomiranda.com

RESUMO PROFISSIONAL

Analista de segurança com experiência prática em Microsoft Sentinel e Defender XDR, desenvolvendo consultas em KQL para investigar telemetria de endpoint, identidade e rede e mapeando achados ao MITRE ATT&CK. Bacharel em Ciência da Computação (EUA) e certificado CompTIA CySA+. Brasileiro e norte-americano, com inglês nativo, apto à contratação CLT ou PJ sem necessidade de visto.

CERTIFICAÇÕES

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

COMPETÊNCIAS TÉCNICAS

Ferramentas de Segurança: Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Endpoint (MDE), Sysmon, Tenable Nessus, Wireshark, Nmap

Linguagens e Consultas: KQL (Kusto Query Language), PowerShell, Python, Bash, SQL

Plataformas: Microsoft Azure, Active Directory, Windows Server, Linux

Áreas de Atuação: Threat hunting, resposta a incidentes, engenharia de detecção, gestão de vulnerabilidades, análise de logs, hardening de sistemas

Frameworks: MITRE ATT&CK, DISA STIG

EXPERIÊNCIA PROFISSIONAL

Engenheiro de Cibersegurança (Estágio) | LOG(N) Pacific (EUA) | Remoto | Junho de 2026 a Agosto de 2026

- Conduziu threat hunts proativos sobre telemetria de endpoint e rede utilizando Microsoft Sentinel e Microsoft Defender for Endpoint.
- Desenvolveu consultas KQL nas tabelas DeviceNetworkEvents e DeviceProcessEvents para isolar atividades suspeitas, incluindo port scan via PowerShell (living off the land) rastreado a partir de mais de 100 conexões internas malsucedidas.
- Mapeou execução de processos e telemetria de rede às técnicas do MITRE ATT&CK para apoiar análise de causa raiz.
- Auditou e corrigiu sistemas Windows conforme controles DISA STIG, implementando mais de 10 tarefas de hardening em políticas de conta, credenciais e restrições administrativas.

PROJETOS DE SEGURANÇA

Estudo de Caso DFIR: Comprometimento de Domínio via Plano de Controle do Azure | Sentinel, Defender XDR, KQL | github.com/jo-marcelo/sentinel-mde-dfir-domain-compromise

- Reconstruiu incidente simulado de comprometimento de domínio de 17 horas em três hosts, com 28 consultas KQL documentadas sobre Microsoft Sentinel (ASIM, Sysmon, Windows Event Log) e Defender XDR; entregou relatório de 20 páginas.
- Identificou o abuso do Azure Run Command (T1651) como vetor de acesso inicial: redefinição de senha administrativa executada como SYSTEM, usada cinco vezes em dois hosts, dispensando escalonamento de privilégios no sistema operacional.
- Detectou backdoor de ACL no objeto AdminSDHolder (T1222.001) concedendo GenericAll a uma conta de serviço, replicando privilégios de administrador de domínio a cada hora, sobrevivendo a resets de senha e reinstalação de hosts.
- Realizou análise estática de cinco artefatos em VM isolada com REMnux, identificando o RemCom e correlacionando seus named pipes à telemetria do Sysmon.
- Elaborou e validou duas regras de detecção no Sentinel para técnicas que não geraram alerta; corrigiu falha de tokenização em KQL que capturava apenas 1 de 7 eventos, revelando uma segunda sessão do atacante não identificada na análise original.

Threat Hunting de Força Bruta em Ambiente Azure | Defender for Endpoint, KQL | github.com/jo-marcelo/azure-threat-hunting-kql

- Investigou VM do Azure com IP público expondo serviços internos de infraestrutura (DNS, DHCP, serviços de domínio) à internet.
- Construiu caça em cinco etapas com KQL: confirmou a exposição via DeviceInfo, classificou os 20 principais IPs de origem por volume de falhas e cruzou tentativas malsucedidas com logons bem-sucedidos.
- Confirmou ausência de acesso não autorizado apesar de tentativas contínuas de adivinhação de credenciais (T1110.001); documentou medidas de hardening como Azure Bastion ou acesso just-in-time em vez de IPs públicos.

Laboratório de Gestão de Vulnerabilidades | Tenable Nessus | github.com/jo-marcelo/tenable-vulnerability-management-lab

- Executou varreduras autenticadas com Nessus em ambiente Windows de laboratório, triando 24 achados por severidade e explorabilidade e reduzindo-os a 4 por remediação direcionada, queda de 83%.
- Identificou a remoção de uma instalação do Wireshark em fim de vida como a ação isolada de maior impacto, eliminando 17 dos 20 achados resolvidos.

Automação de Hardening Windows (DISA STIG) | PowerShell | github.com/jo-marcelo/stig-hardening-monorepo

- Desenvolveu scripts PowerShell pareados de correção e reversão para dez controles DISA STIG (histórico e idade mínima de senha, tela de bloqueio), além de scripts de configuração incorreta intencional para validar a detecção de desvios pelas ferramentas de auditoria.

FORMAÇÃO ACADÊMICA

Bacharelado em Ciência da Computação | Western Governors University, EUA | Julho de 2025