Paulo Henrique da Silva

Cyber Security | Microsoft Security

São Bernardo do Campo, SP, Brasil | +55 11 94419-0192
oluaphenriquesilva@hotmail.com | linkedin.com/in/redepaulosilva

RESUMO PROFISSIONAL

Profissional de cibersegurança com experiência em projetos de implementação, integração, migração e sustentação de soluções Microsoft Security. Atuação em assessments de Sentinel e Entra ID, planejamento de Endpoint DLP e desenvolvimento de rótulos no Purview. Experiência com Defender XDR, Intune, automação, documentação técnica, workshops e treinamentos. Trabalho orientado a fundamentos de segurança, com capacidade de adaptação a diferentes plataformas e ambientes.

COMPETÊNCIAS TÉCNICAS

- **Microsoft Sentinel:** conectores, regras analíticas, investigação, KQL, threat hunting, migração de SIEM, playbooks e tuning.
- **Defender e Intune:** Defender for Endpoint, Identity e Cloud Apps; políticas de segurança para servidores via Intune e MDE.
- **Identidade:** Entra ID, Active Directory e assessments de Conditional Access.
- **Proteção de dados:** Microsoft Purview, planejamento de Endpoint DLP e desenvolvimento de rótulos para o ambiente Microsoft.
- **Integrações e automação:** Azure Logic Apps, Python, PowerShell, APIs, CEF, Syslog, Azure Arc e Azure Monitor Agent.
- **Consultoria:** assessments, arquiteturas, runbooks, workshops e treinamentos.

EXPERIÊNCIA PROFISSIONAL

Cyber Security Specialist | Ipiranga

junho de 2026 - atual

- Atuação em monitoramento, threat hunting e engenharia de detecção com SIEM/XDR; participação em simulações de ataques e avaliações para validar controles.
- Atuação em DevSecOps com integração de segurança em pipelines de CI/CD, automação de controles e colaboração com times de engenharia.

Cyber Security Consultant | Avanade

abril de 2025 - junho de 2026

- Atuei no Itaú com seis instâncias de Microsoft Sentinel em unidades internacionais: duas no Uruguai, duas no Paraguai, uma no Chile e uma em Portugal.
- Conduzi assessments de SIEM, propus melhorias nas regras de detecção e a criação de processos de hunting, apresentei recomendações ao time brasileiro e liderei a execução após aprovação.
- Participei da migração de Splunk para Sentinel: levantamento de casos de uso, conversão de SPL para KQL, migração de regras, validação de coleta, parsers e tuning.
- Desenvolvi consultas e funções KQL, analytics rules, hunting queries, entity mapping, incident grouping, watchlists, dashboards e workbooks.
- Integrei fontes Microsoft, AWS, Windows Server e dispositivos de rede por conectores nativos, Azure Arc, Azure Monitor Agent, CEF, Syslog, APIs e log forwarders.
- Criei playbooks SOAR e automation rules com Logic Apps, Python e PowerShell para revogar sessões, desabilitar contas, isolar dispositivos e apoiar contenção em AD híbrido.
- Apoiei a evolução do Sentinel e a otimização de ingestão, retenção e custos; produzi desenhos de arquitetura, runbooks e documentação técnica.
- Apoiei o CSIRT do Brasil em investigações de incidentes na camada de Azure.

EXPERIÊNCIA PROFISSIONAL - CONTINUAÇÃO

Cyber Security Specialist | Logicalis

novembro de 2024 - abril de 2025

- Atuei em Blue Team com SIEM, SOAR e XDR para clientes dos setores financeiro, governamental e de manufatura.
- Desenvolvi e otimizei casos de uso no Microsoft Sentinel, com investigação, threat hunting, correlação de eventos, tuning e enriquecimento com MISP.
- Implementei playbooks com Azure Logic Apps e integrações nativas, de terceiros e aplicações SaaS com o Microsoft Sentinel.
- Atuei com segurança de APIs, Azure API Management, OWASP API Top 10 e controles para soluções de IA generativa em Azure, AWS e GCP.

Security Analyst Sr. | TIVIT

maio de 2022 - novembro de 2024

- Fui responsável pela sustentação e manutenção de Microsoft Sentinel, Defender for Identity, Defender for Endpoint e Defender for Cloud Apps para a CSN (Companhia Siderúrgica Nacional), em ambiente com cerca de 18 mil endpoints e 48 mil contas humanas e não humanas.
- Liderei a adoção de políticas de segurança para servidores criadas no Intune e aplicadas pelo Defender for Endpoint (security settings management), com escopo definido pela tag MDE-Management, substituindo o SCCM nessa função.
- Utilizei Splunk para análise de eventos e criação de consultas SPL; atuei como usuário de CrowdStrike Falcon, com foco em endpoints, e de Rapid7 InsightIDR.
- Atuei também com migração de proxy Forcepoint/Netskope, ZTNA com Zscaler Private Access, políticas em FortiGate e Palo Alto Networks, acesso remoto e VPN IPsec.

PROJETOS E CAPACITAÇÃO TÉCNICA

- Elaborei planejamento de Endpoint DLP no Microsoft Purview e participei do desenvolvimento de rótulos e de sua aplicabilidade no ambiente Microsoft.
- Realizei assessments de Microsoft Entra ID, com exportação e análise de políticas de Conditional Access para identificar lacunas e oportunidades de melhoria.
- Conduzi workshops técnicos para clientes e ministrei treinamentos em escolas autorizadas.

CERTIFICAÇÕES

- **SC-200** | Microsoft Certified: Security Operations Analyst Associate
- **SC-300** | Microsoft Certified: Identity and Access Administrator Associate
- **SC-400** | Microsoft Certified: Information Protection and Compliance Administrator Associate
- **SC-100** | Microsoft Certified: Cybersecurity Architect Expert
- **SC-900** | Microsoft Certified: Security, Compliance, and Identity Fundamentals
- Third Party Risk Management | SecurityScorecard

FORMAÇÃO ACADÊMICA

Curso Superior em Segurança da Informação | SENAC SP | 2020 - 2023

IDIOMAS

Português: nativo.
Inglês: uso profissional em reuniões técnicas, abertura de chamados e interação com fornecedores internacionais.