RAPHAEL R. DE MOURA NETO
Centro - Avaré (SP)
raphaelmoura@live.com.pt · (14) 99818-9598
https://www.linkedin.com/in/raphaelneto11

OBJETIVO

Atuar como SOC Analyst em empresa que valorize segurança proativa e inovação, aplicando minha experiência em monitoramento, resposta a incidentes e automação para fortalecer a postura de segurança organizacional e evoluir para posições de liderança técnica em Security Operations.

PERFIL PROFISSIONAL

SOC Analyst com 3+ anos de experiência em Security Operations Center, especializado em incident response, threat detection e security monitoring. Expertise em SIEM (Splunk, QRadar, Wazuh), correlação de eventos e análise de logs. Proficiente em Python para automação de processos, ferramentas DLP, AWS Security e compliance (LGPD, ISO 27001). Track record de implementação de playbooks e redução de 40% no tempo de resposta a incidentes.

Métricas de Destaque: MTTD < 15 min | MTTR -40% | SLA 99% | 20+ playbooks criados | 100+ vazamentos prevenidos/mês

EXPERIÊNCIAS PROFISSIONAIS

- **SOC Analyst, NOBUG Tecnologia** – Florianópolis/SC (09/2025 – Presente)

  - Executo monitoramento 24x7 e threat hunting em ambientes cloud (AWS) e on-premise, detectando IOCs através de SIEM (Splunk, Wazuh, QRadar)
  Resultado: Tempo de detecção inferior a 15 minutos

  - Gerencio ciclo completo de resposta a incidentes em Windows, Linux e MacOS, desde detecção até erradicação
  Resultado: Mantendo SLA de 99% com redução de 40% no MTTR

  - Desenvolvi 15+ automações em Python para threat intelligence e resposta automatizada
  Resultado: 20 horas semanais economizadas para a equipe

  - Administro soluções DLP para classificação e monitoramento de dados sensíveis e PII
  Resultado: Prevenção de 100+ tentativas de vazamento mensalmente

- **Cyber Security Analyst, Vultus Cybersecurity Ecosystem** – São Paulo/SP (09/2023 – 07/2025)
  - Integrei eventos IAM com SIEM (QRadar, Splunk, Wazuh) para detecção avançada de anomalias e comprometimento de credenciais

  - Gerenciei identidades e acessos (Oracle IAM, Active Directory) com implementação de RBAC e segregação de funções
  Resultado: Redução de 30% em privilégios excessivos

  - Desenvolvi playbooks de automação para revisão periódica de acessos
  Resultado: Tempo de revisão reduzido de 5 dias para 8 horas

  - Elaborei dashboards executivos e relatórios de segurança para tomada de decisão estratégica

- **Cyber Security Analyst, ISH TECNOLOGIA** – São Paulo/SP (06/2022 – 03/2023)

  - Monitorei acessos críticos usando SIEM (QRadar, Sentinel, RSA NetWitness) com foco em detecção de anomalias comportamentais

  - Implementei políticas de governança de identidade em ambientes Oracle e Active Directory

  - Participei de 30+ respostas a incidentes relacionados a credenciais comprometidas e ataques de força bruta

  - Produzi relatórios e dashboards que melhoraram visibilidade de riscos em 50%

COMPETÊNCIAS TÉCNICAS

Security Operations
Incident Response | Threat Hunting | Digital Forensics | Log Analysis Event Correlation | Security Monitoring | Threat Detection

SIEM & Monitoring
Splunk | QRadar | Wazuh | Microsoft Sentinel | RSA NetWitness | Elastic

Security Tools
DLP: Netskope, Forcepoint | EDR: CrowdStrike | IDS/IPS: Snort, Suricata | Firewall: Palo Alto, Fortinet

Cloud & Identity
AWS Security (CloudTrail, GuardDuty) | Azure Security Center Oracle IAM | Active Directory | Okta | Keycloak

Automation & Development
Python (Security Automation) | API Integration | Bash | PowerShell SOAR Platforms | Regex | JSON/YAML

Frameworks & Compliance
MITRE ATT&CK | ISO 27001 | NIST CSF | CIS Controls | LGPD | OWASP Top 10

FORMAÇÃO ACADÊMICA

FACULDADE IGUAÇU | 2024
Pós-Graduação Lato Sensu **Cybersecurity** Detecção de Ameaças 360 horas
Pós-Graduação Lato Sensu **Perícia Forense Computacional** (360 horas)

CENTRO UNIVERSITÁRIO INTERNACIONAL – UNINTER
Curso Superior em Tecnologia em **Redes de Computadores** (2020 –2023)

IDIOMAS

Português – Nativo
Inglês – Intermediário
Espanhol – Intermediário

CERTIFICADOS E PROJETOS

- Wazuh for Security Engineers – 24 horas (Novembro/2023)
- Cyber Academy Febraban - Laboratório de Segurança Cibernética da Febraban - Média final 8.8 - 40 horas (julho/2023)
- Fundamentos de AWS - Escola da Nuvem - Média final 9,72 – 91 horas (julho/2023)
- Google IT Security Professional Certificate (2024) - 35h
- ISO/IEC 27001 Information Security Associate™ - 20 horas (maio/2023)
- Cisco Net Academy, Network Security – 60 horas (julho/2022)
- CECyber Cybersecurity Foundation – 25 horas (maio/2022)
- Cisco Net Academy, CyberOps Associate v1.0 – 60 horas (abril/2022)
- Cisco Net Academy, CCNAv7 (Cisco Certified Network Associate) – 60 horas (janeiro/2022)

SOFT SKILLS

- Pensamento analítico para resolução de incidentes complexos
- Capacidade de trabalhar sob pressão mantendo qualidade
- Comunicação clara para relatórios técnicos e executivos
- Colaboração efetiva em equipes multidisciplinares
- Aprendizado contínuo e adaptação rápida a novas tecnologias
- Orientação a resultados com foco em métricas e KPIs