

Anderson Pinheiro Aderaldo

Engenheiro de Cibersegurança Sênior

Rio de Janeiro, Brasil · Cidadania brasileira e da UE

✉ andersonaderaldo@gmail.com ☎  +55 21 98771-3425 ·  +351 910 567 868

🔗 linkedin.com/in/andersonaderaldo

Resumo

Engenheiro de Cibersegurança Sênior com 15 anos de experiência na proteção de infraestrutura crítica de telecomunicações, serviços financeiros digitais de grande porte e plataformas de e-commerce: 9 anos na Oi S.A., 3 anos e 7 meses na Ame Digital, depois Juntos Somos Mais e, hoje, a equipe de Cloud Security da VTEX.

Estruturei e operei ambientes de segurança do SOC ao DevSecOps em organizações que operam em escala nacional e com baixa tolerância a falhas. Principais áreas: Blue Team, SOC, SIEM/SOAR, threat hunting e DFIR na frente defensiva; segurança em nuvem (CSPM, CWPP), Zero Trust, DevSecOps e AppSec na frente de engenharia.

Ajudei a proteger a infraestrutura de eventos de alta visibilidade, entre eles o Rock in Rio 2019 e as Eleições Gerais de 2018 e 2020.

Experiência



Senior Security Engineer

VTEX

out de 2026 - o momento · Brasil

Integrante da equipe de Cloud Security, responsável pela proteção da infraestrutura de nuvem que sustenta a plataforma de comércio digital da VTEX.

- **Gestão de postura em nuvem:** monitoramento das contas de nuvem em busca de configurações incorretas e condução da correção junto aos times responsáveis.
- **Proteção de workloads:** segurança de contêineres, hosts e serviços gerenciados, incluindo gestão de vulnerabilidades de imagens e servidores.
- **Identidade e acesso:** revisão de papéis e permissões de nuvem e aplicação do princípio do menor privilégio.
- **Guardrails de segurança:** definição de baselines seguros e revisão de infraestrutura como código antes da entrada em produção.
- **Deteção e resposta:** manutenção de logs e alertas de nuvem, investigação e resposta a incidentes de segurança em nuvem.
- **Parceria com engenharia:** apoio aos times de produto e plataforma em arquitetura segura de nuvem.



Information Security Specialist

Juntos Somos Mais

mar de 2025 - ago de 2026 (1 ano e 6 meses) · Rio de Janeiro, Brasil

Responsável pela resiliência cibernética e governança de segurança da infraestrutura, atuando na proteção de ativos críticos e na disseminação da cultura de segurança com uma abordagem consultiva e técnica.

- **Cloud Security & DevSecOps:** implementação de estratégias de CSPM e CWPP com Orca Security. Atuação direta em SCA (Software Composition Analysis) e patch management em código e servidores cloud, com testes de segurança (security gates) integrados ao pipeline de CI/CD.
- **Segurança de borda e aplicação:** administração e tuning das camadas de proteção Akamai (WAF, Bot Manager e CDN). Implementação de arquitetura de acesso seguro ZTNA (Zero Trust Network Access) com Netskope.
- **Gestão de vulnerabilidades e endpoint:** gestão do ciclo de vida de vulnerabilidades em estações de trabalho com ManageEngine e monitoramento avançado de ameaças com Trend Micro Vision One (XDR).
- **Governança, Risco e Compliance (GRC):** sustentação do SGSI com foco na recertificação ISO 27001; elaboração de normas, padrões de segurança e políticas corporativas.
- **Monitoramento e resposta a incidentes:** implementação e gestão do Elastic SIEM. Threat intelligence com Axur para proteção de marca e mitigação de riscos externos.

- **Cultura de segurança:** gestão do programa de security awareness e execução de simulações de phishing na plataforma KnowBe4.



Security Engineer

Ame Digital

dez de 2020 - jun de 2024 (3 anos e 7 meses) · Rio de Janeiro, Brasil

SOC, Blue Team, threat hunting e security intelligence

- Implantação do SOC (Security Operations Center) do zero: soluções de segurança, documentação básica de processos e procedimentos, coletores de logs e alertas de segurança, com handover para o time de operação.
- Suporte direto ao Blue Team na melhoria das defesas e na implementação das soluções de segurança.
- Competências desenvolvidas: gerenciamento e segurança em cloud, CSPM, CWPP, Next-Generation Antivirus (NGAV), SIEM/SOAR, segurança de borda, Zero Trust, threat intelligence de fontes abertas e threat hunting.

Application Security, DevSecOps e automação

- Implementação do DevSecOps do zero, com um pipeline seguro no GitHub Actions.
- Desenvolvimento e implementação dos testes de SCA, SAST, DAST, Secret Scanning, IaC e Container Security.
- Documentação das ferramentas de segurança e capacitação de todos os desenvolvedores no uso delas e na correção das vulnerabilidades encontradas.
- Competências desenvolvidas: segurança no DevOps, arquitetura segura, desenvolvimento de automações e definição de padrões de segurança.



Especialista em Cyber Security

Oi S.A.

mar de 2019 - nov de 2020 (1 ano e 9 meses) · Rio de Janeiro, Brasil

Líder da equipe de segurança de infraestrutura de TI, coordenando projetos de proteção de perímetro, segurança de sistemas operacionais, dispositivos de rede, bancos de dados e infraestrutura web, e arquitetura segura de nuvem híbrida.

- Gestão de projetos de segurança e infraestrutura.
- Implementação de hardening em Windows e Linux, dispositivos de rede (roteadores e switches) e bancos de dados (Oracle, SQL Server, MongoDB).
- Análise e tratamento de regras de firewall com Tufin SecureTrack.
- Planejamento do gerenciamento de políticas de segurança do Cisco WSA e do Cisco ESA (controle de conteúdo).
- Planejamento da proteção de DNS com Cisco Umbrella.
- Planejamento da solução anti-DDoS com NETSCOUT AED, antigo Arbor Networks Pravail (APS).
- Avaliação de segurança da infraestrutura com Nessus e shodan.io.
- Definição de baselines de segurança para ativos de telecomunicações.
- Análise e proteção da arquitetura de rede e da nuvem híbrida com visão de segurança.
- Gestão de ameaças e vulnerabilidades com RSA Archer.
- Prestação de serviços gerenciados de segurança em eventos patrocinados (proteção de perímetro com firewall L7, controle de conteúdo, anti-DDoS, hardening, monitoramento e segurança de DNS) para proteger a infraestrutura dos eventos contra ataques cibernéticos.

Eventos patrocinados protegidos: Game XP (2017, 2018, 2019), Rio2C (2018, 2019), Comic Con Experience (2018, 2019), Rock in Rio 2019 e Eleições Gerais (2018, 2020).



Analista de Segurança da Informação

Oi S.A.

jul de 2013 - fev de 2019 (5 anos e 8 meses) · Rio de Janeiro, Brasil

Atuação nas equipes internas do Centro de Operações de Segurança (SOC) e de Perícia Digital e Resposta a Incidentes (DFIR).

Centro de Operações de Segurança (SOC)

- Criação e revisão de procedimentos operacionais para tratamento de incidentes de segurança (L1 e L2).

- Projetos de melhoria de infraestrutura em sistemas de coleta de logs e alarmes.
- Suporte operacional e criação de alarmes de segurança.
- Detecção e neutralização de ameaças de vírus e ransomware.
- Facilitação da adoção de novos procedimentos pela operação.
- Análise de incidentes no NetIQ Sentinel SIEM e no ArcSight SIEM e criação de alarmes de correlação.
- Controle da conformidade das regras de firewall com Tufin SecureTrack.
- Operação do antivírus Broadcom SEP para proteção contra vírus, spyware e ransomware.
- Tratamento L2 e L3 de tickets de segurança da informação (regras de firewall, controle de conteúdo).

Perícia Digital e Resposta a Incidentes (DFIR)

- Análise e resolução de incidentes de segurança da informação L3.
- Tratamento de fraudes tecnológicas com base na segurança do negócio.
- Elaboração de procedimentos operacionais internos.
- Aquisição de imagens de disco com Tableau TD3 e Image MASster Solo-5.
- Perícia forense em dispositivos móveis com Cellebrite UFED.
- Perícia forense computacional com EnCase e Autopsy.
- Monitoramento de atividades suspeitas de funcionários com Veriato Investigator.
- Monitoramento do ambiente em busca de ameaças com RSA NetWitness.
- Busca de possíveis novos incidentes em bancos de dados, sistemas operacionais, ativos de rede e sistemas críticos.
- Investigação de violações de segurança e suporte à empresa nas questões disciplinares e legais associadas.
- Abertura de salas de crise e criação de planos de ação para as principais ameaças.



Estagiário de Segurança da Informação

Oi S.A.

nov de 2011 - jun de 2013 (1 ano e 8 meses) · Rio de Janeiro, Brasil

Estagiário da equipe de segurança da informação, atuando na prevenção de segurança de TI.

- Tratamento de tickets L1 (firewall, controle de conteúdo, antivírus).
- Organização das atividades da equipe e consolidação das apresentações de resultados.
- Notificação dos responsáveis pelos ativos quando novas vulnerabilidades eram detectadas.
- Gerenciamento de pequenos projetos de segurança.



Assistente de Serviços Corporativos

Contax S.A.

mai de 2008 - out de 2011 (3 anos e 6 meses) · Rio de Janeiro, Brasil

Operador de atendimento da Oi S.A. na equipe de atendimento personalizado a clientes de alto valor, tratando demandas de telefonia fixa, móvel, banda larga e links de dados de alta velocidade, incluindo suporte remoto.

Formação acadêmica



Universidade Federal do Rio de Janeiro

MBA (especialização), Gerência de Segurança da Informação

2018 - 2020



Centro Universitário Carioca (UniCarioca)

Tecnólogo, Análise e Desenvolvimento de Sistemas

2010 - 2013

Licenças e certificações



GitLab Certified Associate - GitLab

Emitido em abr de 2022 · de2e5529-edf0-44c0-8b92-17ec6a243b3a



Microsoft Certified: Azure Data Fundamentals - Microsoft

Emitido em jun de 2021

**Microsoft Certified: Azure AI Fundamentals** - Microsoft

Emitido em jun de 2021

**Microsoft Certified: Azure Fundamentals** - Microsoft

Emitido em out de 2020 · H551-3317

**Scrum Foundation Professional Certificate (SFPC)** - Certiprof

Emitido em jun de 2020 · CLVSQDQFSS-SQGHLZGJ-XHRHRHPTMH

**ICSI | CNSS Certified Network Security Specialist** - ICSI (International CyberSecurity Institute), UK

Emitido em mai de 2020 · 18218405

**Autopsy 8-Hour Online Training** - Basis Technology

Emitido em abr de 2020 · 17209320

**Firepower Threat Defense FTD NGFW & NGIPS** - Cisco

Emitido em ago de 2018

**Huawei Certified Network Associate - LTE** - Huawei

Emitido em set de 2017

**RSA NetWitness Administration e RSA NetWitness Analysis** - RSA Security

Emitido em out de 2015 e jul de 2015

**Cursos Cisco Networking Academy** - Cisco

CCNA R&S: Introduction to Networks e Routing and Switching Essentials (2016) · Cybersecurity Essentials, Introduction to IoT e Get Connected (2020)

**Linux Unhatched** - Network Development Group

Emitido em mai de 2020

**Cybereason Threat Hunter e Cybereason Certified Threat Analyst** - Cybereason

Emitido em jun de 2021 e mar de 2021 · Expirado em jun de 2023 e mar de 2023

**AccessData Certified Investigator** - AccessData (Exterro FTK)

Emitido em mai de 2020 · Expirado em mai de 2022

**NSE 1 e NSE 2 Network Security Associate** - Fortinet

Emitido em abr de 2020 · Expirado em abr de 2022 · VAr41N1hUD / 0x26FuSum8

Competências

Operações defensivas: Blue Team · Defesa de Perímetro · Operações de Segurança (SOC) · SIEM/SOAR · Threat Hunting · Resposta a Incidentes · Perícia Forense Computacional (DFIR) · Mitigação de DDoS**Engenharia de segurança:** Cloud Security (CSPM, CWPP) · Zero Trust · DevSecOps · AppSec · Segurança de Redes · Firewalls · Hardening**Governança e liderança:** Gestão de Ameaças e Vulnerabilidades · ISO 27001 · Security Awareness · Liderança**Plataformas:** Orca Security · Snyk · Netskope · Akamai · Elastic SIEM · Trend Micro Vision One · Cybereason · Microsoft Sentinel · NetIQ Sentinel · ArcSight · RSA NetWitness · GitHub Actions · Nessus · Cellebrite UFED · EnCase

Idiomas

Português (nativo) · Inglês (nível profissional) · Espanhol (básico)