

# Anderson Pinheiro Aderaldo

## Senior Cybersecurity Engineer

Rio de Janeiro, Brazil · Brazilian & EU citizen

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

🔗 [linkedin.com/in/andersonaderaldo](https://linkedin.com/in/andersonaderaldo)

## Summary

Senior Cybersecurity Engineer with 15 years of experience protecting critical telecommunications infrastructure, large-scale digital financial services and e-commerce platforms: 9 years at Oi S.A., 3 years 7 months at Ame Digital, then Juntos Somos Mais, and now the Cloud Security team at VTEX.

Built and operated security environments from SOC to DevSecOps in organizations running at national scale with low tolerance for failure. Core areas: Blue Team, SOC, SIEM/SOAR, threat hunting and DFIR on the defensive side; cloud security (CSPM, CWPP), Zero Trust, DevSecOps and AppSec on the engineering side.

Helped protect the infrastructure of high-visibility events, including Rock in Rio 2019 and the Brazilian General Elections of 2018 and 2020.

## Experience



### Senior Security Engineer

VTEX

*Oct 2026 - Present · Brazil*

Member of the Cloud Security team, protecting the cloud infrastructure behind VTEX's digital commerce platform.

- **Cloud posture management:** monitor cloud accounts for misconfigurations and drive remediation with the owning teams.
- **Workload protection:** secure containers, hosts and managed services, including vulnerability management for images and servers.
- **Identity and access:** review cloud roles and permissions and enforce least privilege.
- **Security guardrails:** define secure baselines and review infrastructure as code before it reaches production.
- **Detection and response:** maintain cloud logging and alerting, and investigate and respond to cloud security incidents.
- **Engineering partnership:** advise product and platform teams on secure cloud architecture.



### Information Security Specialist

Juntos Somos Mais

*Mar 2025 - Aug 2026 (1 year 6 months) · Rio de Janeiro, Brazil*

Responsible for the cyber resilience and security governance of the infrastructure, protecting critical assets and spreading security culture through a consultative, technical approach.

- **Cloud Security & DevSecOps:** implemented CSPM and CWPP strategies with Orca Security. Hands-on SCA (Software Composition Analysis) and patch management for code and cloud servers, with security gates integrated into the CI/CD pipeline.
- **Edge and application security:** administered and tuned Akamai protection layers (WAF, Bot Manager and CDN). Implemented ZTNA (Zero Trust Network Access) with Netskope.
- **Vulnerability and endpoint management:** managed the vulnerability lifecycle on workstations with ManageEngine and monitored advanced threats with Trend Micro Vision One (XDR).
- **Governance, Risk and Compliance (GRC):** sustained the ISMS for ISO 27001 recertification; wrote security standards and corporate policies.
- **Monitoring and incident response:** implemented and managed Elastic SIEM. Ran threat intelligence with Axur for brand protection and external risk mitigation.
- **Security culture:** ran the security awareness program and phishing simulations on KnowBe4.



## Security Engineer

Ame Digital

*Dec 2020 - Jun 2024 (3 years 7 months) · Rio de Janeiro, Brazil*

### SOC, Blue Team, threat hunting and security intelligence

- Deployed the Security Operations Center (SOC) from scratch: security solutions, baseline process and procedure documentation, log collectors and security alerts, followed by handover to the operations team.
- Supported the Blue Team directly in improving defenses and implementing security solutions.
- Skills developed: cloud management and security, CSPM, CWPP, Next-Generation Antivirus (NGAV), SIEM/SOAR, edge security, Zero Trust, open source threat intelligence and threat hunting.

### Application Security, DevSecOps and automation

- Implemented DevSecOps from scratch with a secure pipeline on GitHub Actions.
- Developed and implemented SCA, SAST, DAST, secret scanning, IaC and container security tests.
- Documented the security tooling and trained all developers on using it and fixing the vulnerabilities found.
- Skills developed: security in DevOps, secure architecture, automation development and definition of security standards.



## Cyber Security Specialist

Oi S.A.

*Mar 2019 - Nov 2020 (1 year 9 months) · Rio de Janeiro, Brazil*

Team lead of the IT infrastructure security team, coordinating projects in perimeter protection, security of operating systems, network devices, databases and web infrastructure, and secure hybrid cloud architecture.

- Managed security and infrastructure projects.
- Implemented hardening on Windows and Linux, network devices (routers and switches) and databases (Oracle, SQL Server, MongoDB).
- Analyzed and handled firewall rules with Tufin SecureTrack.
- Planned security policy management for Cisco WSA and Cisco ESA (content control).
- Planned DNS protection with Cisco Umbrella.
- Planned the anti-DDoS solution with NETSCOUT AED, formerly Arbor Networks Pravail (APS).
- Assessed infrastructure security with Nessus and shodan.io.
- Defined security baselines for telecommunications assets.
- Analyzed and protected the network architecture and the hybrid cloud from a security perspective.
- Managed threats and vulnerabilities with RSA Archer.
- Delivered managed security services at sponsored events (perimeter protection with L7 firewall, content control, anti-DDoS, security hardening, monitoring and DNS security) to protect event infrastructure against cyber attacks.

Sponsored events protected: Game XP (2017, 2018, 2019), Rio2C (2018, 2019), Comic Con Experience (2018, 2019), Rock in Rio 2019 and the Brazilian General Elections (2018, 2020).



## Information Security Analyst

Oi S.A.

*Jul 2013 - Feb 2019 (5 years 8 months) · Rio de Janeiro, Brazil*

Worked on the internal Security Operations Center (SOC) and Digital Forensics and Incident Response (DFIR) teams.

### Security Operations Center (SOC)

- Created and reviewed operational procedures for security incident handling (L1 and L2).
- Ran infrastructure improvement projects for log collection and alarm systems.
- Provided operational support and created security alarms.
- Detected and neutralized virus and ransomware threats.
- Facilitated the adoption of new procedures by the operations team.
- Analyzed incidents in NetIQ Sentinel SIEM and ArcSight SIEM and created correlation alarms.
- Controlled firewall rule compliance with Tufin SecureTrack.
- Operated Broadcom SEP antivirus to protect against viruses, spyware and ransomware.
- Handled L2 and L3 information security tickets (firewall rules, content control).

## Digital Forensics and Incident Response (DFIR)

- Analyzed and resolved L3 information security incidents.
- Handled technology fraud cases based on business security.
- Wrote internal operational procedures.
- Acquired disk images with Tableau TD3 and Image MASSter Solo-5.
- Performed mobile forensics with Cellebrite UFED.
- Performed computer forensics with EnCase and Autopsy.
- Monitored suspicious employee activity with Veriato Investigator.
- Monitored the environment for threats with RSA NetWitness.
- Searched for possible new incidents in databases, operating systems, network assets and critical systems.
- Investigated security breaches and supported the company with the related disciplinary and legal matters.
- Opened crisis rooms and created action plans for major threats.



## Information Security Intern

Oi S.A.

*Nov 2011 - Jun 2013 (1 year 8 months) · Rio de Janeiro, Brazil*

Intern on the information security team, working on IT security prevention.

- Handled L1 tickets (firewall, content control, antivirus).
- Organized team activities and consolidated results presentations.
- Notified asset owners when new vulnerabilities were detected.
- Managed small security projects.



## Corporate Services Assistant

Contax S.A.

*May 2008 - Oct 2011 (3 years 6 months) · Rio de Janeiro, Brazil*

Customer service operator for Oi S.A. on the personalized support team for high-value customers, handling issues with fixed line, mobile, broadband and high-speed data links, including remote support.

## Education



### Universidade Federal do Rio de Janeiro

MBA (specialization), Information Security Management

*2018 - 2020*



### Centro Universitário Carioca (UniCarioca)

Technologist, Systems Analysis and Development

*2010 - 2013*

## Licenses & Certifications



### GitLab Certified Associate - GitLab

Issued Apr 2022 · de2e5529-edf0-44c0-8b92-17ec6a243b3a



### Microsoft Certified: Azure Data Fundamentals - Microsoft

Issued Jun 2021



### Microsoft Certified: Azure AI Fundamentals - Microsoft

Issued Jun 2021



### Microsoft Certified: Azure Fundamentals - Microsoft

Issued Oct 2020 · H551-3317



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

Issued Jun 2020 · CLVSQDQFSS-SQGHLZGJ-XHRHRHPTMH



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

Issued May 2020 · 18218405

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

Issued Apr 2020 · 17209320

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

Issued Aug 2018

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

Issued Sep 2017

**RSA NetWitness Administration** and **RSA NetWitness Analysis** - RSA Security

Issued Oct 2015 and Jul 2015

**Cisco Networking Academy courses** - Cisco

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

**Linux Unhatched** - Network Development Group

Issued May 2020

**Cybereason Threat Hunter** and **Cybereason Certified Threat Analyst** - Cybereason

Issued Jun 2021 and Mar 2021 · Expired Jun 2023 and Mar 2023

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

Issued May 2020 · Expired May 2022

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

Issued Apr 2020 · Expired Apr 2022 · VAR41N1hUD / 0x26FuSum8

## Skills

**Defensive operations:** Blue Team · Perimeter Defense · Security Operations (SOC) · SIEM/SOAR · Threat Hunting · Incident Response · Computer Forensics (DFIR) · DDoS Mitigation**Security engineering:** Cloud Security (CSPM, CWPP) · Zero Trust · DevSecOps · AppSec · Network Security · Firewalls · Hardening**Governance and leadership:** Threat & Vulnerability Management · ISO 27001 · Security Awareness · Leadership**Platforms:** 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

## Languages

Portuguese (native) · English (professional working proficiency) · Spanish (elementary)