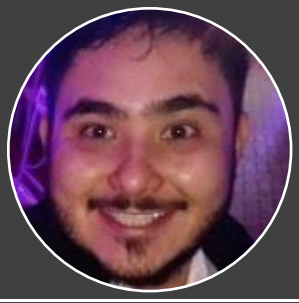

ACADEMIC EDUCATION

Cyber Defense **FIAP,** São Paulo, SP, Graduated in January 2022

LANGUAGES

Brazilian Portuguese: Mother language

English:

Advanced – C1

German:

Beginner – A1

CASSIO NAKAGAWA

@ cassio.nakagawa@gmail.com +55 11 97168-4214 14/01/1990

Londrina, Parana, Brazil

PROFESSIONAL RESUME

With 14 years of experience in IT management and governance, network administration, cybersecurity, incident response, and SOC, I have consistently contributed to strengthening organizational security. Below are key highlights of my expertise:

- **Incident Response:**
  - Created and documented incident response processes, improving team efficiency and accuracy.
  - Designed and delivered training sessions ensuring greater user knowledge and Cybersecurity behavior
  - Response time from incident registration to the first security decision from 18 days to just 15 minutes - a 99% improvement.
  - 18% High vulnerabilities reduction in our cloud environment.
- **SOC Operations:**
  - Acted as a Level 1 and level 2 analyst in SOC, suggesting improvements to detection rules and identifying critical incidents across multiple tools as Microsoft Defender Suit, CrowdStrike Falcon, Splunk and Qradar.
  - Spearheaded the implementation of a SOC using Microsoft Sentinel, including the development of detection rules (Detection engineering), engineering workflows (Security Automation engineer), and documentation.
  - Implementation of a Hybrid operations SOC to a big North American company. This operation was executed in 2 months exceeding the customer expectations.
- **Penetration Testing Support:**
  - Provided support to the penetration testing team, coordinating deliverables and conducting alignment meetings with clients to ensure clarity and successful execution.

CAREER

April 2025 – Current
TCS – Senior Information Security Consultant, Londrina, Parana.

Cybersecurity Analyst - SOC (Level 1 and Level 2):
With extensive experience in cybersecurity incident management and response, I have worked with a hybrid approach between Level 1 and Level 2. Main responsibilities include:

- Incident Triage: Monitoring security alerts and events, analyzing and performing initial incident triage with tools such as Splunk, CrowdStrike, Microsoft Defender, and XDR, escalating to higher levels as needed.
- Awareness and Training: Conducting security awareness sessions for users and training for new SOC agents, focusing on best practices and incident prevention.
- SOC Improvements and Development: Collaborating with the local team and the client's SOC to continuously improve operations, create new detection rules, suggest improvements, and tune tools and processes.
- Threat Management and Response: Using Splunk and XDR to investigate and respond to complex threats, mitigating risks and improving the organization's security posture.

Tools:

- SIEM – Sentinel, Splunk, Qradar.
- EDR – CrowdStrike Falcon, Microsoft Defender

April 2022 – April 2025
Capgemini – Senior Information Security Consultant, Barueri, São Paulo

CSIRT (Computer Security Incident Response Team):
Act on a project to implement a CSIRT. As a member of the team, my work covered several fronts, from creating the processes of a CSIRT and documenting incidents, to more technical situations, such as analyzing malware, phishing, vulnerabilities and gathering evidence. As part of my responsibilities, I was also involved in managing incidents and coordinating efforts between IT, security, and other relevant departments. In short, my experience has allowed me to develop skills in project management, technical leadership and complex problem solving.

- Identification and classification of information security incidents
- Investigation and analysis of security incidents
- Gathering evidence for forensic analysis
- Vulnerability Management
- Development and implementation of security policies
- Notification of security incidents to internal and external stakeholders (such as business partners, cybersecurity authorities, etc.)
- Communication with internal and external stakeholders during and after a security incident

Security Operation Center:
Participating in SOC Planning and implementation.

- SOC Planning and Implementation: Supporting, planning, and implementing a Security Operations Center, including defining its architecture, processes, and technologies.
- Incident Response Management: Developed and implemented incident response plans and procedures to ensure timely and effective handling of security incidents.
- Monitoring and Detection: Established continuous monitoring and detection capabilities using advanced SIEM (Security Information and Event Management) tools and other security technologies.
- Threat Intelligence Integration: Integrated threat intelligence feeds and analysis into SOC operations to enhance the detection and response to emerging threats.

Pentest:
Participation in penetration tests to assess the effectiveness of the organization's security measures.

- Planning and Scope Definition: Organized and defined the scope of penetration testing activities, ensuring alignment with organizational objectives and regulatory requirements.
- Reporting and Documentation: Prepared detailed reports on findings, including risk assessments and remediation recommendations, ensuring clear communication to technical and non-technical stakeholders.
- Remediation Support: Collaborated with IT teams to provide guidance and support for remediation efforts, ensuring vulnerabilities are effectively addressed.
- Continuous Improvement: Participated in post-assessment reviews to identify opportunities for improving the pentesting process and enhancing overall security posture.

April 2012 – April 2022

Pilz from Brazil - IT Analyst, Indaiatuba, São Paulo

IT department management for approximately 10 years, where I apply:

- IT management and governance (ISO20000, ISO27001, ISO27002)
- Development and support of Information Technology and Security
- LGPD (General Data Protection)
- Management of mobile devices (Android and IOS)
- computers
- Network Administration (Switches, Routers, Firewalls)
- Servers (Windows)
- Information Security at Security Awareness Officer level
- Information Security at SOC Analyst level
- User training
- Hyper-V Virtual Environment

SOFT SKILLS

- Crisis management
- Good communication
- Responsibility and ethics
- Problem solving initiative.
- Creation and implementation of new initiatives
- Empathy and ability to understand different perspectives.
- Problem analysis and diagnosis.

HARD SKILLS

Cybersecurity

- CSPM (Microsoft Defender for Cloud)
- SIEM (Microsoft Sentinel, Splunk, Qradar)
- Firewall (Fortigate)
- Pentesting
- EDR(CrowdStrike, Microsoft Defender)

Networking

- Routers (CISCO)
- Switches (CISCO, DELL, ExtremeNetworks)
- Network Architecture

Virtualization and Operating Systems

- Hyper-V Virtual Environment
- Windows Operating Systems (Client and Server)
- Linux Operating Systems (Client and Server)

Process and Automation

- Workflow design
- Microsoft PowerAutomate
- Microsoft PowerApps
- Azure Logic Apps

Standards and Best Practices

- ISO27001/27002
- LGPD
- NIST
- ISO20000
- ITIL v3

CERTIFICATIONS

- Blue Team Level 1 (BTL1)
- Google Cloud Professional Cloud Security Engineer
- Google Cloud Professional Cloud Network Engineer
- Professional Google Workspace Administrator
- SC-200 - Microsoft Certified: Security Operations Analyst Associate
- SC-900 - Microsoft Certified: Security, Compliance, and Identity Fundamentals
- AI-900 - Microsoft Certified: Azure AI Fundamentals
- AZ-900 - Microsoft Certified: Azure Fundamentals
- ServiceNow Certified System Administrator
- ServiceNow Certified Implementation Specialist – Security Incident Response
- ISC^2 - Certified in Cybersecurity
- AWS Certified Cloud Practitioner
- Professional Qualification Certificate in Cybersecurity and Network Architecture by FIAP
- Professional Qualification Certificate in Malwares and Vulnerability Management by FIAP
- Certificate of Professional Qualification in Cybernetic Intelligence and Counterintelligence by FIAP
- Professional Qualification Certificate in Vulnerability and Intrusion Analysis Testing

- Qualys Vulnerability Management Detection & Response