CARLOS ASSIS BRITO DE OLIVEIRA FILHO

Analista Sênior de Segurança da Informação e Infraestrutura de TI

Fortinet Certified Associate · Cisco NetAcad · F5 BIG-IP/WAF · Wazuh SIEM · Zero Trust

Fortaleza, CE, Brasil | +55 85 98134-3937 | cassisfilho@gmail.com
linkedin.com/in/cassisfilho | credly.com/users/cassisfilho | carlosassis.ddns.net

RESUMO PROFISSIONAL

Profissional de TI desde 1995, com mais de 24 anos no setor público em infraestrutura crítica, segurança de redes e liderança técnica. Na SME Fortaleza, administro cerca de 200 VMs que sustentam mais de 266 mil contas ativas e 57 TB de dados, e lidero a equipe de analistas N2/N3. Implantei F5 BIG-IP com ASM/WAF (48 aplicações), Check Point SASE (Zero Trust) e Wazuh SIEM/XDR em produção, e conduzi PoC de EDR SentinelOne a convite do fabricante. Certificado Fortinet e Cisco; pós-graduado em Governança de TI e em IA aplicada à Gestão Pública.

COMPETÊNCIAS TÉCNICAS

Segurança e perímetro: Check Point SASE, FortiGate, SentinelOne (EDR/XDR), F5 BIG-IP/ASM (WAF), SonicWall, pfSense, hardening, LGPD

SIEM e SecOps: Wazuh (agentes Windows e Linux), análise de logs, correlação de eventos, resposta a incidentes

Balanceamento e WAF: F5 BIG-IP: VIPs, pools, iRules, profiles, SNI, ASM com aprendizado supervisionado e geopolicy

Infraestrutura: VMware (~200 VMs), Windows Server, Active Directory/GPO, Linux (RHEL, Ubuntu), patch management, Docker, Apache, Nginx, Tomcat

Redes e serviços: DNS, DHCP, VPN, VoIP/SIP, Wi-Fi (Cisco, TP-Link Omada), MDM

Monitoramento e automação: Zabbix 7.0 LTS, Nagios, Grafana, Python/Shell, Google Workspace (automação), ferramentas internas com IA

Cloud: Google Workspace (administração e automação), Google Cloud (fundamentos)

Governança: ITIL, COBIT, gestão de SLA, continuidade de negócios

EXPERIÊNCIA PROFISSIONAL

Analista Sênior de Infraestrutura de TI e Segurança
Abr 2013 – Presente
SME – Secretaria Municipal de Educação de Fortaleza

- Implantei o F5 BIG-IP do zero, migrando 48 aplicações de proxy reverso Nginx (VIPs, pools, profiles, iRules, SNI); no módulo ASM (WAF), usei aprendizado supervisionado, validação manual de assinaturas e geopolicy, com várias aplicações em bloqueio ativo.
- Implantei o Check Point SASE em produção (Zero Trust) e resolvi incidente crítico no conector Auth0 em servidor essencial, garantindo a continuidade do serviço.
- Implantei o Wazuh SIEM/XDR com agentes em servidores Windows e Linux, centralizando a coleta e a correlação de eventos de segurança.
- Liderei, como responsável técnico, PoC de 3 meses do SentinelOne EDR (2026) a convite do fabricante: deploy, mitigação de ameaças e desinstalação remota, validados em parque legado com HDDs de 5400 rpm.
- Administro cerca de 200 VMs (VMware) para mais de 266 mil contas ativas e 57 TB de dados, com perímetros Fortinet e Check Point, hardening de Windows Server e Linux, DNS, DHCP, VPN, VoIP/SIP, Docker e conformidade com a LGPD.
- Lidero analistas N2/N3 na operação diária de redes, servidores e segurança, com foco em alta disponibilidade e cumprimento de SLA.
- Automatizei o provisionamento e o ciclo de vida de mais de 266 mil contas do Google Workspace via scripts, eliminando processos manuais e erros de provisionamento.
- Desenvolvi ferramentas internas com IA: chatbot integrado ao Zabbix para diagnóstico em tempo real e interface de consulta ao Active Directory.

Analista de Suporte e Infraestrutura de TI
Nov 2007 – Mar 2013
SEDUC – Secretaria Estadual da Educação do Ceará

- Prestei suporte N2/N3 de campo e remoto a mais de 700 escolas estaduais (redes, servidores e aplicações).
- Liderei a migração do Wi-Fi corporativo para Cisco, padronizando a conectividade de toda a rede estadual.
- Implantei o Kaspersky Endpoint Security, centralizando o antivírus e eliminando infecções recorrentes, e o Nagios, ampliando a visibilidade de incidentes.

Técnico de Suporte de Hardware e Software
Jun 2002 – Out 2007
SEDUC – Secretaria Estadual da Educação do Ceará

- Suporte presencial e remoto a hardware, sistemas operacionais e segurança de dados; participação em migrações de sistemas e atualizações tecnológicas em escolas.

CERTIFICAÇÕES

Fortinet: Certified Associate Cybersecurity (FCA), Certified Fundamentals Cybersecurity (FCF) e NSE 1, 2 e 3 Certified, válidas até mai/2028; FortiGate 7.6 Operator (mai/2026)

Cisco NetAcad (2026): Cybersecurity Defense Analyst Career Path; Junior Cybersecurity Analyst Career Path; Cyber Threat Management; Network Defense; Endpoint Security; CCNA: Introduction to Networks; Networking Devices and Initial Configuration; Networking Basics; Introduction to Cybersecurity; Digital Safety and Security Awareness; AI Fundamentals

Cloud e segurança (Coursera, set/2026): Google Cloud Fundamentals: Core Infrastructure (Google Cloud); Cybersecurity and Privacy (Microsoft)

Outras: TP-Link OCNA Wireless (Omada), válida até mai/2029; IBM SkillsBuild AI Fundamentals (2026)

Credenciais verificáveis: credly.com/users/cassisfilho

FORMAÇÃO ACADÊMICA

Pós-graduação Lato Sensu em IA e Tecnologia na Gestão Pública – Gran Faculdade, 360h (Out 2025 – Abr 2026)

Pós-graduação Lato Sensu em Governança de TI – Gran Faculdade, 360h (Out 2025 – Mar 2026)

Superior de Tecnologia em Redes de Computadores – FIC / Estácio (Concluído em Dez 2009)

IDIOMAS

Inglês: intermediário. Leitura técnica e compreensão auditiva boas; conversação em nível intermediário. Cursos Cisco NetAcad English for IT 1 e 2 (out/2026).

EVENTOS E CAPACITAÇÕES

- RSA Conference 2026 (San Francisco, EUA): participante a convite da SentinelOne, com foco em detecção de ameaças com IA e Zero Trust.
- SentinelOne Securing AI Virtual Bootcamp (set/2026, 2h).
- 2º Congresso de Governança, Segurança da Informação e Privacidade de Dados, Rede Governança Brasil (out/2026, 8h).
- Gemini Academy 2026, Amplifica/Google Partner: IA do Google Workspace e Gemini Enterprise (out/2026, 2h).