

Lucas Negrelli

Segurança da Informação

O lado que aparece. E o que ninguém vê.

Estágio ou N1

SOC

NOC

Suporte técnico

Redes

Hardening



QUEM SOU

Faço a parte que aparece e a parte que ninguém vê.

O design e o texto da página, e a configuração que impede ela de cair ou ser invadida. Estudo Segurança da Informação na FATEC São Caetano do Sul e faço a formação CCNA da Cisco. Procuro estágio ou vaga N1 em SOC, NOC ou suporte técnico, em São Paulo, no período diurno.

A+

nota no Mozilla Observatory,
verificável ao vivo no meu site

1

incidente real contido e limpo:
webshell, admin falso e banco
comprometido

7

trabalhos no ar ou entregues, de
site de clínica a produto
próprio

2/3

curso da trilha CCNA
concluídos, o terceiro em
andamento

RESPOSTA A INCIDENTE

O site começou a servir spam. Fui olhar os arquivos e os logs.

■	■	■	■	■
01 · SINAL	02 · ACHADOS	03 · CONTENÇÃO	04 · DESCOBERTA	05 · RECUPERAÇÃO
Spam Site de uma artista, num WordPress antigo, passou a servir spam.	Três indícios Webshell no diretório de uploads, usuário administrador que ninguém criou e entradas plantadas na base.	Isolar e limpar Isolei o site, removi os backdoors, derrubei o usuário falso e limpei a base.	Era maior A hospedagem compartilhada inteira estava comprometida, não só aquele site.	Sem a porta Migrei para base estática, sem painel e sem banco, e desenvolvi o site novo.

Não tentei blindar o WordPress.
O melhor jeito de defender uma porta é não ter a porta.

-23.5505, -46.6333

RESPOSTA A INCIDENTE

HARDENING

Um portfólio que prova a própria segurança.

A página lê os cabeçalhos de resposta do próprio servidor, calcula uma nota e mostra o valor bruto de cada um. Depois executa três ataques contra si mesma: injeção de script, enquadramento em iframe e teste de tipo de arquivo.

CSP estrita

HSTS com preload

X-Frame-Options

Referrer-Policy

Permissions-Policy

Nota A+ no Mozilla Observatory. Zero dependência externa: nenhuma requisição a terceiros.



REDUZIR A SUPERFÍCIE DE ATAQUE

Menos peça ligada é menos peça que pode **vazar**.

ENOKIBARA · ANTES

Clínica de ortopedia

- ✗ WordPress lento, vários segundos para carregar
- ✗ Painel de administração acessível de qualquer lugar
- ✗ Plugin de agendamento pedindo atualização toda semana



ENOKIBARA · DEPOIS

Site estático

- ✓ Carrega na hora, mesmo conteúdo e visual
- ✓ Sem banco, sem login, sem plugin
- ✓ Quase nada sobrou para invadir

enokibara.com.br

PAINEL DE CAPTAÇÃO DE IMÓVEIS · 2026

Autenticação sem banco

Painel sob medida para uma operação imobiliária, com mapa, funil e edição simultânea. Senha forte (bcrypt) e nenhum banco exposto: os dados sensíveis não saem de um único servidor e não existe painel de administração para invadir.

A parte que aparece também é trabalho sério.

PRODUTO PRÓPRIO · 2025 A 2026

Vernissages SP

Agenda diária do circuito de arte de São Paulo, com diretório de cerca de setenta galerias e museus, mapa e montagem de roteiro. Camada de assinatura paga. Deploy, domínio e DNS feitos por mim. Marquei com til o que é aproximado e listei a fonte de cada dado: prefiro um site que admite o que não sabe.

vernissagessp.com.br

REDESIGN · 2025

Manssur Advocacia

Escritório de São Paulo com mais de 25 anos de atuação. Refiz o layout inteiro por cima do conteúdo existente: home, história, equipe, áreas de atuação e recuperação judicial e falência. Via agência parceira.

manssur.adv.br

SITE INSTITUCIONAL · 2025

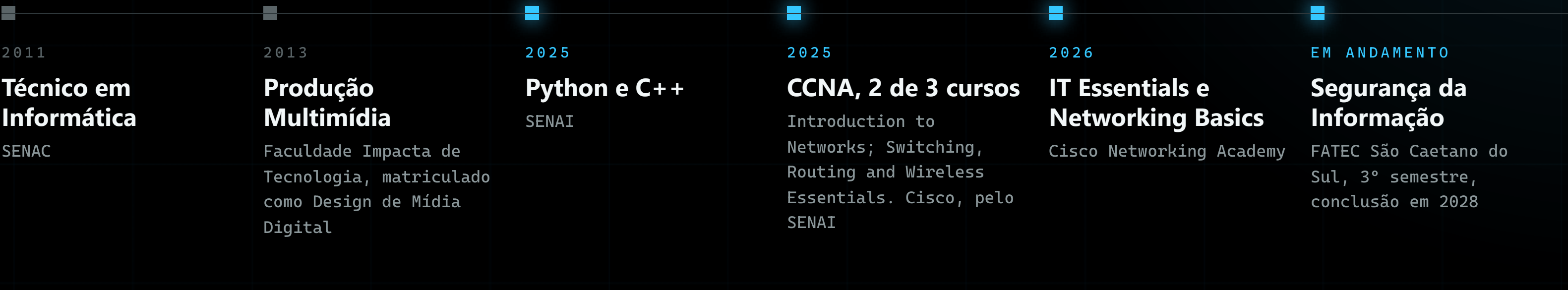
Inicial Transportes

Transportadora de Sorocaba, no transporte dedicado de cargas desde 2006. Organizei o material em serviços, história, diferenciais e perguntas frequentes, desenhei e desenvolvi o site do zero, com pedido de orçamento.

inicialtransportes.com.br

FORMAÇÃO

Redes primeiro. Segurança em cima.



ESTUDANDO AGORA

Protocolos de rede

DHCP, DNS, ICMP e HTTP/HTTPS, com captura e análise de pacotes. Terceiro curso da trilha CCNA: Enterprise Networking, Security and Automation.

POR QUE REDE IMPORTA

Quase todo incidente passa por ela

Entender como um pacote sai, atravessa um switch e chega ao destino ajuda a enxergar onde um ataque pode se esconder, e o que é esperado em um alerta.

DISPONÍVEL

Procuro **estágio ou N1** em SOC, NOC ou suporte técnico.

São Paulo, período diurno (curso a FATEC à noite). Se você conhece uma vaga ou quer trocar ideia sobre resposta a incidente, me chama.

→ lucas.negrelli82@gmail.com

→ lucasnegrelli.com

→ lucasnegrelli.com/curriculo.pdf

→ (11) 9 5293 0145

→ linkedin.com/in/lucasnegrelli

→ github.com/lucasnegrelli

