cais Inteligência em Cibersegurança

Security Operation Center (SOC)

Visão geral

Introdução

Objetivos do SOC-RNP

- Limitar a superfície de ataques cibernéticos.
- Limitar a escalada de um ataque cibernético.
- Cortar a cadeia de um ataque, detectando as movimentações.
- Limitar os impactos de um ataque cibernético.
- Prover visibilidade de cibersegurança para os clientes, em linguagem técnica e executiva.
- Criar uma visão setorial de cibersegurança para a comunidade e atores do ecossistema de ciência, tecnologia e inovação, incluindo Ministérios.
- Criar capacidades de cibersegurança.
- Contribuir para a democratização da segurança cibernética.

Desafios e benefícios

Desafios	Benefícios
Complexidade do ambientes da RNP	Melhora o nível de segurança
Complexidade intrínseca do SOC	Promove a visibilidade de segurança da informação
Multiplicidade de plataformas de cibersegurança	Fortalece a cultura de segurança
Definição tecnológica	Provê informações de segurança para a comunidade, em nível técnico e executivo
Integração tecnológica	Reflete a importância do papel da cibersegurança para a RNP
Time do SOC	Integra e fortalece ações de cibersegurança em andamento
Abrangência dos processos e workflows	Resolve parte de um gap de segurança da RNP
	Promove a aproximação com instituições do Sistema RNP
	Fortalece a segurança de todo o ecossistema (Sistema RNP)

Estrutura

O SOC-RNP surgiu com o intuito de ajudar a elevar o nível de cibersegurança das instituições de ensino e pesquisa, bem como de todas as instituições pertencentes ao sistema RNP. Seu objetivo é identificar incidentes e agir rapidamente para mitigá-los, visando quebrar o ciclo de vida do ataque e reduzir ao mínimo os impactos que a instituição venha a sofrer.

Lançamento SOC-RNP

29 de Agosto de 2023

MEC

Time SOC-RNP

MCTI

Diretoria Executiva RNP

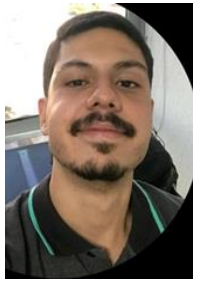
Representantes da Comunidade

Time

Nosso time!

Ivan Benevides
Idade: 38
Histórico: Profissional com 18 anos de experiência nas áreas de Tecnologia e Segurança da Informação, com atuação mais relevante em Cyber Security e com passagens em grandes corporações. Responsável pelo time do SOC e CSIRT.
Curiosidades: Toco saxofone

João Guimarães
Idade: 34
Histórico: Profissional de TI com mais de 15 anos de trajetória, formado em Redes pela Universidade Estácio, desempenha atualmente a função de líder técnico na equipe de SOC da RNP. Com vasta experiência em Cibersegurança e gestão de equipes e já teve a oportunidade de liderar projetos expressivos no setor financeiro e de amplitude nacional.
Curiosidades: Gosto de beber cerveja e fazer churrasco

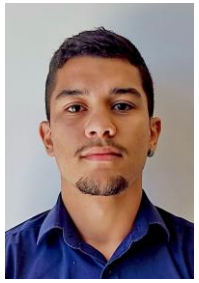


Fabio Lima
Idade: 27
Histórico: Especialista em segurança cibernética com foco em testes de invasão (Pentesting) e atuação em Red Team. Meu objetivo é garantir a proteção e integridade dos ativos de informação das organizações por meio da identificação e exploração de vulnerabilidades em redes, aplicações web e sistemas operacionais.
Curiosidades: Sou marceneiro

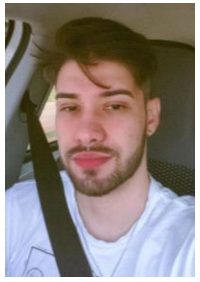
Sidney Ferreira
Idade: 23
Histórico: Profissional da área de segurança da informação, mais especificamente como Blue Team, monitorando logs, mitigando ameaças cibernéticas, sugerindo melhorias e realizando atividades de Treathing Hunter. Me tornar referência no quesito de segurança defensiva, buscando conhecimentos e aprendizados.
Curiosidades: Jogo truco

Thalis Pereira
Idade: 34
Histórico: Tenho 5 anos de experiência com TI, mais voltado a área de redes e desenvolvimento, sou formando em ADS pela Estácio.
Curiosidades: Tocar violoncelo

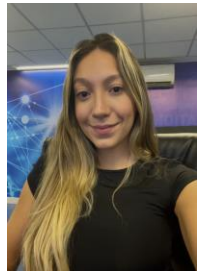
Ricardo Melo
Idade: 25
Histórico: Formado em Segurança da Informação. Estou realizando formação continuada em Ciência da Computação (lic) na UnB. Trabalhei com redes/infra e gestão de SI.
Curiosidades: Amo astronomia



Renan Lima
Idade: 20
Histórico: Apaixonado pelo aprendizado constante e determinado em aprimorar minhas habilidades. Tenho facilidade em assimilar novos conhecimentos e estou empenhado em contribuir ativamente.
Curiosidades: Atleta nato



Tiago Reis
Idade: 25
Histórico: Engenheiro de redes de comunicação pela universidade de Brasília, possui mais de dois anos de experiência em TI. Iniciou certificações na área de segurança da informação em 2023 e apresentou projeto final de graduação sobre sistemas de detecção de intrusão.
Curiosidades: Vice campeão regional de Counter Strike



Bruna Augustinho
Idade: 24
Histórico: Formada em Engenharia de Redes de Comunicação pela Universidade de Brasília, já atuei na área de suporte técnico e em projetos de pesquisa voltados a segurança da informação mais especificamente na área de OSINT.
Curiosidades: Hobby favorito é cozinhar e reunir as pessoas que amo

Nelson Miranda
Idade: 25
Histórico: Engenheiro de Redes pela UnB. Já percorri pelas áreas de infraestrutura de TI, suporte técnico e Cloud Computing, hoje atuando como Analista de Segurança da Informação no SOC-RNP. Busco trazer mais conexão entre os times de Cybersecurity, a fim de consolidar a RNP como referência em segurança no País.
Curiosidades: músico e produtor musical

Estrutura

Abordagem holística

SOC Distribuído

O que é o SOC Distribuído

O SOC Distribuído representa uma ampliação da abrangência do SOC-CAIS. A distribuição do monitoramento visa descentralizar esse processo, proporcionando um atendimento mais personalizado e uma proximidade maior com as instituições. Dessa forma, o SOC Distribuído possibilita uma contingência no monitoramento, pois, caso um SOC esteja inoperante, todo o monitoramento daquela unidade é transferido para outra, garantindo a continuidade da monitoração e assegurando uma alta disponibilidade do serviço.

Localizações

Salvador – SOC Regional

O SOC-CAIS contará com 6* SOCs distribuídos e 1 SOC de coordenação, sendo que cada SOC estará localizado em uma região do Brasil, com o SOC de coordenação situado em Brasília, conforme indicado no mapa abaixo.

Estrutura

- A estrutura do SOC Regional foi pensada para otimizar o monitoramento e garantir a confidencialidade das informações.
  - Sala Fechada
  - Controle de acesso físico
  - Câmera de vigilância
  - Vídeo Wall
  - Estrutura física (Mesa, cadeira...)
  - Equipamentos para a operação

Tipo de Monitoramento

Com o surgimento do SOC Distribuído, o atual SOC-RNP localizado em **Brasília**, DF, torna-se um **SOC de coordenação**, possibilitando que cada SOC regional tenha um segundo nível para escalonar incidentes de maior complexidade. O SOC de coordenação também se torna o **ponto central das atividades do SOC-RNP**, uma vez que todos os treinamentos, processos e procedimentos serão iniciados nele e replicados para os demais SOCs regionais, garantindo assim um padrão na qualidade da prestação de serviço.

Escala Operacional do SOC Distribuído

1. **Cobertura 24x7**
   O SOC Distribuído opera em uma escala 10x5, das 8h às 18h. Após esse horário, o monitoramento é transferido para o SOC de coordenação, garantindo uma cobertura contínua de 24 horas por dia, 7 dias por semana.

2. **Transição de Turno**
   A transição de turno entre os SOCs regionais e o SOC de coordenação é realizada por meio de uma chamada no Teams, assegurando o repasse adequado das informações e a continuidade do monitoramento.

3. **Segurança Física**
   O monitoramento é realizado de forma **presencial** em uma sala com controle de acesso e câmeras de vigilância, garantindo a confidencialidade das informações monitoradas pelo SOC.

Planos

Jornada

cais RNP

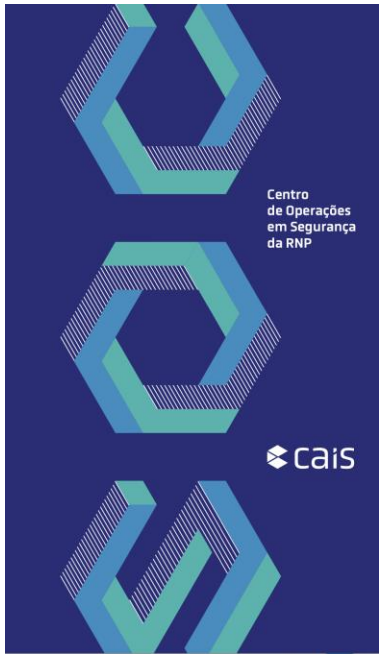
Divulgação

Instituição

Adesão

nas nuvens

Onboarding



Monitoramento

Relatórios mensais

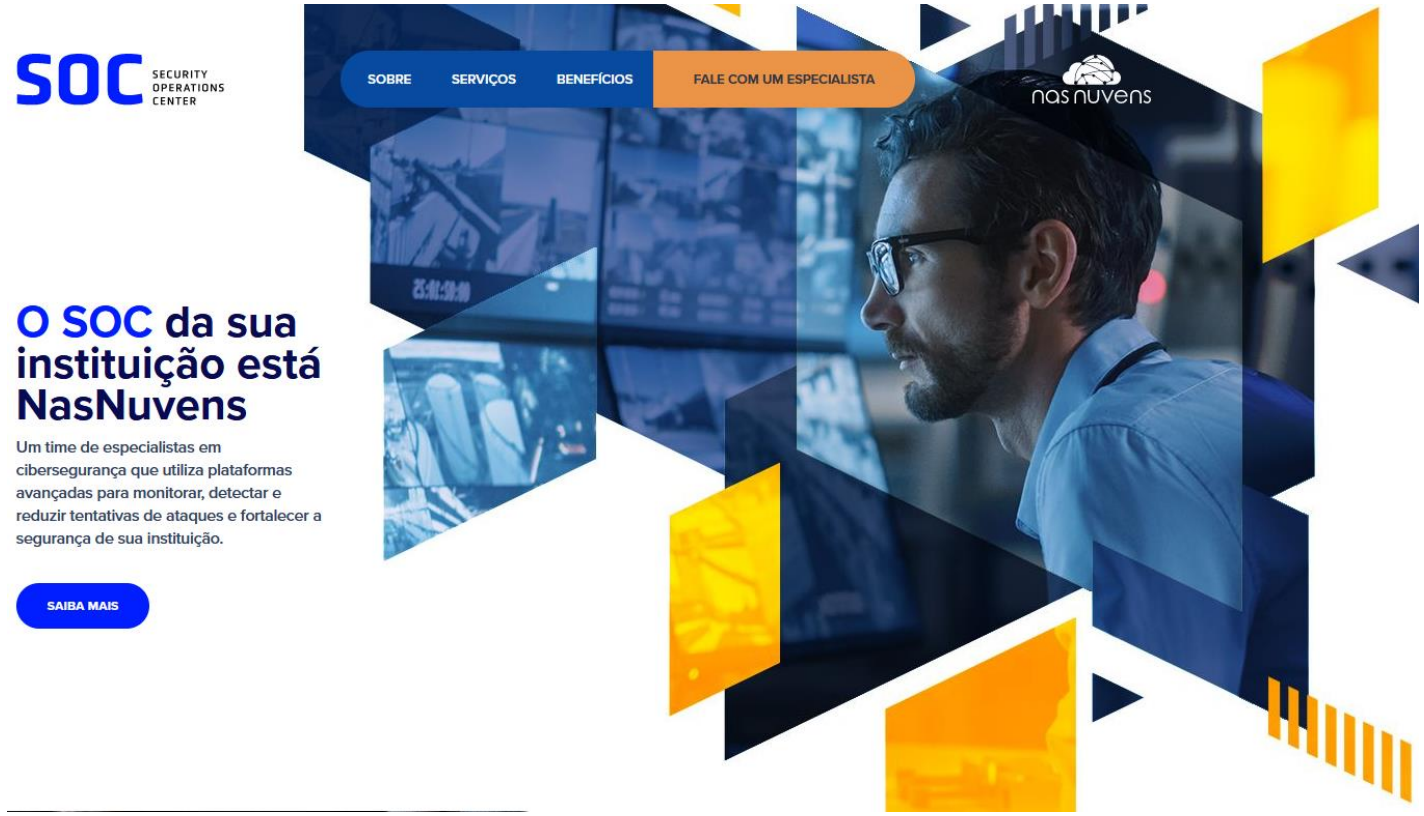
Relatórios semanais

Engajamento mensal

- Básico
- Intermediário
- Avançado
- Executivo

NasNuvens

A adesão ao SOC é feita através da página do SOC no portal do NasNuvens. Basta preencher o formulário de interesse que entraremos em contato para enviar o termo de adesão.



https://www.nasnuvens.rnp.br/soc-rnp

Planos

Nossas possibilidades são infinitas mas como princípio de atividades pensamos em uma abordagem com o olhar no exterior nos primeiros planos e posteriormente adentrando para o ambiente do nosso cliente, também com abordagens para tratativas aos executivos e suas informações espalhadas pela a internet.

Entregáveis	SOC-RNP Básico	SOC-RNP Intermediário	SOC-RNP Intermediário +	SOC-RNP Avançado	SOC-RNP Executivo
Monitoramento e mitigação de ataques de negação de serviço.	X	X	X	X	
Email de Indicadores mensais.	X	X	X	X	
Email de Indicadores semanais.		X	X	X	
Gestão de vulnerabilidades (externas).		X	X	X	
Visibilidade de ataques cibernéticos, vulnerabilidades, ameaças e ataques.		X	X	X	
Classificação de riscos cibernéticos.		X	X	X	
Evolução histórica dos riscos cibernéticos.		X	X	X	
Relatório mensal com análise.		X	X	X	
Notificação / interação.		X	X	X	
Reunião mensal.		X	X	X	
Monitoramento e mitigação de ataques na camada de aplicação.			X	X	
Gestão das vulnerabilidades (internas).				X	
Monitoramento do ambiente de nuvem.				X	
Monitoramento interno multicamadas.				X	
Monitoramento interno endpoints.				X	
Análise de exposição de dados e informações sensíveis dos executivos espalhadas pela internet, dark web e deep web.					X

OBRIGADO(A)!