



CSIRT

Responder rapidamente
a incidentes críticos de
segurança cibernética



DIFERENCIAIS



01

Serviço contínuo 24/7/365

02

Relatórios em tempo real

03

Serviços personalizados gerenciados pelo gerente técnico de contas

04

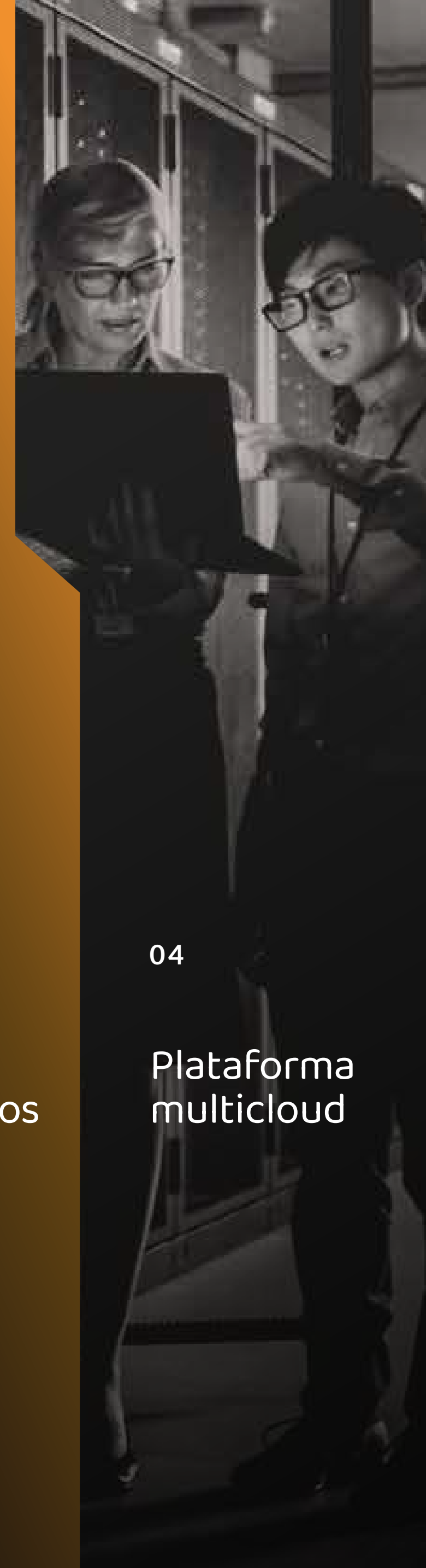
Plataforma multicloud

05

Equipe de resposta a incidentes - CSIRT

06

Serviços modulares





Forensic

Análise forense digital para gerenciamento de incidentes. Colete, analise e determine as causas e os impactos dos incidentes críticos que afetaram sua organização

CARACTERÍSTICAS NOTÁVEIS



Análise abrangente: avaliação completa das causas e do impacto do incidente



Coleta rigorosa de evidências: garantimos a integridade das evidências



Relatório técnico e executivo: resultados detalhados e sugestões para mitigar riscos futuros

PROCESSO

- Coleta de evidências: realizamos uma coleta cuidadosa seguindo protocolos forenses
- Análise e identificação: Determinamos as causas do incidente e seu impacto
- Relatório e recomendações: Apresentamos descobertas e estratégias para evitar incidentes semelhantes
- Conformidade: preservamos evidências para auditorias ou processos legais.

Porquê escolhê-lo?

- Identificação precisa das causas
- Garantia de continuidade operacional
- Fortalecimento da postura de segurança
- Preservação de evidências

Entre em contato conosco em



IRA Emergency

Resposta rápida a incidentes críticos. Nosso serviço de Resposta a Incidentes de Emergência foi projetado para ativar rapidamente uma equipe CSIRT multidisciplinar e certificada pela FIRST. Com tempos de resposta urgentes (SLAs), garantimos ação imediata para minimizar o impacto dos ataques

CARACTERÍSTICAS NOTÁVEIS

Tempos de resposta urgentes (SLA): compromisso com a ação imediata

CSIRT com certificação FIRST: equipe com ampla experiência em gerenciamento de incidentes

Cobertura global: disponibilidade independentemente do local ou fuso horário

PROCESSO

Ativação imediata: solicitação de intervenção em minutos

Análise inicial: identificação do tipo de ataque e de seu escopo

Contenção e mitigação: isolamento do incidente para evitar a propagação

Resolução e relatório: Relatório final com conclusões e recomendações.

Porquê escolhê-lo?

- SLA imediato
- Acesso sob demanda a especialistas
- Minimização do impacto financeiro

Entre em contato conosco em



IRA Retainer

Proteção contínua para sua organização. O serviço Retainer Incident Response oferece cobertura 24 horas por dia, 7 dias por semana e disponibilidade imediata em caso de incidentes declarados, garantindo uma resposta contínua às ameaças cibernéticas críticas



CARACTERÍSTICAS NOTÁVEIS



Monitoramento e análise proativos: avaliação constante do ambiente de ameaças



Planos personalizados: adaptação do serviço às necessidades específicas da organização



Relatórios periódicos: relatórios executivos com recomendações preventivas

PROCESSO

- Avaliação inicial: identificação de riscos e planejamento de resposta
- Monitoramento contínuo: monitoramento 24x7 para detectar e responder a incidentes
- Intervenção imediata: ativação da equipe CSIRT após a declaração de um incidente
- Aprimoramento contínuo: revisão periódica de incidentes e atualização de estratégias

Porquê escolhê-lo?

- Cobertura 24x7
- Disponibilidade garantida
- Acesso contínuo a especialistas

Entre em contato conosco em



Sandbox

Análise avançada de arquivos suspeitos em ambientes isolados. Detecta e analisa arquivos e programas suspeitos em um ambiente controlado e seguro, identificando ameaças avançadas

CARACTERÍSTICAS NOTÁVEIS



Ambiente controlado e seguro: avaliação sem risco para sua rede ou sistemas



Análise dinâmica e detalhada: rastreamento do comportamento de arquivos suspeitos



Evasão da detecção de ameaças: identificação de malware que escapa de outras soluções.

PROCESSO

- Carregamento de arquivos suspeitos: os arquivos são executados em um ambiente isolado.
- Monitoramento comportamental: observamos o impacto do arquivo no ambiente virtual
- Análise detalhada: identificação de ameaças e geração de indicadores
- Relatório final: Resultados da análise e recomendações para mitigação de riscos

Porquê escolhê-lo?

- Detecção proativa de ameaças sofisticadas
- Proteção contra ataques avançados
- Redução de falsos positivos
- Fortalecimento das defesas

Entre em contato conosco em

¿Por qué elegir BASE4 Security?

> **Garantía de servicio**

Brindamos una medida de seguridad y confianza en la calidad de nuestros servicios de ciberseguridad.

> **Respaldo de talentos con renombre global**

Nuestra cultura empresarial, certificada y premiada, es elegida por personas de alto nivel y reconocimiento técnico.

> **Servicio consultivo**

Ofrecemos soluciones adaptadas al cliente para abordar los desafíos o necesidades específicas en materia de ciberseguridad.

BASE4
SECURITY

www.base4sec.com