cloud.target

Transformação Digital
& Inovação

CT Protect & Respond

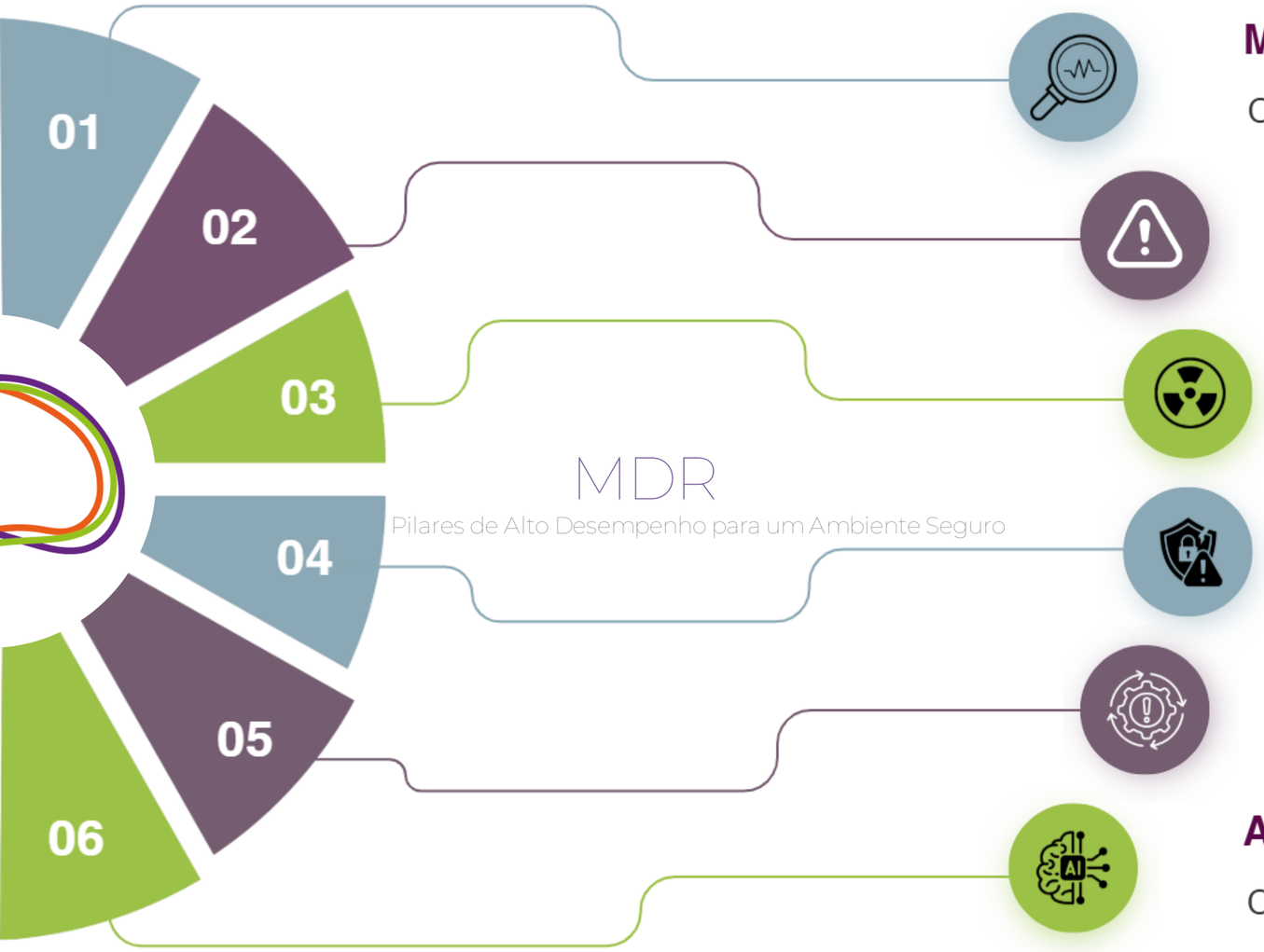
Uma suite de serviços pensada para monitorar, analisar e responder aos incidentes de segurança de um ambiente tecnológico.

SOBRE O

CT PROTECT & RESPOND

cloud.target

CT Protect & Respond



Monitoração 24x7

Coleta e Análise Contínua de logs e Eventos

Detecção e Resposta a Incidentes com DNA Humano

Investigação proativa de alertas

Threat Intelligence

Proteção Contra Ameaças

Detecção de Vulnerabilidade Crítica

Mantenha seu Ambiente Sempre Seguro

Relatórios Gerenciais e Encontros Mensais

Entenda como a Operação Funciona de Forma Simples e Eficaz

AI SOC

Conte com os Recursos da IA para Proteger seu Ambiente

Monitoração 24x7

Equipe especializada operando 24x7 para detectar e reagir a eventos de segurança em tempo real

Integração com ferramentas como Microsoft Sentinel, AzSecOps e outras

Coleta contínua de logs e telemetria de dispositivos, redes e identidades

Alta Disponibilidade operacional com foco em ambientes críticos e compliance

Cobertura para ambientes multi-cloud, híbridos e locais

Pilares

Esses pilares em nossa monitoração 24x7 nos garante uma ampla cobertura de SLA e atendimento diferenciado aos nossos clientes

Detecção e Resposta

Ação Rápida
para conter ameaças ativas: isolamento de estação, bloqueio de IPs e sessões

Integração
com identidade e dispositivos para resposta coordenada

Suporte
à resposta preliminar a incidentes, com foco em minimizar impactos

Gestão de Crises
Temos um add-on para complementar o serviço de resposta para gestão de crises em casos de incidentes

Reduz
tempo de contenção e limita o escopo de ataque

Entrega
Ações de Resposta a incidente de forma coordenada e utilizando ferramentas de alta performance reduz a superfície de ataque dentro do ambiente dos nossos clientes.

Threat Intelligence com DNA Brasileiro

Coleta
e correlação de dados reais do cenário brasileiro de ameaças

Visão Estratégica
Cyber Threat Intel acionável pelo SOC

Entrega
A combinação dessas ações permite a nossa equipe entregar muito mais inteligência da detecção de ameaças Cibernéticas.

Sensores
(honeypots) distribuídos no Brasil para detecção de ameaças

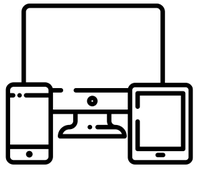
Alimentação
de plataformas como MISP para geração de detecções contextuais

Relatório
Geração de relatórios periódicos com dados relevantes por setor

Detecção de Vulnerabilidades Críticas

Detecção

Identificar Vulnerabilidades de alta severidade em tempo real através das nossas plataformas



Foco

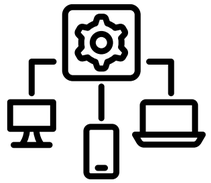
Foco nos endpoints monitorados pela nossa solução de SOC como ativos críticos. Ex: Zero days e CVEs de alta prioridade

Alertas

Envio desses alertas em tempo real para nossa plataforma de monitoração com base em inteligência de ameaças

Relatórios

Envio de Relatórios mensais com as vulnerabilidades classificadas da mais crítica para a menos crítica



Integração

Integração com EDR e outros sistemas de segurança para visibilidade 360 das vulnerabilidades

Entrega

Relatórios completos de vulnerabilidades a serem tratadas dentro do ambiente dos nossos clientes para garantir um perímetro seguro

Atividades Gerenciais

Relatórios
Mensais ou trimestrais com status de segurança e detecções

Visão
Análise tática e estratégica com base em dados operacionais reais

Recomendações
de melhoria, ajustes de políticas e priorização de ações

Governança
Fortalecer a governança e ajuda o cliente a entender seu cenário de risco

Auditoria
Orientação para condução de auditorias dentro dos clientes

Entrega
Nossos serviços gerenciais são desenhados para trazer a melhor experiência para os nossos clientes

Resposta Automatizada com Playbooks

Execução
automatizada de ações em eventos recorrentes, como isolar, bloquear e notificar

Curadoria
manual para definir limites e evitar respostas excessivas ou inadequadas

Redução
do tempo de resposta para segundos em situações críticas

Playbooks
adaptáveis por tipo de ameaça e ambiente

Orquestração
Com ferramentas líderes de mercado com foco na evolução das detecções e respostas automatizadas

Entrega
Com a nossa solução de automatização a operação reduzirá a quantidade de alertas com falso positivo gerando agilidade e assertividades nos eventos que realmente importam

DÚVIDAS?

Av. das Nações Unidas, 12.901 - CENU - Torre Oeste - 16º andar - Brooklin Paulista, São Paulo - SP, CEP 04578-7011

+55 11 3181-7011