DATASHEET ↗

MSS

MANAGED SECURITY SERVICES

Conte com a CG One para obter resiliência, continuidade e confiança para o seu negócio.

CG//One

ÍNDICE

O CENÁRIO

AMBIENTES COMPLEXOS, EQUIPES LIMITADAS E OPERAÇÕES AINDA REATIVAS.

A cibersegurança deixou de ser apenas uma barreira técnica contra ataques: hoje, ela é vista como um **habilitador de negócios e de resiliência organizacional**. O Gartner reforça essa visão ao apontar que, em 2025, os programas de segurança mais eficazes são aqueles que combinam **continuidade do negócio, transformação digital segura e colaboração no gerenciamento de riscos**. Nesse contexto, os CISOs precisam provar o valor da segurança não apenas evitando incidentes, mas garantindo a estabilidade necessária para que a empresa cresça e se transforme.

Na prática, porém, muitas organizações ainda lutam para acompanhar esse ritmo. A pressão por resiliência se soma a um ambiente de ameaças cada vez mais sofisticado, impulsionado por IA, nuvem, trabalho remoto e ecossistemas digitais descentralizados. No Brasil, esse descompasso é evidente: uma pesquisa da Grant Thornton Brasil e Opice Blum revela que **79% das empresas se consideram mais expostas a ataques**, com o **ransomware como principal ameaça em 67% dos casos**.

Mas o problema não está apenas nas ameaças externas. **Manter uma operação de segurança totalmente interna é cada vez mais caro e difícil**. Isso exige investimentos elevados em tecnologia, pessoas e processos, além de escala 24/7, treinar e reter especialistas em um mercado já carente de talentos. Para muitas empresas, esse modelo onera a operação e ainda deixa lacunas críticas expostas.

Esse cenário deixa claro que, enquanto as ameaças evoluem rapidamente, muitas empresas não conseguem sustentar internamente o mesmo ritmo de defesa. Essa disparidade abre espaço para vulnerabilidades críticas, que se manifestam em desafios como:

Altos custos de operação — manter uma operação interna exige grandes investimentos em infraestrutura, equipe e gestão. A empresa precisa investir pesado em CAPEX, retenção de talentos e tecnologias diversas.

Complexidade crescente — ambientes híbridos, nuvem e redes distribuídas ampliam a superfície de ataque, enquanto times de TI e segurança ficam sobrecarregados.

Déficit de especialização — Profissionais de segurança qualificados são caros, difíceis de reter e a alta rotatividade gera perda de conhecimento crítico e lacunas no processo de defesa.

Escalabilidade e resiliência — Equipes internas sofrem com sobrecarga e não conseguem acompanhar picos de incidentes. Em caso de ataques, a empresa pode não ter capacidade de resposta adequada.

Resposta lenta e processos imaturos — incidentes críticos ainda são tratados de forma reativa, ampliando o impacto e o tempo de recuperação.

Muitas empresas já reconhecem a necessidade de amadurecer sua postura de segurança, mas seguem presas a operações fragmentadas e **reativas**, que não acompanham a velocidade dos ataques. O grande desafio agora é dar o próximo passo: conduzir a segurança de forma **contínua, inteligente e proativa,** capaz de reduzir riscos e proteger o negócio em tempo real.

A SOLUÇÃO

MANAGED SECURITY SERVICES CG ONE

É nesse contexto que os **Managed Security Services (MSS)** se consolidam como a forma mais eficiente de garantir proteção contínua. Para as empresas que ainda não contam com esse modelo, o MSS deixou de ser opcional: é a base necessária para enfrentar um cenário em que ameaças evoluem mais rápido do que estruturas internas conseguem acompanhar. Já para aquelas que mantêm SOCs próprios ou equipes internas, o desafio está em sustentar custos, escala 24/7 e gestão de talentos, pontos que tornam a operação pesada e difícil de manter sozinha.

O MSS da **CG One** resolve esses desafios ao unir nossa experiência de mais de quatro décadas a uma estrutura completa de serviços gerenciados. Combinamos **expertise certificada**, **operação 24/7 e acesso a todo o leque de soluções e serviços**, permitindo que nossos clientes:

Tenham previsibilidade de custos, sem surpresas e ajustado ao tamanho da empresa.

Tenham acesso imediato a especialistas e tecnologias de ponta, sempre atualizadas.

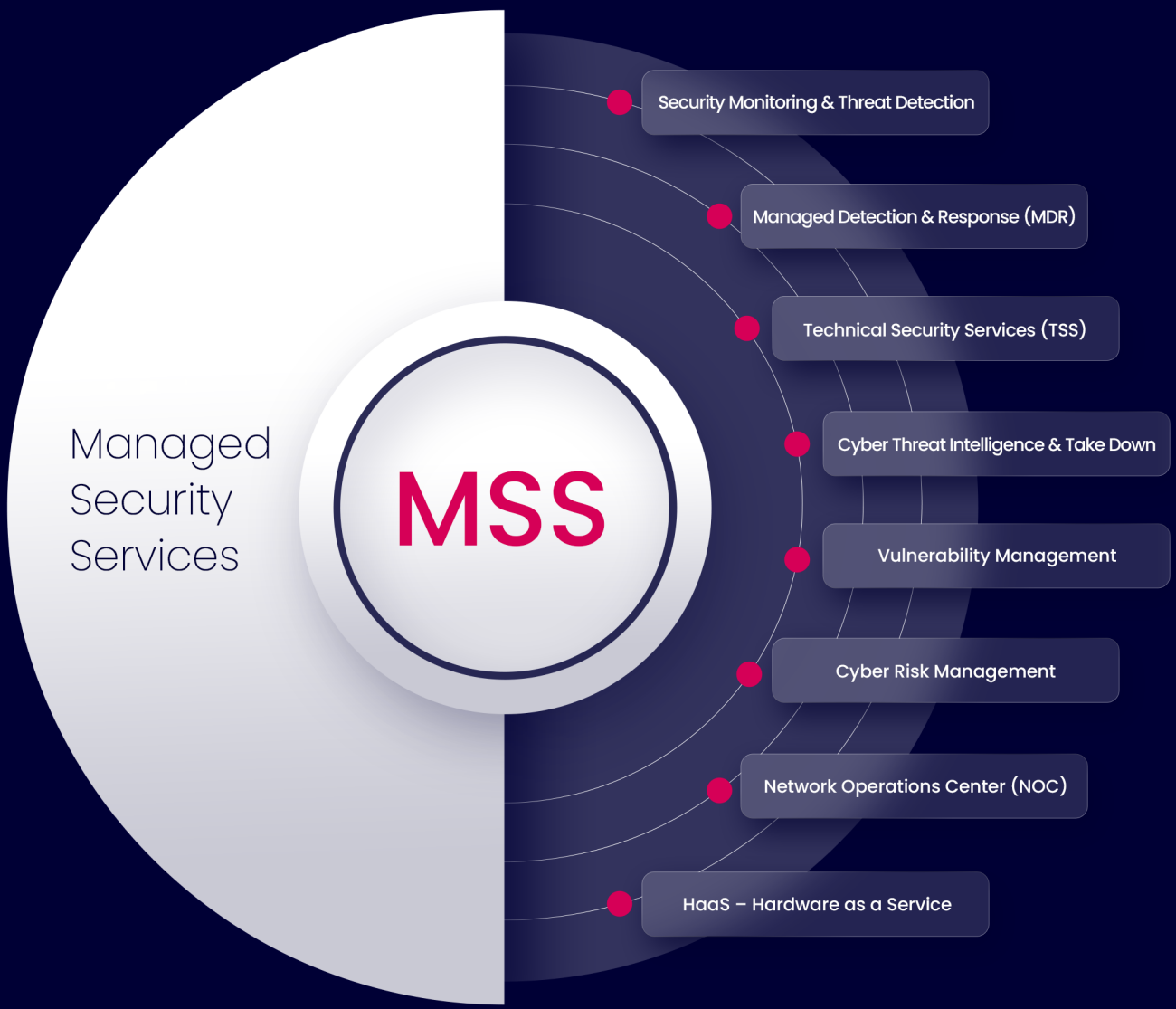
Foquem no core do negócio, enquanto a operação de segurança fica nas mãos de quem vive isso todos os dias.

Reduzam riscos financeiros e reputacionais, contando com uma estrutura preparada para respostas rápidas.

Contem com proteção ponta a ponta, garantindo continuidade de negócio e resiliência a ataques.

Tudo isso estruturado em serviços que se complementam para entregar **segurança contínua, inteligente e proativa**.

O ecossistema de MSS da CG One integra todas as camadas essenciais da cibersegurança moderna.



Nas próximas páginas, apresentamos cada um desses serviços em detalhe, mostrando como se complementam para formar uma operação de segurança contínua e orientada a resultados.

SECURITY MONITORING & THREAT DETECTION

Tenha **visibilidade 24x7** e detecção antecipada de comportamentos suspeitos, reduzindo tempo de exposição e acelerando a resposta.

O serviço de **Monitoramento e Detecção de Ameaças** da CG One combina a parte reativa (monitoramento contínuo) com a parte proativa (detecção inteligente), entregando ao cliente não apenas **visibilidade de eventos**, mas **alertas acionáveis e priorizados**. Com o uso de automação, IA/ML e especialistas em segurança, garantimos que potenciais ameaças sejam identificadas e escalonadas antes que causem impacto real.

NOSSAS ENTREGAS INCLUEM:

- **Coleta e Centralização de Eventos**
  - Ingestão de logs e telemetria de múltiplas fontes: firewalls, EDR, sistemas em nuvem, Active Directory/Identidade e aplicações críticas.
  - Normalização e retenção de dados para garantir consistência e rastreabilidade.
- **Análise Contínua e Automática**
  - Uso de IA/ML para identificar padrões de ataque, anomalias comportamentais (UEBA) e movimentações laterais.
  - Correlação de eventos em tempo real para detectar ataques complexos.
- **Alertas e Escalonamento**
  - Classificação por criticidade (baixa, média, alta, crítica).
  - Notificação imediata em incidentes críticos via ticket, e-mail, API ou war room.
  - Encaminhamento estruturado para o processo de Resposta a Incidentes (MDR), quando contratado.
- **Relatórios e Indicadores de Segurança**
  - Relatórios executivos e técnicos com estatísticas, ameaças detectadas e tendências.
  - Dashboards em tempo real para apoiar tanto times técnicos quanto a gestão do negócio.

MANAGED DETECTION & RESPONSE (MDR)

Quando um incidente acontece, cada minuto conta. Por isso, a CG One atua como **seu time de confiança na linha de frente**, ajudando a analisar, conter e recuperar o ambiente de forma rápida e estruturada. Combinamos tecnologia avançada, automação e a expertise de especialistas em SOC e DFIR para apoiar desde a **contenção imediata até o aprendizado pós-incidente**.

NOSSAS ENTREGAS INCLUEM:

- **Investigação e Validação de Incidentes**
  - Triagem avançada de alertas vindos do Monitoramento e Detecção
  - Contextualização com usuários, ativos críticos e impacto de negócio.
- **Resposta Técnica (Containment, Eradication, Recovery)**
  - Containment: isolamento de hosts, bloqueio de acessos e suspensão de credenciais comprometidas.
  - Eradication: remoção de malware, fechamento de brechas e aplicação de patches emergenciais.
  - Recovery: apoio na restauração de sistemas, uso de backups e validação da integridade do ambiente.
- **Comunicação e Coordenação**
  - Notificação imediata de incidentes críticos.
  - Suporte na comunicação interna entre times de TI, áreas de negócio e executivos.
- **Automação e Playbooks (SOAR)**
  - Uso de playbooks customizados para acelerar resposta.
  - Ações automatizadas em incidentes repetitivos (ex.: bloqueio de IPs maliciosos).
  - Redução drástica do tempo de contenção e recuperação.
- **Relatórios e Pós-incidente**
  - Documentação detalhada de cada incidente tratado.
  - Recomendações de melhoria e retroalimentação de regras, patches e políticas.
  - Insights estratégicos para elevar a maturidade do programa de segurança.

TECHNICAL SECURITY SERVICES (TSS)

O serviço de **Gestão de Dispositivos de Segurança (TSS)** da CG One garante que todos os controles de proteção do cliente estejam **corretamente configurados**, **atualizados e operando em alta performance**, sempre alinhados à estratégia de cibersegurança do negócio.

Mais do que manter dispositivos funcionando, o TSS assegura governança, eficiência e melhoria contínua do ambiente.

NOSSAS ENTREGAS INCLUEM:

- **Configuração e Provisionamento**
  - Levantamento inicial dos dispositivos de segurança.
  - Criação e ajuste de regras de firewall, IPS, WAF, IAM e outros controles.

- **Administração Contínua**
  - Atualizações de versão (pelo menos 1x ao ano).
  - Gestão de regras e políticas (acessos, portas, serviços).
  - Backups regulares de configurações e manutenção preventiva/corretiva.

- **Manutenção preventiva e corretiva**
  - Backups de configurações e sugestões de melhorias.

- **Gestão de Mudanças (Change Management)**
  - Implementação de novas políticas de segurança sob demanda.
  - Governança sobre alterações para garantir conformidade e rastreabilidade.

- **Relatórios e Auditoria**
  - Relatórios periódicos de configuração e auditoria.
  - Análise de desempenho, disponibilidade e capacidade dos dispositivos.

CYBER THREAT INTELLIGENCE & TAKE DOWN

O serviço de **Threat Intelligence da CG One** fornece informações acionáveis e medidas práticas para **antecipar, detectar e responder** a ameaças de forma proativa. Além da coleta e análise de inteligência, o serviço inclui o **Take Down**: a remoção de ativos maliciosos como páginas de phishing, perfis falsos e domínios fraudulentos que impactam diretamente o cliente.

Combinando visibilidade avançada e ação efetiva, a **Inteligência de Ameaças com Take Down** entrega não só conhecimento sobre o que os adversários estão fazendo, mas também **resposta ativa para reduzir riscos reais**.

NOSSAS ENTREGAS INCLUEM:

- **Coleta e Consolidação de Dados**
  - Monitoramento de dark web, deep web e fóruns criminosos.
  - Vigilância de menções envolvendo parceiros, executivos e VIPs.
- **Análise e Enriquecimento**
  - Correlação de IOCs (IPs, domínios, hashes) com campanhas conhecidas.
  - Mapeamento de TTPs via MITRE ATT&CK.
  - Avaliação de ameaças relevantes ao setor e ao ambiente específico do cliente.
- **Disseminação da Inteligência**
  - Alertas em tempo real sobre ameaças emergentes.
  - Relatórios táticos e estratégicos sobre atores e tendências.
- **Integração Operacional**
  - Enriquecimento de alertas já existentes.
  - Contexto avançado para priorizar e acelerar resposta a incidentes.
- **Take Down (ação ativa contra ameaças externas)**
  - Identificação de sites de phishing, domínios falsos e perfis fraudulentos.
  - Solicitação e acompanhamento de remoção junto a provedores, registradores de domínio e redes sociais.
  - Relatórios finais com evidências de remoção e status de cada incidente.

VULNERABILITY MANAGEMENT

O serviço de **Análise e Gestão de Vulnerabilidades da CG One** vai além da simples execução de varreduras técnicas. Ele oferece uma visão clara das falhas que podem ser exploradas em sua infraestrutura e **prioriza correções de acordo com impacto real e risco de negócio**, reduzindo drasticamente a superfície de ataque.

Combinamos automação, inteligência de ameaças e expertise humana para transformar descobertas técnicas em **planos de ação práticos**, acompanhados até o fechamento.

NOSSAS ENTREGAS INCLUEM:

- **Descoberta e Inventário de Ativos**
  - Identificação de sistemas, redes e aplicações críticas.
  - Mapeamento de ativos internos e externos expostos.

- **Varredura de Vulnerabilidades e Validação Contínua**
  - Scans periódicos com ferramentas líderes de mercado.
  - Identificação de falhas conhecidas, sistemas desatualizados e configurações inseguras.
  - Re-scans para confirmar correções e manter um ciclo contínuo de melhoria.

- **Análise e Priorização de Riscos**
  - Classificação baseada em CVSS, EPSS, criticidade do ativo e integração com Threat Intelligence.
  - Priorização de correções com base em risco real de negócio.

- **Recomendações e Correções**
  - Planos de remediação claros e acompanhamento da execução.
  - Suporte consultivo para definição de responsáveis, prazos e exceções.

- **Pentest**
  - Simulação de ataques reais conduzida por especialistas.
  - Identificação de falhas que ferramentas automáticas não detectam.
  - Relatórios detalhados com provas de exploração e recomendações específicas.

- **Simulações de Ataques via BAS (Breach and Attack Simulation)**
  - Execução automatizada de cenários de ataque.
  - Validação contínua dos controles defensivos existentes.

CYBER RISK MANAGEMENT

Mais do que tratar vulnerabilidades técnicas, é essencial traduzir riscos cibernéticos em impactos reais para o negócio. O serviço de Gestão de Riscos da CG One ajuda as empresas a identificar, avaliar, tratar e monitorar riscos de forma estruturada, transformando ameaças em informações estratégicas para a tomada de decisão. Assim, os investimentos em segurança são priorizados com base no que realmente importa: a continuidade do negócio e a resiliência organizacional.

NOSSAS ENTREGAS INCLUEM:

- **Identificação de Riscos**
  - Mapeamento de ativos críticos (informações, sistemas e processos), identificação de ameaças internas e externas e levantamento de vulnerabilidades técnicas e organizacionais.

- **Avaliação de Riscos**
  - Análise de probabilidade e impacto no negócio, classificação por criticidade (baixo, médio, alto, crítico) e priorização de riscos relevantes.

- **Tratamento de Riscos**
  - Definição de estratégias (mitigar, transferir, aceitar ou evitar), recomendações de controles técnicos e processos, apoio em seguros cibernéticos e suporte na implementação das medidas.

- **Monitoramento Contínuo**
  - Revisão periódica dos riscos (trimestral, semestral), atualização da matriz de riscos conforme mudanças no ambiente ou novas ameaças e acompanhamento da evolução da postura de segurança.

- **Relatórios Executivos**
  - Mapas de risco claros, relatórios para auditorias e dashboards executivos que traduzem o nível de exposição em indicadores de negócio.

NETWORK OPERATIONS CENTER (NOC)

Além do SOC voltado à proteção contra ameaças, a CG One também oferece um **NOC para garantir disponibilidade, performance e confiabilidade da infraestrutura de TI e telecom**. Nosso NOC monitora em tempo real ativos críticos, servidores, aplicações, links e nuvem, assegurando que tudo esteja disponível e performando dentro do esperado.

NOSSAS ENTREGAS INCLUEM:

- **Monitoramento de Infraestrutura e Aplicações**
  - Acompanhamento de servidores, bancos de dados, aplicações críticas e serviços em nuvem, além de equipamentos de rede (switches, roteadores, balanceadores, links de internet/MPLS).
  - Coleta contínua de métricas de CPU, memória, disco, latência, jitter e perda de pacotes.

- **Gestão de Eventos e Incidentes Operacionais**
  - Detecção em tempo real de falhas de infraestrutura (queda de link, servidor fora do ar, lentidão de aplicações).
  - Notificação imediata, abertura de tickets e escalonamento para as equipes responsáveis.

- **Gestão de Performance e Capacidade**
  - Análise de tendências de uso para capacity planning, identificação de gargalos e recomendações de melhoria para manter o desempenho sempre alinhado às necessidades do negócio.

- **Relatórios e SLA**
  - Relatórios periódicos de disponibilidade e performance, além de dashboards em tempo real para acompanhamento contínuo da saúde da infraestrutura.

HAAS – HARDWARE AS A SERVICE

Investir em equipamentos de segurança e infraestrutura geralmente significa alto CAPEX inicial, custos de manutenção e risco de obsolescência. O modelo de **Hardware as a Service (HaaS) da CG One** elimina essas barreiras ao fornecer dispositivos críticos sob assinatura (OPEX), com gestão completa, suporte técnico e integração nativa aos nossos serviços MSS. Dessa forma, o cliente tem sempre acesso à **tecnologia mais atualizada, previsibilidade de custos e escalabilidade sob demanda**.

NOSSAS ENTREGAS INCLUEM:

- **Fornecimento de Equipamentos sob Assinatura**
  - Firewalls, switches, roteadores, balanceadores de carga e outros dispositivos de segurança, como WAF e endpoints, fornecidos sob modelo OPEX, sem necessidade de aquisição direta.

- **Gestão de Ciclo de Vida**
  - Instalação inicial e provisionamento, atualizações de firmware e patches regulares, além de substituição em caso de falha.

- **Suporte e Operação**
  - Licenciamento e renovações já inclusos no contrato, monitoramento da saúde dos equipamentos e SLA definido para reparo ou troca imediata.

- **Escalabilidade sob Demanda**
  - Possibilidade de upgrade ou downgrade de equipamentos conforme necessidade, acompanhando o crescimento ou redução do negócio.

- **Relatórios e Compliance**
  - Relatórios periódicos de inventário e status dos equipamentos, além de evidências para auditorias, como histórico de atualizações e ciclos de manutenção.

CG // One

DIFERENCIAIS DO MSS CG ONE

Serviços sob medida

Adaptamos o modelo de MSS ao nível de maturidade de cada cliente, garantindo entregas personalizadas que se integram ao ambiente existente, seja ele gerido internamente ou em parceria conosco.

Escala 24/7 sem sobrecarga interna

Entregamos monitoramento e resposta contínuos sem a necessidade de montar e sustentar equipes próprias em turnos integrais, reduzindo custos operacionais e complexidade de gestão.

Acesso imediato a especialistas e tecnologias

Nossa equipe certificada combina experiência local com ferramentas de ponta utilizadas globalmente, entregando conhecimento que seria caro e difícil manter internamente.

Foco no seu negócio, não na operação

Liberamos os times internos para se dedicarem às prioridades estratégicas, enquanto cuidamos da operação de segurança ponta a ponta.

Parcerias globais + execução local

Aliamos relacionamento com fabricantes líderes de mercado a uma atuação consultiva próxima do cliente, garantindo implementação eficaz, gestão contínua e exploração máxima de cada tecnologia.

Cobertura técnica e estratégica

Não nos limitamos a operar ferramentas: oferecemos gestão de dispositivos, monitoramento, resposta, inteligência e consultoria, conectando operação, gestão e negócio em uma entrega completa de cibersegurança.

CG//One

SOBRE A CG ONE

Somos a evolução da marca Compugraf. Com mais de 40 anos de expertise no mercado de tecnologia, somos especializados em segurança cibernética para todo o ecossistema digital das empresas.

Desenvolvemos e gerenciamos soluções e serviços de cibersegurança alinhados de acordo com as práticas e os padrões de segurança do NIST® Cybersecurity Framework.

Contamos com um time qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores, em todo o Brasil.

ENTRE EM CONTATO