EBOOK EXECUTIVO

RAZÕES ESTRATÉGICAS PARA ADOTAR UM SOC GERIDO

DETEÇÃO, INVESTIGAÇÃO E RESPOSTA A AMEAÇAS ANTES QUE IMPACTEM O NEGÓCIO

Uma abordagem prática aos desafios de segurança modernos e ao papel do SOC da Knowledge Inside

FUNDAMENTOS SOBRE SOC

Num mundo de ameaças contínuas, bloquear tudo deixou de ser realista

A mobilidade, a cloud, as integrações SaaS e a digitalização aumentaram a superfície de ataque. Mesmo com boas ferramentas, políticas e controlos preventivos, é impossível garantir que todos os ataques serão bloqueados antes de entrarem na organização. Um SOC moderno é uma camada operacional de defesa: monitoriza sinais, deteta padrões, investiga contexto, prioriza risco e coordena resposta.

A diferença está na capacidade de transformar eventos dispersos em decisões rápidas. Construir essa capacidade internamente exige tempo, pessoas, processos, tecnologia e maturidade. Enquanto essa maturidade é construída, os atacantes não esperam. Por isso, muitas organizações recorrem a um SOC gerido para acelerar proteção, reduzir ruído e ganhar resposta contínua.

O PROBLEMA NÃO É APENAS TER FERRAMENTAS. É CONSEGUIR OPERÁ-LAS CONTINUAMENTE, INTERPRETAR SINAIS E AGIR ANTES DO IMPACTO

DESAFIOS
DE GERIR SEM SOC

1. Tecnologia isolada não acompanha ameaças em evolução
2. O tempo de reação influencia diretamente o impacto
3. Encontrar e manter especialistas é difícil e dispendioso
4. Acompanhar novas técnicas de ataque exige investimento contínuo
5. Gerir uma operação SOC madura é uma tarefa exigente

BENEFÍCIOS
DE UM SOC GERIDO

1. Maturidade operacional mais rápida
2. Monitorização contínua com Microsoft Defender XDR
3. Investigação e resposta ativa a incidentes
4. Separação clara entre IT, operação e segurança
5. Escalabilidade, reporting e melhoria contínua

CONFIAR APENAS EM TECNOLOGIA NÃO É SUFICIENTE PARA PROTEGER A SUA ORGANIZAÇÃO

As ameaças evoluem continuamente. Isto significa que mesmo soluções recentes podem ficar atrás de atacantes que adaptam técnicas, exploram configurações frágeis e procuram formas de contornar controlos preventivos.

- Controlos configurados uma vez tendem a perder eficácia quando as ameaças mudam.
- Ferramentas como EDR, MFA, firewall e XDR são essenciais, mas precisam de análise e operação.
- Alertas sem contexto aumentam o ruído e atrasam a tomada de decisão.
- A falta de especialização pode levar a falsos negativos ignorados ou a incidentes subestimados.
- Um único ponto mal configurado pode tornar-se uma porta de entrada

SABIA QUE?

32%

de aumento nos ataques de ransomware em 2025 face ao ano anterior.

SINAIS DISCRETOS

Muitos incidentes começam com comportamentos anómalos, não com alertas críticos.

36%

de aumento nos crimes informáticos registados pelas autoridades em 2025.

O TEMPO DE REAÇÃO É CRÍTICO PARA REDUZIR IMPACTO NO NEGÓCIO

Ataques não acontecem apenas em horário de expediente. Muitos são planeados para permanecerem discretos tempo suficiente para mapear sistemas, identificar dados relevantes e preparar uma ação de maior impacto.
As consequências podem ir muito além da tecnologia: indisponibilidade operacional, exposição de dados,

1. Quanto mais tarde for a deteção, maior o espaço para propagação.
2. Quanto mais lenta for a triagem, maior o risco de tratar um incidente crítico como ruído.
3. Quanto menos claro for o processo, maior a dependência de decisões improvisadas.
4. Quanto menos definidos estiverem os contactos de aprovação, mais lenta é a contenção.

Se surgir um incidente agora, quem valida o alerta, quem investiga, quem decide a contenção e quem comunica com o cliente?

ACOMPANHAR ATACANTES EXIGE INVESTIMENTO CONTÍNUO

Atacantes melhoram ferramentas, exploram identidades, abusam de permissões cloud, utilizam phishing sofisticado e adaptam técnicas para reduzir deteção. Ao mesmo tempo, fornecedores de segurança adicionam novas funcionalidades que precisam de configuração, otimização e interpretação.

- A segurança não é um projeto com fim: é uma operação contínua.
- A superfície de ataque muda com novos utilizadores, aplicações, dispositivos e integrações.
- Vulnerabilidades e configurações incorretas acumulam risco se não forem priorizadas.

A GESTÃO DE UM SOC É UMA TAREFA OPERACIONAL EXIGENTE

Uma operação SOC inclui organização de trabalho, gestão de alertas, turnos, documentação, processos, tuning tecnológico, regras de escalamento, reporting, melhoria contínua e articulação com equipas de IT, segurança, aplicações e negócio.

A PERGUNTA DEIXOU DE SER "TEMOS FERRAMENTAS?". A PERGUNTA CERTA É "TEMOS OPERAÇÃO CONTÍNUA PARA TRANSFORMAR SINAIS EM RESPOSTA?".

BENEFÍCIOS

MATURIDADE MAIS RÁPIDA SEM CONSTRUIR TUDO INTERNAMENTE

Construir um SOC do zero pode exigir anos até atingir maturidade operacional: selecionar tecnologia, configurar integrações, definir processos, recrutar equipa, criar turnos, documentar procedimentos, testar respostas e melhorar continuamente.
Um SOC gerido permite acelerar esse caminho, colocando a organização numa operação estruturada desde o início. A maturidade passa a vir da combinação entre tecnologia, processos, equipa e experiência operacional.

- Acesso imediato a uma operação de monitorização e resposta.
- Priorização com base em criticidade, impacto potencial e contexto de negócio.
- Processos já definidos para deteção, triagem, contenção e remediação.
- Melhoria contínua suportada por reporting regular.

EXPERIÊNCIA ESPECIALIZADA MELHORA VELOCIDADE E QUALIDADE DE RESPOSTA

ESCALABILIDADE E FLEXIBILIDADE PARA DIFERENTES REALIDADES

SEPARAÇÃO DE RESPONSABILIDADES AUMENTA VALOR PARA O NEGÓCIO

O SOC DA KNOWLEDGE INSIDE

COMO FAZEMOS ACONTECER

O SOC da Knowledge Inside é um serviço de gestão de ameaças cibernéticas orientado para vigilância contínua, deteção precoce, investigação, resposta, redução de exposição e melhoria contínua. A base tecnológica é Microsoft Defender XDR, que correlaciona sinais para reduzir ruído e acelerar decisão

MONITORIZAR

Eventos, identidades, endpoints, cloud e sinais de segurança através de uma visão centralizada.

DETETAR

Alertas, comportamentos anómalos, phishing, indicadores de compromisso e risco em integrações.

RESPONDER

Triagem, investigação, contenção, mitigação e coordenação com o cliente quando existe impacto.

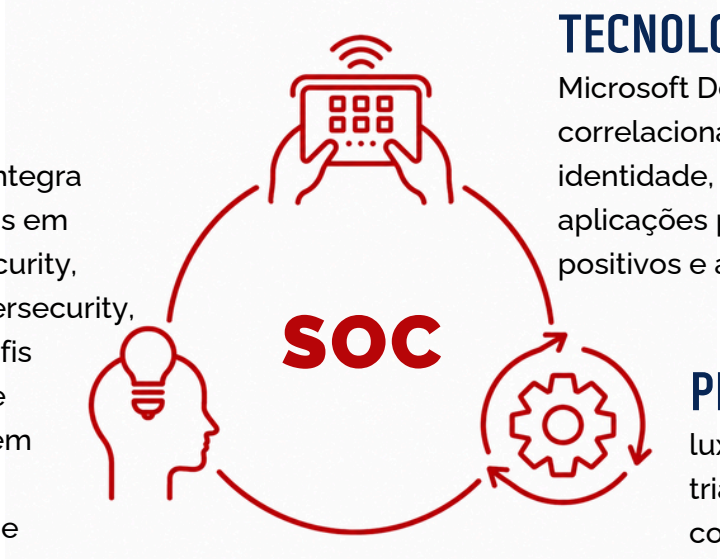
MELHORAR

Recomendações, gestão de vulnerabilidades, revisão de attack surface e reporting mensal

UMA SINERGIA ENTRE TECNOLOGIA, PESSOAS E PROCESSOS

PESSOAS

A equipa KI integra competências em Microsoft Security, Cloud e Cybersecurity, incluindo perfis certificados e experiência em operação, investigação e resposta



TECNOLOGIA

Microsoft Defender XDR permite correlacionar sinais de endpoint, identidade, email, cloud e aplicações para reduzir falsos positivos e acelerar a decisão.

PROCESSOS

luxos definidos para deteção, triagem, investigação, contenção, remediação, escalamento, reporting e melhoria contínua.

PORQUÊ A KNOWLEDGE INSIDE

Menos risco, menos ruído e resposta mais rápida quando é crítico

A Knowledge Inside combina experiência em infraestrutura, cloud, Microsoft Security e cibersegurança para entregar uma operação SOC prática, orientada a risco e ajustada à realidade de cada organização.

O serviço foi desenhado para funcionar em colaboração com o cliente: sistemas críticos, identidades VIP, contactos de aprovação, janelas de intervenção e canais de escalamento são definidos para acelerar decisões sem comprometer a operação.

- Monitorização e correlação com Microsoft Defender XDR.
- Triagem, investigação e resposta a alertas e incidentes. Análise e ação sobre emails suspeitos reportados.
- Gestão de vulnerabilidades, attack surface e recomendações de mitigação.
- Revisão de Enterprise Apps e permissões cloud.
- Relatório mensal unificado com ações, tendências e recomendações.