

Como tornar seu SOC resiliente?

As quatro disciplinas que separam operar de **amadurecer**.

Luciano Lima

Senior Solution Architect, Kaspersky

Mind the Sec 2026





Ferramentas sozinhas não fazem um SOC

Já vi essa cena mais de uma vez: SIEM de primeira linha, EDR premiado, licenças em dia.

E o incidente escalou mesmo assim.



O **alerta certo disparou**, mas ninguém sabia quem deveria agir.



O **playbook** existia, mas só na cabeça de um analista que estava de férias.



A **inteligência de ameaças** chegava, mas virava ruído na fila.

O stack estava pronto. A operação, **não**.

Operar não é o mesmo que amadurecer

Seu SOC funciona.

A pergunta é outra: ele está evoluindo na mesma velocidade do adversário?

O adversário evolui todos os dias; um SOC que não é reavaliado **envelhece parado**.

Operações maduras têm mais dificuldade de enxergar os **próprios pontos cegos**.

Quanto maior a escala, maior o **custo de cada ponto cego**.

Todo SOC de alta performance tem uma disciplina em comum: **ele se mede continuamente**.

As quatro disciplinas de um SOC resiliente

Resiliência não nasce da ferramenta. Nasce do **equilíbrio** entre quatro disciplinas:

Pessoas



papéis bem definidos e estrutura que sustenta continuidade.

Tecnologia



arquitetura integrada, pensada para a operação.

Processos



procedimentos documentados que tornam a operação previsível.

Serviços



modelo de entrega com compromissos claros e mensuráveis.



Nos próximos minutos, percorremos as quatro. E onde cada uma costuma quebrar.

Pessoas: o fator crítico de sucesso

Um SOC robusto exige estrutura humana que sustenta continuidade, qualidade de análise e escala:



Gestão e liderança

SOC Manager, Operations Lead, Research Lead, Technical Lead.



Análise e detecção

analistas T1, T2 e T3, CTI Analyst, Threat Hunter.



Engenharia e suporte

SOC Engineer, SOAR Expert, Vulnerability Analyst.



Reporte e inteligência

Reporting Specialist, Knowledge Management.

Investir em papéis reduz a dependência de heróis individuais.



Papéis ou heróis?

O teste da estrutura

O sinal clássico: a operação funciona bem até a pessoa-chave sair.

Conhecimento concentrado em indivíduos, não em papéis.

Analistas T1 sobrecarregados de triagem, sem trilha de evolução.

Turnover alto tratado como fatalidade, não como sintoma.

Se o seu SOC depende de nomes, ele não tem uma disciplina de pessoas. Tem sorte.

Processos: a base da previsibilidade

Processos claros transformam um conjunto de ferramentas em uma operação confiável e repetível:



Detecção

security monitoring, use case management, threat hunting.



Resposta

incident response, playbooks padronizados.



Inteligência

threat intelligence, vulnerability assessment.



Governança

reporting, knowledge management.

Processos bem definidos reduzem imprevisto e aumentam consistência sob pressão.

Tecnologia: arquitetura pensada para a operação

O valor real não está em cada ferramenta, está na integração entre coleta, correlação, contexto e resposta:



SIEM
centraliza e correlaciona
eventos de múltiplas fontes
em tempo real.



NDR
detecção de comportamentos
suspeitos no tráfego de rede.



EDR/XDR
visibilidade e resposta
rápida no endpoint.



SOAR
automatiza workflows
e acelera a resposta.

Tecnologia bem integrada reduz ruído. Tecnologia empilhada cria ruído.

Serviços: a operação como compromisso

O SOC maduro opera como um serviço contínuo e estruturado, não como um projeto:



Definição

o que monitorar e priorizar.



Fluxo

registro e escalonamento de eventos.



Responsabilidade

funções e accountability claros.



Entregáveis

SLAs e resultados mensuráveis.

A maturidade se mede pela capacidade de traduzir eventos em decisões rápidas e acionáveis.



Inteligência de ameaças: ação, não ruído

O erro comum: consumir feeds como se volume fosse valor.



Inteligência sem contexto

gera fila de alertas e fadiga de analista.



Inteligência contextualizada

prioriza atores, setores e TTPs que representam risco real ao seu negócio.



O ciclo completo

prevenção, detecção, investigação, resposta e reporte estratégico.

A pergunta certa não é "quantos feeds temos", é "quantas decisões a inteligência sustentou este mês".



O ciclo que separa **operar** de **amadurecer**

Resiliência não é um estado, é um ciclo contínuo:



SOC que não se reavalia envelhece parado. SOC que se mede, amadurece.

Cinco perguntas para fazer ao seu SOC amanhã

Tire uma foto deste slide. São as perguntas que separam operar de amadurecer.

- 1 Se o seu melhor analista sair hoje, o que para de funcionar?
- 2 Quantos dos seus playbooks foram testados nos últimos seis meses?
- 3 Suas ferramentas conversam entre si ou apenas coexistem?
- 4 Quantas decisões a sua inteligência de ameaças sustentou este mês?
- 5 Quando foi a última avaliação independente da sua operação?

Se alguma resposta incomodou, você já sabe onde está o próximo salto.



O que muda quando as quatro disciplinas operam **juntas**



Menos risco operacional

exposição reduzida e prevenção proativa.



Resposta mais rápida

contenção e neutralização em ambientes críticos.



Melhor uso de recursos

eficiência da equipe e dos investimentos.



Mais governança

previsibilidade e controle das operações.

O SOC deixa de ser um projeto pontual e vira capacidade estratégica permanente.

Como a Kaspersky acelera essa jornada

Cada disciplina da palestra tem um caminho de aceleração:

Pessoas



assistência na contratação e treinamento da equipe SOC.

Processos



SOC Framework, com estratégia, use cases, playbooks e KPIs.

Tecnologia



KUMA (SIEM), KEDR/KATA, CyberTrace e Threat Intelligence.

Serviços



MDR, DFI, contrato de resposta a incidentes.

Ciclo de evolução



avaliação de maturidade do SOC, red teaming e emulação de adversário.

kaspersky

Seu SOC opera. Faça ele **amadurecer!**

Ferramentas sozinhas não fazem um SOC. As quatro disciplinas, sim.

O próximo salto da sua operação começa com uma pergunta honesta:

onde estamos hoje?



OBRIGADO!
OBRIGADO!
OBRIGADO!

kaspersky



Luciano Lima
Senior Solution Architect



/in/lucianolima

