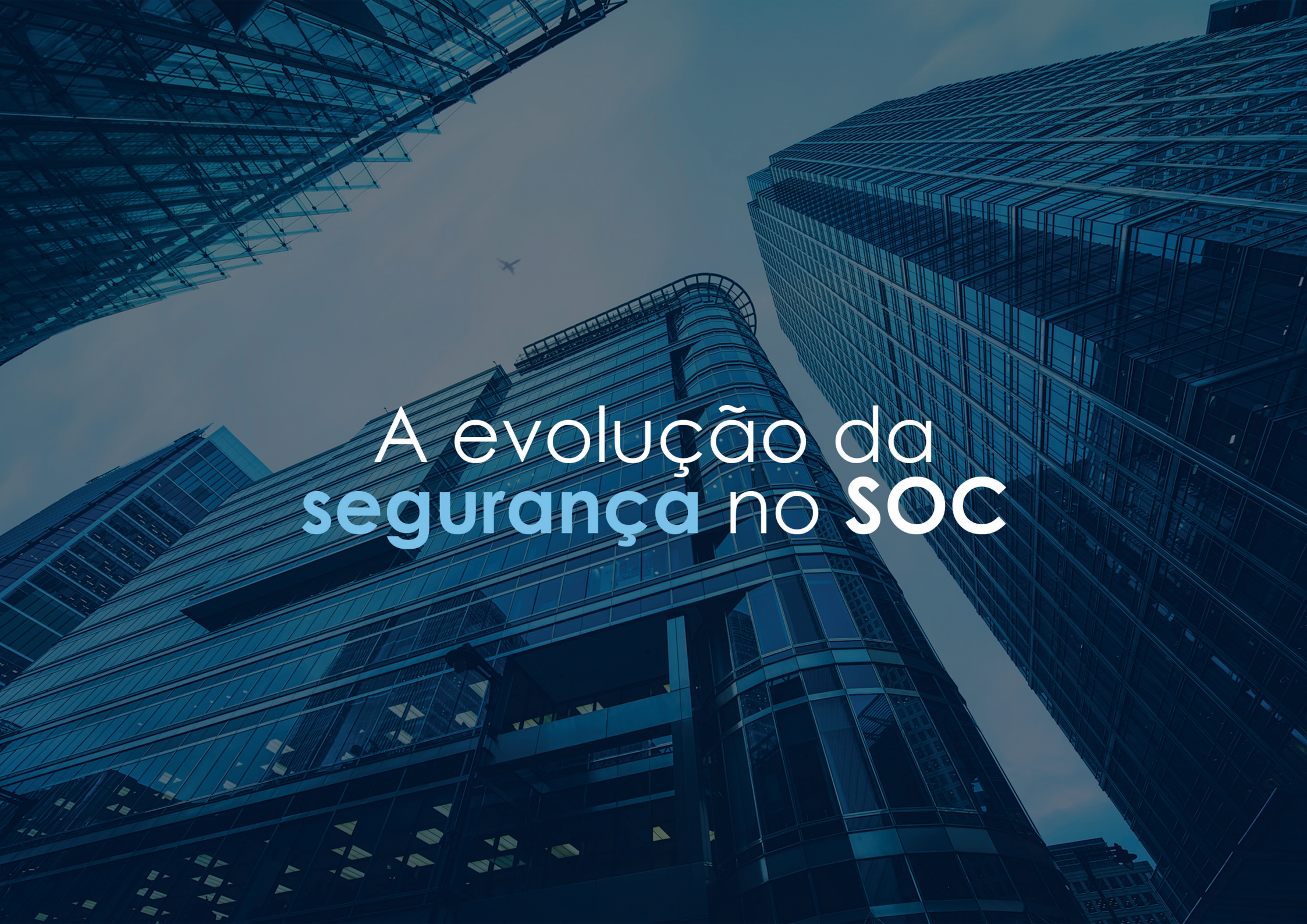

A evolução da
segurança no SOC

O papel do **SOC** no **crescimento** das **empresas**

Um **Centro de Operações de Segurança** (SOC) é **essencial** hoje para os negócios?

Empresas precisam alinhar iniciativas de segurança com as metas de negócios. E um Centro de Operações de Segurança (SOC) fornece a base necessária para a organização proteger dados e informações, detectando e respondendo mais rapidamente às ameaças.

A cada 39 segundos há uma nova tentativa de ataque cibernético.

PROTEGER É FUNDAMENTAL.
Mas, por onde começar?

Por isso, criamos esse material, para falarmos porque **segurança cibernética** se tornou fundamental para empresas que querem crescer e qual o papel dos SOCs nesse contexto.

O QUE VOCÊ ENCONTRARÁ NESTE MATERIAL

Iremos explicar **como nasceu o conceito** de segurança em SOC. Depois, você vai conhecer o **SOC sem fronteiras**, que elevou o nível de proteção e mudou o jogo na segurança cibernética. Na terceira parte, explicamos **a estrutura** do SOC e como o time de profissionais trabalha para levantar muros cada vez mais altos e **barrar invasores**. Por fim, iremos responder por que a sua empresa deveria estar preocupada com isso.

COMO **NASCEU** O **CONCEITO** DE SOC?

A **segurança cibernética** se tornou fundamental para empresas que querem crescer, um processo que envolve pessoas qualificadas e ferramentas de vanguarda. Mas, por onde começar?

Os chamados centros de operações de segurança, os SOCs, têm um papel fundamental nesse contexto.

Não importa o tamanho da empresa. As pequenas e as grandes precisam monitorar sistemas para **detectar possíveis ameaças** e responder nos casos de um evento. Muitas recorrem à implantação ou aprimoramento dos SOCs para potencializar a proteção contra ameaças cibernéticas.

A ideia de operações de segurança nasceu no governo americano em 1966. A finalidade era investigar o que provocou as falhas de estratégia de combate durante a Guerra do Vietnã. Por trás dos processos de investigação daquela época, havia conceitos que, até hoje, são aplicados em segurança cibernética.

São **cinco pilares** que continuam sendo a essência de muitos modelos de mercado, como o ***NIST Cybersecurity Framework***:

- **Identificação de informações críticas;**
- **Análise de ameaças;**
- **Análise de vulnerabilidades;**
- **Avaliação de risco;**
- **Aplicação de plano de ação.**

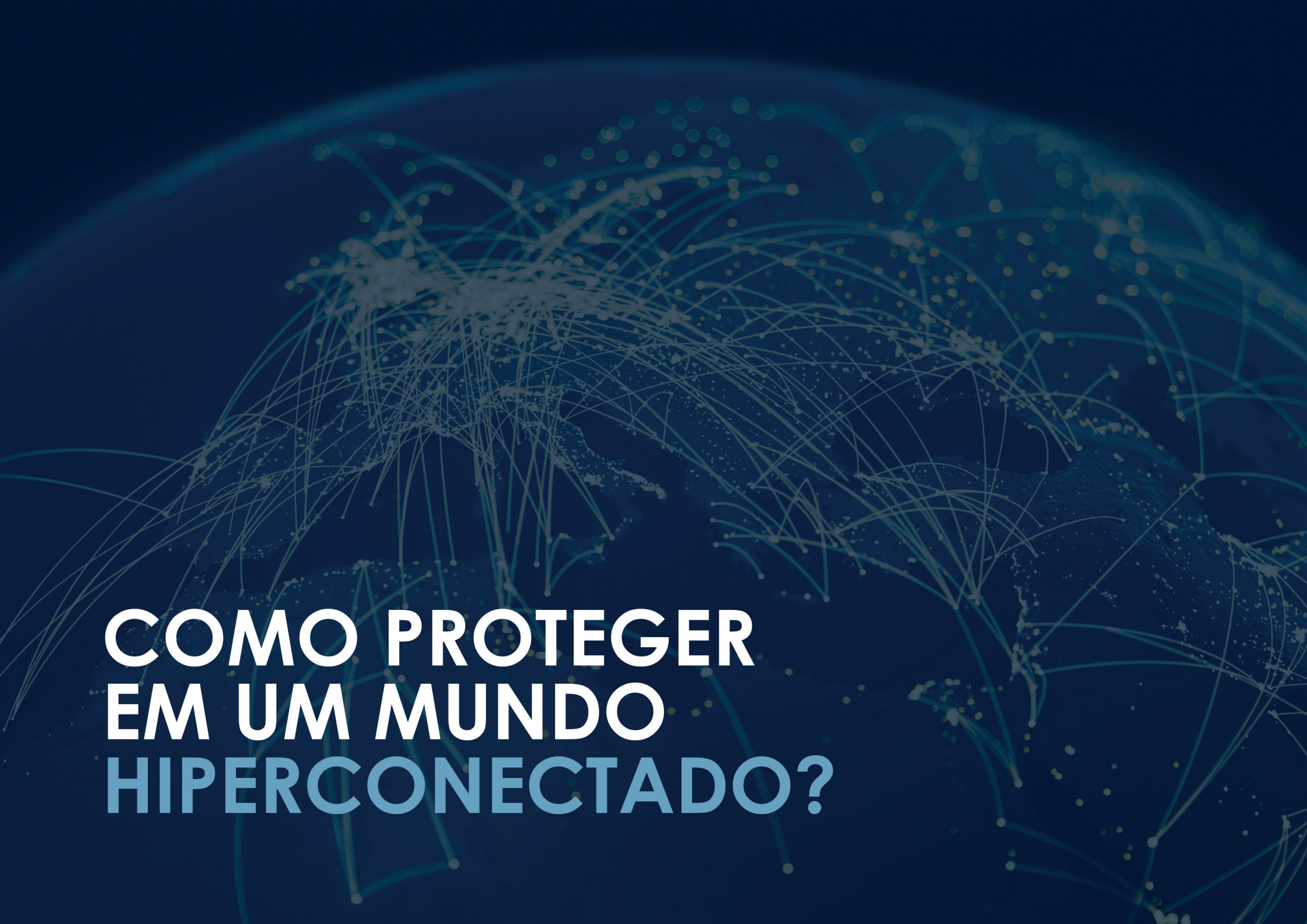
De lá para cá, **o mundo se transformou** e, com **a internet** conectando pessoas e empresas, o índice de **ataques** também cresceu na mesma velocidade.

Tivemos ataques de grande escala nos anos 2000 que causaram prejuízos de milhões de dólares em empresas americanas. Provavelmente você lembra do caso MafiaBoy, que causou um rombo de 1,2 bilhão de dólares na época, com um ataque do tipo DDoS contra sites que incluíam Amazon, eBay, CNN e Yahoo! Ou, o caso em que adolescentes invadiram o Departamento de Defesa Americana, o ano era 1999, obtiveram informações sigilosas e, assim, conseguiram roubar uma parte do código da NASA.

Tudo isso desencadeou uma série de evoluções na segurança cibernética.

Uma delas foi o conceito de SOC, que nasceu no exército americano em meados dos anos 2000.

E que estabeleceu os princípios básicos de monitoramento, operação e controle usados atualmente. Em paralelo a esse contexto histórico, a ISH criava o seu SOC com base nos melhores conceitos que existiam no mercado no ano de 2006. Nos anos seguintes, o SOC foi sendo aprimorado. Mas foi em 2016 que houve um marco, com a revisão dos conceitos de arquitetura do SOC da empresa. Foram abordadas novas metodologias de monitoramento e detecção, e respostas a incidentes. O objetivo era colocar no mercado uma oferta mais avançada de segurança.


COMO PROTEGER
EM UM MUNDO
HIPERCONECTADO?

Monitorar costumava ter o seguinte significado: ter uma solução que detectava eventos já conhecidos e registrados. Funcionava? Sim, mas era incompleto. Porque, não tão raro, acabavam passando despercebidas as ameaças que chamamos de dia zero, aquelas que são novas e diferentes.

O conceito de segurança nasceu décadas atrás. Inspiraram soluções que, nos últimos anos, evoluíram e se tornaram mais complexas. Hoje, o monitoramento de ambientes é feito 24 horas por dia, 7 dias por semana. Sem descanso.
Além disso, as soluções mais modernas de SOC partem de comparações que possibilitam quantificar o risco que uma ameaça representa para um determinado negócio. É uma análise alinhada com o setor em que atua empresa, e com o produto e o serviço que ela oferece.

Esse SOC, que ganhou o apelido de 2.0, também não depende do ecossistema do cliente para monitorar e detectar. O que ele faz é supervisionar o pacote de rede para encontrar comportamentos anômalos. Ou seja, todos os dados que entram e saem do ambiente corporativo passam pelos olhos do SOC.

Mas isso fica **limitado** ao prédio da companhia? Só o tráfego que entra e sai pela **rede corportativa** da sede é vigiado?

Houve atualizações. Transformamos o SOC no que eu gosto de chamar de **SOC Borderless**. Inclusive, um conceito que se mostrou urgente no período de pandemia do coronavírus.

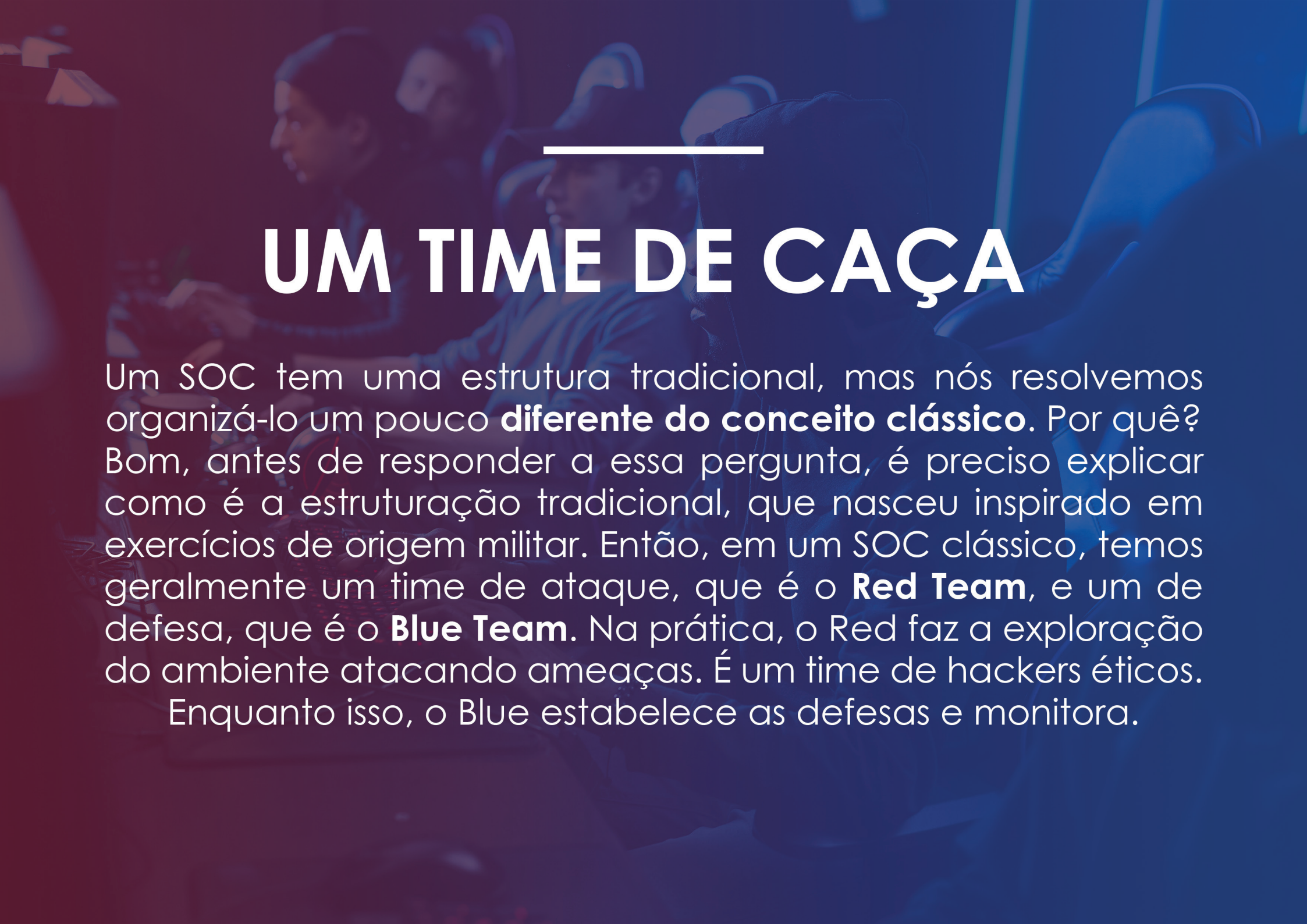
Como ele funciona?

Vamos imaginar que a empresa é um castelo e que o SOC é a defesa desse castelo. E que os moradores precisam fazer negócio além dos muros. O que, traduzindo, seria como trabalhar em casa, em um coworking, na rua potr meio do celular.

Nesse caso, os bens do castelo ficariam desprotegidos? Não.

A verdade é que o usuário troca dados em todos os lugares nos dias de hoje.
E o conceito de SOC acompanhou o comportamento das pessoas. Hoje, onde quer que o usuário esteja, nosso SOC Borderless alcança e monitora.
E não contamos apenas com pessoas extremamente qualificadas para fazer o trabalho.

Profissionais de cibersegurança são fundamentais, mas a verdade é que as ameaças se multiplicam mais rápido do que o mercado forma pessoas. Por isso, contamos com o que chamamos de Orquestração de Segurança, uma camada que une diversos recursos de segurança, somando soluções e equipes. Fazemos tudo isso porque entendemos que dados, hoje, são commodities, decisivos para o crescimento das empresas.



UM TIME DE CAÇA

Um SOC tem uma estrutura tradicional, mas nós resolvemos organizá-lo um pouco **diferente do conceito clássico**. Por quê? Bom, antes de responder a essa pergunta, é preciso explicar como é a estruturação tradicional, que nasceu inspirado em exercícios de origem militar. Então, em um SOC clássico, temos geralmente um time de ataque, que é o **Red Team**, e um de defesa, que é o **Blue Team**. Na prática, o Red faz a exploração do ambiente atacando ameaças. É um time de hackers éticos. Enquanto isso, o Blue estabelece as defesas e monitora.

QUAL É O **DIFERENCIAL** DO SOC DA **ISH**?

Nós contamos com um time a mais. O Hunt Team. É um time de profissionais que conhece todas as táticas de ataque e de defesa. Mas trabalha no que chamamos de pontos cegos.
Ele vai escanear o que o Red não conseguiu ver, vai verificar partes do sistema em que o que o Blue não estabeleceu defesas e vai fazer uma varredura no que a inteligência artificial também não checou.

Ou seja, ele caça tudo aquilo que sai fora do padrão de monitoramento dos outros times.

Esse é o nosso jeito de fazer SOC. Nossa segurança também evoluiu para acompanhar a transformação do mundo em uma rede hiper conectada.

POR QUE **INVESTIR** EM UM **SOC**?

Se você chegou aqui, no **último** post da nossa série sobre a **evolução da segurança no SOC**, você já entendeu como a segurança da informação evoluiu, como ferramentas se tornaram mais complexas e de que forma um SOC moderno é estruturado para conseguir detectar e responder.

Mas afinal, por que a sua empresa deveria estar preocupada com isso?

A cada 39 segundos, há uma nova **tentativa de ataque cibernético** nos EUA. O que quer dizer que não há mais dúvidas de que falhas de segurança vão ocorrer e impactar negativamente os negócios. Portanto, **a pergunta não é mais se uma empresa será hackeada, mas sim quando será**.

Ao fazer as contas sobre quanto custa implantar um bom serviço de proteção de dados, algumas empresas acham tudo caro demais e adiam o planejamento. Somente acreditam que a segurança cibernética pode ficar para depois, as companhias que insistem em se debruçar no cálculo que envolve orçamentos de antivírus e ferramentas para a TI. O problema é que, nesse cenário, o mais importante ficou de fora. Precisamos, antes de tudo, colocar no papel **quanto custa não proteger.**

Os resultados de uma invasão podem ser devastadores. Muito dinheiro perdido. Tempo desperdiçado. Reputações de marcas destruídas.

No Brasil, em 2019, o custo médio de uma violação de dados era de R$ 5,4 milhões, um aumento de 18,93% em relação a 2018. Em 2020, nos Estados Unidos, esse valor já está em US$ 5 milhões.

Ao mesmo tempo, **a indústria de cibersegurança** tem um problema de eficácia. Há milhares de fornecedores no mercado, com bilhões gastos anualmente em defesa. E ainda assim, o número de violações continua a aumentar.

Se as ferramentas sozinhas fossem suficientes para resolver o problema, já teriam resolvido. As violações de dados geralmente ocorrem não porque uma ferramenta falhou em detectar a ameaça ou alertar sobre uma vulnerabilidade, mas devido à falta de fluxos de trabalho adequados, processos e pessoas experientes que sabem priorizar a remediação.

As violações de dados geralmente ocorrem não porque uma ferramenta falhou em detectar a ameaça ou alertar sobre uma vulnerabilidade, mas devido à falta de fluxos de trabalho adequados, e pessoas experientes que sabem priorizar a remediação.

Se você tem interesse em conhecer as **soluções inovadoras** da ISH para proteger e potencializar negócios, converse com uma pessoa do nosso time.

Mande um e-mail para
contato@ish.com.br

OBRIGADO