VisionWare since 2005

por Bruno Castro,
Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

SOC: CONSOLIDAÇÃO DE PLATAFORMAS OU *BEST-OF-BREED*?

EM 2026, POUCOS DEBATES DOMINAM TANTO AS CONVERSAS ENTRE CISOS COMO O CLÁSSICO DILEMA ENTRE CONSOLIDAÇÃO DE PLATAFORMAS E ESTRATÉGIAS *BEST-OF-BREED*.

Durante anos, esta discussão foi apresentada como uma escolha essencialmente tecnológica: optar por um ecossistema unificado de um único fornecedor ou construir um stack composto pelas melhores ferramentas especializadas em cada domínio. No entanto, quando se observa a realidade operacional das equipas de segurança, percebe-se rapidamente que esta decisão raramente é apenas sobre tecnologia. É uma questão de capacidade operacional, de maturidade organizacional e, acima de tudo, de pessoas.

Um único fornecedor promete visibilidade unificada, menos integrações, menos fricção e uma gestão simplificada do ambiente de segurança. Por outro lado, a abordagem *best-of-breed* apresenta-se como a via para atingir níveis superiores de deteção e resposta, recorrendo a ferramentas altamente especializadas em áreas como endpoint detection, análise de tráfego de rede, inteligência de ameaças ou automação de resposta. Em teoria, cada modelo tem as suas virtu-

BRUNO CASTRO, VISIONWARE

"O STACK TECNOLÓGICO DEIXA DE SER UMA DECISÃO RÍGIDA E PASSA A EVOLUIR AO RITMO DAS NECESSIDADES DA ORGANIZAÇÃO E DO PANORAMA DE AMEAÇAS"

des. Na prática, ambos enfrentam limitações quando chegam ao terreno do SOC.

Equipas de SOC vivem o constante: volumes crescentes de alertas, múltiplas superfícies de ataque, integração entre ferramentas que nem sempre comunicam de forma fluída e, talvez o maior desafio de todos, uma escassez de retenção de talento qualificado. Num ambiente *best-of-breed*, a complexidade tecnológica pode tornar-se rapidamente difícil de gerir. Cada ferramenta exige onboarding, afinação de deteções, integração com outras plataformas e formação especializada. Já num ambiente altamente consolidado, as equipas podem ganhar simplicidade e maior personalização operacional

É neste contexto que o modelo de SOC as a Service começa a alterar profundamente a forma como as organizações encaram este dilema. Em vez de se perguntar se deve consolidar ou adotar uma estratégia *best-of-breed*, a discussão passa a centrar-se numa questão mais fundamental: quem tem a capacidade para operar eficazmente o ecossistema de segurança 24 horas por dia, todos os dias do ano? Um SOC as a Service transfere essa responsabilidade operacional para equipas especializadas cuja missão é precisamente garantir que as tecnologias funcionam como esperado, que os alertas são analisados com contexto e que os incidentes recebem resposta atempada.

Ao fazê-lo, muitas organizações descobrem que já não precisam de escolher entre simplicidade e profundidade técnica, já que, um fornecedor de SOC pode integrar múltiplas tecnologias especializadas quando estas trazem vantagens claras, ou operar plataformas consolidadas quando a simplicidade operacional é prioritária. O stack tecnológico deixa de ser uma decisão rígida e passa a evoluir ao ritmo das necessidades da organização e do panorama de ameaças.

Existe ainda um outro fator subestimado: a experiência acumulada. Uma equipa de SOC interna observa apenas os incidentes que ocorrem dentro da sua própria organização; um SOC que opera para múltiplos clientes, em diferentes setores e arquiteturas, acumula uma exposição muito mais ampla a padrões de ataque, técnicas emergentes e comportamentos anómalos. Essa experiência acumulada e coletiva, cria um nível de contexto operacional difícil de replicar internamente.

Ambas as abordagens têm mérito e ambas podem falhar quando não são acompanhadas pela capacidade operacional necessária. Contudo, à medida que as ameaças evoluem mais rapidamente do que as equipas conseguem crescer, torna-se evidente que o verdadeiro desafio não será apenas escolher as ferramentas certas, mas antes garantir que alguém está constantemente a observar, a interpretar e a responder aos sinais que essas ferramentas produzem. E essa, no final, continua a ser a missão central de qualquer SOC, ou seja, transformar tecnologia em segurança real. ◀