

#29 ABRIL 2026

IT ^{Insight} SECURITY



**CONSOLIDAÇÃO VS. BEST-OF-BREED:
UNIR OU FRAGMENTAR?**



ESGOTADO!

#A VOZ DOS CISO

14 ABRIL 2026 | GAIA

A VOZ DOS CISO

Depois do sucesso da primeira edição, a IT Security Summit regressa à região Norte no dia 14 de abril de 2026, no Tivoli Kopke Porto Gaia, em Vila Nova de Gaia, duplicando o espaço em plateia para acomodar um número ainda maior de leitores da revista IT Security e profissionais do setor.

Centrada nos temas da resiliência e compliance com ênfase nas necessidades práticas das empresas da região norte e dando voz aos seus protagonistas, a IT Security Summit será uma oportunidade para explorar as tecnologias mais inovadoras que impactam um grande número de indústrias, para além da partilha de conhecimentos entre CISO, CSO, diretores de segurança e diretores de IT com responsabilidade de cibersegurança, originando um ecossistema único de networking.

CONHEÇA O PROGRAMA

PARCEIROS

DIAMOND



PLATINUM



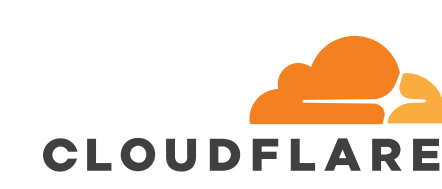
GOLDEN



SILVER



SILVER EXHIBITION



VAD PARTNERS



INSTITUTIONAL PARTNER



SUPPORT PARTNER



COVER



CHAT

▼ MANUEL NEVES, MERCK



BLUE TEAM

▼ ORAMIX



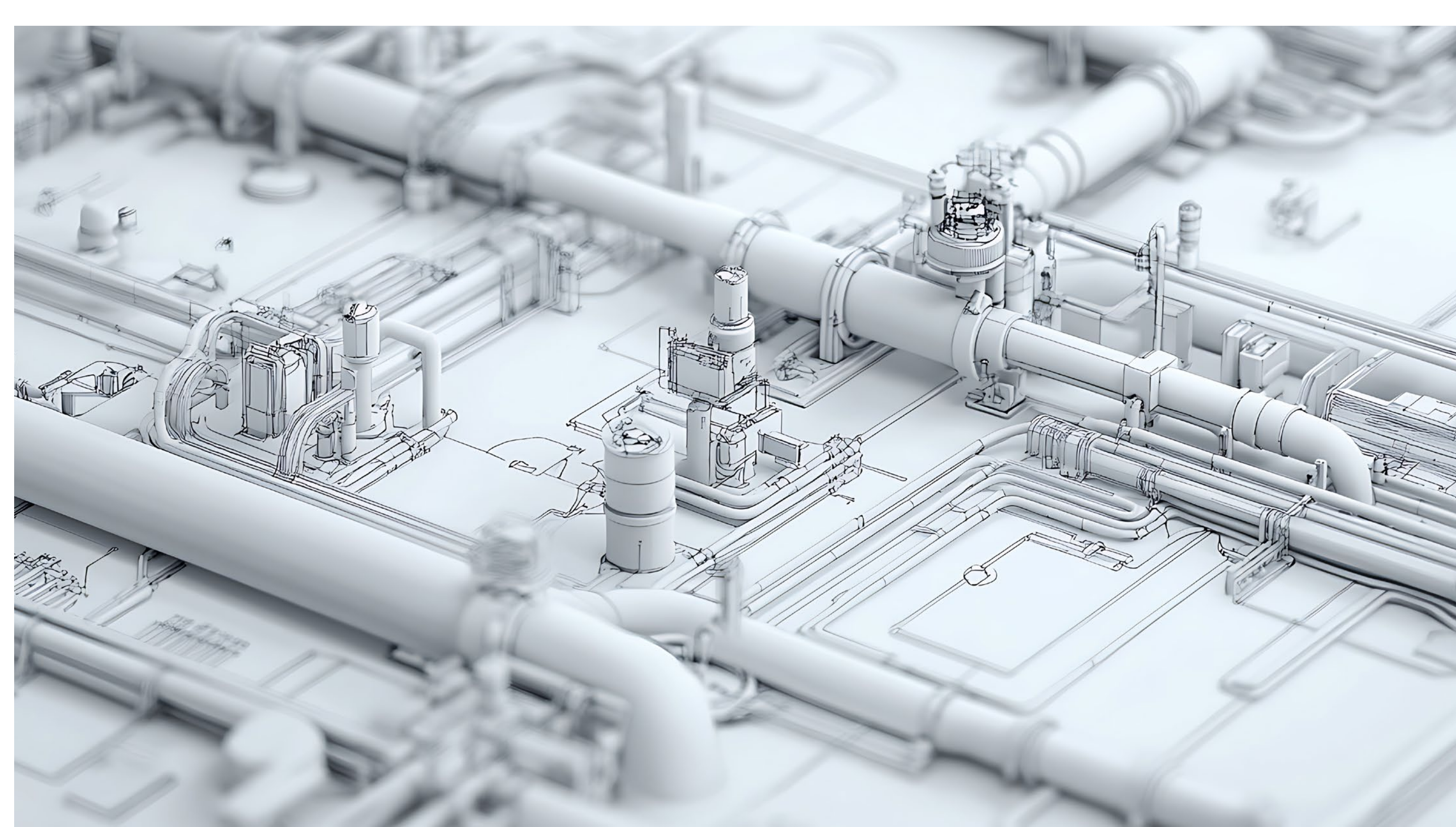
ANCHOR

► HENRIQUE CARREIRO



BRAVE NEW WORLD

▼ SASE MATURATION: BEYOND THE HYPE



EXPERT

▼ CRISTIANE DIAS



▼ MAFALDA DE BRITO
FERNANDES, PLMJ



Security & Networking Re**AI**magined

+ Proteja e acelere dados na cloud e IA, em qualquer lugar.

A cloud e a Inteligência Artificial revolucionaram a forma como trabalhamos. Foi por isso que criamos a Netskope e é também por isso que mais de 30% das empresas da Fortune 100 confiam em nós.

A Netskope nasceu para a era da cloud e da IA.

Com a Netskope, cloud, dados, IA, dispositivos e redes são protegidos de forma contínua, permitindo às organizações defenderem-se ativamente contra ameaças em constante evolução.

Não criamos apenas uma plataforma. Criamos a base para a próxima geração de negócios seguros e de alto desempenho.

Descubra o que nos move.



netskope.com

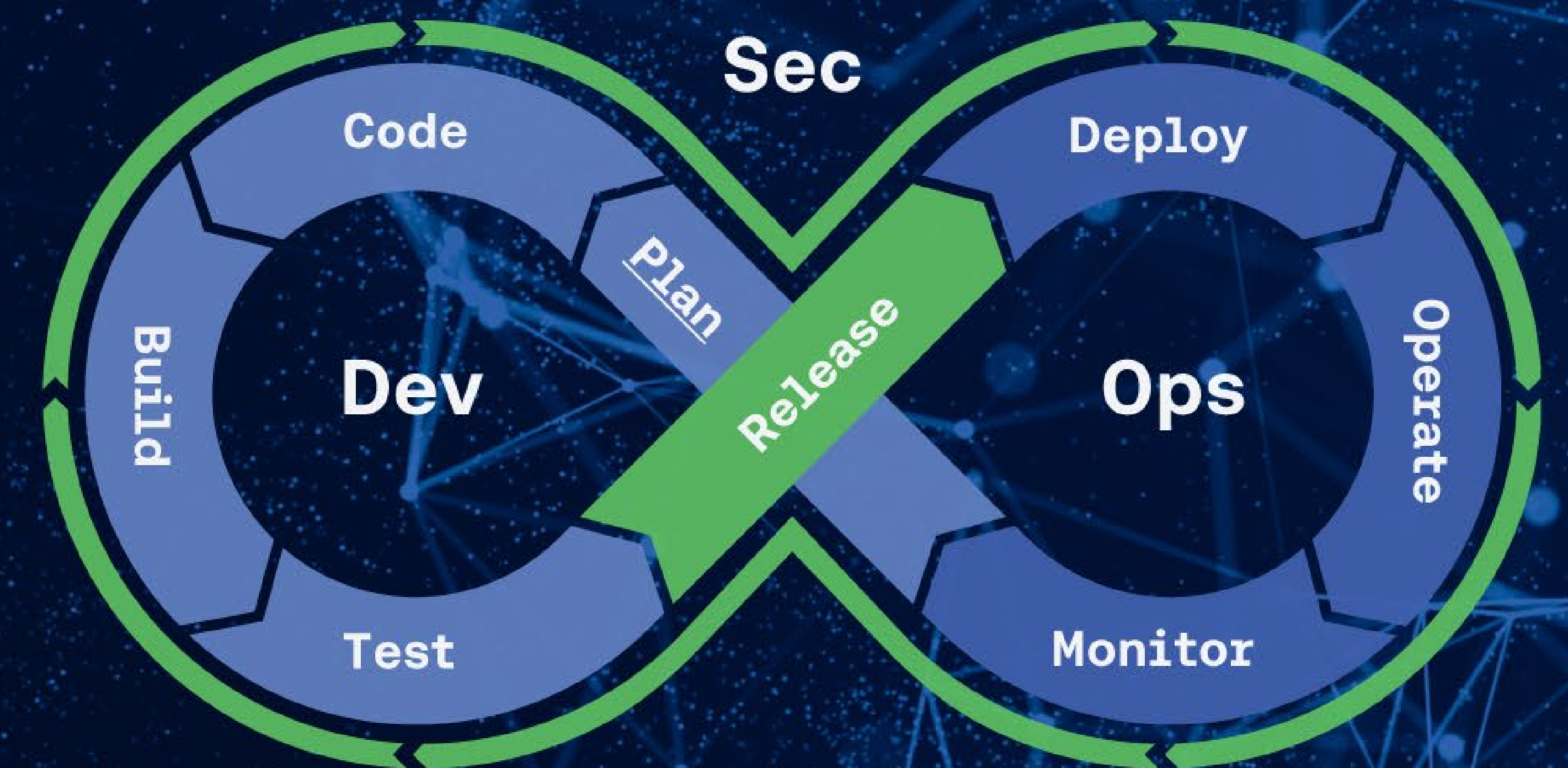


O S.Lab ou Security Labs é um espaço de criação e partilha dentro da IT Security, onde exploramos e desenvolvemos ideias em colaboração com os nossos parceiros. Aqui, transformamos conceitos em conteúdos relevantes e envolventes, seja através de artigos, vídeos, webinars, podcasts ou conferências. O nosso objetivo é dar forma a ideias que não cabem nos formatos tradicionais, criando novas formas de comunicar e inovar.

Shift Left, Secure Right.

→ Reforce a segurança do seu SDLC e assegure a conformidade com requisitos normativos e regulatórios, integrando controlos de segurança segundo os princípios *security by design* e *security by default*.

balwurk cyber security



Modelação de Ameaças



Pentesting



Red Team



Gestão de Vulnerabilidades



Auditoria e Conformidade



Continuidade de Negócio

balwurk.com
mail@balwurk.com

O ELO QUE NÃO CONTROLAMOS

RUI DAMIÃO



Este mês não é um mês qualquer. A 3 de abril, entra em vigor em Portugal o Decreto-Lei n.º 125/2025, que transpõe a Diretiva NIS2. Depois de anos de discussão, o enquadramento jurídico da cibersegurança passa a ser lei com consequências reais: coimas até dez milhões de euros, responsabilização direta da gestão, supervisão pelo Centro Nacional de Cibersegurança. Para quem lê esta publicação, a pergunta relevante não é se está abrangido, mas sim o que é que isto revela sobre como ainda pen-

samos a cibersegurança.

Revela que continuamos a tratar a segurança como um perímetro, o nosso perímetro. A NIS2 obriga a olhar para fora: para a cadeia de abastecimento, para os fornecedores, para as dependências que raramente são auditadas com o mesmo rigor que se aplicam aos próprios sistemas. Um incidente não precisa de entrar pela porta da frente. Entra pelo elo mais fraco de uma cadeia que,

muitas vezes, mal se conhece. Uma cadeia que não se conhece não se consegue proteger.

A gestão da cadeia de valor em cibersegurança exige mais do que avaliar fornecedores na contratação; exige capacidade de agir. Uma organização madura não se limita a avaliar fornecedores, mas mantém a autonomia operacional para os substituir quando o risco o justifica. Isso inclui fornecedores com os quais existe uma relação longa, uma dependência técnica ou até um interesse comercial partilhado. A capacidade de cortar é, ela própria, um controlo de segurança. Sem ela, a avaliação de risco é apenas um exercício de documentação.

A NIS2 não inventou este princípio, mas tornou-o incontornável. Neste abril, vale a pena ser desconfortável. É uma boa altura para começarmos a perguntar se amanhã tivéssemos de prescindir de um fornecedor crítico por razões de segurança, teríamos coragem? Teríamos alternativa? Teríamos processo? Se a resposta a qualquer uma das perguntas for não, a NIS2 chegou, então, na hora certa. ◀



O EQUILÍBRIO ENTRE A DISPONIBILIDADE E O RISCO É A CHAVE PARA A SEGURANÇA DA INFORMAÇÃO

CONHECIMENTO - ÉTICA - RIGOR

www.cso.pt | info@cso.pt



HENRIQUE CARREIRO

OPENCLAW: A SEGURANÇA DOS AGENTES, NUMA FRONTEIRA COM POUCAS REGRAS

Na China tem-se vindo a assistir a uma febre dos cidadão comuns, não necessariamente com base tecnológica, relativamente ao OpenClaw, uma plataforma para agentes de software.

Este é um projeto que deixou de ser apenas de nicho no GitHub e passou a circular num registo raro para algo com estas características: instalação em massa, serviços pagos de configuração, comunidades de utilizadores e uma vaga de curiosidade pública suficientemente forte para chamar a atenção de grandes empresas e das autoridades. Essa veloci-

dade de difusão nasceu de uma proposta técnica muito específica: pôr um agente de IA dentro dos canais de mensagens que as pessoas já usam e dar-lhe continuidade operacional.

O ponto de partida do OpenClaw pode ser descrito como um *gateway* autoalojado, com execução local ou em servidor próprio, que liga aplicações de mensagens a agentes com memória, sessões persistentes e ferramentas. No repositório oficial, o projeto apresenta-se como um “*personal AI assistant*” acessível através de canais como WhatsApp, Telegram, Discord, Slack, Signal ou iMessage. A arquitetura



O PONTO DE PARTIDA DO OPENCLAW PODE SER DESCRITO COMO UM GATEWAY AUTOALOJADO, COM EXECUÇÃO LOCAL OU EM SERVIDOR PRÓPRIO, QUE LIGA APLICAÇÕES DE MENSAGENS A AGENTES COM MEMÓRIA, SESSÕES PERSISTENTES E FERRAMENTAS

ra interessa mais do que o slogan: o *gateway* recebe pedidos, mantém sessões, encaminha mensagens, gere ligações a clientes e expõe o agente configurado pelo utilizador.

O OpenClaw foi, sobretudo, concebido para usar a infraestrutura já existente como interface primária. O pedido entra por uma app de mensagens, é associado a uma sessão, passa pelo *gateway*, chega ao agente e regressa. O que muda é a posição do sistema na cadeia de trabalho. Em vez de ficar na margem, como ferramenta que sugere ou resume, o agente estabelece-se no ponto onde começam as instruções.

Essa escolha explica grande parte dos benefícios. O primeiro destes é o controlo: sendo autoalojado, o OpenClaw pode correr na infraestrutura do próprio utilizador, com configuração, credenciais e integrações geridas por este. Seguidamente, a continuidade: o mesmo agente pode ser usado em vários canais sem reconstruir o contexto a cada interação. Finalmente, a proximidade aos fluxos reais de trabalho. Um pedido feito por mensagem pode acionar ferramentas, usar memória de sessão, consultar serviços e devolver um resultado no mesmo canal em que a instrução foi recebida. No plano funcional, o OpenClaw aproxima o gesto de pedir do ato de executar.

O RISCO MORA AO LADO

É precisamente essa proximidade que define também o perfil de risco. A documentação de segurança do projeto é muito clara quanto ao enquadramento de confiança. O OpenClaw é pensado para servir de base a um assistente pessoal, com uma única fronteira de confiança por *gateway*. A documentação diz explicitamente que o sistema não deve ser tratado como uma fronteira segura *multi tenant* para vários utilizadores mutuamente desconfiados a partilharem o mesmo agente ou o mesmo *gateway*. Quando há utilizadores, agentes ou integrações com níveis de confiança diferentes, a recomendação é separar fronteiras com *gateways* distintos e, de preferência, com utilizadores de sistema operativo, anfitriões ou VPS separados.

Este ponto é menos abstrato do que parece. Um agente só se torna útil quando recebe acesso a contexto, ferramentas, credenciais, integrações e, por vezes, recursos locais. Se as instruções chegam por canais externos e o agente pode tocar em ficheiros, serviços ou extensões, a segurança deixa de depender apenas da qualidade do modelo e passa a depender da qualidade do isolamento. Quem pode falar com o agente, em que condições, e com que privilégios efetivos, torna-se a pergunta central. A documentação oficial recomenda começar com o

menor nível de acesso possível, auditar a configuração e tratar plugins e extensões como parte da base de confiança local. Instalar um plugin é introduzir código com efeito sobre o ambiente do *gateway*.

Há ainda riscos ligados à própria forma de publicar e autenticar o sistema. A documentação do OpenClaw assinala a autenticação delegada em reverse proxy como funcionalidade sensível, avisando que uma má configuração pode expor o *gateway* a acesso não autorizado, porque a autenticação fica dependente do proxy. Este tipo de aviso é revelador. O risco surge aqui nos mesmos pontos em que qualquer serviço exposto se torna vulnerável: identidade, rede, permissões, separação de contextos e confiança excessiva em componentes intermédios.

A receção dos utilizadores chineses tornou visível uma segunda dimensão do OpenClaw: a passagem muito rápida de objeto técnico a fenómeno social de adoção. Essa passagem trouxe também reações insti-

É UM SISTEMA NA FRONTEIRA DAS POSSIBILIDADES NOS MODELOS DE AGENTES EM MODO “LIVRE” (SEM AS RESTRIÇÕES IMPOSTAS NUM SISTEMA MAIS CENTRALIZADO). MAS, COMO EM TODAS AS FRONTEIRAS, OS CUIDADOS NA RESPECTIVA IMPLEMENTAÇÃO NUNCA SERÃO EXCESSIVOS

tucionais. Nos últimos dias, foram noticiados avisos e restrições em organismos do Estado e ambientes regulados, com referências a permissões excessivas, instalação de versões não oficiais, integrações arriscadas com aplicações de mensagens e exposição desnecessária ao exterior. As recomendações públicas relatadas por vários meios vão na mesma direção da documentação do projeto: reduzir privilégios, evitar contas de administrador, usar versões oficiais e reforçar a auditoria e a proteção dos sistemas onde o *gateway* corre.

O OpenClaw é um sistema que transforma canais de mensagens em interface de operação para um agente persistente. A novidade deste projeto está

nessa conversa passar a entrar diretamente num circuito de sessões, memória e ferramentas, com efeitos possíveis sobre sistemas reais. É essa mudança de posição que explica a utilidade do OpenClaw e também a razão por que a sua arquitetura exige uma leitura cuidadosa. O sistema vale menos pelo exotismo do nome do que pelo que representa tecnicamente: a saída do agente do chat e a sua entrada na infraestrutura quotidiana. É um sistema na fronteira das possibilidades nos modelos de agentes em modo “livre” (sem as restrições impostas num sistema mais centralizado). Mas, como em todas as fronteiras, os cuidados na respetiva implementação nunca serão excessivos. ◀

We live and breathe Cyber Security

Soluções de proteção, monitorização e mitigação de riscos, incluindo a formação de colaboradores para uma postura de segurança mais eficaz.

Visite: claranet.pt/cyber-security

claranet

Make
modern
happen®

SIS ALERTA PARA ATAQUES A CONTAS WHATSAPP E SIGNAL

O esquema permite que cibercriminosos tenham acesso a contas de governantes, diplomatas e militares, com acesso a informação privilegiada, aproveitando eventuais falhas de segurança por parte dos utilizadores.



O Sistema de Informações de Segurança (SIS), que integra o Sistema de Informações da República Portuguesa (SIRP), lançou um alerta para a ocorrência de operações de ciberespionagem à escala mundial, patrocinadas por um Estado estrangeiro. O objetivo

passa por aceder a contas de Whatsapp e Signal de governantes, diplomatas, militares e outros responsáveis que tenham acesso a informação sensível e privilegiada de origem nacional, assim como de países aliados.

O esquema leva os utilizadores destas plataformas a partilharem dados sensíveis, permitindo que os cibercriminosos comprometam as respetivas contas de Whatsapp e Signal. Esta ação abre caminho a que os atacantes acessem a diversa informação, nomeadamente conversas individuais e de grupo e ficheiros partilhados. ◀

CAMPANHAS CLICKFIX VISAM MACOS COM INFOSTEALER

Três campanhas ClickFix recorrem a engenharia social para infetar macOS com o MacSync.



Uma série de três campanhas ClickFix está a visar utilizadores de macOS com o infostealer MacSync, recorrendo a técnicas de engenharia social para induzir as vítimas a instalar malware, segundo investigadores da Sophos.

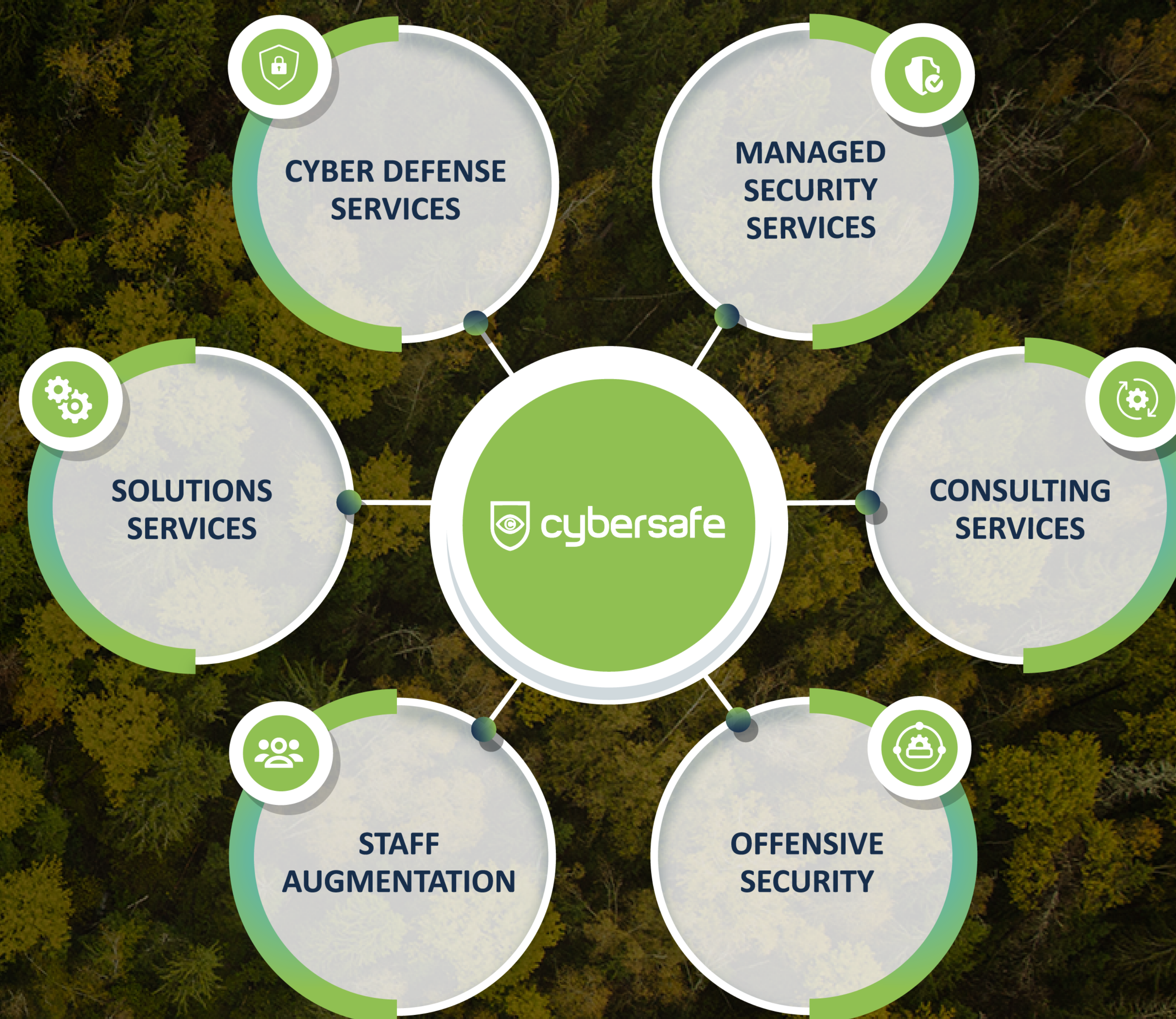
A empresa descreve a evolução da sofisticação das campanhas ao longo dos últimos três meses. A primeira recorreu a anúncios falsos no Google que promoviam um suposto navegador “ChatGPT Atlas”, alojado no Google Sites. Ao tentar descarregar o software, os utilizadores eram levados a executar um comando que instalava o malware; numa segunda fase, os atacantes passaram a utilizar conversas partilhadas no ChatGPT, aparentemente legítimas, com recomendações de ferramentas para macOS. Estas interações direcionavam depois as vítimas para páginas maliciosas que imitavam plataformas de desenvolvimento confiáveis, como o GitHub. ◀



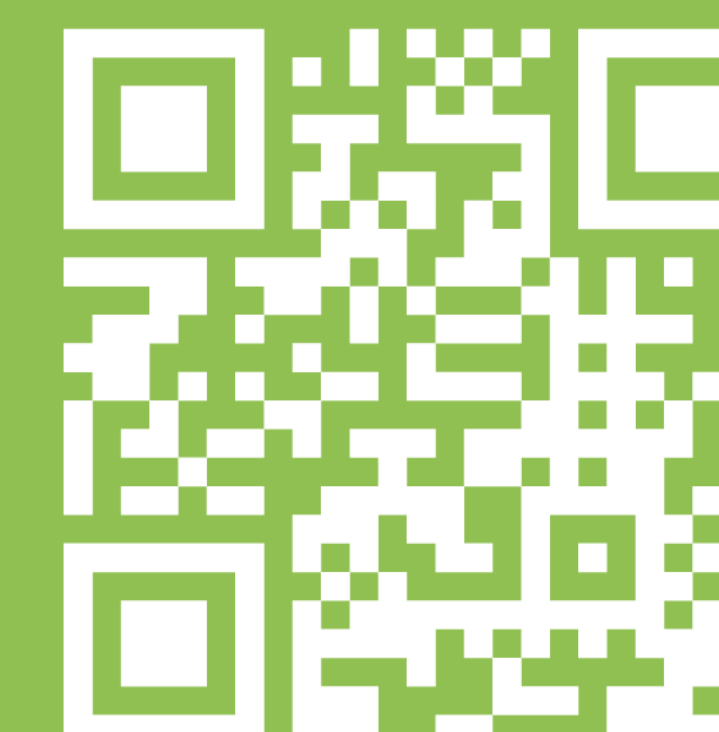
CYBERSECURITY EVERYWHERE

Empresa totalmente focada em soluções e serviços de cibersegurança, empenhada em tornar as organizações mais seguras e resilientes. Defendemos o conceito de “cybersecurity everywhere”: segurança contínua e integrada, desde a infraestrutura ao utilizador.

5 CONTINENTES +150 CLIENTES



SAIBA MAIS:



PME líder



PME
excelência

+351 210 360 276

contacto@cybersafe.pt

www.cybersafe.pt

24% DAS EMPRESAS NUNCA TESTAM DISASTER RECOVERY

Um estudo da Quest Software, que analisa práticas de ITDR em 650 empresas, indica que apenas 24% das organizações testam planos de disaster recovery a cada seis meses.



Um estudo global da Quest Software revela que muitas organizações continuam sem validar regularmente os seus planos de recuperação após incidentes de segurança. De acordo com o relatório “*State of ITDR*”, apenas 24% das empre-

sas testam os planos de *disaster recovery* no intervalo recomendado de seis meses, enquanto outros 24% afirmam nunca realizar esse tipo de teste.

O inquérito foi realizado junto de 650 responsáveis e profissionais de IT e segurança em diferentes regiões e analisa a forma como as organizações estão a abordar estratégias de *Identity Threat Detection and Response* (ITDR). O estudo surge num contexto marcado pelo aumento de ataques alimentados por inteligência artificial, pelo crescimento das identidades não humanas e pela expansão das superfícies de ataque. ◀

FALHA CRÍTICA PERMITE RESET DE PASSWORDS

Vulnerabilidade nos switches Aruba Networking permite contornar autenticação. Atualizações já estão disponíveis para várias versões do AOS-CX.



A HPE disponibilizou atualizações de segurança para corrigir uma vulnerabilidade crítica no sistema operativo Aruba Networking AOS-CX que pode permitir a reposição de passwords de administrador.

A falha, identificada como CVE-2026-23813 e classificada com pontuação CVSS de 9,8, afeta a interface de gestão web dos switches AOS-CX e pode ser explorada remotamente sem necessidade de autenticação, permitindo contornar mecanismos de controlo de acesso.

Segundo o aviso de segurança da HPE, as organizações podem reduzir o risco restringindo o acesso às interfaces de gestão e aplicando políticas rigorosas de controlo de acesso.

As correções foram incluídas nas versões AOS-CX 10.17.1001, 10.16.1030, 10.13.1161 e 10.10.1180. ◀

Paramos ciberataques *em* 38min



Porquê adicionar mais software quando pode adicionar inteligência?
Na Prologin, aproveitamos a sua tecnologia atual para garantir
visibilidade total sobre todas as superfícies de ataque.

Deteção precoce. Resposta imediata. Sem ruído.

SITES FALSOS DE VPN ROUBAM CREDENCIAIS EMPRESARIAIS

Campanha recorre a páginas falsas de VPN para capturar credenciais. Ataques exploram pesquisas online e distribuem malware disfarçado de cliente VPN.



Um grupo de ameaça identificado como Storm-2561 está a distribuir aos clientes VPN falsos de fornecedores empresariais para roubar credenciais de acesso corporativo. A campanha foi identificada por investigadores da Microsoft.

Os atacantes manipulam resultados de pesquisa através de técnicas de SEO poisoning para termos como “Pulse VPN download” ou “Pulse Secure client”. As vítimas são redirecionadas para sites falsos que imitam páginas oficiais de fabricantes como Ivanti, Cisco e Fortinet.

Segundo a Microsoft, a infraestrutura utilizada nesta campanha inclui também domínios associados a outros fabricantes de soluções de segurança e rede, incluindo Sophos, SonicWall, Check Point e WatchGuard, indicando que o objetivo é atingir utilizadores de vários produtos VPN empresariais. ◀

PATCHES CORRIGEM FALHAS CRÍTICAS EM APPLIANCES DE REDE

Falhas críticas afetam o Firewall ASA, Secure FMC e Secure FTD, podendo permitir execução remota de código e acesso root.



A Cisco anunciou a correção de 50 vulnerabilidades nos seus produtos, incluindo 48 falhas que afetam os *appliances* Firewall ASA, Secure FMC e Secure FTD.

As correções fazem parte do pacote de segurança publicado pela empresa em março de 2026, que inclui 25 avisos de segurança que detalham vulnerabilidades nos produtos de rede corporativos. Entre elas, dois alertas descrevem falhas classificadas como críticas.

A primeira, identificada como CVE-2026-20079 (pontuação CVSS 10/10), trata-se de um *bypass* de autenticação na interface web do Cisco Secure FMC.

A exploração bem-sucedida da vulnerabilidade pode permitir que invasores executem scripts arbitrários em sistemas vulneráveis e obtenham acesso root ao sistema operacional subjacente. ◀



A GESTÃO DE RISCO COMEÇA NA ESCOLHA DOS PARCEIROS CERTOS!

☆ **SECURNET** | Parceiro do Ano HPE 2025



CASA BRANCA QUER REFORÇAR DEFESA DIGITAL E REDUZIR REGRAS PARA EMPRESAS

A administração norte-americana revelou uma nova Estratégia Nacional de Cibersegurança, que prevê ações ofensivas contra cibercriminosos e estados adversários, redução de requisitos regulatórios e maior envolvimento do setor privado na defesa digital.



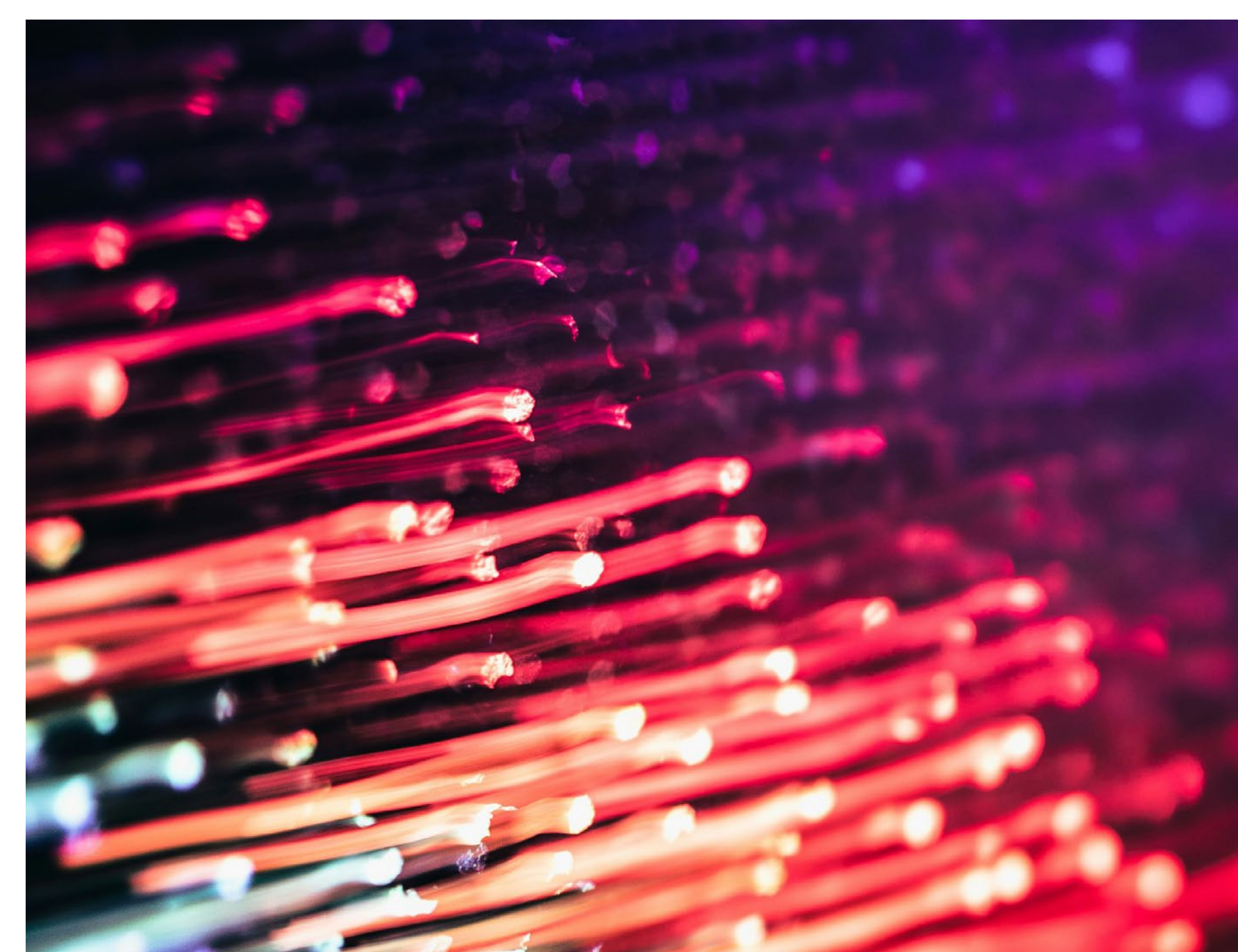
A Casa Branca apresentou uma nova Estratégia Nacional de Cibersegurança, delineando as prioridades da administração de Donald Trump para reforçar a segurança digital dos Estados Unidos até ao final do mandato. O documento, com apenas quatro páginas, destaca uma abordagem mais ofensiva

contra ciberameaças e propõe também reduzir o peso da regulação sobre empresas e infraestruturas críticas.

Entre as principais medidas está o compromisso de intensificar operações cibernéticas ofensivas contra redes criminosas e governos adversários. A estratégia prevê desmantelar infraestruturas de cibercriminosos, sancionar empresas estrangeiras envolvidas em atividades ilícitas e expor campanhas de espionagem digital e operações de influência online. ◀

FALSO SITE DE SEGURANÇA DA GOOGLE USA APP PARA ROUBAR CREDENCIAIS E CÓDIGOS MFA

Campanha de phishing recorre a Progressive Web App para intercetar códigos SMS, roubar dados da área de transferência e transformar o navegador da vítima num proxy para atacantes.



Uma nova campanha de phishing está a utilizar uma página falsa de segurança da Google para instalar uma aplicação web maliciosa capaz de roubar códigos de autenticação multifator, endereços de carteiras de criptomoedas e outros dados sensíveis.

O ataque recorre a funcionalidades de Progressive Web Apps (PWA) e engenharia social para convencer as vítimas de que estão a realizar uma verificação de segurança legítima da sua conta Google. Ao aceitarem as permissões solicitadas, os utilizadores acabam por instalar uma aplicação maliciosa que corre numa janela própria, sem controlos visíveis do navegador, simulando o comportamento de uma aplicação legítima. ◀



+5000 projetos desenvolvidos



+100 colaboradores



A missão da VisionWare é contribuir para o Sucesso das organizações, aumentando a sua cultura e maturidade em Segurança da Informação.



+200 clientes ativos



+10 geografias



Porto | Lisboa | Praia | Mindelo



geral@visionware.pt



+351 225 323 740



visionware.pt

SOPHOS

O PAPEL DOS SERVIÇOS MDR NA RESPOSTA A CIBERATAQUES

A IT SECURITY E A SOPHOS ORGANIZARAM UM PEQUENO-ALMOÇO EXECUTIVO DEDICADO AO TEMA MDR: DA DETECÇÃO À RESPOSTA - PORQUE É QUE AS ORGANIZAÇÕES NÃO O CONSEGUEM FAZER SOZINHAS. REPRESENTANTES DE VÁRIAS ORGANIZAÇÕES ESTIVERAM PRESENTES PARA PARTILHAREM A SUA EXPERIÊNCIA E PONTOS DE VISTA SOBRE O TEMA.

Num contexto de crescente sofisticação das ciberameaças e de forte pressão sobre as equipas internas de segurança, este debate, promovido pela Sophos e organizado pela revista IT Security, reuniu decisores e especialistas para discutir os desafios reais da deteção e resposta a incidentes, bem como o papel do Managed Detection and Response (MDR) no equilíbrio entre capacidades internas e serviços especializados.

Na apresentação de abertura da sessão, Ross McKerchar, CISO da Sophos, explicou a forma como a empresa organiza internamente as capacidades de defesa e gestão de risco, com especial foco na inteligência de ameaças, na resposta a incidentes e na proteção da cadeia de fornecimento. O responsável destacou também o modelo operacional da Sophos, que concentra várias funções de cibersegurança numa única estrutura para melhorar a colaboração e a capacidade de resposta.



ROSS MCKERCHAR, CISO DA SOPHOS



“Juntámos toda a nossa experiência de cibersegurança num único grupo, o X-Ops, com mais de mil especialistas dedicados à investigação de ameaças, resposta a incidentes e serviços de MDR. Essa colaboração permite-nos partilhar inteligência dentro da organização e, no final, defender melhor os nossos clientes”, afirmou.

Ross McKerchar centrou-se também no risco associado à cadeia de fornecimento, ao defender que o desafio já não está apenas no controlo dos fornecedores diretos, mas na capacidade de responder com rapidez e transparência a falhas que podem surgir em cadeias cada vez mais longas e interligadas. “Chegámos a um ponto em que já não basta controlar apenas o risco imediato da cadeia de fornecimento” e que “todos têm incidentes; a diferença está na forma como se responde a eles”, sublinhou.

Paulo Moniz, Global Head of Security Operations, EDP: “Demonstrar risco é difícil. Quantificá-lo é um desafio para qualquer organização, porque o risco não é algo que se consiga medir de forma simples ou direta. Combinamos vários fatores numa equação que nos permite acompanhar a evolução da nossa postura de segurança ao longo do tempo. Para além disso, realizamos avaliações periódicas de maturidade do nosso framework de cibersegurança. Utilizamos um modelo de maturidade de zero a cinco e pedimos a auditores externos que avaliem as nossas capacidades. Esse exercício permite demonstrar de forma objetiva a evolução da organização em termos de maturidade e resiliência”

Ricardo Mendes, Head of IT Security and Infrastructure Division, CM Oeiras: “É comum dizer que não se têm a noção de que um município

é como um pequeno país. Temos saúde, segurança social, polícia, serviços financeiros, tudo. Por causa disso, temos pessoas desde o nível executivo até ao guarda-rio ou a quem limpa as ruas. Toda a gente tem de ter acesso aos recursos digitais da organização, e isso torna muito difícil impor uma política de acessos muito restritiva. Toda a gente tem o direito de ter acesso aos recursos digitais da empresa, das suas propriedades. Dito isto, não é fácil para nós ter uma política forte e forçada de acessos. O que temos é que todos têm acesso ao conteúdo digital”

Pedro Ponte, Head of IT, Alves Ribeiro: “Estou praticamente a reconstruir toda a infraestrutura de IT, desde o Data Center até ao utilizador final. Para muitos dentro da empresa, a segurança é algo que querem ter, mas não compreendem realmente o que significa cibersegurança. Implementámos uma



PEDRO GALVEIAS, HEAD OF CYBERSECURITY OPERATIONS, TAP



TIAGO TORMENTA, TERRITORY ACCOUNT MANAGER EM PORTUGAL, SOPHOS



RUI SOUSA GIL, HEAD OF INFORMATION TECHNOLOGY, JOSÉ DE MELLO

solução para reforçar a segurança do e-mail e das ferramentas de colaboração. A reação inicial foi de frustração, com pessoas a perguntarem porque estavam agora a receber alertas sobre a segurança das mensagens. A resposta é simples: isso é cibersegurança. Significa que também os utilizadores têm de avaliar os e-mails que recebem”

Pedro Galveias, Head of Cybersecurity Operations, TAP: “A taxa de execução orçamental pode dizer mais sobre uma equipa do que qualquer dotação financeira. Durante anos focámo-nos em assegurar um orçamento aprovado e reforçado, mas o desafio era executá-lo na totalidade. Talento escasso, agenda sobrelotada e prioridades a competir. Numa área onde reter especialistas é um desafio real, o músculo de execução cresce mais devagar do

que o próprio orçamento. O resultado é uma alocação financeira que existe no papel mas não chega ao terreno. Para o board, este número é um espelho: mostra onde está o verdadeiro constrangimento. E raramente é o dinheiro.”

Tiago Tormenta, Territory Account Manager em Portugal, Sophos: “Temos um conjunto muito grande de iniciativas e projetos planeados para este ano, todos eles com prioridade e impacto direto no risco da organização. Quando surge uma nova solução ou serviço, mesmo sendo muito interessante, muitas vezes não temos capacidade para o avaliar ou implementar de imediato. Esse é o principal risco: se não conseguirmos concluir esses projetos dentro do prazo, acabamos por acumular atrasos que passam para o ano seguinte. A limitação não está apenas na

vontade de inovar ou adotar novas tecnologias, mas sobretudo na disponibilidade de pessoas e recursos para acompanhar tudo”

Rui Sousa Gil, Head of Information Technology, José de Mello: “Optámos por externalizar o serviço de MDR. Contamos com serviços externos que asseguram a segunda linha de defesa após a deteção e resposta inicial a incidentes. Internamente, a nossa equipa concentra-se sobretudo na componente de rede, na contenção e correção dos incidentes identificados. Muitas organizações não têm dimensão suficiente para garantir internamente todas as capacidades necessárias para monitorizar comportamentos, analisar informação e responder aos incidentes com a rapidez e eficácia exigidas. A implementação de MDR permitiu-nos colmatar essa lacuna” ◀

“UM BOM ZERO TRUST SIGNIFICA QUE NÃO SE DEVE PREOCUPAR QUANDO CARREGAM NUMA LIGAÇÃO DE PHISHING”

O CISO DA SOPHOS, ROSS MCKERCHAR, ABORDOU, EM ENTREVISTA, OS TEMAS QUE HABITUALMENTE NÃO SÃO TÃO TIDOS EM CONTA QUANDO SE FALA DA DEFESA DAS ORGANIZAÇÕES E, PRINCIPALMENTE, DA IMPORTÂNCIA DAS SOLUÇÕES DE CIBERSEGURANÇA.

Ross McKerchar, CISO da Sophos, abordou em entrevista aqueles que, na sua visão, são os temas que estão a receber menos atenção do que deveriam na cibersegurança.

Um dos pontos abordados foram as vulnerabilidades que os produtos dos fabricantes de cibersegurança – que estão no negócio de proteger os seus clientes – têm.

McKerchar refere que “os piores fornecedores são muitas vezes aqueles que não têm CVE, mas têm

muitos incidentes. Identificar e publicar vulnerabilidades exige um nível de maturidade específico. Na Sophos, tenho orgulho em dizer que temos CVE; significa que temos os processos para os encontrar e publicar”.

A estratégia de segurança de produto da Sophos assenta no que McKerchar chama de “espremer o risco em cada etapa”, seja da escrita de código à produção. Isso inclui a utilização de Inteligência Artificial (IA) no processo de desenvolvimento para proteger



o código quando é escrito e um programa de *bug bounty* que o CISO descreve como o mais generoso entre fornecedores de segurança. “Nunca se deve assumir que um passo é suficiente. É sempre defesa em profundidade”, acrescenta.

A CERTEZA QUE DESAPARECEU

Os LLM representam, na visão de Ross McKerchar, uma rutura conceptual com décadas de boas práticas. “Há um conjunto de controlos desenvolvidos ao longo de muitos anos em torno de como desenvolvemos aplicações: todos focados em manter o *input* separado das instruções. Os LLM destroem isso. E não existe base teórica para obter o nível de *assurance* que temos em sistemas determinísticos”, diz.

No entanto, o CISO da Sophos recusa um pessimismo que paralise a inovação e explica que, como CISO, “estamos habituados a olhar não só par ao micro, mas para o macro; uma organização inteira, com todas as suas vulnerabilidades. Quando olhas assim, os LLM não são assim tão diferentes. São mais uma componente difusa e difícil de gerir, tal como os humanos. Temos de pensar nos LLM com essa mesma lente”.

A EXPLOÇÃO DE IDENTIDADES

Com os agentes de IA a se multiplicarem nas organizações, uma empresa com, por exemplo, quinze colaboradores pode, num curto espaço de tempo, ter duzentas ou mais identidades a gerir. McKerchar aponta o caminho nos princípios já conhecidos: “uma boa arquitetura zero trust significa que não se deve

preocupar com os utilizadores quando carregam numa ligação de phishing porque se tem os controlos técnicos para evitar que isso se torne num risco sério. Temos de pegar nesses conceitos e adaptá-los aos agentes”.

O objetivo é colocar fronteiras determinísticas em torno de cada agente. McKerchar introduz o conceito de ‘tríade letal’, ou seja, os agentes que acumulam acesso crítico, dados sensíveis e capacidade de ação autónoma. “Se tenho mil agentes a correr numa organização e apenas meia dúzia está no centro dessa tríade, pelo menos sabes onde concentrar os esforços de proteção e monitorização”, explica.

AS ORGANIZAÇÕES SEM CISO

Na realidade portuguesa, onde a maioria das empresas são de pequena dimensão e não tem um responsável de cibersegurança, McKerchar explica que não é assim tão diferente no resto do mundo. “A nossa investigação mostra que aproximadamente 0,009% das organizações a nível global tem um CISO. Se não tens um equivalente, não tens estratégia. E se não tens estratégias, como é que estás a governar as tuas decisões de compra?”

Para este segmento, a Sophos adquiriu recentemente a Arco Cyber e está a lançar o produto CISO Advantage, uma abordagem que combina tecnologia, IA e parceiros para escalar competências de CISO a organizações que, historicamente, não têm acesso a esse perfil.

Para orientação imediata, McKerchar é pragmático na sua abordagem: monitorização contínua em primeiro lugar. “O nosso último Active Adversary Report



mostra o acesso inicial a domain admin em menos de três horas. Se não estás a monitorizar, não chegas a tempo. Os ataques correlacionam fortemente com fins de semana e noite e é uma tática deliberada. Se não se consegue fazer isso internamente, é preciso um serviço externo”, explica.

A segunda prioridade é a identidade, até porque estas “já não existem atrás da firewall; estão na Internet. Tolerância zero para erros de configuração. Qualquer identidade mal configurada resulta em comprometimento”.

O ÂNGULO CEGO

Questionado sobre qual o ponto que a maioria dos CISO não está a olhar, McKerchar partilha a cadeia de valor. “Sou muito cético quanto à eficácia dos programas *standard* de gestão de risco de terceiros. Geram uma quantidade enorme de papelada. As organizações tornam-se muito boas a colocar as respostas certas nos questionários. E simplificam problemas complexos em respostas binárias de ‘sim’ ou ‘não’”.

A solução é uma melhor estratificação de risco, não mais processo. “Não é 80/20. É mais como 2% a 5% dos teus fornecedores onde deves exigir responsabilidade extrema. Para os restantes, assume que vão ser comprometidos e garante que estão ligados aos teus sistemas de forma que não seja crítica para o negócio”, defendeu.

O alvo mais preocupante são, no entanto, os próprios fornecedores de segurança. Ross McKerchar explica que, “como indústria, temos um problema de confiança. Focamo-nos demasiado em funcionalidades de segurança em vez de produtos seguros. Se os clientes pedem funcionalidades, as organizações focam-se em funcionalidades. Se pedem produtos seguros, as organizações focam-se em produtos seguros”. ◀



IT SECURITY CONFERENCE

LISBOA

2026
OCT 08

conf.itsecurity.pt

#A VOZ DOS CISO

08 OUT 2026 | LISBOA

A VOZ DOS CISO

A quarta edição da IT Security Conference 2026 já tem data marcada para **08 de outubro, em Lisboa**, onde os temas mais relevantes sobre o ecossistema da cibersegurança voltam a estar em debate e análise pelos mais proeminentes especialistas da área.

A IT Security Conference 2026 será uma oportunidade para explorar as tecnologias mais inovadoras que impactam um grande número de indústrias, para além da partilha de conhecimentos entre CISO, CSO, diretores de segurança e diretores de IT com responsabilidade de cibersegurança, originando um ecossistema único de networking.

**MARQUE A DATA NA SUA AGENDA.
JÁ PODE FAZER A SUA PRÉ-INSCRIÇÃO.**

REGISTE-SE AQUI!

RESPONSABILIDADE PESSOAL, RISCO EMPRESARIAL: O NOVO PARADIGMA DA NIS2

NIS2 E A RESPOSTA OPERACIONAL: O PAPEL DA PROLOGIN E DO SOPHOS MDR NA CONFORMIDADE.

A Diretiva NIS2 marca uma mudança profunda na forma como a cibersegurança é encarada pelas organizações europeias. Deixa de ser um tema exclusivamente técnico para se tornar uma responsabilidade direta da gestão de topo, com impactos claros ao nível da governação, do risco e da continuidade do negócio. A conformidade deixou de ser opcional e passou a exigir capacidade operacional real.

Um dos aspetos mais relevantes da NIS2 é a responsabilização direta dos órgãos de gestão. Administradores e diretores executivos passam a ter o dever de aprovar, supervisionar e garantir a implementação de medidas adequadas de gestão de riscos de cibersegurança, podendo ser responsabilizados pessoalmente em caso de falha. Este novo enquadramento elimina a tradicional delegação total da segurança às equipas técnicas e obriga a uma abordagem estruturada, contínua e demonstrável.

Paralelamente, a diretiva introduz requisitos rigorosos ao nível do reporte de incidentes. A obrigação de notificar incidentes significativos em 24 horas, atua-



VICTOR ANDRADE, CEO, PROLOGIN

UM DOS ASPETOS MAIS RELEVANTES DA NIS2 É A RESPONSABILIZAÇÃO DIRETA DOS ÓRGÃOS DE GESTÃO. ADMINISTRADORES E DIRETORES EXECUTIVOS PASSAM A TER O DEVER DE APROVAR, SUPERVISIONAR E GARANTIR A IMPLEMENTAÇÃO DE MEDIDAS ADEQUADAS DE GESTÃO DE RISCOS DE CIBERSEGURANÇA, PODENDO SER RESPONSABILIZADOS PESSOALMENTE EM CASO DE FALHA

lizar a informação em 72 horas e apresentar um relatório final detalhado num prazo máximo de um mês impõe um desafio operacional significativo. Cumprir estes prazos exige visibilidade permanente, deteção avançada de ameaças e capacidade de resposta imediata — requisitos que a maioria das organizações não consegue assegurar apenas com recursos internos.

É neste contexto que a **PROLogin** se afirma como um parceiro estratégico para a conformidade com a NIS2, apoiando as empresas através das soluções da Sophos, com destaque para o **Sophos Managed Detection and Response (MDR)**. Este serviço disponibiliza monitorização contínua 24/7, investigação ativa de ameaças e resposta em tempo real, assegurada por equipas especializadas. Mais do que detetar ataques, o **Sophos MDR** permite conter incidentes de forma rápida e estruturada, reduzindo o impacto operacional e o risco regulatório.

Um dos fatores críticos para o cumprimento da NIS2 é a capacidade de produzir informação fiável e atempada para efeitos de reporte. O **Sophos MDR** fornece dados forenses detalhados e uma linha temporal clara dos eventos, facilitando a comunicação com as autoridades competentes e permitindo que a gestão demonstre diligência e controlo sobre a postura de segurança da organização.

A **PROLogin** complementa esta capacidade tecnológica com uma abordagem alinhada com a realidade operacional de cada cliente. Ao integrar o **Sophos MDR** nos processos de negócio existentes, garante que a resposta a incidentes é eficaz sem comprometer a continuidade da operação. Esta combinação de tecnologia, experiência e proximidade permite transformar a conformidade com a NIS2 num processo sustentável e operacionalmente sólido.

Num cenário marcado pela fragmentação tecnológica, o **Sophos MDR** destaca-se ainda pela sua abordagem aberta e interoperável, integrando telemetria de múltiplas soluções de segurança, incluindo firewalls, sistemas de identidade, segurança de e-mail e ambientes cloud. Esta visão unificada reduz pontos cegos, acelera a deteção de ameaças e melhora significativamente os tempos de resposta.

A NIS2 não deve ser vista apenas como uma obrigação legal, mas como uma oportunidade para elevar o nível de maturidade em cibersegurança. Através do **Sophos MDR**, implementado e operado pela **PROLogin**, as organizações conseguem alinhar governação, operação e tecnologia, reforçando a sua resiliência digital e a confiança do mercado. ◀

CONSOLIDAR PARA NÃO FRAGMENTAR



► POR MARTA QUARESMA FERREIRA

ACRESCENTAR MAIS TECNOLOGIA FOI, EM TEMPOS, A RESPOSTA ÀS AMEAÇAS. HOJE, ESTE MODELO REVELA-SE LIMITADO. A ESCOLHA ENTRE CONSOLIDAÇÃO DE PLATAFORMAS OU BEST-OF-BREED TORNOU-SE UMA DECISÃO ESTRATÉGICA QUE REFLETE AS PRIORIDADES DO NEGÓCIO, COM BASE NO RISCO E NA CAPACIDADE OPERACIONAL DE CADA CONTEXTO ORGANIZACIONAL.

A fragmentação do ecossistema de cibersegurança tem-se revelado um desafio. O debate centrado na consolidação de plataforma vs. best-of-breed coloca, frente a frente, a consolidação como resposta à necessidade de simplificação, visibilidade e eficiência operacional e uma abordagem mais especializada em determinados contextos onde a adaptação a requisitos específicos é crítica.

UMA VISÃO PREDOMINANTEMENTE CONSOLIDADA

Ricardo Evangelista, Information Security Manager da Ageas Portugal, começa por partilhar o exemplo da organização, que optou por um “modelo híbrido”, orientado, no entanto, para a consolidação de plataformas. “Esta orientação resulta de vários fatores: **a necessidade de controlar custos de forma sustentável, reduzir o esforço operacional das equipas e acelerar a capacidade de resposta perante ameaças cada vez mais sofisticadas**”.

A decisão sobre a escolha da arquitetura foi “predominantemente técnica”, ainda que “integrada num contexto natural de racionalização de custos”. Em “domínios muito específicos”, o especialista de cibersegurança afirma que a empresa recorre a soluções best-of-breed sobretudo devido à especialização de determinados fornecedores que continuam a “acrescentar valor que as plataformas consolidadas ainda não abrangem”.

A complexidade do atual panorama tecnológico, aliada à necessidade de dar resposta às ameaças emergentes, tem contribuído, no entanto, para intensificar a discussão sobre qual o melhor rumo a seguir.

No espectro oposto, e com base na sua experiência e opinião pessoal, Miguel Gonçalves, CISO da CUF, acredita que a decisão se coloca sobretudo ao nível “operacional e estratégico”. “A escassez de recursos humanos especializados, a necessidade de redução da complexidade operacional e a pressão sobre tempos de resposta”, defende, “tornam a consolidação uma escolha natural”; já o

modelo best-of-breed apresenta mérito para “casos específicos”. No fim, “a simplificação operacional” é, para o especialista, o “fator mais relevante”.

NÃO HÁ ABORDAGENS PERFEITAS

Na visão dos fabricantes, o debate entre consolidação e best-of-breed tornou-se “particularmente relevante” num contexto em que as superfícies de ataque são também elas cada vez mais distribuídas.

Para Manu Santamaría Delgado, Director of Product Management da WatchGuard Iberia, não existem soluções perfeitas, uma vez que as duas abordagens apresentam falhas: no caso do best-of-breed, as soluções podem falhar quando a organização “não tem capacidade operacional para integrar e gerir múltiplas ferramentas especializadas”, o que leva à criação de silos e, consequentemente, aumenta a “dificuldade em correlacionar dados”, o que, por si só, representa um risco. Por outro lado, no caso da consolidação de segurança em plataformas, **as falhas também podem ocorrer quando a abordagem “é entendida apenas como simplificação**



tecnológica e não como uma arquitetura integrada”. Manu Santamaría Delgado considera que, neste contexto, existe o “risco de substituir a fragmentação por dependência excessiva de um único fornecedor”. Ainda assim, e com base na experiência da WatchGuard, esta é a abordagem com maior tração ao permitir “reduzir a complexidade operacional sem limitar a capacidade de evolução tecnológica”.

No entanto, há outros fatores a ter em conta nos dois cenários. Na opinião de Thom Langford, CTO da EMEA da Rapid7, “se as pessoas e processos não



▼
"A CONSOLIDAÇÃO REDUZ RISCO, MAS TAMBÉM O TRANSFORMA". A CONCENTRAÇÃO É, ENTRETANTO, COMPENSADA "POR MAIOR COERÊNCIA, MELHOR CAPACIDADE DE MONITORIZAÇÃO E PROCESSOS MAIS ESTRUTURADOS DE DETEÇÃO E RESPOSTA"

RICARDO EVANGELISTA, INFORMATION SECURITY MANAGER DA AGEAS PORTUGAL



MIGUEL GONÇALVES, CUF

estiverem apreendidos, estabelecidos e compreendidos, a tecnologia irá apenas amplificar ainda mais as lacunas”.

Os líderes de cibersegurança necessitam de explicar as vantagens de determinada abordagem, em detrimento da outra, a fim de capacitarem as equipas com melhores ferramentas e uma visão mais clara sobre a escolha certa para a sua realidade operacional. “A compreensão da política organizacional e dos processos de aquisição”, explica, contribui

para “manter o envolvimento e a resolver obstáculos antes que impeçam o progresso”. É este alinhamento entre liderança, operação e tecnologia que irá determinar, segundo Thom Langford, “se as iniciativas têm sucesso ou falham”.

Qualquer que seja a escolha, o especialista da Rapid7 acredita que a integração de ferramentas, processos e pessoas é tão importante quanto a consolidação, cabendo aos CISO a avaliação sobre a abordagem a adotar consoante os resultados pretendidos e a flexibilidade de adaptação a necessidades futuras.

QUEM PROCURA O QUÊ?

Em qualquer uma das arquiteturas, há tempo e recursos dedicados para garantir que cada uma funciona no ambiente devido. Do lado de uma integração best-of-breed, explica Ricardo Silva, Security Solutions Senior Consultant da Claranet Portugal, **é necessário um "investimento contínuo e elevado em recursos humanos com competências heterogêneas"**; por sua vez, a consolidação de plataformas requer um *time-to-value* mais curto, com recursos canalizados para otimizar "políticas de segurança,

"A ESCASSEZ DE RECURSOS HUMANOS ESPECIALIZADOS, A NECESSIDADE DE REDUÇÃO DA COMPLEXIDADE OPERACIONAL E A PRESSÃO SOBRE TEMPOS DE RESPOSTA TORNAM A CONSOLIDAÇÃO UMA ESCOLHA NATURAL"

MIGUEL GONÇALVES, CISO DA CUF



"QUALQUER
 DEPENDÊNCIA
 EXCESSIVA DE UM
 ÚNICO FORNECEDOR"
 REPRESENTA "UM
 RISCO ESTRATÉGICO SE
 LIMITAR A CAPACIDADE
 DE ADAPTAÇÃO
 DA ORGANIZAÇÃO
 ÀS MUDANÇAS
 TECNOLÓGICAS OU ÀS
 NOVAS AMEAÇAS"

MANU SANTAMARÍA DELGADO,
 DIRECTOR OF PRODUCT
 MANAGEMENT DA WATCHGUARD
 IBERIA



realizar *benchmarks* de boas práticas e fortalecer a postura de compliance da organização".

A abordagem de cada arquitetura varia também consoante os objetivos de cada organização. Ainda assim, **a dimensão da empresa não é necessariamente o fator mais determinante: "o verdadeiro *driver* é a complexidade dos próprios processos de negócio"**, admite Jorge Miranda, Executive Manager da CSO.

Se, por um lado, a consolidação está mais presente em empresas que "procuram eficiência operacio-

nal, visibilidade centralizada e uma resposta a incidentes mais ágil", refere Ricardo Silva, por outro, o best-of-breed tem tendência para funcionar melhor "em organizações com equipas de cibersegurança altamente especializadas e com maturidade técnica elevada, que operam em setores com requisitos de nicho, onde a funcionalidade máxima de um componente específico é crítica para o negócio".

Neste último caso, Jorge Miranda explica que **esta tipologia de arquiteturas tende a surgir em grandes organizações de setores como telecomunicações, energia, infraestruturas críticas, que operam em "ambientes tecnológicos complexos e altamente regulados"**, com equipas especializadas e recursos canalizados à integração. Aqui, "a prioridade não é simplificar o ecossistema tecnológico, mas garantir o máximo nível de proteção possível em cada camada".

No caso das médias empresas, onde existe maior preocupação em equilibrar investimento, eficiência e desempenho tecnológico, a consolidação de plataformas pode revelar-se vantajosa.



FALTA DE PROFUNDIDADE VS DEPENDÊNCIA COMO UM RISCO

A consolidação de plataformas estabelece-se como uma escolha comum e consensual entre os especialistas e diretores de cibersegurança. Ainda assim, Jorge Miranda lembra que em contextos de infraestruturas heterogêneas, ambientes híbridos complexos, casos de requisitos regulatórios exigentes e integração com sistemas industriais ou *legacy* podem estar em causa limitações, uma vez que **as plataformas consolidadas nem sempre são capazes de oferecer “a mesma profundidade funcional” que as soluções mais especializadas oferecem nestes cenários.**

Em linha com esta ideia, Ricardo Silva, da Claranet Portugal, reitera que uma plataforma consolidada pode até garantir uma cobertura abrangente; porém “pode não atingir o nível de detalhe de uma ferramenta dedicada em cenários muito específicos, como em atividades de segurança ofensiva profunda, análises forenses complexas ou auditorias de conformidade com normativos muito granula-



THOM LANGFORD, RAPID7



res”. Em determinados contextos, alguns vetores de ataque mais particulares podem ser inclusivamente ignorados caso a plataforma se revele “demasiado generalista”.

No lado do best-of-breed, Manu Santamaría Delgado admite que “qualquer dependência excessiva de um único fornecedor” representa “um risco estratégico se limitar a capacidade de adaptação da organização às mudanças tecnológicas ou às novas ameaças”. A consolidação revela-se, assim, como um facilitador de eficiência operacional quando a plata-

"SE AS PESSOAS
E PROCESSOS
NÃO ESTIVEREM
APREENDIDOS,
ESTABELECIDOS E
COMPREENDIDOS,
A TECNOLOGIA IRÁ
APENAS AMPLIFICAR
AINDA MAIS AS
LACUNAS"

THOM LANGFORD, CTO DA EMEA DA
RAPID7



forma de segurança é concebida como um ecossistema, com correlação de dados e sinais de segurança entre diferentes domínios, que permite às organizações “evoluir gradualmente e integrar novas capacidades sempre que necessário”.

“A consolidação reduz risco, mas também o transforma”, defende Ricardo Evangelista. Apesar da maior concentração numa única arquitetura, o Information Security Manager não tem dúvidas de que o risco operacional diminui e a concentração é, entretanto, compensada “por maior coerência, melhor capacidade de monitorização e processos mais estruturados de deteção e resposta”.

FRUSTRAÇÃO OPERACIONAL E FALHAS NAS IMPLEMENTAÇÕES

Na escolha de abordagens, um dos problemas elencados pelos especialistas prende-se com o excesso de ferramentas. Ricardo Silva lembra que “a fragmentação obriga equipas a gerir múltiplas consolas” e a conectarem pontos entre “ferramentas

dispersas”, o que resulta no comprometimento do tempo de resposta e no aumento da frustração.

Por outro lado, as plataformas demasiado fechadas também podem revelar-se um problema: “quando uma solução limita a integração com outras ferramentas ou cria dependência excessiva de um único fornecedor, a organização perde flexibilidade e capacidade de adaptação”, constata Jorge Miranda, da CSO. No seu ponto de vista, o problema está quando “a arquitetura de segurança deixa de refletir a realidade operacional da organização”. “Quando um projeto de segurança corre mal, a causa raramente é tecnológica. Na maioria das situações, os problemas surgem porque a implementação não teve em conta fatores fundamentais como processos, operação e alinhamento com o negócio”, justifica.

CONSOLIDAÇÃO: EVOLUÇÃO NATURAL OU UMA RESPOSTA DOS TEMPOS?

Existe hoje um paradoxo: as ferramentas concebidas para proteger as organizações são as mes-

mas que adicionam uma camada de complexidade. “Durante anos, a resposta instintiva às novas ameaças tem sido comprar mais um produto, seja outra *dashboard*, outro *feed* ou, agora, outro agente de IA. O resultado tornou-se um mosaico desarticulado de sistemas sobrepostos que prometem visibilidade, mas frequentemente causam fadiga”, analisa Thom Langford, da Rapid7. A multiplicidade de fornecedores de segurança traduz-se, por isso, em “múltiplos fluxos de trabalho, contratos e definições de risco”, um terreno fértil para o aumento das ameaças.

Neste ponto, o CTO garante que as organizações encaram atualmente a consolidação como “uma potencial forma de melhorar a visibilidade, reduzir o atrito operacional e criar uma base para um segurança escalável”.

Manu Santamaría Delgado, da WatchGuard Iberia, reitera a ideia de Thom Langford sobre o panorama de arquiteturas complexas e difíceis de gerir, provocado pelo excesso ferramentas especializadas. Na



sua visão, “a consolidação é, simultaneamente, uma consequência da maturidade crescente das estratégias de segurança e uma resposta à fragmentação tecnológica acumulada ao longo da última década”.

O Diretor acredita que **existe uma “consciência crescente de que a eficácia da segurança não depende apenas da quantidade de ferramentas disponíveis, mas da capacidade de essas ferramentas trabalharem em conjunto”**.

E é aqui que entra a consolidação de plataformas. “Não deve ser vista apenas como uma estratégia de racionalização tecnológica porque representa sobretudo uma evolução na forma como as organizações encaram a segurança, menos centrada em ferramentas isoladas e mais orientada para uma plataforma integrada que permita proteger ambientes cada vez mais distribuídos com maior eficiência e simplicidade operacional”, afirma Manu Santamaría Delgado.

O ANTES E DEPOIS DA ESCOLHA DE CADA REALIDADE

No contexto da Ageas Portugal, a escolha da arquitetura privilegiou métricas que refletissem parâmetros como eficiência operacional e redução de risco de segurança. Do ponto de vista operacional, Ricardo Evangelista revela que na decisão sobre a melhor abordagem pesou também – para além dos fatores inicialmente elencados – a avaliação da melhoria do tempo de resposta e as métricas financeiras que sus-

UMA PLATAFORMA CONSOLIDADA PODE ATÉ GARANTIR UMA COBERTURA ABRANGENTE; PORÉM "PODE NÃO ATINGIR O NÍVEL DE DETALHE DE UMA FERRAMENTA DEDICADA EM CENÁRIOS MUITO ESPECÍFICOS, COMO EM ATIVIDADES DE SEGURANÇA OFENSIVA PROFUNDA, ANÁLISES FORENSES COMPLEXAS OU AUDITORIAS DE CONFORMIDADE COM NORMATIVOS MUITO GRANULARES"

RICARDO SILVA, SECURITY SOLUTIONS SENIOR CONSULTANT DA CLARANET PORTUGAL



tentam e justificam o *business case*. “No conjunto, estas métricas demonstraram que a consolidação aumenta eficiência, reduz risco e melhora a previsibilidade a médio prazo”, com ganhos ao nível da coerência, controlo e simplicidade operacional e eficiência de equipas.

As vantagens são notórias: “Ao substituir várias plataformas por uma abordagem mais integrada, beneficiámos de controlos mais modernos e sofisticados, superando algumas limitações de soluções mais antigas que existiam com propósitos muito específicos. Isso permitiu não só consolidar, mas também elevar a maturidade tecnológica em áreas que antes estavam limitadas por soluções mais antigas”, partilha o especialista de segurança.

Na opinião de Miguel Gonçalves, a consolidação traz “ganhos claros ao nível da eficiência operacional, visibilidade e foco das equipas”, ainda que implique “algumas perdas” como a “ausência de funcionalidades muito específicas”. Entre as lições aprendidas neste processo, o especialista de cibersegurança não



JORGE MIRANDA, CSO

tem dúvidas de que, no decorrer do processo de consolidação, “não se seleciona apenas uma tecnologia”; o peso da decisão é co-partilhado com a escolha de “um parceiro estratégico”.

Mais do que contar com a melhor tecnologia em cada domínio, Miguel Gonçalves sublinha que o verdadeiro desafio passa por “conseguir operá-la de forma eficaz”, num momento em que “a consolidação deixou de ser apenas uma opção para se tornar uma necessidade”. ◀

"QUANDO UM PROJETO DE SEGURANÇA CORRE MAL, A CAUSA RARAMENTE É TECNOLÓGICA. NA MAIORIA DAS SITUAÇÕES, OS PROBLEMAS SURGEM PORQUE A IMPLEMENTAÇÃO NÃO TEVE EM CONTA FATORES FUNDAMENTAIS COMO PROCESSOS, OPERAÇÃO E ALINHAMENTO COM O NEGÓCIO"

JORGE MIRANDA, EXECUTIVE MANAGER DA CSO

FERRAMENTAS DE CIBERSEGURANÇA: A TECNOLOGIA POR SI SÓ NÃO GARANTE A PROTEÇÃO DOS ATIVOS DIGITAIS

AS EMPRESAS ESTÃO A INVESTIR CADA VEZ MAIS EM **FERRAMENTAS DE CIBERSEGURANÇA**.
FIREWALL, ANTIVÍRUS, EDR, SIEM, PLATAFORMAS DE MONITORIZAÇÃO, ENTRE OUTRAS SOLUÇÕES.

Todas elas são peças essenciais para qualquer ecossistema de segurança digital, mas é importante mantermos sempre presente que **a tecnologia, por si só, não garante segurança**.

As ferramentas são absolutamente fundamentais, desde que totalmente ajustadas à realidade e necessidades de cada organização, mas o fator diferenciador está na forma **como são configuradas, e integradas nas operações diárias**.

Sem pessoas competentes, processos bem definidos e validação contínua, até as soluções mais avançadas acabam por falhar.

A ILUSÃO DA PROTEÇÃO AUTOMÁTICA

São muitas as empresas que continuam a adequir tecnologia e que acreditam que estão seguras apenas porque têm ferramentas implementadas. Mas segurança não é um produto, é um processo.



RICARDO RODRIGUES, CEO BALWURK

Um sistema pode ser monitorizado 24/7 e, ainda assim, permitir uma intrusão se não houver análise contextual ou correção rápida de vulnerabilidades.

Um SIEM que não é revisto regularmente gera alertas que ninguém lê, um EDR que não é ajustado à realidade da empresa pode deixar portas abertas, e uma política de **backup** sem testes de recuperação pode falhar exatamente quando mais for necessária.

E neste caso o erro não está na tecnologia, mas sim na forma como está a ser usada e gerida.

EQUIPAS E PROCESSOS: O NÚCLEO DA SEGURANÇA

A cibersegurança eficaz resulta da união entre **tecnologia, metodologia/processos e pessoas**. Ferramentas sem equipas são como alarmes sem vigilantes, elas sinalizam os problemas, mas não os resolvem necessariamente.

Uma estratégia sólida exige:

- **Monitorização ativa e contextualizada**, para distinguir o ruído das ameaças reais.
- **Validação regular de controlos de segurança**, através de *Pentesting e Red Teaming*.
- **Gestão de vulnerabilidades contínua**, para garantir que as falhas são mitigadas antes de poderem ser exploradas.
- **Formação das equipas**, criando uma verdadeira cultura de segurança.

A **ENISA** reforça esta visão: “A segurança deve ser abordada como um ciclo contínuo de melhoria, e não como um evento pontual.”

A IMPORTÂNCIA DA VALIDAÇÃO INDEPENDENTE

Ter as ferramentas certas é crucial, mas saber se elas estão realmente a cumprir o seu papel é ainda mais importante. É aqui que entram os **Testes de Intrusão recorrentes** e as Auditorias de Segurança.

Esses exercícios permitem avaliar, se as soluções implementadas estão a detetar, bloquear e reagir de acordo com as expectativas.

E, acima de tudo, se as equipas sabem **responder rapidamente** quando algo corre mal.

Para compreender como esta abordagem se traduz em retorno de investimento, consulte também o artigo *Pentesting: como calcular o ROI da cibersegurança*.

As empresas que mais evoluem em cibersegurança são as que **tratam a segurança como parte da cultura organizacional**, não como um projeto de IT.

A **Comissão Europeia** tem vindo a reforçar esta ideia: segurança digital constrói-se com **formação, planeamento e responsabilidade partilhada**. Prova disto é a existência do *Cyber Resilience Act (CRA)* que se encontra em vigor desde dezembro de 2024 e cuja sua aplicabilidade será exigida integralmente a partir de dezembro de 2027. O seu principal objetivo é a garantir que todos os produtos comercializados na EU que contenham elementos digitais (Hardware e/ou Software), respeitem o conjunto de requisitos de segurança, tais como avaliação contínua de vulnerabilidade, Gestão de Vulnerabilidades e Gestão do Risco. Podem, também, consultar o nosso artigo: <https://balwurk.com/the-impact-of-the-new-cyber-resilience-act-proposal/> ◀

PLATAFORMIZAÇÃO VS. BEST-OF-BREED: O FALSO DILEMA DA CIBERSEGURANÇA

HÁ DEBATES NA CIBERSEGURANÇA QUE REGRESSAM CICLICAMENTE. UM DOS MAIS PERSISTENTES OPÕE PLATAFORMIZAÇÃO A SOLUÇÕES BEST-OF-BREED.

A primeira vista, parece uma questão estratégica e relevante, mas na realidade, não é mais do que um falso dilema. O problema não está na escolha entre modelos, está na ideia de que esta escolha binária, por si só, resolve o desafio da *segurança*. A opção entre consolidação e especialização é, na verdade, a pergunta errada.

PLATAFORMIZAÇÃO: A PROMESSA DO “TUDO-EM-UM”

A narrativa é sedutora: consolidar o stack de *segurança* numa única plataforma significa menos complexidade, menos integrações frágeis, menos

fadiga de alertas e, claro, um único contrato para gerir. Teoricamente, traduz-se em eficiência operacional e visibilidade centralizada. Na prática, não é tão simples.

A plataforma promete uma ação mais eficaz com menos ferramentas, menos integrações e mais controlo. No entanto, esta simplificação tem sempre um custo: ao consolidar, aceitamos implicitamente soluções que consideramos “suficientemente boas” – mas que, muitas vezes, não são as mais adequadas.

Quando uma organização concentra grande parte dos seus serviços num único fornecedor, a capacidade de negociação diminui. Além disso, fica mais



DAVID GRAVE, CLARANET PORTUGAL

QUANDO ADAPTAMOS PROCESSOS À TECNOLOGIA E CRIAMOS DEPENDÊNCIAS NÃO APENAS COMERCIAIS, MAS TAMBÉM DE COMPETÊNCIAS, UMA LIMITAÇÃO DEIXA DE SER PONTUAL E PASSA A SER SISTÊMICA.

exposta a riscos, dado que uma plataforma única é também uma superfície de falha única. Se a *threat intelligence* do fornecedor for limitada, o impacto torna-se transversal.

Mas o lock-in mais perigoso é o das competências. As equipas tornam-se especialistas numa plataforma específica, e não em princípios de *segurança*. E quando a tecnologia muda (como sabemos que muda sempre) as equipas ficam inevitavelmente condicionadas.

Quando adaptamos processos à tecnologia e criamos dependências não apenas comerciais, mas também de competências, uma limitação deixa de ser pontual e passa a ser sistémica.

BEST-OF-BREED: A FALÁCIA DA “MELHOR FERRAMENTA PARA CADA FUNÇÃO”

Do outro lado do espectro, temos os defensores do best-of-breed: escolher a melhor solução para cada necessidade específica. Optam pelo EDR da empresa A, pelo SIEM da empresa B, pela firewall da empresa C e pelo CASB da empresa D. Uma abordagem que, à primeira vista, parece infalível por permitir escolher o que há de melhor em cada categoria.

Na realidade, não é isso que se verifica.

A ambição da especialização traz fricção – e custos:

1. Integração: cada ferramenta promete APIs “totalmente compatíveis” e “fácil integração” – até ao dia em que deixa de cumprir esta promessa. Uma atualização inesperada de um dos fornecedores pode quebrar ligações críticas entre sistemas. Esta alteração leva a que as equipas passem mais tempo a manter integrações do que a detetar ameaças. Assim, quando algo falha, surgem lacunas de telemetria críticas e a integração transforma-se num imposto que nunca para de crescer.

2. Fadiga cognitiva e mudança constante de contexto: cada ferramenta tem a sua linguagem, a sua lógica e os seus alertas formatados de maneira diferente. Para um analista de *SOC*, que navega em múltiplas consolas diariamente, mudar constantemente de contexto não é um inconveniente menor: é uma vulnerabilidade operacional. Quando um incidente real acontece, os segundos perdidos a saltar entre sistemas podem fazer a diferença entre a contenção e a catástrofe.

A CIBERSEGURANÇA MODERNA EXIGE ESPECIALIZAÇÃO PROFUNDA, OPERAÇÃO CONTÍNUA E UMA CAPACIDADE DE ORQUESTRAÇÃO QUE POUCAS EQUIPAS CONSEGUEM SUSTENTAR INTERNAMENTE, DE FORMA CONSISTENTE.

3. Exigências de maturidade difíceis de cumprir: orquestrar um modelo best-of-breed exige maturidade técnica, escala e recursos que a maioria das organizações não tem. São necessários arquitetos de *segurança* que entendam profundamente cada tecnologia, engenheiros capazes de construir e manter integrações complexas, e processos rigorosos de governação. Sem isto, a especialização transforma-se rapidamente em caos operacional – e o caos é o melhor aliado dos atacantes.

Perante integrações que falham, ferramentas que não comunicam e equipas sobrecarregadas, a promessa de excelência do best-of-breed transforma-se, frequentemente, em desordem.

A PERGUNTA CERTA

O verdadeiro erro está no enquadramento: assumir que a organização tem de escolher e gerir, sozinha, este nível de complexidade.

Antes de discutir plataformização ou best-of-breed, há uma pergunta que devia vir primeiro: “temos capacidade interna para orquestrar, integrar e operar este nível de complexidade?”. Sem essa capacidade, qualquer escolha – seja qual for o modelo – está condenada a falhar na execução. E é aqui que muitas organizações se enganam. Partem diretamente para a escolha tecno-

lógica, sem validar se têm maturidade, competências e escala para a suportar. O resultado é previsível: soluções subaproveitadas, integrações frágeis e uma falsa sensação de controlo.

A verdade é simples: a maioria das organizações não tem essa capacidade. A *Cibersegurança* moderna exige especialização profunda, operação contínua e uma capacidade de orquestração que poucas equipas conseguem sustentar internamente, de forma consistente.

É precisamente por isso que a resposta, muitas vezes, não está numa escolha entre modelos, mas numa terceira via. Um modelo orquestrado – como um MSSP (Managed Security Service Provider) – permite combinar múltiplas tecnologias sem transferir a complexidade para a organização, adaptando a solução às necessidades reais do negócio.

Não se trata de escolher ferramentas. Trata-se de garantir capacidades: deteção eficaz, resposta rápida e adaptação contínua.

Insistir no debate entre plataformização e best-of-breed é continuar a discutir meios, ignorando o essencial. E o essencial é simples: estar preparado quando o ataque acontecer. O problema é que muitas organizações só percebem o que isso implica quando já é tarde demais – a menos que tomem as decisões certas hoje. ◀



por Paulo Vieira,
Country Manager, Netskope

4 CONSIDERAÇÕES DE SEGURANÇA À MEDIDA QUE A UTILIZAÇÃO DA IA SE EXPANDE PELAS EQUIPAS

O AUMENTO DA ADOÇÃO DA IA ESTÁ A AMPLIAR A SUPERFÍCIE DE ATAQUE PARA OS AGENTES MALICIOSOS.

De acordo com a IDC, os investimentos globais em IA deverão atingir os 750 mil milhões de dólares em 2028, refletindo tanto a rápida adoção desta tecnologia como o aumento dos desafios de segurança de dados. Os especialistas em cibersegurança enfrentam crescentes dificuldades em manter a visibilidade e o controlo sobre os dados empresariais num ambiente cada vez mais dominado pela IA.

Tal como aconteceu com a adoção da cloud, as ameaças relacionadas com a IA não se limitam a um único modelo ou comportamento, tornando o panorama de riscos ainda mais complexo.

A «Shadow IT» representa um risco significativo, visto que muitos colaboradores optam pela conveniência ao invés da conformidade. Segundo o relatório "*Cloud and Threats 2026*" da Netskope, cerca de 47% dos utilizadores de IA generativa recorrem a aplicações pessoais. O que pode resultar na divulgação involuntária de dados sensíveis a aplicações de terceiros, dificultando a supervisão e os controlos de segurança por parte das organizações.

As empresas que desenvolvem modelos privados de IA enfrentam desafios adicionais, nomeadamente no que se refere à proteção dos dados



PAULO VIEIRA, COUNTRY MANAGER, NETSKOPE

de treino e dos resultados gerados, o que aumenta a complexidade da gestão de riscos.

O setor que mais está a crescer é o dos agentes autónomos, capazes de realizar tarefas com pouca intervenção humana. Embora melhorem a produtividade, levantam sérias dúvidas quanto ao acesso e controlo dos dados. A Gartner estima que, até 2028, um quarto das violações de segurança corporativa envolverá o abuso de agentes de IA.

Tendo em conta estas tendências, apresentam-se quatro propostas úteis para que uma organização aborde os riscos sob todos os ângulos.

1) ADOTE UMA ABORDAGEM ZERO TRUST EM TERMOS DE SEGURANÇA DE IA.

A segurança da IA exige novas estratégias, dado que os modelos processam os dados de forma diferente. A aplicação de uma estrutura de zero trust implica verificar cada pedido e monitorizar todos os fluxos de dados, concedendo acesso com base no risco e não através de permissões estáticas. Muitas organizações têm dificuldade em proteger as identidades não humanas (NHIs), cujo crescimento em breve ultrapassará o das identidades humanas. Integre a segurança da IA em estruturas existentes e evite soluções complexas e dispendiosas. - Utilize plataformas unificadas para reduzir a carga administrativa;

2) OBTENHA VISIBILIDADE SOBRE A UTILIZAÇÃO DA IA.

O seu plano de segurança da IA deve abranger mais do que apenas novas aplicações. As ferramentas SaaS adicionam funcionalidades de IA sem supervisão das equipas de segurança. A supervisão manual não é suficiente: utilize uma

gestão de riscos de IA semelhante à da cloud. O Netskope Cloud Confidence Index (CCI) fornece informações em tempo real sobre os riscos de milhares de aplicações na cloud e SaaS.

3) REDUZA A LACUNA DE GOVERNANÇA.

A maioria das organizações tem apenas uma governança de IA reativa ou em desenvolvimento, sendo que muitas desejariam ter começado mais cedo. Antes de expandir a implementação da IA, defina políticas claras para a sua utilização adequada.

4) MELHORE AS COMPETÊNCIAS E AS FERRAMENTAS.

A maioria das pessoas carece de formação em IA e confiar apenas em políticas escritas aumenta o risco de utilização indevida. Embora seja essencial investir em formação e ferramentas, a formação por si só não basta: até mesmo os funcionários experientes precisam de apoio. Segundo a Gartner, em 2028, a IA será responsável por 15% das decisões empresariais, pelo que é fundamental combinar a experiência humana com ferramentas de segurança robustas. Proteja os modelos e os dados da sua empresa utilizando soluções como gateways de IA e guardrails, que o ajudarão a tomar decisões seguras.

A Netskope ajuda as empresas a adotarem a IA de forma segura, protegendo utilizadores, agentes, aplicações e dados em todos os ambientes. O **Netskope One AI Security** proporciona proteção unificada, reforça os modelos antes da sua implementação e previne ameaças em tempo real, sem comprometer a velocidade ou a experiência do utilizador. ◀

FAZER MAIS E MELHOR COM MENOS

HÁ DILEMAS QUE VOLTAM CICLICAMENTE AO LONGO DAS NOSSAS VIDAS, AINDA QUE COM DIFERENTES ROUPAGENS. E NAS TECNOLOGIAS DE INFORMAÇÃO NÃO É DIFERENTE. MAINFRAMES VS. SISTEMAS DISTRIBUÍDOS, COMPUTADORES PESSOAIS VS. DESKTOPS VIRTUALIZADOS E, MAIS RECENTEMENTE, TAL COMO HÁ MAIS DE UMA DÉCADA COM OS DIFERENTES NÍVEIS DE FIREWALL, PLATAFORMAS VS. MULTI-TECNOLOGIA *BEST-OF-BREED*.

A cibersegurança tem evoluído a um ritmo alucinante. A crescente sofisticação e expansão da superfície de ataque pressionam as organizações e o negócio de forma inimaginável. Organizações já não dependem exclusivamente de tecnologia, mas de maior eficiência, simplicidade, autoconhecimento e visibilidade.

Durante anos, escolher o melhor que a indústria nos oferecia em função dos domínios de segurança abordados era a fórmula que parecia garantir a melhor proteção. A estratégia permitia beneficiar de tecnologias altamente especializadas e inovadoras, com a melhor solução para cada problema.

Contudo, à medida que aumentava o “arsenal de defesa” era desprezado aquele que se afirmou como o maior dos desafios: a interseção de todas as peças do puzzle, de múltiplas e heterogêneas tecnologias, difíceis de integrar, com custos operacionais elevados e uma visibilidade fragmentada.

Em fevereiro de 2016, a Gartner explicava, num estudo que à data tive a oportunidade de ler, que “*múltiplos fabricantes de firewall aumenta a complexidade, não a segurança*”, alertando para a necessidade de “*normalizar a infraestrutura sob uma única plataforma*” por forma a “*minimizar erros de configuração, otimizar custos e aplicar recursos em outras tecnologias de*



segurança de rede para mitigar os mais recentes ataques”. De entre outros benefícios, o documento evidenciava ainda os potenciais ganhos financeiros com economia de escala ao negociar com um único fabricante.

Uma década depois, o dilema repete-se e as organizações enfrentam a necessidade de **uma decisão que, ao invés de técnica, é estratégica**: apostar na plataforma ou manter uma abordagem *best-of-breed*?

A consolidação não é isenta de riscos. Depender de um só fornecedor pode limitar a flexibilidade e a inovação ou dificultar a adaptação a algumas necessidades específicas. Em alguns casos, as soluções *best-of-breed* continuam a oferecer capacidades importantes em nichos específicos que são isso mesmo.

A resposta não é necessariamente binária, nem a solução passa exclusivamente por uma substituição total de uma abordagem pela outra. Em última análise, a decisão deve ser guiada pelo contexto organizacional: maturidade de segurança, recursos disponíveis e requisitos de negócio, aplicando uma **estratégia híbrida, pragmática e inteligente**, que consolide áreas críticas para ganhar eficiência e visibilidade, através de um ecossistema unificado e modular, de um único fabricante e principalmente gerido com o esforço adequado, mas mantendo soluções especializadas onde acrescentam realmente valor.

No fundo, a questão deixa de ser “qual a melhor abordagem?”, sendo substituída por novas pertinentes interrogações como: “**Quantas ferramentas são realmente necessárias para proteger o negócio com eficácia?**”, “**Temos visibilidade e controlo suficientes para responder às ameaças atuais?**”, “**A nossa**

arquitetura ajuda ou dificulta a capacidade de resposta?” e “**Investimos mais tempo a gerir tecnologia ou a proteger o negócio?**”.

Existe forte probabilidade da solução estar na Fortinet que há muitos anos iniciou o caminho de convergência e até antecipação desta nova realidade, liderando na visão e inovação com o Fortinet Security Fabric que, suportado no FortiOS presente em todos os produtos, integra múltiplas camadas de segurança, correlaciona eventos em tempo real e proporciona eficácia operacional e visibilidade unificada, confluindo numa melhor e mais rápida resposta às ameaças. Integrando diferentes camadas é possível identificar padrões de ataque com maior eficácia relativamente a ambientes fragmentados e, graças à base comum de todos as componentes, potenciar a automação e orquestração com grande eficiência, reduzindo o tempo de resposta.

Declaração de interesses: A SECURNET tem com a Fortinet uma parceria estratégica, sendo um dos mais relevantes e antigos parceiros do fabricante em Portugal, contando com inúmeros projetos de referência nos mais diversos setores.

Se faz sentido simplificar, ganhar visibilidade e aumentar a eficácia da cibersegurança da sua organização, este é o momento certo para reavaliar a sua estratégia! Fale connosco e descubra como uma abordagem equilibrada entre consolidação e especialização pode **reduzir risco, otimizar custos e acelerar a sua capacidade de resposta a ameaças**.

Contate-nos em: info@securnet.pt ou comercial@securnet.pt ◀

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 detecções, 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. ◀

► POR INÊS GARCIA MARTINS

SASE ENTRE A PROMESSA E A MATURIDADE

O SASE PASSOU RAPIDAMENTE DE CONCEITO A ARQUITETURA DOMINANTE NA CONVERGÊNCIA ENTRE REDE E CIBERSEGURANÇA. À MEDIDA QUE AS PRIMEIRAS IMPLEMENTAÇÕES ENTRAM NO TERCEIRO ANO DE OPERAÇÃO, A QUESTÃO PASSA A SER EXECUÇÃO. ENTRE INTEGRAÇÃO, POLÍTICAS E DEPENDÊNCIA DE FORNECEDORES, A REALIDADE OPERACIONAL ESTÁ A EXPOR FRAGILIDADES QUE SÓ SURGEM À ESCALA.

O Secure Access Service Edge (SASE) está a avançar nas organizações, mas a maturidade continua longe de acompanhar o ritmo. De acordo com o relatório “*State of Secure Network Access 2025*”, realizado pela Hughes, 32% das organizações já estão a implementar este modelo, enquanto 31% o avaliam e 24% planeiam adotá-lo no curto prazo. Ainda assim, apenas 8% afirmam ter uma implementação completa, o que expõe um fosso entre adoção e execução.

A arquitetura, desenhada para resolver limitações estruturais dos modelos legados, através da integração da segurança diretamente na rede, permitiu eliminar a dependência de perímetros físicos. **Simplificação, visibilidade e controlo fazem parte de uma promessa, que, no entanto, assenta em pressupostos que raramente se mantêm intactos à medida que a escala aumenta.**

A principal motivação para a adoção continua a ser o acesso remoto seguro, apontado por 45% das

organizações, num contexto em que 42% identificam os próprios colaboradores como o maior risco de segurança. O SASE surge, assim, como resposta a um problema, mas a sua implementação introduz novos níveis de complexidade.

O DESAFIO DA INTEGRAÇÃO

A integração com sistemas existentes continua a ser o principal entrave, apontado por 48% das organizações, seguida da gestão de políticas em ambientes distribuídos (44%) e da disrupção para os utilizadores durante a transição (38%). Estes números ajudam a explicar por que razão a maioria das implementações permanece em estado intermédio.

A simplificação prometida acaba muitas vezes por redistribuir a complexidade. Em vez de múltiplas *appliances* físicas, as organizações passam a gerir camadas lógicas – políticas, identidades, integrações e fluxos de tráfego – que introduzem novos pontos de dependência.

GOVERNAR A COMPLEXIDADE OPERACIONAL

Essa realidade é particularmente evidente na operação. André Chibeles, Cybersecurity Sales Engineer da Logicalis Portugal, afirma que, em ambientes maduros, **o desafio não é a tecnologia, mas a sua governação, sobretudo na definição de políticas, que combina aspetos técnicos e conceptuais.** Estes tipos de soluções obrigam “a definir estrategicamente que política aplicar, e depois a aplicação técnica da política definida”.

Os custos associados ao SASE surgem tanto na fase inicial de implementação como na operação contínua. Segundo André Chibeles, “sempre que é comprada uma solução tecnológica de segurança, deve haver primeiro uma definição de políticas ao nível conceptual e depois a configuração inicial da solução de SASE, com a aplicação e manutenção dessas políticas”. Esta configuração inicial envolve interligar os utilizadores às aplicações e definir quem tem acesso a quê, quando e como.



A operação continua a gerar custos, já que “será sempre necessária alteração de políticas, pois a organização pode redefini-las ou ocorrer alterações na arquitetura de rede – mudanças de rede, novos sites, fusões e aquisições”. A gestão de políticas não é, portanto, um esforço único, mas um processo contínuo que exige atenção e recursos constantes para que a solução SASE funcione de forma eficaz e segura.

"SEMPRE QUE É COMPRADA UMA SOLUÇÃO TECNOLÓGICA DE SEGURANÇA, DEVE HAVER PRIMEIRO UMA DEFINIÇÃO DE POLÍTICAS AO NÍVEL CONCEPTUAL E DEPOIS A CONFIGURAÇÃO INICIAL DA SOLUÇÃO DE SASE, COM A APLICAÇÃO E MANUTENÇÃO DESSAS POLÍTICAS"

A operação contínua levanta ainda desafios de visibilidade e *troubleshooting*. Quando o tráfego passa por infraestruturas que não pertencem à organização, identificar a origem de um problema torna-se mais complexo. Ainda assim, a observabilidade integrada nas plataformas pode ajudar, ao permitir distinguir entre problemas no *last mile* e no *backbone* do fornecedor e identificar gargalos com maior precisão.

Esta transferência parcial de controlo é acompanhada por uma mudança no modelo operacional. Com base no relatório da Hughes, apenas 16% das organizações gerem o SASE totalmente de forma interna, enquanto 46% optam por modelos de cogestão e 32% externalizam completamente a operação para MSP. A prevalência de cogestão e externalização indica que muitas equipas internas não dispõem de recursos ou experiência suficiente para gerir o SASE sozinhas.

ENTRE ESTRATÉGIA E EXECUÇÃO TÉCNICA

A maturidade das organizações na adoção de SASE varia significativamente, sobretudo ao nível de competências internas. André Chibeles sublinha que “depende muito de cliente para cliente” e que a adoção deve começar pela definição de estratégia e políticas, enquadradas por funções como CISO e GRC, muitas vezes impulsionadas por requisitos como *zero trust* e DLP associados a diretivas como a NIS 2, ISO 27001 ou *frameworks* como a NIST.

A partir daí, torna-se necessário garantir capacidade técnica para gerir um ecossistema que agrega múltiplas camadas de segurança, de firewall e IPS a CASB e controlo de acessos. Se por um lado, “há organizações que focam os seus recursos mais na vertente de GRC, tendo mais falta de recursos na componente técnica”, por outro, “há clientes que focam os seus recursos mais na componente técnica, tendo mais falta na componente de GRC”, acrescenta.

SASE NO TERRENO

O caso da Sonae MC mostra como os benefícios do SASE coexistem com desafios operacionais, num contexto próximo da realidade no terreno – neste

caso, no universo do retalho, mas com paralelos evidentes em múltiplos setores onde a gestão de redes distribuídas e acessos seguros é crítica. João Pedro Rosário, Head of IT Security and Operations, reconhece ganhos operacionais e afirma que “com a integração de várias capacidades numa única ferramenta e visibilidade que passámos a ter, sem dúvida que já é possível tirarmos partido da simplicidade e capacidade operacional que estas soluções entregam”.

Ao mesmo tempo, admite que a escala introduz desafios, já que “há sempre alguns casos de configurações particulares que vamos encontrando em cada site o que acaba por obrigar a intervenção mais cuidada das equipas”, mesmo com “*templates e blueprints* de rede das nossas lojas”.

A Sonae MC não mantém infraestrutura tradicional em paralelo, uma vez que “toda a nossa rede faz parte da nossa plataforma SASE”, afirma o responsável. Ainda assim, o *troubleshooting* continua a envolver vários intervenientes, já que “a componente de circuitos de dados mantém-se naturalmente responsabilidade dos operadores de telecomunicações, mas a clareza da origem do problema visível nas plataformas SASE torna mais simples identificar a *root cause* e endereçar com as equipas responsáveis mais depressa”.

▼

"COM A INTEGRAÇÃO DE VÁRIAS CAPACIDADES NUMA ÚNICA FERRAMENTA E VISIBILIDADE QUE PASSAMOS A TER, SEM DÚVIDA QUE JÁ É POSSÍVEL TIRARMOS PARTIDO DA SIMPLICIDADE E CAPACIDADE OPERACIONAL QUE ESTAS SOLUÇÕES ENTREGAM"



OPERAÇÃO DO SASE AO LONGO DO TEMPO

Do ponto de vista estratégico, a principal conclusão não é que o SASE falha, mas que a sua implementação está longe de ser um processo linear. A complexidade não desaparece, desloca-se, sobretudo para a definição e gestão contínua de políticas,

que concentram hoje o maior esforço operacional. À medida que mais organizações entram na fase de operação, torna-se claro que o desafio não está apenas na implementação inicial, mas na sua manutenção ao longo do tempo, num ciclo contínuo de adaptação e ajustamento.

Essa leitura não coloca em causa a maturidade tecnológica do modelo. “Ainda não tivemos nenhum projeto que tenha sido revertido para o modelo anterior. A tecnologia, nesta fase, já está madura”, sublinha André Chibeles. A base, lembra, assenta em elementos já bem consolidados, como túneis IPsec e agentes nos dispositivos. O maior desafio surge depois, na definição e implementação de políticas, onde está concentrada a maior parte da complexidade. É também nesse momento que o foco muda, com menos atenção ao que o SASE permite fazer e mais às exigências da sua implementação. ▼

por Álvaro Godinho,
Security Consultant na CSO

SASE: DA PROMESSA AO IMPACTO REAL

O SASE EVOLUIU DE UM CONCEITO ESTRATÉGICO PARA UMA ABORDAGEM CADA VEZ MAIS RELEVANTE NA ARQUITECTURA DE CIBERSEGURANÇA DAS ORGANIZAÇÕES.

Num contexto de infraestruturas híbridas, utilizadores distribuídos e aplicações em múltiplas clouds, a fragmentação das soluções de rede e segurança tornou-se um desafio significativo para a visibilidade e gestão operacional. Ao propor a convergência entre conectividade e segurança num modelo unificado, orientado por princípios de Zero Trust, o SASE procura responder a essa complexidade. Contudo, a maturidade desta abordagem depende não apenas da tecnologia adoptada, mas também da capacidade das organizações para integrar processos, alinhar equipas e ultrapassar silos operacionais.

DA TEORIA À OPERAÇÃO

Um dos equívocos mais frequentes é a confusão entre SSE (Security Service Edge) e SASE. O primeiro concentra-se na componente de segurança — secure web gateway, Firewall-as-a-Service, CASB e DLP. O segundo acrescenta a dimensão de conectividade inteligente, optimização WAN, controlo unificado e gestão centralizada.



ÁLVARO GODINHO, SECURITY CONSULTANT NA CSO

A maturidade do SASE mede-se na capacidade de correlacionar eventos de rede e segurança numa única camada de controlo. Não basta agregar alertas, é necessário contextualizá-los. Latência anómala, picos de tráfego, acessos privilegiados e comportamentos suspeitos devem ser analisados como parte de um mesmo fluxo operacional.

Num ambiente unificado, a consola deixa de ser apenas um painel de alertas e passa a representar uma visão integrada da postura de risco. A visibilidade transversal elimina a fragmentação entre equipas de rede e segurança, permitindo respostas mais rápidas e reduzindo fricção operacional.

O OBSTÁCULO HUMANO

Apesar das vantagens técnicas, a transição para SASE raramente é linear. O maior bloqueio não é tecnológico, mas organizacional. Equipas habituadas a operar de forma autónoma enfrentam agora um modelo convergente que exige colaboração permanente.

A resistência à mudança, combinada com infraestruturas legacy profundamente enraizadas, transforma muitos projectos SASE em implementações parciais. Integrações com firewalls existentes, arquitecturas VPN complexas e dependências específicas de fabricantes continuam a atrasar a consolidação.

Existe ainda a preocupação com dependência excessiva de um único fornecedor. A centralização traz simplicidade operacional, mas também levanta questões estratégicas sobre resiliência e poder negocial. A maturidade passa, por isso, por equilibrar consolidação com gestão consciente de risco.

ORÇAMENTO E PRIORIDADES

Num cenário de pressão orçamental, muitas organizações questionam se o SASE é uma prioridade ou mais uma camada tecnológica. A resposta depende do ponto de partida. Para ambientes altamente fragmentados, a consolidação pode representar redução de custos operacionais e simplificação estrutural.

Ainda assim, nenhum modelo SASE compensa a ausência de fundamentos. Backups isolados, segmentação adequada, autenticação multifactor e planos de resposta testados continuam a ser a base da resiliência. A transformação não deve ocorrer em modo “big bang”, mas sim por camadas: primeiro visibilidade e conectividade, depois políticas unificadas, e finalmente automação avançada.

ALÉM DO HYPE

O SASE não é uma moda passageira. É uma resposta estrutural a um mundo onde o perímetro tradicional desapareceu. No entanto, a maturidade não se mede pela adopção da sigla, mas pela capacidade real de integrar rede, segurança e inteligência num modelo operacional coerente.

As organizações que conseguirem ultrapassar a fragmentação, alinhar equipas e integrar tecnologia com estratégia estarão melhor posicionadas para enfrentar um cenário de ameaças cada vez mais distribuído e sofisticado.

A mudança é complexa e raramente confortável. Mas, no actual ecossistema digital, a convergência deixou de ser opcional. É uma inevitabilidade estratégica. ◀



por Dinis Fernandes
Executive Manager, Cybersafe

SASE MATURATION: BEYOND THE HYPE

NOS ÚLTIMOS ANOS, O CONCEITO DE SASE (SECURE ACCESS SERVICE EDGE) GANHOU UM PROTAGONISMO SIGNIFICATIVO NO MERCADO.



DINIS FERNANDES, EXECUTIVE MANAGER, CYBERSAFE

Isto porque os modelos tradicionais de segurança de perímetro deixaram de ser eficazes num mundo onde os utilizadores, as aplicações e os dados já não residem maioritariamente no data center corporativo. Com aplicações SaaS, workloads em múltiplas clouds e colaboradores a trabalhar remotamente a partir de qualquer local, tornou-se evidente a necessidade de aproximar a segurança do utilizador e do ponto de acesso à rede. A proposta do SASE combina capacidades como SD-WAN, Cloud Secure Web Gateway (SWG), CASB, Firewall as a Service (FWaaS) e Zero Trust Network Access (ZTNA), entregues a partir da cloud e geridas de forma unificada.

O conceito de SASE foi criado em 2019, pela consultora Gartner. Entre 2020 e 2022, impulsionadas pelo crescimento do trabalho remoto durante a pandemia, vários fabricantes passaram a posicionar plataformas SASE, consolidando aquisições e integrando funcionalidades numa única solução.

Agora, passados já alguns anos de implementações de SASE importa constatar quais os benefícios concretos que obtiveram as organizações que adotaram esta tecnologia.

Um dos benefícios mais evidentes surge na redução de custos de conectividade e infraestrutura. Muitas organizações conseguiram substituir ligações MPLS dispendiosas, mantendo ou até melho-

rando o desempenho. Simultaneamente, a consolidação de múltiplas soluções, como firewalls locais, proxies web e concentradores VPN, reduziu despesas de hardware, contratos de manutenção e ciclos de renovação tecnológica. Em ambientes distribuídos com dezenas ou centenas de filiais, estes ganhos financeiros tornam-se relevantes.

Outro benefício muito visível está na melhoria da experiência do utilizador. Ao permitir acesso direto e otimizado a aplicações SaaS, eliminando o tradicional “backhauling” do tráfego para o data center central, o SASE reduz latência e melhora o desempenho de aplicações SaaS. Utilizadores, que antes dependiam de VPNs subdimensionadas para contextos de trabalho remoto ou híbrido, passaram a beneficiar de ligações mais estáveis e específicas por aplicação.

No domínio da segurança, os benefícios são igualmente significativos. Implementações maduras de SASE permitem aplicar princípios de Zero Trust de forma consistente e transversal. Em vez de con-

ceder acesso amplo à rede interna, as organizações passam a definir políticas baseadas na identidade do utilizador, no estado do dispositivo e no contexto de risco. A segmentação granular de aplicações reduz a superfície de ataque e limita o impacto potencial de credenciais comprometidas. A visibilidade centralizada constitui outro ganho importante. Ao integrar capacidades como SD-WAN, Secure Web Gateway, CASB e Firewall as a Service numa única plataforma, as equipas passam a dispor de uma visão global do tráfego, dos utilizadores e das aplicações. A gestão unificada de políticas contribui ainda para maior consistência. A telemetria unificada permite melhorar a correlação de eventos, reduzir falsos positivos e acelerar tempos de resposta (MTTR). Atualmente, há soluções SASE que se diferenciam por fazer utilização de IA para deteção de ameaças mais rápida, políticas de segurança automatizadas e resposta a incidentes em tempo real.

Também a resiliência e continuidade de negócio ganharam com as plataformas SASE. As mes-

mas operam sobre infraestruturas cloud distribuídas globalmente, com múltiplos pontos de presença e redundância nativa. Isto reduz dependências de infraestruturas locais e minimiza o impacto de falhas regionais. A capacidade de failover automático e de rerouting dinâmico de tráfego aumenta significativamente a disponibilidade dos serviços críticos e reforça os planos de Business Continuity e Disaster Recovery.

Por fim, a escalabilidade e a agilidade operacional destacam-se como vantagens estratégicas. A entrega de serviços a partir da cloud permite abrir novas filiais ou integrar novos utilizadores com rapidez.

Em síntese, quando implementado com planeamento faseado, com alinhamento entre equipas de rede e segurança, e suportado por uma equipa competente e experiente como a da CyberSafe, o SASE gera benefícios reais e tangíveis: redução de custos, melhoria da experiência do utilizador, reforço da postura de segurança, simplificação operacional e maior capacidade de adaptação estratégica. ◀

A portrait of Rui Damião, a man with a beard and mustache, wearing a light-colored V-neck sweater over a dark collared shirt. He is smiling and has his arms crossed.

► RUI DAMIÃO

"AS PESSOAS TÊM DE
ENTENDER PORQUE
É QUE AS REGRAS
EXISTEM. AÍ ESTÃO
MAIS DISPOSTAS A
COLABORAR"

MANUEL NEVES,

HEAD OF CYBERSECURITY FOR ENABLING FUNCTIONS NA MERCK

MANUEL NEVES, HEAD OF CYBERSECURITY FOR ENABLING FUNCTIONS NA MERCK, FALA SOBRE FRAGMENTAÇÃO REGULATÓRIA, CADEIA DE FORNECEDORES E O QUE REALMENTE FUNCIONA NA CONSTRUÇÃO DE UMA CULTURA DE CIBERSEGURANÇA.

Existe, atualmente, uma fragmentação regulatória a nível global; temos a NIS2 na Europa, há requisitos específicos para os EUA, assim como outras jurisdições. Como é que se mantém a coerência estratégica com tantos regimes diferentes?

Todos eles têm pontos em comum, não são completamente diferentes. Obviamente, com base na sua geografia, os requisitos podem mudar aqui e ali e, em alguns casos, serem mais flexíveis e outros não tão flexíveis.

Acho que o que se tenta fazer, da minha experiência nas várias empresas onde estive, é adaptar as políticas globais ao contexto que existe. Isso é feito não só para este tipo de requisitos legais, mas até para o contexto operacional.

Vamos supor que uma empresa tem muitas fábricas, armazéns, para além

daquilo que são os escritórios, o chamado IT normal. Uma pessoa não pode criar as mesmas regras no mesmo padrão para todos porque podemos ter, como já tive no passado certos exemplos, em que temos armazéns com cem ou 200 pessoas a trabalhar com uma logística relevante, e outros com cinco ou seis pessoas; não posso exigir àquele pequeno que implemente todo o tipo de regras.

Agora, os requisitos legais tomam sempre precedência sobre qualquer regra interna que tenhamos e, portanto, temos de nos adaptar às regras onde elas existem.

Gerir cibersegurança numa multinacional farmacêutica significa estar entre duas realidades: as diretrizes globais da sede e o contexto local. Como é que isto se equilibra na prática?

Isto foi uma grande lição. Venho de trabalhar sempre em equipas corporativas, globais, e isso, por um lado infelizmente, faz-nos ver as coisas sempre de uma maneira padrão e olhamos sempre para o todo; às vezes, falta-nos conhecer a pessoa, todas as unidades de negócios e o detalhe de toda a organização. Falta-nos a capacidade para conhecer essas realidades mais locais.

Acho que uma das formas de resolver, e foi isso que aprendi no passado e que resultou, é que cada vez que estamos a criar as nossas regras, ou seja, as nossas políticas, *standards* e regras, temos de incluir pessoas que vivem essa realidade de uma forma diária.

Acho que a melhor maneira é nós termos uma ideia daquilo que queremos implementar, mas depois temos de chamar essas pessoas para percebermos se na realidade onde elas estão no seu dia a dia isso funciona ou não. Elas vão nos dizer que, em certos casos, aquilo não vai funcionar e temos de nos adaptar.

Eu tinha uma chefe noutra empresa que ela gostava muito de usar a expressão *t-shirt size*, ou seja, nós definimos as coisas, mas, dentro nos nossos próprios *standards*, vamos ter de nos adaptar a certas realidades, vamos ter de fazer várias t-shirts de vários tamanhos diferentes porque as realidades são diferentes e só quem está lá no dia a dia é que nos sabe responder a isso.

É impossível para uma pessoa que está numa equipa global conseguir saber todas as realidades, pelo menos nas empresas de maior dimensão. Obviamente que em PME é diferente e há uma proximidade maior, é mais fácil. A solução é incluir as pessoas que vivem essa realidade para que nos digam se o caminho está certo ou está errado.

Tendo em conta a realidade específica, não só que o Manuel enfrenta, mas também agora este contexto global onde as ciberameaças estão a crescer bastante, qual é o desafio que mais o preocupa atualmente?

Uma das respostas já foi dada: é o aumento não só em quantidade, mas também em complexidade das ciberameaças. Vou usar a palavra qualidade, não porque elas sejam boas, mas porque são mais bem feitas.

Dou um exemplo muito básico. Há meia dúzia de anos, muitos dos emails de



phishing que as pessoas recebiam não eram bem feitos; com alguma atenção, mesmo alguém que não fosse de segurança conseguia perceber. Hoje, há coisas que são perfeitas. Esse é um dos desafios.

Outro é a automatização, os LLM, a Inteligência Artificial [IA]. Há ferramentas que permitem a quem quer usar estas novas tecnologias de forma não legítima a serem mais eficazes. Qualquer criminoso em qualquer área tenta estar

sempre com um passo à frente das regras, das leis. Agora, com estas novas tecnologias, conseguem crescer em quantidade, também em qualidade e em capacidade. Ou seja, menos pessoas para ciberataques de grande dimensão, serão precisos menos recursos humanos, ou seja, menos atores com vontade de ter um comportamento ilegítimo, porque já têm ferramentas que exponenciam a sua capacidade.

A IA generativa está certamente a mudar o que é preciso defender e as ferramentas que estão disponíveis. Como é que se olha para isto? Mais do ponto de vista de ameaça ou de oportunidade?

Para o meu trabalho em particular, sei que isto vai trazer outro tipo de ameaças; é normal. Mas tenho uma visão positiva da inteligência artificial, ou seja, acho que é algo que vem para ficar, como outras transformações tecnológicas do passado, como há 20 e tal anos a Internet de forma mais massificada, mesmo que tivesse mais anos, ou como quando há 40 ou 50 anos vieram os computadores. Todas essas transformações tiveram a fase inicial e trouxeram novas oportunidades em termos de eficiência, mas também novos desafios em termos de segurança.

Quando veio o computador, passou-se muito dos dados físicos para os dados digitais. Quando veio a Internet, obviamente melhorou a nossa capacidade de trabalho, de logística, de eficiência, mas também trouxe outro tipo de desafios para salvaguardar os tais dados digitais.

"SINTO QUE A INTELIGÊNCIA ARTIFICIAL, OU AS SUAS CAPACIDADES, VIERAM PARA FICAR. NÃO ESTÁ AINDA MADURA, OBVIAMENTE; COMO QUALQUER TRANSFORMAÇÃO TECNOLÓGICA VAI TER DE PASSAR POR UMA FASE DE MATURAÇÃO"

Acho que a IA é a mesma coisa. Sinto que a inteligência artificial, ou as suas capacidades, vieram para ficar. Não está ainda madura, obviamente; como qualquer transformação tecnológica vai ter de passar por uma fase de maturação. Eventualmente, menos historicamente, todas estas transformações tornam-se mais eficazes ao longo do tempo, com menos custos. Por outro lado, como já referi, existe uma pequena percentagem que quer usá-la para outros fins que não são lícitos e também vai potenciar as suas capacidades.

É uma oportunidade e também traz ameaças, mas, globalmente, é uma coisa boa. Não vejo a IA como uma ameaça, mesmo estando na parte de segurança. Vejo como algo que nós podemos utilizar e que podemos tirar partido para nos tornar mais eficientes. A IA também nos ajuda nas capacidades de defesa. Mas vejo como algo globalmente positivo, naturalmente.

▼

"ACHO QUE CADA EMPRESA DEVE DEFINIR QUAIS SÃO OS SEUS LIMITES, AQUILO QUE ACEITA ENQUANTO RISCO, OU SEJA, O SEU APETITE DE RISCO, NA RELAÇÃO COM OS FORNECEDORES E DIZER, 'ATÉ ESTE LIMITE, EU CONSIGO VIVER COM ISTO E PERCEBO QUE ESTE FORNECEDOR LOCAL NÃO VAI CONSEGUIR CUMPRIR COM ISTO TUDO, MAS EU ACEITE ESSE RISCO"

Academia de fornecedores é, historicamente, um dos vetores de ataque mais explorados na farmacêutica. Como é que se gere esse risco quando fornecedores, parceiros e distribuidores têm maturidades de segurança muito diferentes?

Sou apologista de começar sempre as coisas pelas suas, vou-lhe chamar, fundações, pela sua base. Quando queremos proteger algo ou ter um conhecimento sobre um assunto, temos de saber o que é que temos. Neste caso, penso que é importante que consigamos ter, por um lado, um inventário de fornecedores para saber com quem nós trabalhamos, para podermos também avaliar a sua criticidade, quais é que trazem mais riscos e quais é que trazem menos riscos devido à sua maturidade porque não são todos iguais.

Depois, obviamente que um fornecedor global tem outra capacidade para implementar controlos de segurança, mas também temos os fornecedores locais que, muitas vezes, são muito pequenos, mas também são importantes.

Todo o ecossistema tem diferentes desafios, mas acho que o início é sempre esse, é percebermos o que é que temos e com quem trabalhamos, em ter-

mos de segurança qual é a sua criticidade. É aí que entram os tais *third-party assessment* que sei que muita gente não gosta; é normal, dá trabalho responder a coisas. Mas esse é o primeiro passo.

Outro passo importante é também as equipas de segurança serem capazes de trabalhar não só com o *procurement*, mas também com os departamentos legais para tentar incluir todas essas cláusulas de segurança nos contratos. Se eu, enquanto fornecedor, garanto que faço isto, que tenho um bom processo de gestão de risco, que comunico os riscos aos meus clientes e como os afeta, se garanto que tenho um processo de gestão de vulnerabilidades maduro, isso também tem de ficar registado para dar segurança para ambos os lados.

Outro passo é sermos capazes de introduzir todos esses requisitos legais na relação que temos com o fornecedor e creio que são os primeiros passos para termos alguma boa visibilidade; não diria perfeita, mas para termos alguma visibilidade sobre os riscos que temos nas diferentes relações, com os diferentes fornecedores.

Isto é válido para pequenas e médias empresas como é para empresas globais. Obviamente a capa-



cidade de uma empresa pequena de fazer todos estes passos é diferente; percebo isso. Sei que é muito difícil para uma pequena e média empresa e é muito fácil eu estar a dizer isto, mas ter os recursos de implementar isto e, mais importante, operacionalizar – porque formalizar nem é a parte mais difícil, mas sim operacionalizar todos estes processos – é que é difícil.

Diria que os maiores desafios para as empresas é ter as fundações já bem definidas e, depois, ter a capacidade de trabalhar entre os diferentes departamentos

para garantir que todo o tipo de riscos é primeiro identificado, avaliado e depois monitorizado ao longo do tempo.

Como é que se pode fazer com que um fornecedor mais pequeno em dimensão, mas não necessariamente em termos de importância, cumpra todas as regras que uma grande empresa precisa que sejam cumpridas?

Numa perspetiva de segurança, diria que a primeira tem a ver com o tipo de dados e com a criticidade dos dados que esse fornecedor vai guardar ou transmitir. Logo aí, temos de nos adaptar aos requisitos de segurança e à criticidade do fornecedor. A segunda, na minha opinião, é que acho que cada empresa deve definir quais são os seus limites, aquilo que aceita enquanto risco, ou seja, o seu apetite de risco, na relação com os fornecedores e dizer, ‘até este limite, eu consigo viver com isto e percebo que este fornecedor local não vai conseguir cumprir com isto tudo, mas eu aceite esse risco’ ou, por outro lado, dizer, ‘a partir daqui, não trabalho com este fornecedor, seja local ou global’.

Falamos muito de tecnologia, mas o fator humano continua a ser o principal vetor de ataque. Como é que se trabalha a cultura de cibersegurança internamente e o que é que, na vossa experiência, funciona?

Noutras empresas, já tive a meu cargo a responsabilidade da parte de *awareness*. Às vezes, parece uma parte menos relevante da cibersegurança, mas aprendi grandes lições com o tema de *awareness*.

Embora possa ser imprevisível, o comportamento humano é algo que tem

certos padrões e certo tipo de comportamentos que, quem percebe o assunto e estuda, nos consegue ajudar.

Sei que há visões diferentes, mas o fator humano é extremamente importante. Não estou a falar de atores que queiram deliberadamente fazer mal a uma empresa; estou a falar mesmo de nós, no nosso dia a dia. Todos cometemos erros; até as pessoas de segurança cometem erros.

Alguém que esteja num departamento que não tem nada a ver com segurança, sabemos que este tema não estará presente nas suas tarefas. Não está a pensar, como é óbvio, porque trabalha num outro mundo completamente diferente. Da mesma maneira, se me pedirem para fazer um Power Point e para ter uma grande qualidade em termos visuais ou de marketing para saber vender, eu tenho mais dificuldades porque não é a minha área, não estudei. Percebo isso e tem de partir do nosso lado a capacidade para trazer esse conhecimento às pessoas de uma forma que elas também estejam abertas a receber.

Quando me perguntam o que é que funciona e o que é que não funciona... ponto um: as pessoas têm de entender porque é que as regras existem. É muito mais fácil, e já vi isso ao longo destes anos todos, se as pessoas perceberem o racional que está por trás daquelas regras que criamos, que são todas regras de segurança, vão estar mais dispostas a colaborar, e também percebem melhor o que é que está ali, porque é que lhes estamos a pedir estes requisitos, porque é que pedimos que façam desta maneira, porque é que pedimos que não partilhem dados do seu trabalho com terceiros com os quais não temos relações oficiais.

As pessoas podem, no seu dia a dia, esquecer-se disso, mas se nós explicarmos o que é que está por trás disso, as pessoas percebem.

A segunda é tornar aquilo que nós chamamos de formações de *awareness* em algo mais dinâmico, que puxe por elas, que não seja só ler uma folha. Se tiver de ler uma folha, se calhar vou decorar 5% ou 10% na primeira vez, mas se já tiver de escrever, se calhar já vou decorar mais 15% ou 20%. Se tiver de interagir, tiver de tomar decisões ou tiver de tomar ações durante o treino, parece-me que isso também torna as coisas mais *engaged*, as pessoas retêm mais informação.

Como disse, numa experiência no passado tinha a parte de *awareness* e tive de implementar um treino global e eu tive esse *feedback*, que foi passar de ler um documento para ter um treino mais interativo, mais dinâmico e o *feedback* que recebi na altura foi muito positivo. Ninguém ficou extasiado por ter de fazer mais um treino, mais uma formação, mas gostaram. A referência e a expectativa era ‘vamos ler mais um documento, responder umas perguntas no fim, está feito’; quando viram que eram coisas diferentes, que criávamos pequenos vídeos de 30 segundos, um minuto para cada tema, muitas vezes com algo para fazer no meio, as pessoas gostavam mais.

Funciona claramente explicar o racional por trás de todas as decisões. Funciona também trazer quem está dentro das diferentes organizações ou unidades de negócio para essa tomada de decisão porque, depois, eles também são promotores dentro das suas organizações mais locais daquilo que estamos a fazer e as pessoas já os conhecem. É diferente eu chegar a alguém que não me conhece de

lado nenhum e dizer-lhe algo do que ser alguém com quem ela trabalha ou com alguém que uma pessoa vê no dia a dia; essa proximidade também funciona.

Depois, há obviamente coisas que se podem também experimentar em termos de *storytelling*, contar uma história. Já vi há muitos anos na empresa uma formação em que se tinha de fazer a formação como se fosse uma personagem de ‘*Star Wars*’. A formação era obrigatória, todos aqueles treinos das mais variadas áreas foram postos numa história onde a personagem tinha de passar pelas diferentes aventuras.

Houve algum momento que lhe ensinou algo que não foi possível aprender em mais nenhum lado?

Tenho algumas aprendizagens que mudaram bastante a minha forma de estar e de ver as coisas. Falámos no início da capacidade de trazer as pessoas que têm outro conhecimento das diferentes organizações, ou mais locais, ou de diferentes unidades de negócio que operam com outro tipo de regras.

Posso contar duas histórias rapidamente. Como disse, venho de empresas sempre a trabalhar num âmbito global e, nessa empresa, com essa falta de visão de algumas unidades de negócios. Na altura, era o manager da equipa de Cybersecurity Governance, Risk and Compliance, tinha tudo o que era gestão de risco, *awareness*, *security controls* para validar a *compliance* e, depois, também a parte de políticas, *standards* e *procedures*. Portanto, a minha equipa tinha todo esse âmbito e quando eu estou a liderar essa equipa começámos a produzir a documentação que fazia parte do nosso trabalho e dia a dia; não tivemos em



conta muitas dessas opiniões e isso foi um choque de realidade. Tive muita gente, o que me deixou surpreendido na altura, devido à minha falta de conhecimento quando isso aconteceu, que me disse que estava a cometer exatamente o mesmo erro que já cometerem no passado, que é não incluir quem conhece as realidades e depois criam regras que ninguém consegue cumprir nesses pontos, ou certas regras que ninguém vai conseguir cumprir, e depois temos de estar a discutir se temos de criar exceções ou se são riscos. Essa foi uma grande lição



"TEMOS DE TER UMA FLEXIBILIDADE PARA ENTENDER OS DIFERENTES NEGÓCIOS E SABER QUE NUNCA VAMOS IMPLEMENTAR TODO O TIPO DE CONTROLOS QUE ESTAS FRAMEWORKS CONHECIDAS INDICAM"

que aprendi e foi um choque com a realidade e, a partir daí, mudei a minha forma de encarar estas coisas.

A segunda... às vezes trabalhar em empresas com pessoas espalhadas pelo mundo traz-nos também visões muito interessantes da vida e do que é o trabalho. Quando tive de montar aquilo que estávamos a falar, um programa global de *cybersecurity awareness*, um treino, uma formação, segui todo o processo que havia na altura. Pesquisámos, fizemos avaliações no mercado para ver fornecedores que nos pudessem trazer novas capacidades porque internamente era difícil começar a criar vídeos. Lembro-me, na altura, da minha chefe me perguntar qual seria o tempo estimado para ter, após escolhermos o fornecedor, para produzirmos o treino internamente, para o testar e para depois comunicar e implementar, porque o treino seria obrigatório para todos.

Hoje sei que ela me estava a testar, mas sou demasiado otimista e ela perguntou se achava que quatro meses chegava. Eu disse com certeza, nós em quatro

meses temos isso, sem problema nenhum; ela riu-se. O meu choque de realidade foi de facto grande porque aprendi que aquilo que para nós, quando recebemos, parece ser algo muito simples de fazer, tem por trás um processo bastante pesado, principalmente em empresas de grande dimensão, mas que faz sentido.

Se pudesse dar um conselho, ou um conjunto de conselhos, a um CISO que está a construir a função de raiz numa empresa, o que diria?

É difícil. Cada contexto organizacional traz desafios diferentes. Não só a indústria traz desafios diferentes, mas mesmo dentro da indústria vai depender. Posso sugerir algumas coisas que eu vi até nos tempos em que, noutra vida, estive na parte da auditoria de sistemas de informação das *big four* e vi empresas de todos os tamanhos, desde empresas pequenas subsidiárias cá em que o IT era uma pessoa, até empresas de grande dimensão em Portugal que tinham equipas mais robustas.

Nunca estive como CISO de raiz, mas já tive de construir equipas quase de raiz pelo menos uma vez na área de cibersegurança. Uma das minhas primeiras perguntas, quando começo algo, é perceber quais são as expectativas de quem lidera, o que é que eles estão à espera de conseguir, principalmente no curto prazo, e alinhar as expectativas deles com aquilo que nós entendemos ser os requisitos principais de segurança quando se está a montar algo de raiz e essa cultura. Acho que isso é essencial para começar a estar alinhado.

Houve uma frase que aprendi há muitos anos que é, em termos de segurança, temos de ser orientados ao negócio sem descurar a parte de segurança. Temos

de ter uma flexibilidade para entender os diferentes negócios e saber que nunca vamos implementar todo o tipo de controlos que estas *frameworks* conhecidas indicam.

Tinha um colega americano, noutra empresa, que me dizia que se quisessem implementar tudo, a melhor maneira é desligar. Desligam e não há como sofrer um único ataque, se não tivermos sistemas. E é verdade. Temos de ter essa flexibilidade.

Outra coisa que acho muito relevante e tenho a certeza de que quem vai construir uma equipa de raiz sabe disso, é perceber que vai ter de ter um misto de equipas, ou seja, vai ter de conseguir algumas internas, mas vai ter que, principalmente até ter maior maturidade e conseguir crescer, ter fornecedores de serviços na parte de cibersegurança, vai ter os chamados *contractors* durante algum tempo e vai ter de gerir todo esse diferente ecossistema de recursos e de ligação à empresa. Isso é algo garantidamente que tem de ter.

Outra coisa que tento fazer e que acho que é relevante não só para quem quer construir de início é a capacidade de falar com diferentes pessoas para perceber o que elas fazem, que visão é que têm da parte da segurança, porque é impossível em empresas de grande dimensão, em pouco tempo, conhecer a empresa toda. Criamos essa rede de contactos que vai ser importante para o futuro. Por outro lado, aprendemos logo mais sobre a empresa, sobre o que as pessoas fazem e, por último, percebemos também qual é a visão que as pessoas têm da parte de segurança e as expectativas que têm desta equipa e que impacto é que isso vai ter no seu dia a dia. Se as pessoas estiverem logo de início mais alinhadas,

estarão logo mais abertas para criar essas relações e essa colaboração. Se precisar de implementar um novo processo, quando for preciso pedir da parte do negócio que cumpram com o requisito de segurança ou que sigam os processos de segurança, ou fazer um *impact analysis* de uma ferramenta, se eu já tiver essa ligação criada, vai ser sempre mais fácil de eu tirar algum tempo, porque isto são atividades que vêm em cima daquilo que as pessoas fazem no seu dia a dia, é trabalho adicional que estamos sempre a pedir.

Depois, penso que grande parte tem a ver com a capacidade e de comunicação, o que e não é relevante atingir nos primeiros tempos. Acho que vai variar de CISO para CISO onde é que ele se vai focar primeiro. Já vi casos onde se focaram primeiro em formalizar as coisas e depois operacionalizar, mas também já vi mais vezes o contrário, que é primeiro operacionalizar porque é mais importante ter as coisas a andar e depois formalizar a documentação, até porque é preciso fazer escolhas porque numa pequena e média empresa os recursos vão ser limitados, e quando falo de recursos falo de pessoas, processos e tecnologia. Tudo vai ser limitado.

O último ponto é dar prioridade de forme bem vincada, definir sejam duas, três ou quatro prioridades e não fugir daí no início. Acho que no início é extremamente importante e contra mim falo porque adoro um bom desafio e às vezes chegam ao pé de mim com uma iniciativa nova e digo que aquilo é extraordinário e adorava fazer parte daquilo, mas depois tenho de me lembrar que já não dá, ou vai alguém diferente ou não dá. Priorizar de forma bastante convicta é outro ponto. ◀

EXECUTIVA COM 28 ANOS DE EXPERIÊNCIA EM TI A FRENTE DE CIBERSEGURANÇA, INFRAESTRUTURA, PRIVACIDADE, GOVERNANÇA, RISCOS E COMPLIANCE NO SEGMENTO DE LOGÍSTICA, SERVIÇOS, RETAIL E INDÚSTRIA. ESPECIALISTA SEGURANÇA DA INFORMAÇÃO - ITA - INST. TEC. AERONÁUTICA, MIN. DEFESA/COMANDO AERONÁUTICA - BRA; MBA TRANSFORMAÇÃO DIGITAL - MIT - MASSACHUSETTS INSTITUTE OF TECHNOLOGY, EUA; LIVROS CO-AUTORA: PRODUTO E TECNOLOGIA, POR TRÁS DA TI E MULHERES EM TECNOLOGIA.



POR CRISTIANE DIAS

ESTRATÉGIA DIGITAL NA ERA QUÂNTICA: O NOVO PAPEL DA CIBERSEGURANÇA

TENHO ACOMPANHADO DE PERTO AS TRANSFORMAÇÕES QUE ESTÃO MOLDANDO O FUTURO DOS NEGÓCIOS E DA SOCIEDADE. A COMPUTAÇÃO QUÂNTICA SE DESTACA NÃO APENAS COMO UMA PROMESSA TECNOLÓGICA, MAS COMO UM VERDADEIRO DIVISOR DE ÁGUAS — ESPECIALMENTE QUANDO ANALISADA SOB A ÓTICA DA CIBERSEGURANÇA E DA RESILIÊNCIA DIGITAL.

Entramos em uma era em que os paradigmas tradicionais de Segurança já não serão suficientes. A Computação Quântica tem o potencial de quebrar algoritmos criptográficos amplamente utilizados hoje e que sustentam grande parte das comunicações seguras globais. Isso não é apenas uma questão técnica, é um tema estratégico que impacta Governos, Instituições Financeiras, Indústrias de Infraestrutura Críticas e toda a Economia Digital.

Ao mesmo tempo, é importante destacar que a Computação Quântica não representa apenas risco — ela também abre oportunidades. Estamos observando o avanço da Criptografia Pós-Quântica e de novos modelos de Segurança baseados em princípios quânticos, como a distribuição de chaves quânticas. O

desafio está em equilibrar essa dualidade: proteger o presente enquanto nos preparamos para um futuro.

Quando ampliamos essa análise para além da Cibersegurança, o impacto se torna ainda mais abrangente. Infraestruturas Críticas — como energia, telecomunicações, transporte e sistemas de água — estão cada vez mais conectadas e dependentes de Tecnologias Digitais. A introdução de capacidades quânticas, aliada à Inteligência Artificial, pode tanto fortalecer quanto expor essas estruturas. A automação inteligente, por exemplo, pode antecipar falhas e mitigar riscos em tempo real, mas também pode ampliar a superfície de ataque se não for devidamente protegida. Isso também vale para agentes maliciosos onde sistemas mais inteligentes e interconectados tornam-se também mais complexos de proteger. E, nesse contexto, a Cibersegurança deixa de ser uma camada adicional — passa a ser um elemento estrutural da Inovação o que torna a corrida tecnológica ainda mais crítica.

▼
"INFRAESTRUTURAS
CRÍTICAS —
COMO ENERGIA,
TELECOMUNICAÇÕES,
TRANSPORTE E
SISTEMAS DE ÁGUA
— ESTÃO CADA VEZ
MAIS CONECTADAS
E DEPENDENTES DE
TECNOLOGIAS DIGITAIS.
A INTRODUÇÃO
DE CAPACIDADES
QUÂNTICAS, ALIADA
À INTELIGÊNCIA
ARTIFICIAL, PODE
TANTO FORTALECER
QUANTO EXPOR ESSAS
ESTRUTURAS"

A Inteligência Artificial desempenha um papel central nesse cenário. Observamos uma convergência entre IA, Computação Quântica e Cibersegurança que redefine a forma como lidamos com riscos. Modelos avançados de IA já são capazes de identificar padrões de ataque com uma precisão sem precedentes e, no futuro, a combinação com Algoritmos Quânticos poderá elevar esse nível a patamares ainda inimagináveis.

Essa abordagem integrada — combinando Computação Clássica, Quântica e Inteligência Artificial — é particularmente relevante. O surgimento de novos paradigmas, como o Quantum Machine Learning, que poderão redefinir desde a detecção de ameaças cibernéticas até à otimização de sistemas complexos em setores como energia, mobilidade e saúde.

Outro ponto que considero essencial é o Impacto Ambiental e Social dessas tecnologias. A Computação Quântica ainda demanda ambientes extremamen-

"COMPUTAÇÃO QUÂNTICA, COMBINADA COM INTELIGÊNCIA ARTIFICIAL E UMA ABORDAGEM ROBUSTA DE CIBERSEGURANÇA, PODE NÃO APENAS PROTEGER O FUTURO DIGITAL, MAS TAMBÉM IMPULSIONAR INOVAÇÃO EM ESCALA GLOBAL. MAIS DO QUE ISSO, É FUNDAMENTAL INTEGRAR ESSA AGENDA NA ESTRATÉGIA DE INOVAÇÃO. O VERDADEIRO VALOR ESTÁ NA CONVERGÊNCIA"

te controlados e alto consumo de energia. Ao mesmo tempo, ela pode acelerar descobertas em áreas como Sustentabilidade, Novos Materiais, Eficiência Operacional e Energética. Pode permitir avanços significativos, como previsão de eventos climáticos extremos, otimização de redes energéticas e aceleração na descoberta de novos materiais sustentáveis.

Do ponto de vista executivo, o maior desafio não é apenas tecnológico — é estratégico que envolve a tomada de decisão em cenários de incertezas. As organizações precisam começar agora a mapear seus Ativos Críticos, entender suas dependências criptográficas e desenvolver planos de transição para um

cenário Pós-Quântico. Isso envolve investimento, capacitação e, principalmente, uma mudança de mentalidade. Não se trata de “se” a Computação Quântica irá impactar os negócios, mas de “quando” e “como estaremos preparados”. A Resiliência Organizacional será cada vez mais definida pela capacidade de antecipar e se adaptar a essas disrupções tecnológicas.

Por fim, acredito que estamos diante de uma oportunidade única de liderar essa transformação com responsabilidade e visão de longo prazo. A Computação Quântica, combinada com Inteligência Artificial e uma abordagem robusta de Cibersegurança, pode

não apenas proteger o futuro digital, mas também impulsionar Inovação em escala global. Mais do que isso, é fundamental integrar essa agenda na estratégia de Inovação. O verdadeiro valor está na convergência.

A Inovação precisa ser vista de forma integrada. Não podemos tratar Cibersegurança como um elemento isolado mas como parte central da Estratégia de Transformação Digital. Isso inclui Governança, Compliance, Sustentabilidade e Continuidade dos Negócios.

A Computação Quântica ainda está em evolução, mas os seus impactos já são suficientemente claros para exigir ação imediata.

Estamos perante uma mudança estrutural que irá redefinir não apenas a forma como protegemos sistemas, mas como concebemos o próprio conceito de confiança digital.

Cabe a nós, líderes de tecnologia, garantir que essa evolução aconteça de forma segura, ética e sustentável aliado a visão Estratégica e com Responsabilidade. ◀

LICENCIADA EM DIREITO
PELA FACULDADE DE
DIREITO DA UNIVERSIDADE
DE LISBOA, MESTRADO EM
DIREITO E TECNOLOGIA
PELA UNIVERSIDADE
DE TILBURG, INICIOU O
PERCURSO PROFISSIONAL
NUMA CONSULTORA NA
ÁREA DE CIBERSEGURANÇA.
É ADVOGADA NA PLMJ E
PRESTA ASSESSORIA NA ÁREA
DA CIBERSEGURANÇA E DAS
TECNOLOGIAS DE INFORMAÇÃO



POR MAFALDA DE BRITO FERNANDES, ADVOGADA, PLMJ

NO MÊS DA ENTRADA EM VIGOR DO TÃO AGUARDADO
DECRETO-LEI N.º 125/2025 (“REGIME JURÍDICO DA
CIBERSEGURANÇA”), VALE A PENA VOLTAR A CENTRAR
A DISCUSSÃO NUM DOS TEMAS MAIS FALADOS DESTE
PERÍODO (ALARGADO) DE TRANSPOSIÇÃO: O REGIME
SANCIONATÓRIO.

NA CIBERSEGURANÇA, O EXEMPLO TAMBÉM VEM DE CIMA

Para mal dos pecados de todos aqueles que promovem a cibersegurança como uma necessidade e com a devida atenção à importância que deverá assumir no futuro, os efeitos deste regime jurídico têm vindo a evidenciar, de uma maneira geral, uma maior preocupação com as consequências do não cumprimento com este regime, do que com as oportunidades que lhes estão associadas.

Os melhores sistemas de gestão de segurança da informação não nascem do receio de coimas, mas sim de escolhas previamente discutidas, iteratividade e predisposição para assumir as falhas, porque só através das falhas é possível promover uma melhoria contínua. O novo regime não muda esta realidade, apenas lhe dá alguma “dignidade” legislativa para que as empresas olhem para este quadro

regulatório como uma bússola orientadora de boas práticas a aplicar (e manter).

Para tal, é inegável que os órgãos de gestão, direção e administração assumem, agora, um papel fundamental na definição destas linhas orientadoras – a máxima que dita que “o exemplo vem de cima” deve ser tomado como um dos princípios mais importantes deste novo e aprimorado regime, não porque o seu incumprimento poderá resultar numa responsabilização individual, mas porque o um dos propósitos de um membro da gestão de topo é garantir a continuidade e sucesso do seu negócio e evitar, sempre que possível, falhas humanas e/ou tecnológicas que resultem em danos, por vezes, irrecuperáveis.

Fazer parte da gestão de topo tornou-se uma responsabilidade efetiva, com funções e envolvimento legalmente definidos e, por muito que se esmiúce e analise o que significa, na prática, a responsabilização destes órgãos pela “ação ou omissão, com dolo ou culpa grave, nos termos da legislação aplicável, pelas infrações previstas no presente decreto-lei”, a

" TRATA-SE DE ASSEGURAR QUE AS EMPRESAS QUE GEREM ESTÃO A SEGUIR AS ORIENTAÇÕES EUROPEIAS E NACIONAIS NESTE SENTIDO, DE ASSEGURAR E APROVAR UMA ANÁLISE E GESTÃO DO RISCO A QUE ESTÃO EXPOSTAS, DE PROMOVER A DEVIDA SENSIBILIZAÇÃO E FORMAÇÃO INTERNAS E DE COOPERAR E RESPEITAR AS DECISÕES DAS AUTORIDADES NACIONAIS COMPETENTES"

conclusão será a de que esta disposição não é um labirinto, mas sim um espelho da realidade existente – uma realidade em que os bons gestores e as boas estruturas de cibersegurança não estão focados na letra da lei mas sim no seu espírito e na construção da cultura de cibersegurança que tanto se promove (e se tem promovido) nos últimos anos.

Trata-se de assegurar que as empresas que gerem estão a seguir as orientações europeias e nacionais neste sentido, de assegurar e aprovar uma análise e gestão do risco a que estão expostas, de promover a devida sensibilização e formação internas e de coo-

perar e respeitar as decisões das autoridades nacionais competentes – trata-se, assim, de um maior envolvimento do que aquele a que temos tendencialmente assistido. Se esse envolvimento, investimento, gestão e cooperação acontecerem, não se espera que as autoridades acionem este mecanismo sancionatório.

O verdadeiro risco, afinal, nunca foi a coima. O verdadeiro risco é o incidente em si – a interrupção de um serviço crítico, a exposição de dados sensíveis, a gestão apressada de crise de um incidente publicamente exposto, a perda de confiança de clientes e

▼

"O NOVO REGIME TEM, ASSIM, O MÉRITO DE EVIDENCIAR AQUILO QUE OS PROFISSIONAIS DE CIBERSEGURANÇA JÁ RECONHECEM HÁ MUITO TEMPO: A CIBERSEGURANÇA NÃO É UM FIM EM SI MESMO, MAS SIM UM MEIO PARA GARANTIR A ESTABILIDADE, E ESSA ESTABILIDADE COMEÇA NA CULTURA E, SUBSEQUENTEMENTE, ESSA CULTURA DEVE SER PROMOVIDA PELA GESTÃO DE TOPO.

parceiros que, muitas vezes, não tem retorno. E é precisamente aqui que reside a maior oportunidade deste novo quadro regulatório: ao obrigar as organizações a pensar sistematicamente sobre os seus riscos, a documentar as suas decisões e a envolver os seus órgãos de gestão neste processo, o Decreto-Lei n.º 125/2025 cria as condições para que a cibersegurança deixe de ser uma preocupação exclusiva das equipas técnicas e passe a ser uma prioridade intrínseca de toda a organização, sem exceção.

Não menos importante é o reconhecimento de que este exercício não se esgota no momento da entrada em vigor do regime. A conformidade não é um estado que se atinge e se mantém automaticamente – é um processo contínuo,

que exige revisão, atualização e adaptação permanentes. O panorama de ameaças muda, as tecnologias evoluem e as organizações transformam-se. Um plano de cibersegurança que era adequado há dois anos pode não o ser hoje.

Neste sentido, o momento que atravessamos, marcado por uma crescente instabilidade geopolítica e por uma dependência cada vez maior das infraestruturas digitais, não podia ser mais oportuno para esta clarificação de responsabilidades. A cibersegurança é, hoje, uma questão de Estado, mas também de cada empresa individualmente, de cada gestor e de cada colaborador que, no seu dia a dia, toma decisões que podem ter consequências muito além do que se imagina.

O novo regime tem, assim, o mérito de evidenciar aquilo que os profissionais de cibersegurança já reconhecem há muito tempo: a cibersegurança não é um fim em si mesmo, mas sim um meio para garantir a estabilidade, e essa estabilidade começa na cultura e, subsequentemente, essa cultura deve ser promovida pela gestão de topo.

Essencialmente, o valor do Regime Jurídico da Cibersegurança mede-se fora do regime sancionatório e esse nem sempre é o espírito das empresas que estão abrangidas por este regime. Os próximos meses serão decisivos para percebermos se a NIS2 cumprirá o seu objetivo primordial ou se, pelo contrário, devem os legisladores europeus começar a preparar uma nova Diretiva NIS3. ◀



**“PROTEGER OS DADOS NÃO É UM OBJETIVO
TÉCNICO, MAS UMA CONDIÇÃO DE
CONTINUIDADE DO NEGÓCIO”**

► MARTA QUARESMA FERREIRA

A ORAMIX DEFENDE UMA ABORDAGEM À CIBERSEGURANÇA CENTRADA NA PROTEÇÃO DOS DADOS, NUM CONTEXTO DE AUMENTO DAS AMEAÇAS E EXIGÊNCIAS REGULATÓRIAS. A SOFISTICAÇÃO DOS ATAQUES E A PRESSÃO DA NIS2 REFORÇAM A POSIÇÃO DA SEGURANÇA COMO UMA PRIORIDADE ESTRATÉGICA PARA AS ORGANIZAÇÕES.

A gestão de risco e compliance, a tecnologia e engenharia, aliada sempre às pessoas e ao *user awareness*, são os três pilares que integram a abordagem da Oramix à cibersegurança. A empresa de IT, especializada na gestão de dados e na transformação digital, conta com 25 anos de presença no mercado, com clientes nos mais diversos verticais, entre eles saúde, banca, seguros, indústria, administração pública e serviços.

“A nossa filosofia *“Data Security First”* parte de uma convicção simples: os dados são o ativo mais valioso de qualquer organização e, por isso, a sua proteção deve ser tratada como uma prioridade estratégica e não como uma camada adicional”, começa por explicar Carlos Caldeira, Cybersecurity Manager & CISO da Oramix.

DADOS: O ALVO A PROTEGER

Com um panorama de cibersegurança a evoluir “de forma significativa”, o especialista afirma que os dados continuam a ser o “alvo comum” para a maioria dos atuais incidentes de segurança, que contam agora com uma ajuda “extra” – a Inteligência Artificial (IA) –, utilizada até pelos próprios atacantes.

Seja sob a forma de ataques ransomware, campanhas ou exfiltração de informação, o Cybersecurity Manager reitera que “é nos dados que reside o verdadeiro objetivo dos atacantes”.

A mudança no mercado tem sido testemunhada pelo próprio integrador, que considera que o investimento feito pelas organizações em cibersegurança é hoje “mais consciente” e estratégico, com o tema a deixar de ser uma “responsa-

bilidade exclusiva das equipas técnicas” para passar a constar da “agenda das administrações”.

CORRESPONDER ÀS EXIGÊNCIAS DO MERCADO

Apesar da entrada de novos *players* e, consequentemente, de um leque de soluções mais alargado, Carlos Caldeira defende que, na hora de escolher um parceiro, os critérios das organizações mantêm-se inalterados: a receita inclui conhecimento técnico, maturidade e capacidade de entrega comprovada, que se traduz, no fim da linha, em confiança e parcerias mais fortes.

A evolução do mercado português tem criado uma maior maturidade nos clientes, que chegam à Oramix com ideias concretas e com uma noção de segurança de um ponto de vista estratégico e não apenas técnico. O CISO reitera que esta “mudança de postura” tem acelerado a adoção de Managed Security Service Provider (MSSP), o que se traduz numa externalização da gestão de segurança. A escas-



sez de recursos humanos especializados em cibersegurança tem empurrado igualmente para a adoção deste tipo de modelos, com os clientes à procura de “parceiros a quem possam confiar a gestão da sua segurança de forma contínua, libertando as suas equipas internas para iniciativas mais estratégicas”.

NOVAS AMEAÇAS OBRIGAM A OLHAR MAIS AMPLO

A experiência acumulada em projetos de segurança permite à Oramix endereçar o leque de exi-

gências impostas pelos diversos setores onde atua, onde se inclui a adoção de uma “abordagem verdadeiramente integrada”. Na visão do Carlos Caldeira, as organizações necessitam “de uma visão end-to-end, que cubra tecnologia, processos e pessoas, e que seja capaz de responder com velocidade quando um incidente ocorre”. Questões como o alargamento da superfície de ataque, a adoção de infraestruturas cloud e o trabalho remoto culminaram em “novos vetores” que contribuíram para “tornar o conceito de perímetro de segurança tradicional obsoleto”.

Outras tendências que marcam igualmente o atual panorama de cibersegurança incluem ataques à cadeia de abastecimento, que “obrigam as empresas a olhar para a segurança de forma mais sistémica e não apenas para dentro”, e o ímpeto da IA, que ocorre hoje nos dois sentidos. “Se, por um lado, os atacantes a utilizam para lançar campanhas mais sofisticadas e difíceis de detetar, por outro as organizações e os integradores recorrem cada vez mais à IA para automatizar a deteção de ameaças, acelerar

▼
 "HOJE, A
 CONSCIENCIALIZAÇÃO
 SOBRE O POTENCIAL DE UM
 INCIDENTE DE SEGURANÇA
 OCORRE SOBRETUDO NUMA
 LÓGICA DE “QUANDO”
 E NÃO DE “SE”, O QUE
 LEVA AS ORGANIZAÇÕES
 A ALOCAREM PARTE
 DO INVESTIMENTO NAS
 ÁREAS DE RESPOSTA E
 RECUPERAÇÃO"

a resposta a incidentes e reduzir a dependência de intervenção humana em tarefas repetitivas. É uma corrida tecnológica que veio para ficar”, garante o CISO.

O PESO DA EXIGÊNCIA REGULATÓRIA

O cumprimento de normas e diretivas, como a NIS2 e o RGPD, conquistaram um lugar prioritário e de destaque no negócio. No caso da Oramix, os clientes chegam “cada vez mais preparados, com perguntas mais precisas e expectativas mais elevadas”. Na perspectiva do especialista, o aumento do nível de maturidade tem-se refletido de forma positiva em todo o ecossistema.

No que diz respeito à transposição e à entrada em vigor da NIS2, a organização conta com uma equipa dedicada para acompanhar este “processo exigente”.

A abordagem inicia-se com um *assessment* técnico que vai permitir à Oramix compreender “onde cada organização se encontra face aos requisitos do Decreto-Lei 125/2025”. Este diagnóstico primordial assenta na metodologia do Quadro Nacional de Referência para a Cibersegurança e está igualmen-

te alinhado com os critérios definidos pelo Centro Nacional de Cibersegurança. Segue-se depois a definição de um plano de implementação desenhado à medida da empresa. “A resiliência é peça principal nesta nova lei, e inclui não só um plano de resposta a desastres, mas também um plano de continuidade de negócio, assente em recursos humanos, tecnologia e recursos físicos na resposta a um incidente, permitindo a uma organização responder de uma forma adequada”, explicita o Manager.

A oferta da Oramix inclui ainda o acompanhamento da cadeia logística e de parceiros, bem como um conjunto de serviços complementares, desde formação e *user awareness*, pentesting, *CSIRT* as a service, e uma plataforma integrada que cruza a gestão de vulnerabilidades com a gestão de riscos. “É esta visão de acompanhamento *end-to-end*, do diagnóstico à operação, que diferencia a abordagem da Oramix de uma resposta puramente consultiva ou exclusivamente tecnológica. O objetivo é que a NIS2 não seja tratada como uma *checklist*, mas como uma oportunidade para construir uma postura de segurança mais robusta e sustentável”.

A CONSCIENCIALIZAÇÃO DA SEGURANÇA COMO UM TODO

Dado o atual contexto, Carlos Caldeira não tem dúvidas da criticidade dos dados e da importância de integrarem o centro da estratégia de segurança das organizações: “proteger os dados não é um objetivo técnico, mas sim uma condição de continuidade do negócio”.

O Cybersecurity Manager & CISO defende que as organizações devem “resistir à tentação” de resolver as questões de segurança apenas com recurso à tecnologia, uma vez que, relembra, “nenhuma solução tecnológica, por mais avançada que seja, é suficiente por si só”.

Há, no entanto, uma outra mensagem importante a reter: a cibersegurança não deve ser tida e vista apenas como um “tema exclusivo das equipas de IT”. Aqui enquadram-se também os colaboradores como potenciais portas de entrada para ataques, sendo necessário “construir uma cultura de segurança sustentável”, que implica o investimento em “formação e na consciencialização das pessoas, de forma contínua e não apenas reativa”.



A exigência do atual quadro regulatório tira o foco exclusivo das equipas de IT e responsabiliza também as administrações pelas falhas de segurança. Para a Oramix, este é um sinal de que “a segurança tem de estar na agenda dos conselhos de administração, com a mesma seriedade com que se tratam os riscos financeiros ou operacionais”.

De uma forma geral, o atual mercado de cibersegurança e a experiência da Oramix permitem concluir que “o foco deixou de estar exclusivamente

na prevenção”. Carlos Caldeira sublinha que, hoje, a consciencialização sobre o potencial de um incidente de segurança ocorre sobretudo numa lógica de “quando” e não de “se”, o que leva as organizações a alocarem parte do investimento nas áreas de resposta e recuperação. A par das vantagens de uma abordagem *Zero Trust*, os planos de business continuity, disaster recovery e simulações de incidentes são agora parte integrante das agendas de segurança das organizações. ◀



#29 ABRIL 2026

OBRIGADO POR TER LIDO A

IT^{Insight} SECURITY

Se ainda não é um leitor registado da IT Insight Security e para ter acesso a todo o nosso conteúdo registe os seus dados profissionais [aqui](#)

Conheça a política de privacidade da IT Insight Security [aqui](#)

IT^{Insight} SECURITY

PUBLISHER: Jorge Bento

DIRETOR : Rui Damião - rui.damiao@medianext.pt

ANCHOR: Henrique Carreiro

COORDENADORA EDITORIAL: Marta Quaresma Ferreira

REDAÇÃO: Inês Garcia Martins, Flávia Gomes

BUSINESS DEVELOPMENT:

Catarina de Brito - (+351) 910 121 200 - catarina.brito@medianext.pt

João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt

MARKETING & EVENTS DIRECTOR:

Rosa Bento - rosa.bento@medianext.pt

MARKETING COMMUNICATIONS:

Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt

ARTE E PAGINAÇÃO: Teresa Rodrigues

FOTOGRAFIA: Luciano Reis

DESENVOLVIMENTO WEB: Global Pixel

COLABORARAM NESTE NÚMERO: Cristiane Dias, Mafalda de Brito Fernandes

CEO: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116 Linda-a-Velha, Portugal

TEL: (+351) 214 147 300 | **FAX:** (+351) 214 147 301

REGISTO E.R.C

Entidade Reguladora para a Comunicação Social n° 127602

Consulte [aqui](#) o Estatuto Editorial

PROPRIEDADES E DIREITOS

A propriedade do título “IT Insight Security” é de MediaNext Lda., uma empresa Jornalística registada da Entidade Reguladora da Comunicação Social com o n° 224011 e NIPC 510 551 866. Proprietários com mais de 5% de Capital Social: Margarida Bento e Pedro Botelho. Todos os direitos reservados. A reprodução do conteúdo (total ou parcial) sem permissão escrita do editor é proibida. O editor fará todos os esforços para que o material mantenha fidelidade ao original, não podendo ser responsabilizado por gralhas ou erros gráficos surgidos. As opiniões expressas em artigos assinados são da inteira responsabilidade dos seus autores.

O IT Insight Security e a MediaNext utilizam as melhores práticas de privacidade sobre dados pessoais e empresariais. Os dados fornecidos para uso exclusivo do serviço de assinantes do IT Insight Security não serão cedidos a qualquer entidade terceira. As informações sobre leitores constantes na base de dados de subscritores do site www.itsecurity.pt estão protegidos pelas melhores práticas de segurança informática.

A REVISTA DIGITAL INTERATIVA IT INSIGHT SECURITY É EDITADA POR:
MediaNext Professional Information Lda.

PERIODICIDADE: Bimestral

IT Insight Security é membro de:



Editado por:

