

Desenvolver uma postura de segurança mais madura e resiliente

Benchmarking das melhores
práticas das operações de segurança





Índice

- P 3** Resumo executivo

- P 4** Uma responsabilidade claramente definida é a base da maturidade em segurança

- P 5** A visibilidade integrada transforma os dados de segurança em ação

- P 6** A capacidade de resposta contínua é um fator determinante da maturidade da segurança

- P 7** A deteção orientada por inteligência aumenta a confiança e melhora a priorização

- P 8** A IA está a acelerar o imperativo da maturidade

- P 9** Uma resposta testada e automatizada transforma a preparação em resiliência

- P 10** O ransomware expõe a diferença entre preparação e resiliência

- P 11** Desenvolver uma postura de segurança mais madura através de operações de segurança adaptativas

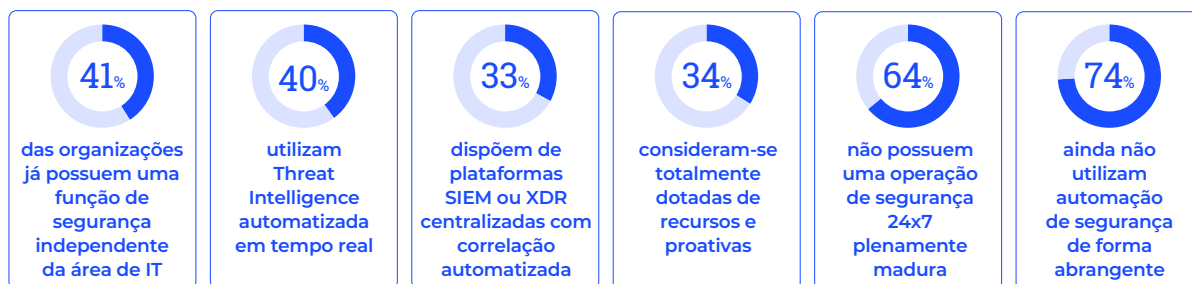
Sobre o relatório

O mais recente relatório de cibersegurança da Logicalis baseia-se em 357 respostas de profissionais de IT e segurança de organizações da região EMEA e Ásia-Pacífico. O estudo avalia o nível de maturidade nas capacidades que definem operações de segurança eficazes, incluindo governação, resposta 24x7, visibilidade, deteção, preparação para incidentes e acesso a conhecimento especializado externo, identificando as práticas que ajudam as organizações a reduzir as suas lacunas de maturidade.

Resumo Executivo

A cibersegurança está a entrar numa nova era operacional. A IA está a aumentar a velocidade, escala e adaptabilidade tanto dos ataques como das defesas, enquanto a crescente complexidade dos ambientes digitais dificulta a obtenção de visibilidade total. Neste contexto, consciência e investimento já não são suficientes. As organizações precisam de capacidade para detetar e responder continuamente, da maturidade necessária para coordenar pessoas, processos e tecnologia, e da resiliência para recuperar e adaptar-se quando ocorre um incidente.

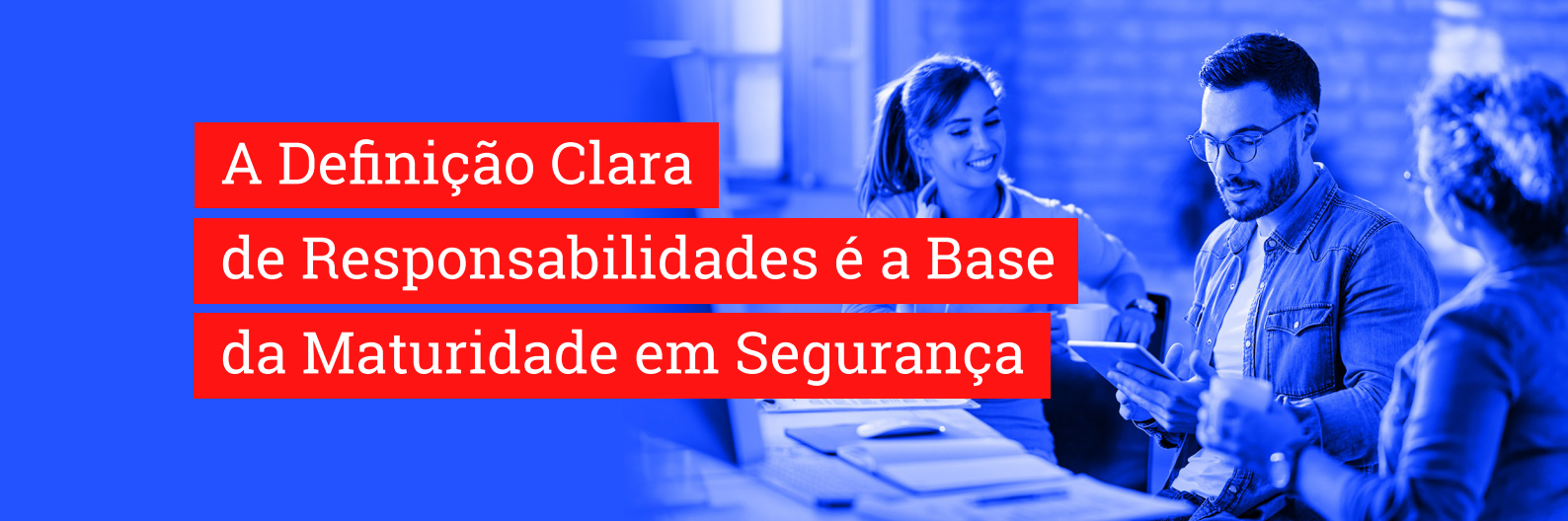
Com base em 357 respostas recolhidas em mercados-chave da EMEA e Ásia-Pacífico, os dados da Logicalis revelam progressos significativos, mas também uma lacuna persistente entre ambição e capacidade operacional:



Os resultados retratam um mercado em transição para níveis superiores de maturidade, e não apenas um cenário de subinvestimento. Muitas organizações estão a implementar os componentes da ciberdefesa moderna, mas ainda não os integraram num modelo operacional contínuo e orientado por inteligência.

Os dados apontam para uma clara jornada de maturidade: estabelecer responsabilidade e capacidade, expandir a resposta para além do horário laboral, integrar visibilidade de ativos, telemetria e Threat Intelligence, testar e automatizar processos de resposta a incidentes e recorrer a especialistas externos para acelerar a evolução quando as competências internas são limitadas.

As organizações que estão a reduzir esta lacuna não se limitam a adquirir mais ferramentas. Estão a construir funções de segurança adaptativas, capazes de antecipar, agir, recuperar e aprender continuamente.



A Definição Clara de Responsabilidades é a Base da Maturidade em Segurança

A maturidade começa com a definição clara de responsabilidades. O estudo revela que muitas organizações estão a estabelecer maior responsabilização em matéria de cibersegurança: 41% dos inquiridos já operam com uma função de segurança claramente separada e um modelo próprio de governação, enquanto 24% possuem liderança dedicada à segurança, embora com alguma sobreposição com IT.

Em conjunto, isto significa que quase dois terços das organizações já começaram a distinguir a segurança das operações gerais de IT. O valor desta separação não está apenas na estrutura organizacional, mas também numa maior responsabilização, melhores mecanismos de governação e decisões mais rápidas quando surgem prioridades concorrentes ou incidentes críticos.

No entanto, 36% das organizações continuam a gerir a segurança principalmente através das equipas de IT. À medida que as ameaças evoluem, esta abordagem pode criar desafios. Apesar de 39% das organizações afirmarem gerir eficazmente as tarefas de segurança do dia a dia, muitas têm dificuldade em acompanhar a rápida evolução das ameaças.

39% das organizações afirmam gerir eficazmente as tarefas de segurança do dia a dia, mas têm dificuldade em acompanhar a rápida evolução das ameaças.

Apenas 34% consideram estar devidamente dotadas de recursos e preparadas para atuar de forma proativa, tanto na gestão operacional quotidiana como na resposta a novos riscos.

A dimensão das equipas também evidencia esta diferença de maturidade. Enquanto 28% das organizações contam com dez ou mais profissionais dedicados à segurança, 26% não possuem qualquer equipa de segurança dedicada, dependendo exclusivamente dos recursos de IT.

As organizações mais maduras abordam este desafio através da definição clara de responsabilidades, da proteção da capacidade especializada e da utilização de especialistas externos sempre que necessário. O objetivo não é criar equipas autónomas apenas por princípio, mas sim estabelecer um modelo operacional de segurança com responsabilidade definida, competências adequadas e autoridade para responder à evolução das ameaças.

A Visibilidade Integrada Transforma Dados de Segurança em Ação

A visibilidade é a base de uma segurança eficaz. Ainda assim, 45% das organizações continuam a manter inventários de ativos manualmente, enquanto apenas 1% dispõe de inventários totalmente automatizados.

Além disso, 14% têm apenas visibilidade parcial dos seus ativos e 8% não mantêm qualquer inventário.

70% das organizações não possuem visibilidade completa nem gestão automatizada de ativos.

Isto significa que cerca de 70% das organizações não possuem visibilidade completa nem gestão automatizada de ativos, dificultando a compreensão do risco, a priorização de vulnerabilidades e a resposta rápida a incidentes.

A visibilidade de ativos vai muito além da manutenção de registos atualizados. Sem uma visão clara sobre ativos distribuídos por ambientes cloud, aplicações SaaS, endpoints remotos e third-party environments, torna-se impossível avaliar corretamente a exposição ao risco ou verificar a eficácia dos controlos de segurança.

As organizações mais maduras tratam o inventário de ativos como uma fonte contínua de inteligência de segurança, associando cada ativo ao respetivo proprietário, criticidade de negócio e nível de risco.

O mesmo desafio verifica-se na monitorização de segurança. Embora 33% das organizações utilizem plataformas SIEM ou XDR centralizadas com capacidades de correlação automatizada, a maioria continua a enfrentar limitações ao nível da visibilidade. Cerca de 27% dispõem de soluções SIEM ou XDR, mas com visibilidade limitada, 24% recolhem logs sem conseguir correlacioná-los de forma eficaz e 14% ainda dependem de logs armazenados localmente.

Por outras palavras, 65% das organizações não dispõem de uma telemetria de segurança totalmente integrada e automatizada, limitando a sua capacidade de deteção e resposta. As organizações mais maduras vão além da simples recolha de dados. Conectam telemetria de todo o ambiente, enriquecem-na com informação sobre ativos e inteligência de ameaças, e utilizam automação para transformar sinais dispersos em ações prioritárias.



A capacidade de resposta contínua é um fator determinante da maturidade da segurança

A capacidade de responder de forma contínua continua a ser um desafio para muitas organizações. Embora 36% dos inquiridos indiquem dispor de operações de segurança totalmente operacionais 24 horas por dia, 7 dias por semana, com equipas dedicadas, 64% ainda não possuem essa capacidade. Entre estas, 17% dependem de equipas de prevenção em regime rotativo, 31% conseguem monitorizar a atividade fora do horário de expediente, mas têm capacidade limitada de resposta, e 16% não monitorizam nem respondem ativamente após o horário laboral.

31% das organizações conseguem monitorizar a atividade fora do horário de expediente, mas têm uma capacidade de resposta limitada.

Os dados evidenciam uma distinção clara e importante entre visibilidade e prontidão operacional. Monitorizar a atividade fora do horário de expediente é valioso, mas, sem a capacidade de investigar e responder rapidamente, as organizações continuam expostas a ameaças em constante evolução. Os 31% que conseguem monitorizar, mas têm uma capacidade de resposta limitada, ilustram bem este desafio. Podem identificar potenciais incidentes, mas não dispõem dos recursos, processos ou capacidade operacional necessários para agir de forma consistente quando surge um risco.

A atividade maliciosa nunca para, e a maturidade da segurança é cada vez mais definida pela capacidade de responder, e não apenas de detetar. As organizações com operações de segurança mais maduras combinam monitorização contínua com processos de resposta claramente definidos, recursos especializados e capacidade de atuação a qualquer momento. Com quase dois terços dos inquiridos ainda sem operações 24x7 plenamente maduras, os dados sugerem que alargar a capacidade de resposta para além do horário laboral tradicional continua a ser um passo crítico para reduzir o fosso na maturidade da cibersegurança.

A Detecção Orientada por Inteligência Aumenta a Confiança e a Capacidade de Priorização

A adoção de Threat Intelligence está a ganhar cada vez mais relevância. Atualmente, 40% das organizações recorrem a feeds automatizados de inteligência de ameaças em tempo real, enquanto 30% dependem de relatórios periódicos, 18% recolhem informação de forma ad hoc e apenas 12% não possuem qualquer capacidade de threat intelligence.

40% das organizações recorrem a feeds automatizados de inteligência de ameaças em tempo real.

O próximo passo passa por integrar esta inteligência nas decisões diárias de segurança, nas investigações e nas atividades de resposta a incidentes.

As capacidades de deteção também estão a evoluir. Cerca de 28% das organizações utilizam deteção comportamental baseada em IA e 45% combinam deteção baseada em assinaturas com deteção de anomalias, o que significa que 73% já ultrapassaram as abordagens tradicionais assentes exclusivamente em assinaturas. Ainda assim, 14% continuam a depender maioritariamente deste método e outros 14% não dispõem de capacidades dedicadas de deteção de ameaças.

O maior desafio continua a ser a confiança nos resultados obtidos. Apenas 28% das organizações afirmam ter um elevado grau de confiança na capacidade de distinguir ameaças reais de falsos positivos, enquanto 43% revelam apenas uma confiança moderada e 29% admitem ter dificuldades em identificar ameaças genuínas ou em lidar com o elevado volume de falsos positivos.

As organizações mais maduras respondem a este desafio através da combinação de inteligência de ameaças, análise comportamental e automação, reduzindo o ruído operacional e permitindo que as equipas concentrem o seu conhecimento e capacidade de decisão nos riscos que realmente importam.



A IA Está a Acelerar o Imperativo da Maturidade

O estudo retrata um momento decisivo para as organizações. A importância estratégica da IA resulta da capacidade dos sistemas agênticos realizarem sequências complexas de tarefas, analisarem código e adaptarem fluxos de trabalho a um ritmo que reduz drasticamente o tempo entre a descoberta de uma vulnerabilidade e a sua exploração.

Assim, a preparação em segurança deve ser avaliada através de uma nova questão: a organização consegue compreender e interromper um ataque que evolui à velocidade das máquinas?

A IA pode apoiar atividades como a investigação de incidentes, a correlação de eventos, a identificação de vulnerabilidades e a resposta a tarefas de rotina, enquanto as pessoas continuam a assegurar a supervisão, a capacidade de decisão e a responsabilização.

Esta realidade não elimina a importância da intervenção humana. Apenas altera o local onde essa intervenção cria maior valor. A IA pode apoiar atividades como a investigação de incidentes, a correlação de eventos, a identificação de vulnerabilidades e a resposta a tarefas de rotina, enquanto as pessoas continuam a assegurar a supervisão, a capacidade de decisão e a responsabilização. As organizações mais bem preparadas para esta nova fase serão aquelas que conseguirem combinar uma telemetria abrangente, automação inteligente, orquestração governada e analistas especializados numa função de segurança capaz de aprender, adaptar-se e evoluir continuamente.



Uma resposta testada e automatizada transforma a preparação em resiliência

A detecção só gera valor quando as organizações conseguem responder de forma eficaz. 40% das organizações dispõem de um plano de resposta a incidentes regularmente testado, mas 60% ainda não contam com uma capacidade de resposta totalmente validada. Entre estas, 27% têm um plano que não é testado regularmente, 16% trabalham com planos desatualizados e 17% não possuem qualquer plano formal.

São os testes regulares que transformam um plano numa verdadeira capacidade de resiliência.

40% das organizações dispõem de um plano de resposta a incidentes regularmente testado

A mesma lacuna é visível nos processos de resposta. Apenas 33% das organizações dispõem de playbooks de resposta a incidentes completos, enquanto 35% possuem documentação parcial e 32% dependem de processos ad hoc ou não têm playbooks definidos.

A automação representa outro desafio significativo. Apenas 26% das organizações utilizam automação de forma extensiva nos seus processos de resposta a incidentes, o que significa que 74% ainda não tiram partido da automação de forma abrangente. Em concreto, 35% recorrem a níveis limitados de automação e 39% continuam a operar maioritariamente através de processos manuais.

À medida que os ataques se tornam mais rápidos e sofisticados, as organizações mais maduras apostam em planos testados, playbooks bem definidos e automação devidamente governada para responder de forma rápida, consistente e escalável.



O ransomware expõe a lacuna entre preparação e resiliência

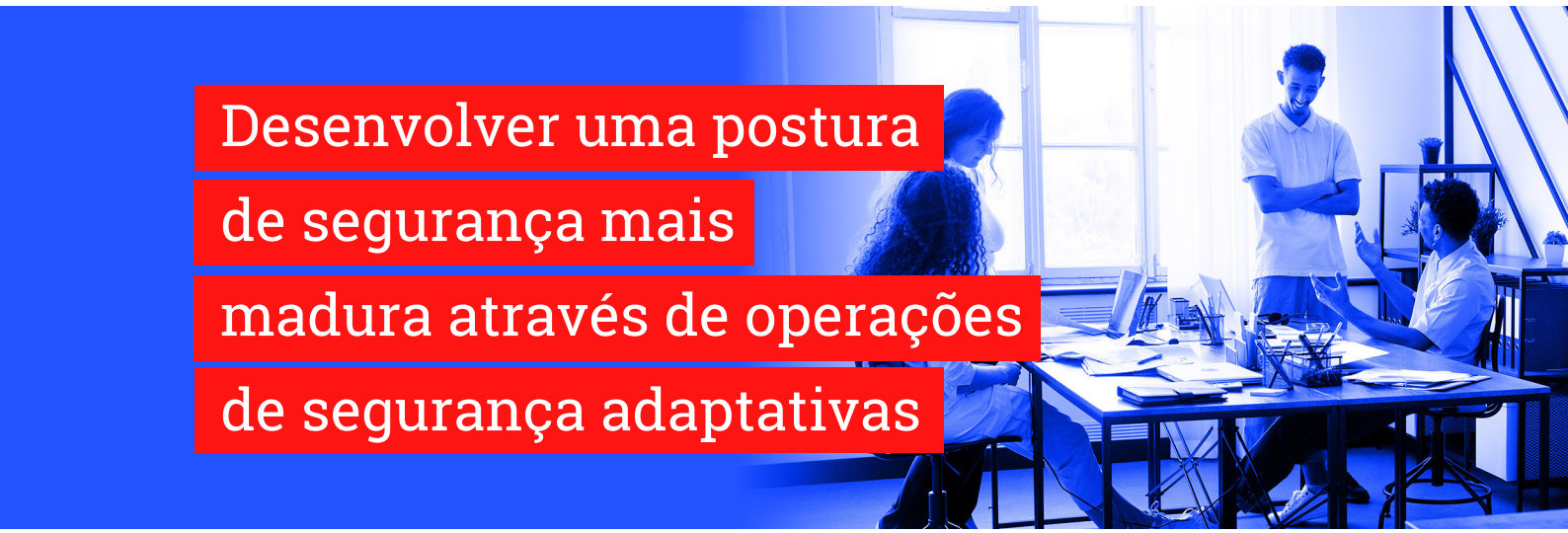
O ransomware constitui um dos testes mais exigentes à resiliência organizacional. Apenas 36% dos inquiridos consideram estar totalmente preparados para enfrentar um ataque de ransomware. Por outro lado, 38% afirmam estar moderadamente preparados, mas reconhecem a existência de lacunas, enquanto 26% admitem ter uma preparação limitada ou inexistente. Isto significa que quase dois terços das organizações não têm total confiança na sua capacidade de responder eficazmente a um ataque de ransomware. As boas práticas vão muito além da prevenção e da deteção. Exigem capacidades comprovadas de contenção, estratégias de backup fiáveis, prioridades claras de recuperação e decisões de negócio previamente definidas sobre a continuidade das operações em cenário de crise.

Quase dois terços das organizações não têm total confiança na sua capacidade de responder eficazmente a um ataque de ransomware

41% não têm seguro ou ainda estão a avaliar opções

O ciberseguro, por si só, não substitui estas capacidades. 32% das organizações dispõem de uma cobertura abrangente, 27% possuem uma cobertura limitada e 41% não têm seguro ou ainda estão a avaliar opções. Embora o seguro possa ajudar a mitigar parte do impacto financeiro, não consegue restaurar sistemas, preservar a confiança dos clientes, nem tomar decisões críticas durante um incidente. Por isso, a verdadeira resiliência operacional tem de ser construída antes de qualquer necessidade de acionar uma apólice.





Desenvolver uma postura de segurança mais madura através de operações de segurança adaptativas

A procura por serviços de segurança geridos continua a crescer. 34% das organizações acreditam que um serviço de MXDR melhoraria os tempos de resposta e a eficácia operacional, enquanto 28% o veem como uma extensão valiosa da sua equipa de segurança. Além disso, 25% reconhecem o seu valor, embora manifestem preocupações relacionadas com visibilidade e capacidade de resposta.

No total, 87% dos inquiridos reconhecem o papel positivo, ou potencialmente positivo, dos serviços geridos de SOC e MXDR, enquanto apenas 13% acreditam que estes serviços reduzem o controlo ou tornam a resposta mais lenta. Esta tendência reflete uma necessidade crescente de apoio especializado que vai além da monitorização e da gestão de alertas. As organizações procuram parceiros capazes de combinar cobertura 24x7, conhecimento especializado, inteligência de ameaças, automação e capacidade de resposta rápida.

Para prestadores de serviços de segurança como a Logicalis, a oportunidade não passa apenas pela externalização das operações de segurança, mas também por ajudar os clientes a reforçar as suas próprias capacidades. Os parceiros mais eficazes funcionam como uma extensão da equipa do cliente, melhorando a visibilidade, a capacidade de resposta e a resiliência, sem comprometer a transparência nem o controlo.

Com 87% dos inquiridos a reconhecem o papel positivo, ou potencialmente positivo, dos serviços geridos de SOC e MXDR, o mercado demonstra estar preparado para um modelo de segurança adaptativo, capaz de operar à velocidade das máquinas, mantendo as pessoas no centro da tomada de decisão.

87% dos inquiridos reconhecem o papel positivo, ou potencialmente positivo, dos serviços geridos de SOC e MXDR.

Somos Architects of Change™. Ajudamos as organizações a prosperar num mundo digital-first. Na Logicalis, colocamos a nossa experiência tecnológica coletiva ao serviço dos nossos clientes, ajudando-os a desenhar um blueprint para o sucesso, para que possam alcançar resultados sustentáveis com impacto real.

Enquanto provider global de serviços tecnológicos, disponibilizamos soluções baseadas em IA, concebidas para garantir fiabilidade e escalabilidade, nas áreas de cloud, conectividade, colaboração e segurança.

A nossa equipa de cerca de 7.000 especialistas, presente em 30 países, apoia mais de 10.000 clientes de diversos setores de atividade, capacitando-os para alcançar resultados sustentáveis através da tecnologia.

A Logicalis regista receitas anuais de cerca de 1,7 mil milhões de dólares, com operações na Europa, América do Norte, América Latina, Ásia-Pacífico e África. Integra o grupo Datatec Limited, cotado na Bolsa de Joanesburgo, com receitas superiores a 3,7 mil milhões de dólares.

pt.logicalis.com