Buddy Email

**Capacitar as equipas de segurança na era dos agentes de IA com o Microsoft Sentinel**

* **Microsoft apresenta uma nova vaga de inovação em segurança, disponibilizando uma plataforma agêntica para proteger organizações em escala.**

**Lisboa, 03 de outubro de 2025** – Estamos numa era de transformação na forma como as organizações trabalham e se defendem. Em todos os setores, estão a surgir “*Frontier Firms*”, isto é, organizações onde humanos e agentes de Inteligência Artificial (IA) colaboram em tempo real para resolver problemas, inovar e construir estruturas resilientes.

Para as equipas de segurança, esta mudança traz novas oportunidades, bem como desafios. A complexidade e velocidade das ciberameaças modernas exigem soluções que vão além das ferramentas tradicionais. Para responder a estas necessidades, a Microsoft está a introduzir novas capacidades de segurança agêntica, concebidas para capacitar as equipas de segurança a inovar de forma ousada e segura nesta nova era da IA.

**Microsoft Sentinel: A plataforma de segurança para a era dos agentes de IA**

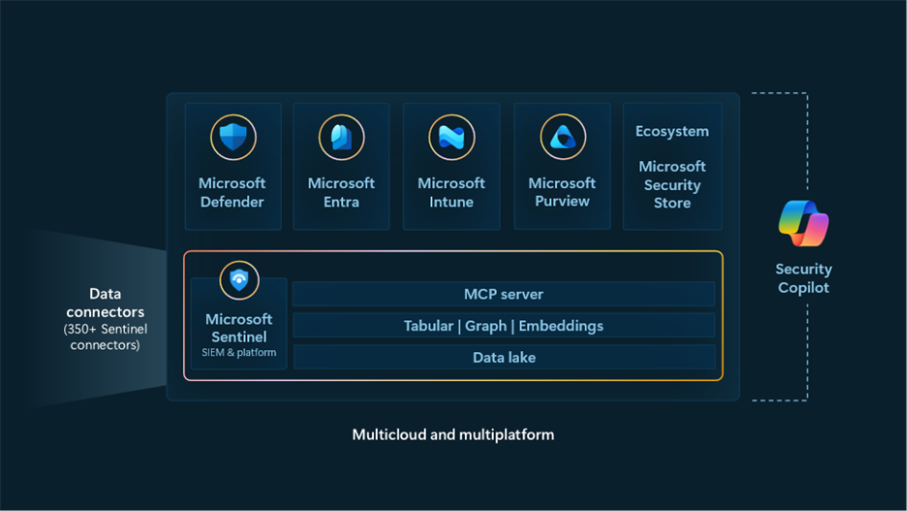
As equipas de segurança precisam de proteger a IA em toda a cadeia de valor e, para isso, necessitam de uma plataforma que reúna dados, contexto, automatização e agentes inteligentes, permitindo-lhes defender e adaptar-se à velocidade da IA. Essa plataforma é o [Microsoft Sentinel](https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel).

O Sentinel surgiu como uma solução de gestão de informação e eventos de segurança (SIEM) nativa na *cloud* e, [em julho, passou a incluir também um *data lake* de segurança unificado](https://www.microsoft.com/en-us/security/blog/2025/07/22/microsoft-sentinel-data-lake-unify-signals-cut-costs-and-power-agentic-ai/). Hoje, evolui para uma plataforma agêntica com a [disponibilidade geral da *data lake* do Sentinel](https://aka.ms/sentinel/datalake/gablog) e a *public preview* do [Sentinel Graph](https://aka.ms/sentinel/graph/techblog) e do [servidor Sentinel Model Context Protocol (MCP)](https://aka.ms/sentinel/mcp/techblog).  Com contexto baseado em gráficos, acesso semântico e orquestração agêntica, o Sentinel oferece às equipas de segurança uma plataforma única para receber sinais, correlacionar domínios e capacitar agentes de IA integrados no Security Copilot, no VS Code através do GitHub Copilot ou noutras plataformas para *developers*.

O Sentinel recebe sinais, estruturados ou semiestruturados, e constrói uma compreensão profunda e contextual do seu património digital através de dados de segurança vetorizados e relações baseadas em gráficos. Ao integrar estes *insights* com o Microsoft Defender e o Microsoft Purview, o Sentinel acrescenta um contexto potenciado por gráficos para as ferramentas que as equipas de segurança já utilizam, ajudando-as a monitorizar trajetórias de ataque, compreender o impacto e priorizar a resposta — tudo dentro dos fluxos de trabalho conhecidos.

“Com o Microsoft Security e o *data lake* do Sentinel, unificámos silos, escalámos operações, automatizámos processos e expandimos o alcance, transformando a forma como detetamos padrões e nos preparamos para o futuro com uma postura de segurança unificada e ágil.” afirma **Bernard Knaapen, Chief Product Owner, Monitoring and Incident Response da Microsoft**.

O Sentinel também organiza e enriquece os dados de segurança, adaptando-os para os agentes de IA detetarem problemas mais rapidamente, investigarem com maior clareza e responderem automaticamente quando necessário. E a [abordagem baseada em gráficos do Sentinel](https://aka.ms/sentinel/graph/techblog) permite que os agentes do Security Copilot raciocinem sobre o seu ambiente com precisão e velocidade, graças ao servidor MCP incorporado, que utiliza padrões abertos para facilitar o acesso e ação dos agentes. Para equipas avançadas, o servidor MCP do Sentinel permite extensibilidade para agentes predefinidos e personalizados, permitindo raciocínio potenciado por IA sobre dados unificados. Isto transforma a segurança reativa em preditiva, ajudando as equipas a antecipar ameaças e automatizar respostas em escala.



O Sentinel é aberto e extensível, permitindo que parceiros construam os seus próprios agentes e soluções. E com a [Microsoft Security Store](https://aka.ms/securitystore/techblog), encontrar e implementar estes agentes é simples. A Microsoft já está a colaborar com a Accenture, ServiceNow e Zscaler [para reforçar o ecossistema de segurança em conjunto](https://aka.ms/sentinel/isvblog).

O Sentinel é uma solução SIEM líder na indústria e a espinha dorsal escalável que as equipas de segurança necessitam na era da IA. Em conjunto, o Sentinel e o Security Copilot oferecem às equipas de segurança a visibilidade, automatização e escala necessárias para se manterem à frente das ciberameaças.

**O Security Copilot permite criar agentes individuais, sem necessidade de código**

O Security Copilot foi criado para ajudar as equipas de segurança a enfrentar os desafios mais exigentes, tais como alertas incessantes, ferramentas isoladas e pressão constante para fazer mais com menos recursos.

Neste contexto, a ferramenta permite [criar agentes próprios](https://aka.ms/SCP-Secure-2509). O portal do Security Copilot inclui uma plataforma para a criação de agentes sem código que permite descrever as necessidades em linguagem natural e criar, otimizar e publicar agentes adaptados aos fluxos de trabalho de cada utilizador em minutos.

Também possibilita a criação de agentes numa plataforma de codificação com suporte para o servidor MCP do Sentinel, como o VS Code através do GitHub Copilot. Depois de criados, é possível aperfeiçoar e implementar os agentes no espaço de trabalho do Security Copilot de cada indivíduo, mantendo o processo dentro da plataforma de desenvolvimento.

Os agentes do Security Copilot foram concebidos para se integrarem nas ferramentas e fluxos de trabalho diários, quer estejam incorporados nos produtos Microsoft Security já utilizados, naqueles criados por parceiros ou personalizados para o contexto de cada utilizador.

Desde o lançamento dos [agentes do Security Copilot, em março de 2025](https://techcommunity.microsoft.com/blog/SecurityCopilotBlog/automate-cybersecurity-at-scale-with-microsoft-security-copilot-agents/4394675/), a Microsoft já disponibilizou [mais de uma dúzia de agentes](https://aka.ms/mechanics-scp-agents) para cenários como triagem de *phishing* e otimização de acesso condicional. Além disso, a empresa continua a adicionar agentes incorporados, como o  [Access Review Agent no Microsoft Entra](https://techcommunity.microsoft.com/blog/microsoft-entra-blog/the-microsoft-entra-agent-for-smarter-access-governance-access-review-agent/4279689). Os agentes criados pela Microsoft e respetivos parceiros já estão disponíveis para teste, aquisição e implementação na Security Store.

Com base no contexto gráfico do Sentinel, os agentes do Security Copilot conseguem raciocinar de forma mais eficaz sobre o ambiente de cada utilizador, correlacionando alertas, enriquecendo o contexto com relações, priorizando pelo impacto e automatizando ações comuns. Isto permite menos falsos positivos, uma triagem mais rápida e menor tempo médio de resolução (MTTR). O trabalho passa de triagem manual para fluxos de trabalho liderados por agentes, que organizam e automatizam tarefas rotineiras, enquanto os analistas revêm e aprovam os resultados, focando-se em decisões estratégicas e sinalização proativa de ameaças.

**Proteger e controlar a IA de forma global**

À medida que as organizações adotam a IA, a Microsoft continua a investir em ferramentas que ajudam as equipas de segurança a proteger e controlar as suas plataformas, aplicações e agentes de IA em toda a organização.

Nos últimos meses, a Microsoft expandiu as capacidades de *Security for IA*, nomeadamente através do [Entra Agent ID](https://techcommunity.microsoft.com/blog/microsoft-entra-blog/announcing-microsoft-entra-agent-id-secure-and-manage-your-ai-agents/3827392), para ajudar a descobrir e gerir o património de agentes; de controlos para evitar a partilha excessiva de [dados em aplicações e agentes de IA personalizados](https://techcommunity.microsoft.com/blog/microsoft-security-blog/enterprise-grade-controls-for-ai-apps-and-agents-built-with-azure-ai-foundry-and/4414757); de ferramentas de descoberta de riscos para fornecedores de modelos de IA e [servidores MCP](https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/discover-risks-in-ai-model-providers-and-mcp-servers-with-microsoft-defender/4440050); e de deteção avançada de ataques por introdução de *prompts*

No Microsoft Build 2025, a empresa anunciou novas melhorias no Azure AI Foundry que oferecem mais proteção para agentes de IA ao longo do seu ciclo de vida. Estas melhorias estarão disponíveis em breve e incluem:

* Controlo de adesão à tarefa do agente para garantir alinhamento em tempo real
* Barreiras para proteção de informações pessoalmente identificáveis (PII)
* Capacidade de destaque de mecanismos de segurança de *prompt* para reforçar a proteção contra ataques de introdução cruzada de *prompts.*

Estas inovações ajudam a proteger e controlar as aplicações e agentes de IA no Microsoft 365 Copilot, Copilot Studio e Azure AI Foundry, permitindo aos utilizadores construir sobre ferramentas de confiança que as suas equipas já utilizam e oferecendo proteções nativas para as plataformas de IA da Microsoft.

**A segurança é um trabalho de equipa**

Estamos a entrar numa nova era onde a segurança é adaptativa, inteligente e atua à velocidade do pensamento. Os avanços anunciados hoje são os pilares para a construção de uma nova geração de defesa.

A Microsoft acredita que a segurança é um trabalho de equipa que inclui cada um dos utilizadores em prol da inovação, aprendizagem e defesa contra ameaças em conjunto.

**CONTACTOS**

|  |  |  |
| --- | --- | --- |
| **Catarina Brito** | **Inês Filipe** |  |
| [catarina.brito@lift.com.pt](mailto:catarina.brito@lift.com.pt) | [ines.filipe@lift.com.pt](mailto:ines.filipe@lift.com.pt) |  |
| 914 310 661 | 910 283 054 |  |

**SOBRE A MICROSOFT**

Microsoft (Nasdaq "MSFT" @microsoft) cria plataformas e ferramentas robustecidas por Inteligência Artificial para entregar soluções inovadoras que correspondam às necessidades crescentes dos nossos clientes. Enquanto empresa de tecnologia está comprometida com a democratização do acesso a Inteligência Artificial de forma responsável, mantendo a missão de capacitar todas as pessoas e organizações no planeta para atingir mais.