CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 05/10

08:30 - 09:10 REGISTER & WELCOME COFFEE

09:20 - 09:30 EVENT OPENING

09:30 - 10:10

David Cass

Global Chief Information Security Officer | Speaker, Educator, Advisor

KEYNOTE

When AI Meets the Courtroom: Building Trustworthy AI Systems Through Legal and Technical Governance

As organizations race to embed AI into their products, platforms, and decision-making pipelines, a critical question often goes unanswered until it's too late: what happens when AI systems fail, produce harmful outputs, or become the subject of litigation?

This session, led by David Cass–bridges the gap between AI engineering and the legal frameworks now shaping how AI is built, deployed, and defended in court. David will walk attendees through the real-world legal risks that product teams, CTOs, and AI engineers face today.

Key takeaways include:

- AI in litigation: How courts are evaluating AI-generated evidence, model outputs, and synthetic media–and the technical standards emerging from these rulings.
- Dispute-ready architecture: Practical engineering decisions (logging, versioning, documentation) that protect AI products when disputes arise.
- The JAMS AI Rules framework: A first look at the dispute resolution rules purpose-built for AI conflicts–covering IP infringement, data privacy breaches, synthetic content misuse, and LLM-related trade secret claims.
- Governance as competitive advantage: How proactive AI governance (cybersecurity audits, compliance frameworks, board-level oversight) reduces risk and accelerates enterprise adoption.

Whether you're building AI products, leading engineering teams, or advising executive stakeholders, this session delivers the practical legal and technical intelligence you need to ship AI that's not only powerful–but defensible.

10:10 - 10:30

Erik de Lopes Morais

Co-Founder & COO

Penso | veeam

Data Protection & Disaster Recovery

Governe a IA sem bloquear a inovação: o novo perímetro é o prompt

Como proteger dados e governar o uso da IA generativa sem limitar seu potencial? Uma visão prática sobre Shadow AI, DLP, resiliência de dados e os novos desafios de segurança em um cenário onde o prompt se tornou parte do perímetro corporativo.

10:30 - 11:05

Allan Muller Buscarino

Gerente Sênior I Banco Bradesco

Arthur Paixão

Head of Cybersecurity I Einstein Hospital Israelita

Lucas Santos

BISO LATAM I Mercado Livre

Davi Gardin

Superintendente de Engenharia de Software I Itaú Unibanco

Security by Design: protegendo aplicações na era dos agentes e da IA de fronteira

A ascensão da inteligência artificial está transformando profundamente a forma como software é desenvolvido, testado e operado. Modelos de IA de fronteira e agentes autônomos aceleram a inovação, mas também introduzem novos riscos relacionados à segurança de aplicações, à governança de código, à proteção de dados e à confiabilidade dos sistemas.

Neste cenário, o Security by Design deixa de ser apenas uma prática de engenharia para se tornar uma estratégia essencial de gestão de riscos. O desafio do CISO é garantir que a segurança acompanhe a velocidade da inovação, incorporando controles desde a concepção das aplicações e fortalecendo a colaboração entre segurança, engenharia e negócio.

Nesta seção, serão discutidos os impactos da IA no ciclo de desenvolvimento de software, os novos vetores de ataque, o papel da segurança de aplicações em ambientes orientados por agentes e as estratégias que permitirão às organizações inovar com confiança, resiliência e escala.

SPONSORS:

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 05/10

11:05 - 11:25

Rafael Santos
CISO
AZION

Your Next Privileged User Isn't Human

Passamos décadas protegendo identidades humanas. Agora teremos agentes de IA acessando APIs, bancos, código, infraestrutura, pipelines e tomando decisões.

11:25 - 12:00

Julio Concilio
Global Information Security Leader I Braskem

Grace Meireles
CISO I Aegea Saneamento

Daniel Botelho
CISO I Axia Energia

Cleber Guimarães Ferreira
CISO | Klabin

Infraestrutura crítica brasileira: onde estaria nosso Volt Typhoon?

Os ataques mais perigosos já não são, necessariamente, os que causam impacto imediato, mas aqueles que permanecem invisíveis por meses, comprometendo silenciosamente ambientes críticos e aguardando o momento certo para agir. Em um cenário marcado por tensões geopolíticas, ameaças patrocinadas por Estados e ataques cada vez mais sofisticados, a proteção da infraestrutura crítica deixou de ser apenas uma preocupação operacional para se tornar uma questão de segurança nacional e continuidade dos negócios.

Este painel discutirá como organizações responsáveis por serviços essenciais estão se preparando para enfrentar esse novo cenário de ameaças. O debate abordará estratégias para fortalecer a resiliência cibernética, aumentar a visibilidade sobre ambientes de TI e OT, proteger sistemas industriais, aprimorar a detecção de ameaças avançadas, responder a incidentes de grande impacto e garantir a continuidade das operações críticas. Um encontro para discutir como líderes de segurança podem antecipar riscos, fortalecer a colaboração entre setores e preparar suas organizações para um ambiente em que a indisponibilidade deixou de ser apenas um problema tecnológico e passou a representar um risco estratégico para o país.

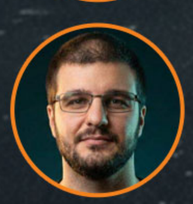
12:00 - 13:35 LUNCH / ALMOÇO

13:45 - 14:20

Fernando Bruno
Superintendente de Segurança Cibernética | Bradesco

Leonardo Muroya
CISO | Banco BMG

George S. Silva
CISO | Banco Industrial do Brasil



Fernando Polla
Head of Cyber | Superintendent Santander

20 anos de evolução em detecção. O atacante ainda entra. O que precisa mudar agora?

Nas últimas duas décadas, a cibersegurança avançou significativamente em tecnologias de detecção, monitoramento e resposta. Ainda assim, os ataques continuam acontecendo, explorando não apenas vulnerabilidades técnicas, mas identidades, pessoas, processos, terceiros e decisões de negócio. Este painel propõe uma reflexão sobre o que realmente precisa mudar na estratégia de segurança: estamos reduzindo riscos ou apenas aumentando nossa capacidade de enxergá-los? Com a chegada da IA e de novas formas de automação, a discussão se torna ainda mais urgente: estamos diante de uma oportunidade para repensar o modelo de segurança ou apenas acelerando abordagens que já mostraram seus limites? A conversa reunirá líderes para discutir priorização, redução de exposição, efetividade dos investimentos e como construir uma estratégia mais resiliente, adaptável e conectada aos riscos reais do negócio.

14:20 - 14:35

Daniel Ortiz
Regional Sales Manager
Ping Identity

Escalando IA com Confiança: Estratégias de Identidade para a Era da IA Agêntica

Seus agentes de IA são identidades não-humanas atuando de forma autônoma. Como você sabe em quem confiar? Descubra como provisionar, governar e monitorar milhares de agentes autônomos sem sacrificar segurança ou compliance. A IA agêntica já está aqui - você está preparado?

SPONSORS:

okta · Penso Data Protection & Disaster Recovery · veeam · AZION · CROWDSTRIKE · SecOffice A DAREDE COMPANY · perforce Delphix · Ping Identity · knowbe4 · iTeam fazendo diferente · Akamai · ManageEngine · OAKMONT GROUP · NSFOCUS · ABSOLUTE · SecurityScorecard · VIWSEC · RAPIDA · Netconn driven by passion

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 05/10

14:35 - 14:50

Rafael Borges
Regional Director LATAM
perforce Delphix

DevSecOps na Era da IA AgênticaDados seguros e prontos, na velocidade que a IA agêntica exige

A IA agêntica já está dentro dos pipelines de desenvolvimento e trouxe ganhos inéditos de velocidade, mas também um alerta vermelho para segurança e qualidade. Com 41% do código sendo gerado por IA e 45% contendo vulnerabilidades, a pressão por entregar rápido coloca em risco dados sensíveis e modelos consolidados há décadas. Nesta palestra, vamos mostrar por que o gargalo agora está nos dados e como líderes podem adotar automação inteligente, proteção de dados pessoais e práticas de DevSecOps para garantir segurança e compliance sem frear a inovação. Prepare-se para entender como tornar dados seguros, rápidos e prontos para IA, no ritmo que o negócio exige.

14:50 - 15:20

Fernando Ortega Ferasoli
Chief Information Security Officer I CISO na Paschoalotto Serviços Financeiros

Thomaz Russi
CEO & Founder
iTeam fazendo diferente

Fernando Ceolin
Regional Vice President
Akamai

Agente contra Agente: a IA já ataca em escala. A defesa ainda pede aprovação

A inteligência artificial está transformando o ataque cibernético em uma operação cada vez mais automatizada. Reconhecimento, engenharia social, geração de pretextos, exploração e movimentação dentro dos ambientes podem ser acelerados por agentes capazes de executar diferentes etapas com níveis crescentes de autonomia. O resultado é uma mudança fundamental na velocidade e na escala das operações ofensivas.

Do outro lado, grande parte das decisões críticas de defesa ainda mantém o humano no loop – por razões legítimas: auditoria, requisitos regulatórios, risco de falsos positivos, impacto operacional e responsabilidade sobre as decisões tomadas. Surge, assim, uma nova assimetria: enquanto o adversário automatiza a ação, a defesa ainda precisa avaliar, aprovar e assumir o risco de responder.

Ao mesmo tempo, uma nova superfície começa a ganhar relevância. Navegadores e agentes de IA passam a executar ações em nome dos usuários, interagindo com aplicações, APIs, sessões e identidades legítimas. Nesse cenário, distinguir automação autorizada de comportamento malicioso passa a exigir novas abordagens de identidade, contexto, proteção da superfície digital e resposta em tempo real.

Neste painel, líderes discutirão onde a automação defensiva já pode avançar, quais decisões ainda devem permanecer sob controle humano e quem assume a responsabilidade quando uma máquina decide bloquear, conter ou interromper uma operação.

A questão central deixa de ser apenas tecnológica e passa a ser também de governança e tolerância a risco:

Se o atacante automatizou a decisão, até onde estamos dispostos a automatizar a defesa?

15:20 - 16:05 COFFEE-BREAK

SPONSORS:

okta · Penso Data Protection & Disaster Recovery · veeam · AZION · CROWDSTRIKE · SecOffice A DAREDE COMPANY · perforce Delphix · Ping Identity. · knowbe4 · iTeam fazendo diferente · Akamai · ManageEngine · OAKMONT GROUP · NSFOCUS · ABSOLUTE · SecurityScorecard · VIWSEC · RAPID7 · Netconn driven by passion

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 05/10

16:15 - 16:50

Wellington Capitani

CISO | ZAMP SA

Amaro Neto

CISO | Afpergs HED HRSJ

Mayara Guerrini

Information Security and Technology Risk Manager | iFood

Franklin Cavalcante

CISO I Grupo OLX

IA no C-Level: entre a promessa e o risco – o que todo executivo de segurança precisa decidir em 2026

A inteligência artificial está redefinindo a forma como organizações operam, desenvolvem produtos, tomam decisões e gerenciam riscos. Ao mesmo tempo em que promete ganhos inéditos de produtividade e inovação, também pode amplificar vulnerabilidades quando aplicada sobre processos pouco conhecidos, dados de baixa qualidade e modelos de governança ainda imaturos.

Nesse contexto, a grande decisão do C-Level não é apenas onde investir em IA, mas como evitar que ela acelere processos que a organização ainda não compreende, não governa e não controla. O desafio deixou de ser exclusivamente tecnológico e passou a ser uma questão de liderança, governança e gestão de riscos.

Neste painel, líderes discutirão como transformar a IA em uma vantagem competitiva sem comprometer a resiliência, a conformidade e a confiança. O debate abordará temas como governança de IA, agentes autônomos, automação inteligente, gestão de riscos, qualidade dos dados, accountability, segurança por design, critérios para adoção de fornecedores e o papel do C-Level na construção de organizações preparadas para inovar com responsabilidade.

Mais do que discutir ferramentas, este painel propõe uma reflexão sobre as decisões estratégicas que definirão quais organizações conseguirão acelerar a transformação digital preservando aquilo que mais importa: a confiança.

16:50 - 17:05

TBD

TBD

TBD

17:05 - 17:25

Rodrigo Raiher

Executivo de Segurança da Informação | Head de Segurança | Especialista em Gestão de Riscos Cibernéticos

KEYNOTE

Quando o alvo é a confiança: cibersegurança na era da IA

A sociedade digital foi construída sobre uma infraestrutura que raramente enxergamos: a confiança. Confiamos em identidades, sistemas, transações, informações, organizações e, cada vez mais, em decisões mediadas por inteligência artificial. Mas o que acontece quando essa confiança pode ser manipulada em escala?

Nesta talk, proponho uma reflexão sobre segurança cibernética a partir de uma perspectiva diferente: o verdadeiro alvo de muitos ataques não é apenas a tecnologia, mas a confiança que depositamos nela.

Partindo da mentalidade do atacante, vamos explorar como engenharia social, fraude, comprometimento de identidade, manipulação de informações e inteligência artificial estão ampliando a capacidade de explorar relações de confiança. O impacto deixa de ser apenas tecnológico e passa a atingir empresas, infraestruturas críticas e a própria sociedade.

Mais do que proteger sistemas, o próximo grande desafio da segurança será preservar a confiança na era digital.

SPONSORS:

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 05/10

17:25 - 18:10

João Passos
CISO | Brasilseg

Christian Coutinho
Superintendente de Segurança | B3

Rogerio Silveira
CISO I Conta Azul

Jorge Gomes
Chief Information Security Officer I CISO

Willlians Santos
CISO I Banco Carrefour

O Elo Invisível: risco de terceiros e supply chain de software no Brasil – quando o ataque entra pela porta do fornecedor

A crescente digitalização dos negócios ampliou a dependência de fornecedores, parceiros, plataformas em nuvem, bibliotecas de código e serviços terceirizados. Hoje, poucas organizações desenvolvem ou operam seus ambientes de forma totalmente independente. Nesse contexto, a cadeia de fornecimento digital tornou-se uma das maiores superfícies de ataque para empresas de todos os setores.

Os ataques à supply chain de software demonstram que basta comprometer um único elo para impactar centenas ou milhares de organizações simultaneamente. Ao mesmo tempo, a expansão do uso de componentes open source, APIs, provedores de identidade, soluções SaaS e fornecedores estratégicos amplia o desafio de garantir visibilidade, controle e confiança em um ecossistema cada vez mais distribuído.

Neste painel, líderes de segurança discutirão como fortalecer a gestão de riscos de terceiros em um cenário onde o perímetro tradicional deixou de existir. O debate abordará estratégias para avaliação contínua de fornecedores, segurança da cadeia de desenvolvimento de software, gestão de dependências, monitoramento de riscos, requisitos contratuais, resiliência operacional, resposta a incidentes envolvendo parceiros e os novos desafios impostos pela crescente adoção de inteligência artificial em produtos e serviços de terceiros.

Mais do que proteger a própria organização, o desafio passa a ser construir uma cadeia de confiança capaz de reduzir riscos sistêmicos e fortalecer a resiliência de todo o ecossistema digital.

18:10 ENCERRAMENTO

18:15 - 19:15 HAPPY HOUR

SPONSORS:

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 06/10

08:30 - 09:10 REGISTER & WELCOME COFFEE

09:20 - 09:30 EVENT OPENING

09:30 - 10:15

Amanda Kollmorgan

Security Architect | Veolia North America Defensive Cybersecurity Operations Element I Wisconsin Army National Guard

KEYNOTE

Ctrl + Alt + Lead: Rebooting Cyber Culture with Human Skills When Trust is Under Attack, Human Capability is the Layer That Holds

The industry has spent decades investing in tools, frameworks, and controls. Budgets have grown. Sophistication has grown. And yet the outcomes of a real incident still turn on something less visible: whether the humans in the room trust each other enough to speak plainly, escalate quickly, and decide under pressure.

This keynote reframes the human side of cybersecurity as strategic infrastructure. Not a support function. Not the "people" line item at the bottom of the org chart. Load-bearing infrastructure; the layer that determines whether the tools we buy and the frameworks we adopt actually perform when it counts. When this layer is weak, technical excellence cannot compensate. When it is strong, ordinary teams produce extraordinary outcomes.

Drawing on nearly twenty years across federal and state government service, Amanda Kollmorgan names the specific human capabilities that decide incident outcomes: psychological safety on technical teams, conflict without eroded trust, mentorship that grows judgment, communication that survives pressure, and leadership that operates from any seat regardless of title.

In an environment where trust itself has become the target, the message is direct: the layer many programs have been treating as optional is the layer everything else runs on. The human side of cyber is not soft. It is structural. And it is the most strategically underweighted investment in most cyber programs today.

10:15 - 10:35

Weberton Souza

Head of Security na Darede

SecOffice A DAREDE COMPANY | CROWDSTRIKE

Visibilidade, política e comprometimento. A cadeia do prompt à execução.

Anatomia de um ataque à camada agêntica e o ponto onde o controle precisa existir.A autorização de um agente de IA acontece em uma política. A execução acontece em arquivos, credenciais e chamadas de rede. A sessão percorre os três elos dessa cadeia, da visibilidade sobre os agentes em operação até o comprometimento real, e examina onde o controle precisa existir para que a governança deixe de ser declarativa.

10:35 - 11:10

Cássio Menezes

CISO I Grupo Amil

Arthur Magalhães

CISO | Rede D'Or São Luiz

Leandro Ribeiro

CISO | Hospital Sírio-Libanês

Lucio Comanche

CISO | A.C.Camargo Cancer Center

A Nova Agenda da Cibersegurança na Saúde: protegendo um ecossistema cada vez mais conectado

A transformação digital está redesenhando o setor de saúde. Hospitais, laboratórios, plataformas digitais, dispositivos médicos, fornecedores e diferentes agentes do ecossistema estão cada vez mais conectados, ampliando oportunidades de inovação, mas também criando novas dependências e superfícies de risco.

Nesse cenário, o papel da cibersegurança também está mudando. Proteger dados e sistemas continua sendo essencial, mas já não é suficiente. Líderes de segurança precisam participar das decisões sobre novas tecnologias, compreender riscos que atravessam toda a cadeia de saúde e criar condições para que inovação, conectividade e proteção avancem de forma sustentável.

Neste painel, executivos discutirão quais riscos e prioridades estão redefinindo a agenda de cibersegurança na saúde, passando por temas como Inteligência Artificial, identidade, terceiros, dispositivos e ambientes conectados, proteção de dados e governança.

SPONSORS:

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 06/10

11:10 - 11:30

Caetano Becker
AE Enterprise
okta

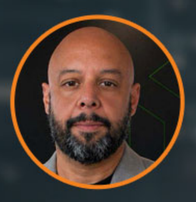
Evandro Macahuba
Director of Identity Management and Operations at ySec

Plataformas de Identidade: A Okta Protege a IA

À medida que a Inteligência Artificial transforma os negócios, a segurança da identidade torna-se fundamental. Nesta sessão, descubra como as soluções de plataforma da Okta protegem a infraestrutura, os dados e os fluxos de trabalho impulsionados por IA, garantindo acesso seguro e mitigando novas ameaças no ecossistema digital.

11:30 - 12:00

Silvio Hayashi
Chief Information Security Officer
CISO



Gilberto Mota
Chief Information Security Officer
Grupo Sada

Lucas Correa
Gerente de Cyber Security e Segurança da Informação
GOL Linhas Aéreas

Resiliência Cibernética e Confiança Digital em Ambientes Críticos

Em um cenário de ameaças cibernéticas cada vez mais sofisticadas e da crescente dependência de infraestruturas digitais, a resiliência cibernética tornou-se um elemento estratégico para garantir a continuidade dos negócios e a confiança de clientes, parceiros e da sociedade. Mais do que prevenir ataques, as organizações precisam estar preparadas para resistir, responder e se recuperar rapidamente de incidentes, preservando a integridade de seus serviços e operações.

Este painel discutirá como líderes de cibersegurança estão fortalecendo a confiança digital em ambientes críticos por meio de estratégias de resiliência, gestão de riscos, governança, proteção de infraestruturas essenciais e adoção de novas tecnologias. Os participantes compartilharão desafios, experiências e boas práticas para construir organizações mais preparadas para enfrentar um cenário de ameaças em constante evolução, equilibrando segurança, inovação e continuidade operacional.

12:00 - 12:20

Raquel Tortoretti
Superintendente de Prevenção a Fraudes, Segurança da Informação e Operações | Livelo

A convergência entre Prevenção à Fraude e Segurança na proteção do negócio

A evolução tecnológica vem transformando não apenas os negócios, mas também a forma como as fraudes são planejadas e executadas. Ataques cada vez mais sofisticados exploram identidades, credenciais, vulnerabilidades e engenharia social, aproximando definitivamente os universos de Prevenção a Fraudes e Cibersegurança.

Nesta palestra, vamos discutir como essa convergência vem acontecendo na prática e por que uma atuação integrada entre as duas disciplinas se tornou essencial para uma estratégia de proteção mais efetiva. A partir de experiências e aprendizados do dia a dia, serão compartilhadas práticas para aproximar times, dados, tecnologias e processos, ampliando a capacidade de prevenção, detecção e resposta às ameaças.

Mais do que integrar áreas, o desafio é construir uma visão única de risco e proteção, acompanhando a velocidade com que as ameaças e o próprio comportamento dos fraudadores estão evoluindo.

12:20 - 13:50 LUNCH / ALMOÇO

SPONSORS:

okta · Penso Data Protection & Disaster Recovery · veeam · AZION · CROWDSTRIKE · SecOffice A DAREDE COMPANY · perforce Delphix · Ping Identity. · knowbe4 · iTeam fazendo diferente · Akamai · ManageEngine · OAKMONT GROUP · NSFOCUS · ABSOLUTE · SecurityScorecard · VIWSEC · RAPID7 · Netconn driven by passion

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 06/10

14:00 - 14:30

Fernando Madureira
Corporate Global CISO | Credicorp

Felipe Prado
Head of Artificial Intelligence & Cyber Analytics | Credicorp

Rafael Narezzi
Chairman | Grupo SUMMIT

Em um grupo de empresas com negocios distintos, quem está no comando? Liderança, IA e as decisões que definirão o futuro da cibersegurança

Como definir estrategia associado a efiencia e efetividade para um grupo de empresas com negocios distintos. A Inteligência Artificial já não é apenas uma ferramenta de apoio. Ela está influenciando decisões, automatizando operações e transformando a forma como as organizações protegem seus ativos, gerenciam riscos e conduzem seus negócios. Nesse cenário, uma pergunta torna-se inevitável: quem está realmente no comando?

À medida que a IA assume um papel cada vez mais estratégico, cresce também a responsabilidade da liderança em definir limites, estabelecer governança e garantir que inovação, segurança e objetivos de negócio avancem na mesma direção. Afinal, quais decisões podem ser delegadas à tecnologia? E quais continuarão sendo exclusivamente humanas? Como encontrar o equilibrio entre centralizar capacidades de cyber versus dar a autonomia com cada empresa do grupo?

Reunindo uma perspectiva de liderança global, construída à frente de programas de cibersegurança em organizações multinacionais, e uma visão prática sobre estrategia e corporativizaçao de um conglomerado de empresas, a aplicação da Inteligência Artificial neste conexto, este painel discutirá como líderes estão equilibrando estratégia, tecnologia e tomada de decisão para construir organizações mais resilientes, acelerar a inovação com responsabilidade e fortalecer a confiança em um cenário de transformação contínua.

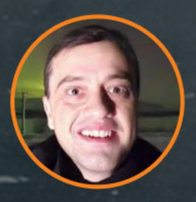
14:30 - 14:40

Rafael Peruch
Technical CISO Advisor
knowbe4

Humanos & Agentes de IA: Como fica a Gestão de Risco da nova força de trabalho hibrida

A força de trabalho moderna integra pessoas e agentes de IA – e qualquer um deles pode ser a causa do seu próximo incidente de segurança. Como líder em cibersegurança, a KnowBe4 resolve esse desafio protegendo a força de trabalho digital ao oferecer, de forma integrada: simulação de ataques, treinamentos de conscientização, segurança em ferramentas de colaboração e proteção para agentes de IA.

14:40 - 15:00



Igor Hjelmstrom Vinhas Ribeiro
Engineering Director | iFood

Ataques de agentes em enxame: quais mudanças fundamentais eles provocam na defesa de cibersegurança e como reagir?

TBD

SPONSORS:

okta · Penso Data Protection & Disaster Recovery · veeam · AZION · CROWDSTRIKE · SecOffice A DAREDE COMPANY · perforce Delphix · Ping Identity. · knowbe4 · iTeam fazendo diferente · Akamai · ManageEngine · OAKMONT GROUP · NSFOCUS · ABSOLUTE · SecurityScorecard · VIWSEC · RAPIDN · Netconn driven by passion

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 06/10

15:00 - 15:30

Andre Tritapepe
CISO | Cogna Educação

Rafaela Galvão
SEO/GEO, Content & Digital Marketing
ManageEngine

Renato Jager
Chief Technology Officer
OAKMONT GROUP

Jason Fielding-Tweedie
Sales Manager
ABSOLUTE

Você Não Usa IA. Mas Seus Fornecedores Usam

Sua empresa pode ter políticas rígidas para o uso de Inteligência Artificial, ferramentas homologadas e controles sobre quais plataformas podem acessar dados corporativos. Mas existe uma nova variável fora do seu perímetro: a IA utilizada pelos seus fornecedores.

APIs e integrações que foram aprovadas para conectar parceiros, plataformas SaaS e sistemas corporativos agora podem estar sendo consumidas por agentes de IA capazes de consultar dados, correlacionar informações, construir contexto e executar ações em uma escala que talvez não existisse quando aquele acesso foi originalmente autorizado.

Isso cria uma pergunta crítica para CISOs e líderes de tecnologia:

Quando sua empresa autorizou o fornecedor a acessar seus dados, também autorizou os agentes de IA dele?

Neste painel, discutiremos como Agentic AI, APIs, identidades não humanas (NHI) e terceiros estão criando uma nova camada de risco para as organizações – e colocando em xeque modelos tradicionais de acesso, identidade, governança e Third-Party Risk Management.

Como saber se quem está consumindo uma API é uma pessoa, uma aplicação ou um agente autônomo? Uma autorização concedida a um fornecedor continua válida quando muda a forma como ele utiliza e processa os dados? E quem assume a responsabilidade quando o agente pertence ao terceiro, mas os dados e o impacto pertencem à sua organização?

Em um ambiente no qual sistemas começam não apenas a acessar informações, mas também a interpretá-las e agir sobre elas, controlar quem tem acesso já não é suficiente.

A próxima fronteira da segurança será controlar também o que máquinas autorizadas podem fazer em nome de terceiros.

15:30 - 16:00 COFFEE-BREAK

15:00 - 15:30

Thiago Cunha
VP Trust, Security & Financial Crime - LATAM | Dock

Rodrigo Colossi
CISO and Head of Financial Crime Prevention | Banco BV

Marcelo Henrique Leite Ferreira
CISO | Banco do Brasil

Redesenhando a Confiança: o novo modelo de segurança no sistema financeiro

A transformação digital, a inteligência artificial, a evolução das fraudes e a crescente interconexão do ecossistema financeiro estão redefinindo o conceito de confiança. Em um cenário em que bancos, bolsas, fintechs, meios de pagamento e reguladores compartilham responsabilidades, a segurança deixa de ser apenas um mecanismo de proteção e passa a ser um elemento essencial para garantir a continuidade dos negócios, a estabilidade do mercado e a confiança dos clientes.

Este painel reunirá líderes do setor financeiro para discutir como as organizações estão adaptando seus modelos de segurança diante de novos desafios, como identidades digitais, agentes de IA, fraudes cada vez mais sofisticadas, ataques à cadeia de suprimentos, resiliência operacional e exigências regulatórias. Um debate sobre como construir um modelo de segurança mais inteligente, integrado e resiliente, capaz de acompanhar a velocidade da inovação sem comprometer a confiança que sustenta o sistema financeiro.

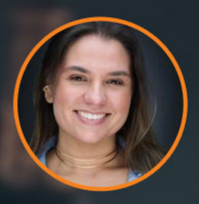
SPONSORS:

okta · Penso Data Protection & Disaster Recovery · veeam · AZION · CROWDSTRIKE · SecOffice A DAREDE COMPANY · perforce Delphix · Ping Identity. · knowbe4 · iTeam fazendo diferente · Akamai · ManageEngine · OAKMONT GROUP · NSFOCUS · ABSOLUTE · SecurityScorecard · VIWSEC · RAPID7 · Netconn driven by passion

CYBER SECURITY SUMMIT 2026 | 10TH EDITION

KEYNOTE E GENERAL SESSION - 06/10

16:45 - 17:10



Tatiane Romano

CISO I Diretora de segurança da informação - Riachuelo

Como construir um time de alta performance em um cenário em que o adversário evolui todos os dias?

TBD

17:10 - 17:40

André Magalhães

Global Chief Information Security Officer | LATAM Airlines

KEYNOTE

O valor de conhecer nosso risco cibernético: da intuição à decisão

Esta apresentação compartilha aprendizados práticos sobre a adoção de uma metodologia de quantificação do risco cibernético. Aborda os principais mitos, desafios e barreiras culturais envolvidos em sua implementação, destacando que se trata de um programa contínuo e complementar aos modelos já existentes.

Também mostra como essa metodologia contribui para uma visão mais precisa e executiva dos riscos, permitindo priorizar recursos escassos e acelerar a tomada de decisões nos níveis de liderança.

17:40 - 18:00 ENCERRAMENTO, SAMEDAY VIDEO E SORTEIO

SPONSORS: