

KEYNOTE E GENERAL SESSION - 27/10

08:30 - 09:20 REGISTER & COFFEE BREAK

09:20 - 09:30 EVENT OPENING

09:30 - 09:40



Vitor Garcia

Global CIO - EMBRAER

KEYNOTE

Segurança como parceira estratégica do negócio

Esta apresentação explora o papel estratégico da cibersegurança nas organizações, analisando os fatores que a moldam hoje e seu impacto na construção do futuro dos negócios. A abordagem considera múltiplas dimensões - tecnológicas, humanas e organizacionais - que influenciam o tema, revelando suas complexidades e oportunidades. Mais do que uma estrutura de defesa, aqui a segurança é considerada motor de crescimento e inovação - deixando de ser apenas suporte operacional, para integrar decisões corporativas de forma ativa e estratégica.

09:40 - 10:00



Ivo Peixinho

Vice-Chair do Investigation Pillar
do Cybercrime Expert Goup
(CyberEx) da Interpol

Crimes Cibernéticos em tempos de Inteligência Artificial

A Inteligência Artificial tem promovido mudanças significativas na forma em que trabalhamos. A IA Generativa (Gen AI) tem acelerado a produção de documentos, a tradução de informações e o desenvolvimento de software, entre outros. Mas e os criminosos cibernéticos?

Nesta palestra serão apresentadas as últimas evoluções nos ataques cibernéticos no que tange a atual revolução da IA Generativa. Exemplos reais e potencialidades serão mostrados, além de oportunidades para defensores e investigadores de crimes cibernéticos.

10:00 - 10:25



Rogerio Rizzi

VP of Corporate Strategy - OKTA



O Papel Essencial da Identidade no Futuro Seguro da IA

A evolução da IA exige uma redefinição da segurança, colocando a identidade em primeiro plano. Este keynote aborda como as organizações podem construir o futuro da IA com segurança, focando na criação de experiências confiáveis e na gestão do crescente número de agentes de IA. Você conhecerá as abordagens para capacitar desenvolvedores a construir um agente de IA seguro e como a identidade atua como o framework para ver, gerenciar e proteger esses agentes em toda a sua organização.

10:25 - 10:50



Leandro Granja

CISO - Santander
MODERADOR



**Marcelo Henrique
Leite Ferreira**

CISO - Gerente Geral
Cibersegurança/Soluções de
Prevenção a Fraude/ Segurança
da Informação e LGPD -
Banco do Brasil

Cultura Anticrime: Como Criar um Ambiente onde o colaborador é o Primeiro Firewall

Mesmo com protocolos, MFA, e SIEMs avançados, um único colaborador comprometido pode abrir a porta para um ataque devastador. Em um cenário onde credenciais legítimas são exploradas com intenções ilegítimas, como cultivar uma cultura em que os próprios funcionários sejam agentes ativos da proteção?

Este painel explora como criar mecanismos de incentivo ético, canais anônimos de denúncia e programas de valorização da integridade.



Willians Santos

CISO - Banco Carrefour



Fernando Bruno

Superintendente de Cyber -
Bradesco

SPONSORS:



KEYNOTE E GENERAL SESSION - 27/10

10:50 - 11:15



**Thiago Madeira
de Lima**

CEO - Penso

Penso

Resiliência de Dados: Lições de Batalha contra Ameaças Potencializadas por IA

Inteligência artificial trouxe velocidade, escala e sofisticação inéditas aos ataques cibernéticos. Phishings hiperpersonalizados, deepfakes realistas e ataques em larga escala desafiam a segurança das organizações e colocam os dados como alvo prioritário dos criminosos.

Nesta palestra, Thiago Madeira de Lima, CEO da Penso Tecnologia, compartilha a trajetória da empresa ao longo de mais de 20 anos em resiliência de dados e apresenta como a combinação entre Veeam e estratégias avançadas de proteção, backup imutável e Disaster Recovery podem garantir a continuidade dos negócios em cenários críticos. A sessão trará insights práticos, exemplos reais e lições extraídas da experiência em batalhas contra ransomwares cada vez mais potencializados pela IA.

11:15 - 11:40



Juliana Pivari

Gerente de segurança da
informação - CIMED

Confiança Sob Ataque: Por que proteger sua marca é uma decisão cibernética

Em um mundo onde a marca é sinônimo de confiança e a confiança é construída (ou destruída) digitalmente, proteger a reputação vai além do marketing – é uma decisão crítica de cibersegurança. Essa palestra traz uma reflexão estratégica sobre como empresas que investem apenas em tecnologia, mas ignoram a blindagem da sua reputação digital, estão vulneráveis ao colapso de valor, confiança e mercado. Exploraremos:

Por que a confiança digital é o novo ativo mais valioso de uma organização

Casos reais onde o incidente cibernético destruiu a imagem em horas

O papel do CISO, do marketing e da diretoria na resposta de crise

Estratégias de brand protection aliadas à segurança cibernética

Como preparar sua empresa para responder a um ataque sem perder a narrativa.

11:40 - 12:05



Fernando Ortega

CISO - Paschoalotto

Fortalezas Digitais: E se proteger sua empresa fosse como defender um castelo medieval em pleno século XXI ou como um Médico apresentando diagnósticos de um corpo humano?

Entre muralhas invisíveis, ataques silenciosos e decisões críticas em tempo real, a Cibersegurança moderna exige mais que tecnologia: exige Estratégia de Guerra!

Nesta palestra, conduzida por um CISO com experiência em Guerra Cibernética e Resposta a Incidentes (Táticas de Guerrilha), mergulharemos em uma abordagem visual e técnica para projetar fortalezas digitais sob medida para cada tipo de negócio – combinando modelos arquitetônicos com analogias poderosas como castelos ingleses, o corpo humano e zonas de combate digital.

Explore conceitos como:

- Fossos e torres como Firewalls, WAFs e zonas de vigilância avançada (SIEM/UEBA);
- O corpo humano como arquitetura viva: autenticação como pele, dados como órgãos vitais, e o sistema imunológico como XDR e Zero Trust;
- Arquiteturas em camadas que unem segmentação de rede, Criptografia, Proteção de Endpoints, Gestão de Identidade e Automação de Resposta.
- Identidade perímetro funcional de ataque;
- Desenvolvimento Seguro e Security by Design;

A palestra também apresenta modelos de integração entre SOC e NOC, torres Network Security vs Blue Team e a importância de Salas de Guerra e Salas de Crise multidisciplinares em um olhar operacional, onde decisões severas precisam ser tão rápidas quanto seguras, onde mais que proteger Infraestruturas e Perímetros Cibernéticos, o foco real garantir a Alta Disponibilidade, proteger reputações, valor de marca e continuidade de negócios.

Com o dissolvimento dos Perímetros de Segurança, vide Cloud, SaaS, PaaS, IaaS, não existem apenas as fronteiras físicas, porém conceitos de fortalezas devem ser estrategicamente estudados, e estas precisam ser adaptativas e estratégicas.

12:05 - 13:45

LUNCH / ALMOÇO

SPONSORS:



okta



Data Protection & Disaster Recovery



ManageEngine



a CISCO company



an IBM Company



KEYNOTE E GENERAL SESSION - 27/10

13:45 - 14:05



Wellington Capitani
CISO - ZAMP

Liderança Digital em Tempos de Choque: Redefinindo Segurança com Confiança e Responsabilidade

A cada dia, a transformação digital acelera mais do que nossa capacidade de absorvê-la com segurança. Mas e se a segurança não fosse vista como obstáculo, e sim como direção que orienta a inovação? A verdadeira liderança digital nasce quando conseguimos equilibrar velocidade e resiliência, criatividade e responsabilidade. Segurança deixa de ser barreira para se tornar confiança, mais do que proteger sistemas, o desafio está em proteger o futuro: criando ambientes onde pessoas, tecnologia e negócios evoluem juntos.

14:05 - 14:25



Anthony Pierce
Splunk Field CTO for cybersecurity
and infrastructure - SPLUNK

splunk>
a CISCO company

Data Doesn't Have Borders, But You Do: Embrace the Fusion Center for Today's Digital World

Data does not have borders – but nations, companies, and people do. In today's global digital ecosystem, data moves freely across infrastructures that are not aligned to national or corporate borders. With the rapid expansion of cloud computing, your data may not even reside on your continent – yet it can, and must, be monitored and protected.

This session explores how achieving end-to-end visibility across your digital footprint is no longer optional: it's the foundation of resilience. We will examine how organizations can adopt a Fusion Center approach – integrating data, intelligence, and operational telemetry from across federal, state, local, tribal, territorial (SLTT), and private-sector partners – to build a shared threat picture, accelerate detection, and coordinate responses.

Participants will walk away with a practical framework for operationalizing end-to-end visibility using a fusion model: unifying disparate security, IT, and engineering data sources into a trusted information-sharing environment (ISE) to support mission outcomes, meet evolving GRC requirements, and counter emerging threats.

14:25 - 14:45



Rafael Ribeiro
Diretor de Pré-Vendas na Netbr

netbr



Alessandro Rossini
Solutions Engineer - SailPoint

SailPoint

A evolução da governança de identidade: agora com o poder da IA

A transformação digital trouxe novos desafios para a gestão de identidades e acessos, exigindo abordagens mais inteligentes, escaláveis e proativas. Neste cenário, a governança de identidade evolui para além dos controles tradicionais, incorporando o poder da Inteligência Artificial para oferecer visibilidade, contexto, automação inteligente e resposta ágil a riscos.

Será uma oportunidade para entender, na prática, como a combinação entre tecnologia de ponta e experiência local pode acelerar a maturidade em governança de identidade, reduzir riscos e fortalecer a confiança digital nos ambientes corporativos.

SPONSORS:



okta



Data Protection & Disaster Recovery



a CISCO company



an IBM Company



fazendo diferente



by Broadcom



See it. Secure it. Assess it.



KEYNOTE E GENERAL SESSION - 27/10

14:45 - 15:15



João Gilberto Passos
CISO - BrasilSeg, uma empresa
BB Seguros
MODERADOR



Thomaz Russi
CEO - iTeam
iTeam
fazendo diferente



Wilson Piedade
COB - Oakmont Group
OAKMONT
GROUP



Pedro Henrique Cheganças
Business Solutions Strategist
SEC4U semperis

Cibersegurança em Tempos de Fragmentação Geopolítica: Como Construir Confiança Local em um Mundo Hiperconectado

Vivemos uma era de contradições: enquanto as infraestruturas digitais estão cada vez mais interconectadas globalmente, a confiança e os dados estão sendo cada vez mais exigidos em âmbito local. Pressões geopolíticas, políticas de nacionalização de dados e o crescimento de regulamentações regionais estão transformando a forma como empresas estruturam suas operações de segurança cibernética.

Este painel reúne especialistas e líderes do setor para discutir como organizações ao redor do mundo estão redesenhando seus SOC's (Security Operations Centers), SIEMs (Security Information and Event Management) e arquiteturas de cibersegurança para se tornarem "Compliance Fit" – prontas para operar sob diferentes regimes regulatórios, mantendo eficiência, resiliência e confiança.

Abordaremos como a fragmentação digital está elevando os custos operacionais, exigindo decisões estratégicas sobre infraestrutura local versus serviços globais. Discutiremos ainda como tecnologias como IA, automação e threat intelligence local estão sendo utilizadas para enfrentar esses desafios, garantir soberania cibernética e atender as exigências de clientes multinacionais que agora priorizam fornecedores com conformidade local sólida.

Este painel é essencial para CISOs, líderes de SOC, reguladores, fornecedores de soluções e executivos que buscam entender como alinhar resiliência cibernética com estratégia geopolítica, em um mundo onde os dados cruzam fronteiras – mas a confiança não.

15:15 - 16:10

COFFEE BREAK

16:10 - 16:35



Jose Luiz Santana
CISO - C6 Bank
MODERADOR



Humberto Guimaraes
CISO - Banco BMG



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



Gabriel Borges
Global CISO - Banco BTG

Da Tempestade de Fraudes ao Laboratório Global de Inovação em Autenticação

O Brasil atravessa uma verdadeira tempestade de fraudes digitais: em 2024, os prejuízos decorrentes de golpes financeiros atingiram R\$ 10,1 bilhões, conforme relatório da Febraban.

Poder360

Esse montante elevadíssimo revela mais do que vulnerabilidade – revela um mercado criminoso em constante evolução, transformando o país em um laboratório global de inovação em autenticação e detecção antifraude.

A alta conectividade, a disseminação dos pagamentos instantâneos (como o Pix) e o comportamento digital intensificado criaram terreno fértil para a experimentação de novas técnicas de fraude. Não é por acaso que o Brasil passou a ser visto como incubadora de golpes – modelos criados ou refinados aqui tendem a "exportar" para outros países com algum atraso, conforme alertam especialistas.

Mercado&Consumo

Assim, da tempestade conspiram-se oportunidades: golpes sofisticados pressionam bancos, fintechs, reguladores e empresas de tecnologia a inovar em sistemas de verificação, autenticação biométrica, análise comportamental e orquestração de riscos. O resultado é paradoxal: enquanto criamos cada vez mais mecanismos defensivos, simultaneamente exportamos know-how (tanto criminoso quanto protetivo) para além das fronteiras.

SPONSORS:



KEYNOTE E GENERAL SESSION - 27/10

16:35 - 16:55



Rafael Borges

Regional Director Latam - Delphix



Dev/Test Sem Proteção é Aposta Perigosa. Escolha velocidade com segurança

Executivos investem pesado em segurança para ambientes de produção, mas é nos ambientes de desenvolvimento, teste e demais projetos que muitas vezes moram os maiores riscos: cópias de dados reais se acumulam, são multiplicadas e ficam sujeitas a controles frágeis. Nesse cenário, a busca por velocidade sem segurança se transforma em uma aposta perigosa, que expõe informações sensíveis, fragiliza a conformidade e compromete a qualidade dos testes.

Soluções caseiras, como scripts customizados, e a reutilização de tecnologias pensadas para produção falham em proteger, degradam a qualidade dos testes e ainda deixam trilhas reidentificáveis. O resultado: risco elevado, desperdício de recursos e dificuldade em conciliar agilidade com conformidade.

Vamos mostrar como é possível escolher velocidade com segurança em Dev/Test:

Por que controles de produção não bastam para não-produção

Como automatizar a descoberta de dados sensíveis em escala

De que forma aplicar mascaramento determinístico que preserva formato e integridade referencial.

Também compararemos três abordagens: copiar e adaptar; improvisar soluções manuais; e implementar descoberta e mascaramento governado, destacando o impacto real em risco, velocidade de releases e custos.

Acelerar releases sem proteção é perigoso. O diferencial para o negócio vem de unir agilidade com segurança, reduzindo exposição, aumentando velocidade e garantindo conformidade à LGPD.

16:55 - 17:15



Daniel Ortiz

Regional Sales Manager - Ping Identity



Speed of Trust

Mais usuários, mais bots, mais dispositivos, mais IA - mais de tudo está ampliando a lacuna na confiança digital e dando vantagem aos adversários.

Descubra como a confiança contínua, contextual e verificada permitirá que sua empresa cresça com segurança, adote agilidade e opere na velocidade da confiança.

17:15 - 17:45



Raphael Luna

CIO | CISO - MDS Group
MODERADOR



Eduardo Cabral

Diretor de vendas - Zscaler Brasil



Daniel Gomes

Regional Sales Director LATAM na Cymulate



Fernando Ceolin

Regional Sales Director - AKAMAI



Hiperconexão sem Controle é Caos: O Futuro da Segurança Digital

Vivemos em um mundo onde nuvens, dispositivos e identidades estão interligados em escala nunca vista. Essa hiperconexão, ao mesmo tempo que gera eficiência, expõe empresas a riscos que não respeitam fronteiras. Neste painel, especialistas vão mostrar como transformar esse cenário em vantagem competitiva, trazendo três visões complementares: Zscaler (Eduardo Cabral) com a liderança em Zero Trust e proteção de acessos em escala global; Cymulate/ServiceIT (Daniel Gomes) com a capacidade de validar continuamente defesas e simular ataques reais para medir resiliência; e Akamai, que garante segurança e disponibilidade em ambientes multi-cloud e hiperdistribuídos.

O futuro da segurança digital não será definido apenas pela tecnologia adotada, mas pela capacidade de garantir confiança em cada conexão.

SPONSORS:



KEYNOTE E GENERAL SESSION - 27/10

17:45 - 18:15



Carlota Bindner

Lead Product Security Researcher -
Thermo Fisher Scientific

KEYNOTE

Exploration of Cellular-Based IoT Inter-Chip
Communications

As IoT devices increasingly adopt cellular technologies such as NB-IoT and CAT-M for both primary and fallback connectivity, assessing their security remains challenging. Traditional methods of testing cellular communication are often limited by regulatory restrictions around RF interception and a lack of accessible tools or methodologies. This talk presents a hardware-focused approach to analyzing the security of cellular-enabled IoT devices. Attendees will learn how to tap into the communication between microcontroller units (MCUs) and cellular modules to capture, analyze, and manipulate data in transit. Techniques will include performing Machine-in-the-Middle (MitM) analysis to extract sensitive information. The session will also explore how modifying this communication can extend device capabilities or expose weaknesses that impact backend systems.

18:15

ENCERRAMENTO E HAPPY HOUR

SPONSORS:



KEYNOTE E GENERAL SESSION - 28/10

08:30 - 09:20 REGISTER & COFFEE BREAK

09:20 - 09:30 EVENT OPENING

09:30 - 10:00



Andrew Bindner
Senior Cybersecurity Engineer -
United Natural Foods, Inc. (UNFI)
KEYNOTE

From Pixels to Protection: How Cybersecurity is Powering the Digital Transformation

This talk explores the role of cybersecurity in driving digital transformation across industries. We'll dive into how businesses are leveraging emerging technologies like AI, IoT, and cloud computing to grow their operations while simultaneously addressing the security challenges these innovations create. In this context, key concepts of risk management, compliance, and security protocols will be highlighted for both technical and business professionals.

10:00 - 10:25



Julio Silvello
VP de Product Marketing - AZION
AZION

AI Agents na Linha de Frente: Do Custo Crescente à Segurança Autônoma e Distribuída

Atacantes estão cada vez mais bem equipados com IA generativa para lançar campanhas de phishing hiper-realistas, acelerar o desenvolvimento de aplicações maliciosas e automatizar ataques em larga escala. Nesse cenário, stacks tradicionais de segurança – como WAF, DDoS Protection e Bot Management – permanecem essenciais, mas já não bastam sozinhas. A resposta exige plataformas programáveis, que permitam criar AI Agents capazes de detectar ameaças emergentes, orquestrar respostas a incidentes, automatizar takedowns e aplicar políticas de mitigação em tempo real. Nesta sessão, exploraremos como adotar uma abordagem de Autonomous Security para construir um perímetro inteligente e distribuído, protegendo aplicações modernas e legadas – sem a necessidade de migrações complexas.

10:25 - 10:50



Paulo Conduitta
CISO - Ouribank
MODERADOR



Vanessa Pestana
Director, Fraud Prevention for
Latam - Quinto Andar



Gisele Marquesim
Gerente de Prevenção a Fraudes &
Investigações - Azul Linhas Aéreas
Brasileiras



Ádiva Fickert Graziosi
Head de Criminal Investigation &
Outreach - NUBANK

Prevenção a Fraudes ou Cibersegurança: Quem Gera Mais Valor de Retorno ao Negócio?

Fraude corporativa e cibersegurança sempre andaram juntas – mas será que já viraram uma coisa só? Ou será que, na nova era digital, combater fraudes oferece mais ROI direto e rápido do que investimentos em ciberproteção tradicional? Este painel convida executivos a analisar essa convergência, priorização orçamentária, e novas abordagens integradas para proteger receita e reputação.

SPONSORS:



KEYNOTE E GENERAL SESSION - 28/10

10:50 - 11:15



Diego Yudi Miamoto

Especialista Técnico -
ManageEngine

ManageEngine

Proteção avançada contra ransomware

Entenda as táticas mais recentes utilizadas por cibercriminosos e descubra como adotar uma abordagem proativa para se defender contra ataques de ransomware. Serão abordadas estratégias avançadas de prevenção, resposta e recuperação, essenciais para proteger seus dados, minimizar riscos e garantir a continuidade das operações em um cenário digital cada vez mais ameaçador.

11:15 - 11:40



Marco Tulio Moraes

Head of Information Security -
COSAN

Gestão de Riscos Cibernéticos: Risco, Valor e Tomada de Decisão

gestão de riscos cibernéticos continua sendo um ponto cego para muitas equipes técnicas, mesmo em organizações com estruturas avançadas de segurança. Esta apresentação discute caminhos práticos para aplicar os princípios de gestão de riscos no contexto da cibersegurança, com foco em como transformar a identificação de ameaças em decisões que façam sentido para o negócio. A quantificação entra como um apoio importante nesse processo, permitindo priorizar ações com base em impacto estimado, ainda que os dados disponíveis sejam limitados. Serão abordados exemplos simples de como utilizar abordagens quantitativas mesmo em ambientes com pouca maturidade, sem perder a conexão com o cotidiano operacional. A proposta é oferecer um olhar objetivo sobre como tratar riscos com mais método, clareza e utilidade, para que os profissionais da área possam entender, adaptar e aplicar esses conceitos no seu dia a dia.

11:40 - 12:05



Tiago Macedo

CISO - Grupo Moura
MODERADOR



Mario Conte

Head of Cyber Security - RAIZEN



Renato Lima

Information Security, Operacional
Resilience and Thread Manager -
Eletrobras



Carlos Minami

CISO - Solfacil

OT Sob Ataque: Quando o Alvo Não é o Dinheiro, é a Destruição

A nova era dos ataques cibernéticos operacionais não é mais guiada por lucro – é orientada por dano. Grupos apoiados por estados-nação, milícias digitais e atores ideológicos têm como alvo infraestruturas críticas com o objetivo de desestabilizar, sabotar ou simplesmente destruir. O ransomware tradicional está sendo substituído por ataques sem chave decriptografia, onde o objetivo não é o resgate – é o colapso.

Neste painel, vamos discutir:

- A evolução da ameaça: de cibercrime para ciberterrorismo industrial;
- Casos recentes onde o hardware foi deliberadamente danificado;
- A responsabilidade crescente de CISOs e vPs de OT como gestores de risco nacional;
- A infiltração silenciosa de lobby geopolítico em cadeias de suprimento;
- Estratégias para proteger ambientes OT em um cenário de guerra assimétrica digital.

Com grandes líderes do setor, este painel abordará como operar e proteger-se em um mundo digital sem fronteiras – onde a próxima ameaça não virá com pedido de resgate, mas com intenção de destruição total.

12:05 - 13:45

LUNCH

SPONSORS:



okta



Data Protection & Disaster Recovery



a CISCO company



an IBM Company



fazendo diferente



by Broadcom



See It. Secure It. Assess It.



KEYNOTE E GENERAL SESSION - 28/10

13:45 - 14:05



Leandro Ferreira

CISO - Superior Tribunal de
Justiça (STJ)

Da Fadiga à Clareza: Redefinindo a Liderança em Cibersegurança na Era da Sobrecarga de Informação

Líderes de cibersegurança convivem diariamente com uma avalanche de dados, ferramentas e alertas - um cenário que alimenta a fadiga da informação e ameaça decisões críticas. Neste bate-papo estratégico, vamos explorar como organizar um pouco melhor essa dinâmica e transformar sobrecarga em clareza de forma a manter o foco no que realmente importa: proteger o negócio e gerar valor sustentável para as organizações.

14:05 - 14:15



Rafael Peruch

Sales Architect LATAM - KnowBe4
knowbe4

O Que Os Olhos Corporativos Não Veem, O Bolso Sente: Trazendo à Luz o Risco Oculto

Explore como riscos cibernéticos invisíveis ameaçam financeiramente as organizações. Abordaremos a Gestão de Risco Humano, como falhas na percepção de vulnerabilidades humanas resultam em perdas significativas; estatísticas atuais e estudos de ROI da KnowBe4 que demonstram o impacto econômico de incidentes versus prevenção, comprovando o retorno de programas de conscientização.

14:15 - 14:25



Weberton Souza

Head of Cybersecurity - Darede



Rodrigo Santi

Cloud Security LATAM - CrowdStrike



A nova era da Segurança de Cloud em meio aos Adversários empoderados por AI

A era da Inteligência Artificial não transformou apenas os negócios, mas também a forma como os adversários cibernéticos atacam. Neste painel a Darede e a CrowdStrike debatem como organizações podem fortalecer a segurança em Cloud diante de ameaças cada vez mais sofisticadas, explorando práticas modernas, visibilidade em tempo real e estratégias para construir resiliência digital em escala.

14:25 - 14:35



Thiago Amorim

Head of Detection & Incident
Response - SIC00B

Quando o ataque veste crachá: Como proteger o setor financeiro da ameaça interna

Esqueça a imagem do hacker invadindo sistemas. A maior ameaça da atualidade é interna. No setor financeiro, onde a agilidade e a conformidade são cruciais, o funcionário cooptado não precisa invadir: ele usa credenciais legítimas para contornar perímetros e defesas tradicionais. Ele se move com nossa confiança.

Nesta apresentação rápida de 10 minutos, vamos explorar porque os controles de segurança de "fora para dentro" são insuficientes e como a ameaça interna opera. Em seguida, apresentarei um framework prático de quatro frentes para mitigar riscos de forma eficaz:

- Dissuadir: Fortalecendo a cultura de segurança e criando incentivos positivos.
- Dificultar: Adotando o princípio de privilégio mínimo e ferramentas como JIT/JEA/PAM.
- Detectar: Usando UEBA, telemetria de identidade e honeytokens para identificar comportamentos anômalos.
- Responder: Através de playbooks claros e uma resposta integrada com as equipes de RH e Jurídico.

SPONSORS:



okta

Penso



veeam

Data Protection & Disaster Recovery

AZION

ManageEngine

splunk>

a CISCO company

netbr

SailPoint

perforce
Delphix

Ping
Identity

knowbe4

DAREDE
a nuvem

CROWDSTRIKE

Strike

HashiCorp
an IBM Company

team
fazendo diferente

CLOUDFLARE

SERVICEIT

Akamai

transmit
security

OAKMONT
group

NSFOCUS

SEC4U

semperis

zscaler

scunna

XM Cyber

kaspersky

ESY

Symantec
by Broadcom

Defcon1

WebSIA

zluri

SCANSEC

FORESCOUT
See It. Secure It. Assess It.

HITACHI

Commvault

Netconn
driven by passion

RAPID7

KEYNOTE E GENERAL SESSION - 28/10

14:35 - 15:05



Diogo Santos
Cybersecurity Manager, Natura
MODERADOR



Daniel Cardoso
Diretor Comercial , Cloudflare
CLOUDFLARE



Ricardo Dastis
CTO - Scunna S.A.
scunna



Fernando Andreazi
Solution Sales Manager - Kaspersky
kaspersky

Tríade da segurança: Zero Trust + Threat Intelligence + Continuous Attack Simulation

A superfície de ataque não para de crescer – e os velhos modelos de defesa já não bastam. O futuro da cibersegurança passa pela tríade da segurança: Zero Trust, Threat Intelligence e Continuous Attack Simulation. Neste painel, vamos explorar como redefinir a borda digital com Zero Trust e proteção em escala global; como transformar exposição em ação ao simular continuamente os caminhos reais de um atacante; e como fornecer inteligência global de ameaças para antecipar o próximo movimento antes que ele aconteça. O resultado é um modelo integrado onde confiança zero, visibilidade total e inteligência contínua deixam de ser slogans e se tornam a base de resiliência real para empresas digitais e infraestruturas críticas.

15:05 - 15:45

COFFEE BREAK

15:45 - 16:10



Pedro Alfradique Lohmann
CISO - L'Oréal Brazil



Diego Mariano
CISO e Superintendente de Canais Digitais - Hospital Israelita Albert Einstein



Ticiano Benetti
Global CISO - Natura

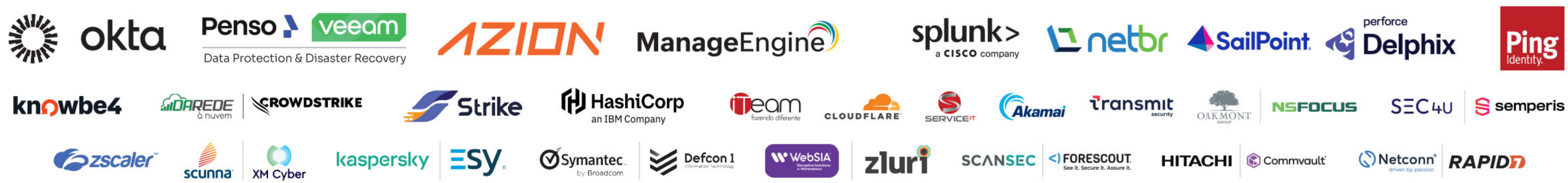


Marcelo Amaral
CISO - SAFRA

Ransomware Polimórfico e a Nova Era da Inteligência Artificial: A Tempestade Perfeita da Ciberameaça

A ascensão da Inteligência Artificial tem impulsionado a sofisticação dos ataques cibernéticos, especialmente no desenvolvimento de ransomwares polimórficos, capazes de se modificar a cada execução para escapar de antivírus tradicionais e EDRs. Nesta palestra, vamos explorar como a IA está sendo usada por cibercriminosos para automatizar a mutação de códigos maliciosos, tornando os ataques praticamente indetectáveis. Discutiremos casos reais e recentes, como: RansomHub: grupo que assumiu ataques devastadores contra Christie's (maior casa de leilões do mundo) e sistemas de saúde nos EUA. Black Basta: ligado ao ransomware polimórfico que comprometeu o sistema da Ascension Health, impactando hospitais em 20 estados americanos. Cactus Ransomware: uma nova cepa que usa criptografia dupla com polimorfismo para enganar ferramentas de detecção durante ataques em setores de energia e manufatura. O objetivo é mostrar que estamos diante de uma guerra assimétrica alimentada por algoritmos, onde os atacantes evoluem mais rápido que as defesas. Será abordada a necessidade de mudança urgente nas estratégias de defesa, com uso de inteligência comportamental, Zero Trust adaptativo e ciber-resiliência baseada em IA.

SPONSORS:



KEYNOTE E GENERAL SESSION - 28/10

16:10 - 16:20



Davi Ortiz

Senior Accountant Executive - Strike



Reputação Digital como Pilar da Continuidade de Negócios

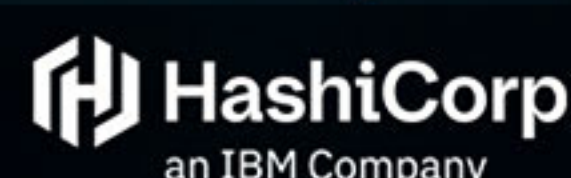
Nesta palestra iremos discutir como a reputação se tornou um ativo crítico e como incidentes cibernéticos podem afetar tanto a confiança do cliente quanto a operação da empresa. Incluir frameworks de monitoramento da marca e mitigação de riscos operacionais.

16:20 - 16:30



Wallace Figueiredo

Staff Solutions Engineer - HashiCorp



Dominando a Segurança na Nuvem: As 5 Principais Estratégias para uma Gestão Eficaz do Ciclo de Vida de Chaves

Nos ambientes híbridos de nuvem cada vez mais complexos de hoje, gerenciar segredos e chaves de segurança tornou-se um desafio crítico para as organizações. Esta sessão explorará as estratégias essenciais para implementar uma abordagem abrangente de gestão do ciclo de vida da segurança. Aprenda como empresas líderes estão transformando sua segurança na nuvem - de processos fragmentados e manuais para estruturas centralizadas e automatizadas. Descubra os passos-chave para padronizar a gestão de chaves, reduzir riscos de segurança e melhorar a produtividade dos desenvolvedores. Com base em experiências reais dos setores financeiro, de telecomunicações e varejo, esta apresentação oferecerá insights práticos para executivos e líderes técnicos que buscam fortalecer sua postura de segurança na nuvem.

16:30 - 17:00



Christian Coutinho

Superintendente de Segurança Cibernética - B3
MODERADOR



Wagner Brunca

Principal, LATAM Security Solution Engineer at Broadcom Software



Luiz Veloso

Regional Sales Manager - Transmit



Julian Andrew Hoche

Senior Manager de Operações LATAM - Dafiti



Identidade, Compliance e Defesa: Como transformar exigências regulatórias em vantagem competitiva

A nova moeda do mercado é a confiança digital.

Em 2025, a pressão regulatória (NIS2, DORA, LGPD/GDPR, AI Act) se une à explosão de identidades digitais e à necessidade de defesas corporativas em larga escala. Este painel mostra como empresas podem transformar exigências regulatórias em vantagem competitiva, conectando três pilares: Identidade, Segurança Corporativa e Governança & Compliance. O resultado? Negócios que não apenas sobrevivem às pressões digitais e regulatórias, mas ganham mercado ao serem vistos como players confiáveis, resilientes e prontos para o futuro.

SPONSORS:



okta



Data Protection & Disaster Recovery



ManageEngine



KEYNOTE E GENERAL SESSION - 28/10

17:00 - 17:30



Yuri Diogenes

PhD em Cybersecurity

KEYNOTE

Quando as Fronteiras ficam Nebulosas: Ciberataques de Estados-Nação em Conflitos Modernos

Em uma era definida por tensões geopolíticas e conflitos globais, o ciberespaço tornou-se uma poderosa extensão da diplomacia. Atores estatais estão lançando ciberataques cada vez mais sofisticados que visam governos, infraestruturas críticas e empresas privadas. Esta sessão examinará como as ameaças cibernéticas evoluíram em paralelo com guerras e mudanças nas alianças geopolíticas, com exemplos reais da guerra Rússia-Ucrânia, conflitos no Oriente Médio e campanhas que visam cadeias de suprimentos e indústrias críticas.

Os tomadores de decisão obterão insights sobre como esses ataques remodelam o risco, a política e a resiliência global dos negócios. Líderes técnicos também verão como os adversários exploram vulnerabilidades, armam infraestruturas e se movem lateralmente em ambientes de nuvem híbrida. Nessa sessão você vai entender melhor a interseção entre conflito cibernético e geopolítica, e o que os líderes devem fazer para se defender contra as ameaças de estados-nação do futuro.

17:30

ENCERRAMENTO, SAMEDAY VIDEO E BRINDES

SPONSORS:



okta

Penso



veeam

Data Protection & Disaster Recovery

AZION

ManageEngine

splunk>
a CISCO company

netbr

SailPoint

performe
Delphix

Ping
Identity

knowbe4

DAREDE
a nuvem

CROWDSTRIKE

Strike

HashiCorp
an IBM Company

team
fazendo diferente

CLOUDFLARE

SERVICEIT

Akamai

transmit
security

OAKMONT
GROUP

NSFOCUS

SEC4U

semperis

zscaler

scunna

XM Cyber

kaspersky

ESY

Symantec
by Broadcom

Defcon 1

WebSIA

zluri

SCANSEC

FORESCOUT
See It. Secure It. Assess It.

HITACHI

Commvault

Netconn
driven by passion

RAPID7