CYBER SECURITY

BANK & GOVERNMENT

CONFERENCE 2023

15 DE MARZO

CHILE

Sheraton Santiago Hotel and Convention Center

EVENTO PRESENCIAL

ALL TRENDS HERE & NOW

MTics

THE COMMITMENT IDENTIFIES US

CYBER SECURITY
BANK & GOVERNMENT
CONFERENCE 2023

EN ESTA EDICIÓN PARTICIPARON

1000 REGISTRADOS

+ 400 ASISTENTES PRESENCIALES

CYBER SECURITY
BANK & GOVERNMENT
CONFERENCE 2023

26 SPEAKERS INTERNACIONALES

CYBER SECURITY
BANK & GOVERNMENT
CONFERENCE 2023

CONFERENCIAS CON EXPERTOS INTERNACIONALES

09:00 AM

Bienvenida y Apertura

Construyendo una resiliencia colectiva contra el Cibercrimen Hoy

Mónica Tasat *- Founder & CEO Mtics Latam*
Katherina Canales Madrid *- Miembro del Comité Académico Internacional Cybersecurity Bank & Government; Directora de Estrategia en Nivel4*

09:05 AM

Panel de Gobierno

Avanzando hacia un Estado Digital: Retos y desafíos

Ponentes: ***Kenneth Pugh*** *- Senador en Senado de la República de Chile.*
Daniel Álvarez *- Coordinador Nacional de Ciberseguridad - Ministerio del Interior y Seguridad Pública de Chile*
José David Montilla *- Viceministro de Agenda Digital - Ministerio de la Presidencia República Dominicana*
Moderadora: ***Katherina Canales Madrid*** *- Miembro del Comité Académico Internacional Cybersecurity Bank & Government; Directora de Estrategia en Nivel4*

09:30 AM

Prilex: la amenaza a los sistemas de pagos globales

Prilex es un singular actor de amenazas originado en Brasil que ha evolucionado de un malware centrado en cajeros automáticos a un malware de punto de venta modular único. Estuvieron detrás de uno de los mayores ataques a cajeros automáticos del país, infectando más de 1.000 cajeros automáticos y clonando 28.000 tarjetas de crédito a la vez, en un ataque sincronizado. Pero la codicia de los delincuentes no tenía límite, querían más y lo consiguieron.
El grupo está bien organizado, pudiendo huir de la operación de LEA en un intento de atraparlos. En 2016, abandonaron el malware para cajeros automáticos y concentraron todos sus ataques en los sistemas de punto de venta, apuntando al núcleo de la industria de pagos. Rápidamente, adoptaron las operaciones de Malware-as-a-Service y ampliaron su alcance en el extranjero, atacando empresas en EE. UU., Alemania y países de América Latina. Desde entonces, hemos estado rastreando el movimiento de cada actor de amenazas, siendo testigos del daño y las grandes pérdidas financieras que se produjeron en la industria de pagos.
Prilex es un malware muy avanzado y complejo que adopta un esquema de criptografía único, realiza parches en tiempo real en el software de destino, obliga a degradar el protocolo, cambia de un ataque basado en repeticiones para poder manipular criptogramas con transacciones GHOST. La amenaza es uniforme, capaces de bloquear transacciones de pago sin contacto, lo que les permite capturar pistas y realizar fraudes incluso en tarjetas de crédito protegidas con tecnología CHIP y PIN.
En esta presentación, mostraremos todas las capacidades de Prilex y cómo el sector financiero debe prepararse para combatirlo.

KeyNote: ***Fabio Assolini*** *- Director del equipo de investigación y análisis para América Latina en* ***Kaspersky.***

09:55 AM

Estrategia de Zero Trust para cumplimiento en Banca y Gobierno en Chile

Conocer la mirada de Akamai para los desafíos a nivel regulatorio tanto de la Banca, Finanzas e Instituciones Públicas en Chile puedan ser abordadas desde un planteamiento de Confianza Cero (Zero Trust) validando el acceso correcto por los usuarios correctos a la Información Correcta; los modelos modernos de Confianza Cero deben estar sustentados en la segmentación de los activos de información que forman la base del negocio bancario y los servicios de digitales de cara a los ciudadanos, y es bajo este contexto que la Microsegmentación juega un rol clave en no solo garantizar esto sino que también en simplificar la operación y la visibilidad sobre la que se puedan definir y aplicar nuevas políticas y estructuras de gobierno.
Los invitamos a conocer nuestra mirada aplicada sobre control regulatorio de Banca y Gobierno
KeyNote: ***Patricio Villacura*** *- Enterprise Security Sales (SOLA),* ***Akamai.***

10:20 AM

Gestión de exposición: nuestra visión para proteger la superficie de ataque moderna.

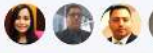
Las amenazas han evolucionado: vaya por delante del riesgo cibernético. Su superficie de ataque crece, está en constante cambio y está cada vez más interconectada. Con herramientas de seguridad especializadas que ofrecen un panorama incompleto, puede llegar a parecer imposible responder la pregunta: "¿Qué tan seguros estamos?"
El abordaje hacia la gestión de exposición de Tenable combina visibilidad sobre todos los aspectos de la superficie de ataque con contextos de negocios, para que usted pueda comprender con precisión el riesgo cibernético de su organización y priorizar las mitigaciones.

KeyNote: ***Mario Benedetti*** *- Enterprise Territory Manager para Chile en* ***Tenable.***

10:45 AM

Networking: ***Visita Stands***

11:15 AM



Panel de Bancos

Banca y regulación: Desafíos de una industria esencial

Ponentes: ***Karina Bunster*** *- Senior de Riesgo Operacional Tecnología y Seguridad- Banco BCI.*
Robinson Cáceres Reballedo *- CISO Corporativo en Grupo Security.*
Abraham Ermann *- Gerente Internacional de Ciberseguridad y Fraude en Banco ITAU.*
Moderador: ***Freddy Macho*** *- Presidente del IoT Security Institute, Capítulo Chile*

11:45 AM

Ciber Higiene y mitigación del riesgo cibernético en el sector financiero y gobierno

El modo de trabajo mixto de la fuerza laboral ha ampliado la superficie de los ataques, y el cibercrimen se está volviendo más sofisticado. Esto es evidente con echar un vistazo a las últimas noticias, que cuentan historias de redes de gobiernos, organismos públicos y empresas privadas presas del ransomware.
En esta sesión, se compartirán estrategias sobre la implementación de buenas prácticas de higiene de TI como apoyo en materia de gestión de riesgos cibernéticos.

Keynote: ***Ana Álvarez*** *- Gerente Técnica de Cuentas en* ***Tanium***

CYBER SECURITY BANK & GOVERNMENT CONFERENCE 2023

12:10 PM

Evolución del Cyber Threat Hunting: caza, detección y respuesta.

Los ataques cibernéticos son cada vez más comunes y los atacantes están evolucionando todos los días sus técnicas, para poder lograr sus objetivos, sin embargo, también existen algunas buenas prácticas que se pueden seguir para evitar ser una presa fácil en este mundo, y más bien poder, porque no, convertirse en un cazador de ciberataques, incluso antes de que estos ocurran o ejecuten completamente su objetivo.

Keynote: *Weimar Gutierrez* - *Technical Consultant en* ***ManageEngine LATAM***

12:35 PM

Las Personas son el Nuevo Perímetro: Cómo Proteger la Capa Humana

Las amenazas internas se están convirtiendo rápidamente en uno de los mayores desafíos de ciberseguridad que enfrentan las organizaciones en la actualidad. Son responsables de tres millones de registros robados todos los días y estuvieron en el centro del 57 % de todas las filtraciones de bases de datos el año pasado. Las investigaciones muestran que el tiempo promedio para detectar y contener una amenaza interna es de 77 días: solo el 13 % de los incidentes se detectan en 30 días.
La razón por la que son tan altos y tardan tanto en procesarse es porque cualquier persona con acceso legítimo y confiable a los sistemas y datos de una organización, ya sea un empleado, un contratista a tiempo parcial o un socio comercial, puede ser una amenaza. La gestión de amenazas internas requiere fundamentalmente un enfoque centrado en las personas, por lo que en esta charla analizaremos cómo las vulnerabilidades, los ataques y los privilegios están transformando el panorama de amenazas y por qué es importante adoptar una postura de seguridad centrada en las personas.

KeyNote: *Jorge Peña* - *Sales Manager en* ***ProofPoint***.

01:00 PM

Los retos de ciberseguridad que se avecinan con Open Banking-Finance-Data

Open Banking consiste en descentralizar/compartir los datos de los clientes. Normativa PSD2. Las finanzas abiertas consisten en ampliar e integrar el ecosistema del sector (gestión de patrimonios, aplicaciones KYC, gestión de riesgos, prestamistas, transacciones p2p, criptomonedas, agregadores de API, etc.).
Los datos abiertos se refieren a un modelo centrado en el cliente en el que las necesidades primarias, secundarias y terciarias del ser humano se ofrecen en un mercado abierto.
Para hacer posible esta evolución, las empresas deben utilizar API para conectarse entre sí.
En la búsqueda de datos sensibles, los ciberdelincuentes se centrarán más en los puntos finales vulnerables de las API que se conectan directamente a la base de datos subyacente de una organización.
Los bots se convertirán en un desafío más persistente y generarán más ataques de scraping en API individuales que conducirán a la fuga de datos.
Las API se convertirán en el principal objetivo de los bots maliciosos en el presente/futuro próximo.

KeyNote: *Sara Zuleta* - *Technical Project Manager en* ***hCaptcha***.

02:45 PM

Cómo fortalecer su última capa de seguridad: su firewall humano

La realidad del trabajo remoto ha dejado muy claro que las tecnologías pasadas y presentes diseñadas para proteger a los humanos y los datos confidenciales no funcionan como se esperaba. Es hora de un nuevo enfoque para la capacitación en concientización sobre seguridad cibernética para motivar a los usuarios finales como la última línea de defensa (firewall humano) y permitirles tomar decisiones de seguridad más inteligentes.

Keynote: *Oliver Garcia* - *Regional Account Manager Latam in* ***KnowBe4***

03:10 PM

Secure Service Edge Adoption

Cómo proteger el acceso cloud de las aplicaciones y la tendencia relacionada con SASE.
Prevención de fuga de datos cuando se migra a la nube. Estadísticas y tendencias.

KeyNote: *Roberto Moreno* - *Regional Manager South Latam para* ***Netskope***

03:35 PM

Un nuevo paradigma de pentesting: Las claves para entender la plataforma que te conecta con los mejores ethical hackers del mundo

En una región como Latinoamérica, que sufre un ciberataque cada 17 segundos, se necesitan nuevas formas para encontrar vulnerabilidades críticas y resolverlas a tiempo.
Los procesos de Pentesting tradicionales son lentos, burocráticos y no necesariamente de alta calidad. Los Red Teams cuentan con un exceso de herramientas, pero ninguna ayuda a encontrar vulnerabilidades de alto impacto.
En esta sesión, se discutirán posibles soluciones ante esta problemática y se presentarán herramientas para facilitar este trabajo, como la plataforma end-to-end de Strike que conecta a los mejores hackers éticos con tecnología

KeyNote: *Ivan Lendner* - *Pentesting Solutions Facilitator en* ***Strike***

04:00 PM

Protección de Datos personales, un enfoque práctico y efectivo

En un mundo cada vez más digitalizado y global, donde los datos se encuentran en el centro de toda estrategia de negocios, las empresas capturan, procesan y transmiten enormes cantidades de información de sus clientes como parte de sus operaciones diarias. Al mismo tiempo, las constantes fugas de información y ciberataques ponen en riesgo todos los días la información de las empresas y sus clientes. Esto coloca a las empresas en una situación de extrema vulnerabilidad, no solo por el hecho de ser susceptibles a recibir multas o sanciones económicas, sino también por el inminente riesgo de ver afectada su reputación.
En la presentación se abordará la importancia de implementar una gobernanza de datos en la organización a la luz de las regulaciones actuales y futuras. También propondrá un enfoque práctico para implementar los controles necesarios que permitan resguardar la confidencialidad, integridad y resiliencia de los sistemas de tratamiento de datos.

KeyNote: *Ricardo Gadea* - *Gerente General, Director de* ***Assertiva S.A.***

04:25 PM

MITRE ATT&CK y La Anatomía de una Operación de Ransomware

El incremento en los ataques de ransomware continúan siendo una de las preocupaciones principales de los funcionarios en el sector financiero y de gobierno en toda la región, Chile no es la excepción. Sin embargo, el enfoque de los equipos de seguridad se ha concentrado fundamentalmente en el impacto que los mismos pueden causar en la disrupción de las operaciones, ignorando en algunos casos todo el modus operandi de estos procesos maliciosos.
Conozcamos un poco del panorama de amenazas Chileno, Cómo estos atacantes operan y qué podemos hacer para prepararnos y prevenir que afecten nuestra infraestructura.

KeyNote: *Héctor Díaz* - *Head of Marketing & Senior Technical Marketing Manager en* ***RAN Security***

04:35 PM

Abordando los requisitos de auditoría de seguridad de TI para cuentas privilegiadas

Aprenda cómo mantener las demandas de cumplimiento de TI administrando de forma centralizada la seguridad de identidad y la actividad de acceso privilegiado. El enfoque único y unificado para la auditoría de TI orientada a la identidad y los requisitos de cumplimiento, puede eliminar riesgos, brindar inteligencia, cumplir con auditorías de seguridad y habilitar sus negocios de manera continua.

KeyNote: *Jorge López Miranda* - *Sales Manager, SOLA,* ***CyberArk***

05:20 PM

Women in Cyber: Amenazas actuales, una necesidad integral

Ponentes: *Alexandra Barros* - *Gerente de Riesgo operacional y ciberseguridad, Coopeuch.*
Sara Herrera - *Gerente de riesgo operacional y tecnológico, Banco Estado.*
Katherina Canales Madrid - *Miembro del Comité Académico Internacional Cybersecurity Bank & Government, Directora de Estrategia en Nivel4.*
Moderadora: *Mary Cruz Rosas* - *Information Security and Risk Management, Digital Transformation Advisor, Womcy*

CYBER SECURITY
BANK & GOVERNMENT
CONFERENCE 2023

PANEL DE GOBIERNO
“Avanzando hacia un Estado Digital: Retos y desafíos

PANEL DE BANCOS
“Banca y regulación: Desafíos de una industria esencial”

PANEL - Women in Cyber
“Amenazas actuales, una necesidad integral”

CYBERSECURITY BANK & GOVERNMENT CHILE 2023
en los medios

[Prensario IT Latam]

[Trendtic.cl]

CYBER SECURITY BANK & GOVERNMENT CONFERENCE 2023

Imágenes del evento

CYBER SECURITY
BANK & GOVERNMENT
CONFERENCE 2023

VIEW GALLERY: ingrese al siguiente LINK

PRÓXIMAS EDICIONES

PERÚ

ECUADOR **COLOMBIA**

PANAMÁ

REPÚBLICA DOMINICANA

Si desea participar

CONTÁCTESE CON NOSOTROS AQUÍ