# infosecurity®

## MEXICO

**22 - 23 05/2019**

Ciudad de México
Centro Citibanamex

**EL EVENTO LÍDER EN CIBERSEGURIDAD**


**Rubén Galicia**
**Key Account Manager**
**Panda Security**


Parte de infosecurity GROUP

Organizado por Reed Exhibitions®

infosecurity MEXICO

# Problemas, soluciones y tendencias en Ciberseguridad: Threat Hunting

**Rubén Galicia**
**Key Account Manager**
**ruben.galicia@mx.pandasecurity.com**

panda

pandasecurity.com/business

# CIBERGUERRA Y LA TRANSFORMACIÓN DIGITAL

## "Sin Ciberseguridad NO hay Transformación digital"

### ¿Cuáles son las motivaciones de los ciberdelincuentes?

- Beneficio personal
- Objetivos políticos
- Robo de propiedad intelectual en busca de ventajas competitivas.
- Interrumpir las infraestructuras críticas que buscan causar estragos.
- Represalias: Empleados despedidos con un profundo conocimiento sobre cómo acceder a los sistemas.
- Notoriedad y fama.

# Tendencias de Ciberseguridad y prevención de riesgos

infosecurity MEXICO


- Las inversiones en seguridad están cambiando de la prevención de riesgos a la detección de amenazas basada en SOC.
- Las declaraciones de prevención de riesgos se vinculan a los resultados de negocio.
- Los proveedores de productos de seguridad apuestan por la formación en nuevas capacidades.
- Aumentan las inversiones destinadas a incrementar las competencias en seguridad en la nube.
- El entorno del gobierno de seguridad de datos priorizará las inversiones en seguridad de la información.
- La autenticación sin contraseña se abre paso.
- Otros factores a tener en cuenta en la ciberseguridad y gestión de riesgos.

# SEGURIDAD REACTIVA VS SEGURIDAD PROACTIVA

## Panda siempre un paso adelante

# Factores importantes dentro de la Ciberseguridad

En la actualidad es necesario contar con plataformas TECNOLOGICAS que combinen perfectamente proactividad, orquestadas por PROCESOS automatizados en constante aprendizaje y adaptación , todo esto soportado por un grupo de PERSONAS expertas y creativas en identificar las técnicas de los atacantes y/o ciberdelincuentes.

## TECNOLOGÍAS

Tecnologías Big Data y Machine Learning

## PROCESOS

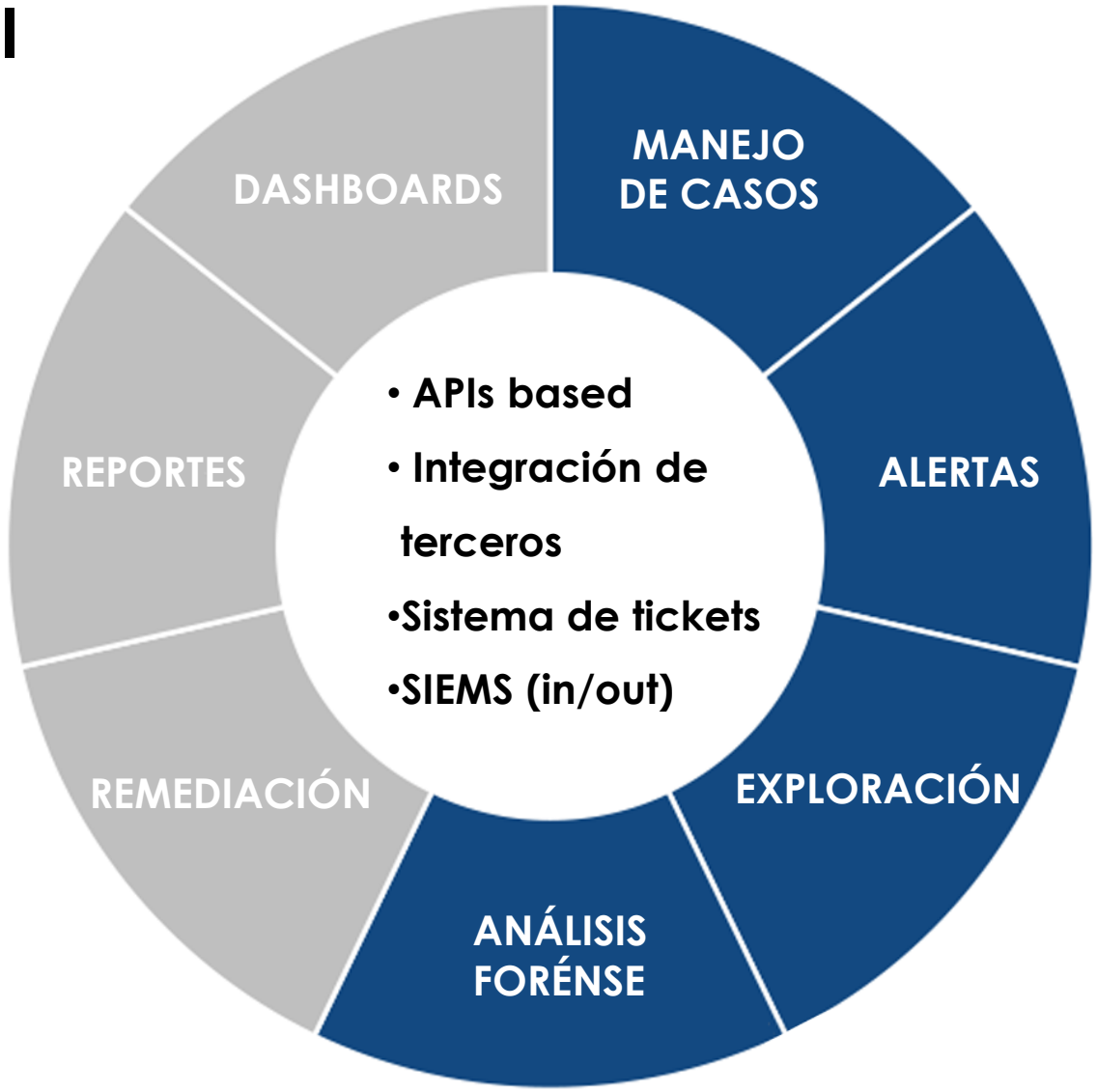
Monitorización Continua de todas las aplicaciones

## PERSONAS

Análisis de Comportamiento realizado por Técnicos


Identificar Amenazas
Identificar Vulnera-bilidades
Evaluar la Exposición al riesgo
Desarrollar Medidas de Protección y Detección
Establecer Planes de contingencia
Respuesta a Incidentes de ciberseguridad
EVOLUCIÓN DE LAS ESTRATEGIAS DE CIBERSEGURIDAD

# Principales características por área funcional



# Nuevos modelos de Seguridad

infosecurity MEXICO

## ¿Por qué incorporar tecnologías de detección y respuesta para la protección del usuario final?

- Monitorización Continua de todas las aplicaciones
- Clasificación de todos los procesos de todos los endpoints
- Tecnologías Big Data y Machine Learning
- Análisis de Comportamiento realizado por Técnicos
- Prevención Contra Malware Conocido
- Detección del Malware Avanzado
- Detección Dinámica de Exploits
- Detección Basada en Comportamientos

# NUESTRA VISIÓN SOBRE LAS AMENAZAS

## Tendencias

### Control de Ejecución
- Aplicaciones de Mercado
- Modelo de Attestation

### Número de hackers está creciendo exponencialmente
- Más Ciber expertos = Más Hackers
- Adopción a los modelos de seguridad

## Consecuencias

### Evasión
- Exploits
- Aplicaciones maliciosas

### Robo de Identidad
- Los hackers se hacen pasar por administradores y/o usuarios corporativos
- Ataques de Malwareless

# RETOS PRINCIPALES PARA SECURITY OPERATION CENTERS (SOCs)

- Las restricciones presupuestarias con incidentes de seguridad son cada vez más costosas.
- Aumento de alertas de seguridad.
- Falta de personal calificado.
- Gestión de numerosas herramientas de seguridad

# LAS PREGUNTAS DE SEGURIDAD **MÁS URGENTES**

**¿Somos los siguientes en sufrir un ataque?**

**¿Estamos listos para un ciber ataque?**

**¿Estamos siendo atacados?**

infosecurity MEXICO

# ¿Alguna vez nos hemos preguntado?...

¿Por dónde estamos siendo atacados?

¿Qué daño está causando?

¿Qué técnicas y/o tácticas esta utilizando?

¿Fue un incidente al azar o dirigido?

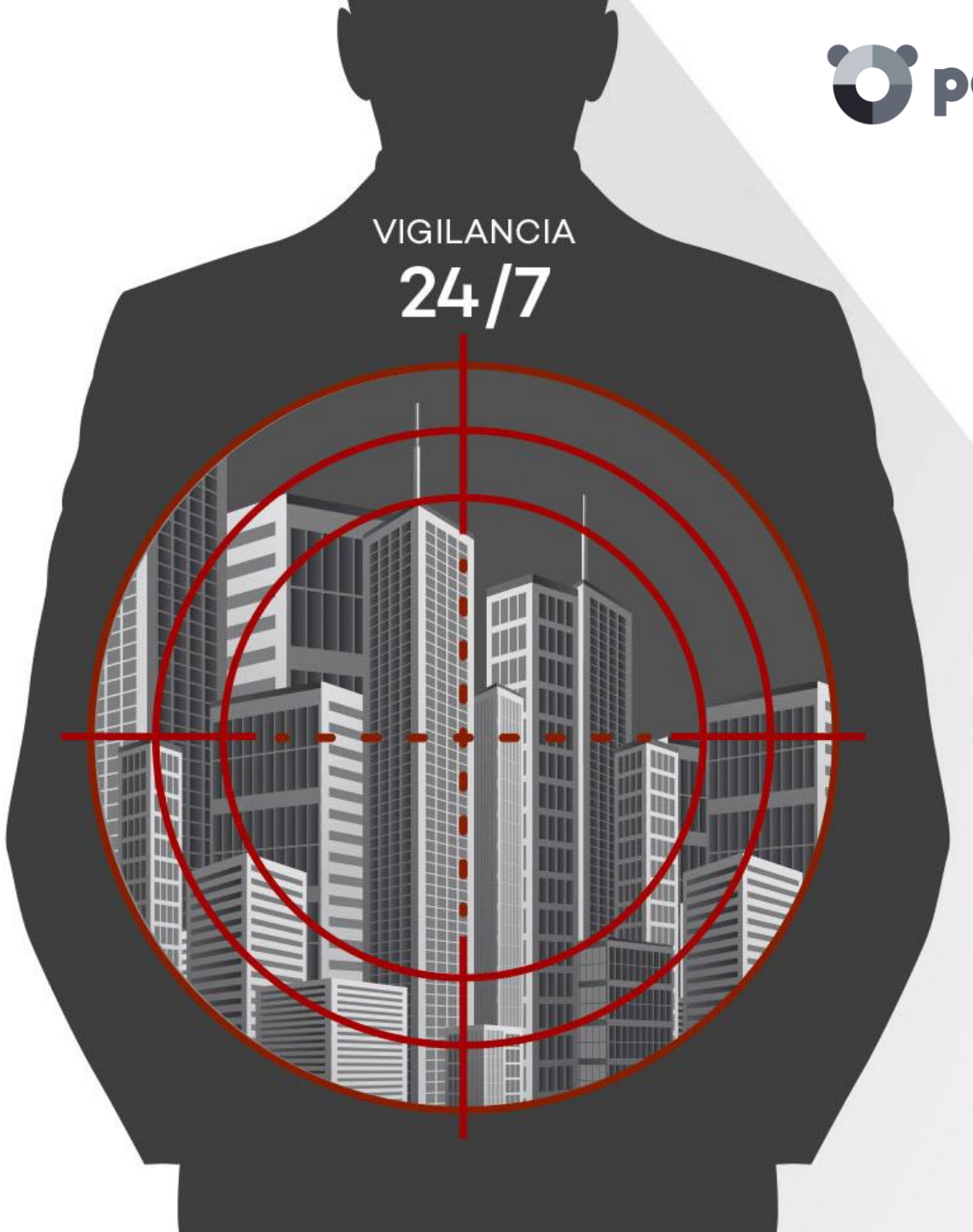
infosecurity MEXICO

Algunas cosas no se pueden predecir…

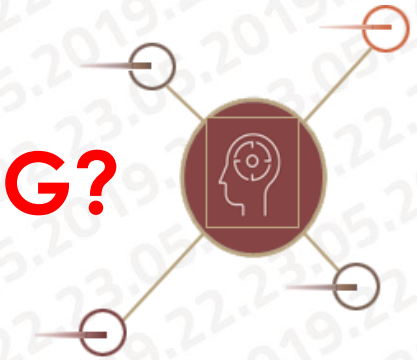
# 99% no es suficiente

panda

# ¿Qué es
# THREAT HUNTING?



# ¿THREAT HUNTING?



**Servicio de búsqueda proactiva de amenazas avanzadas, ejecutado por analistas de ciberseguridad especializados.**

**Objetivos:**

- Descubrir los TTP (tácticas, técnicas y procedimientos) utilizados por los hackers.
- Detectar ataques en sus primeras etapas antes de que puedan cumplir sus objetivos.

# ¿Cómo identificar un ataque?

## ARQUITECTURA DEL THREAT HUNTING

# Detección Pro Activa de Ataques

**El servicio de Threat Hunting nos permite detener los ataques en cualquier etapa de la CADENA CYBER KILL.**


**Ataque explicado siguiendo el modelo de Cyber Kill Chain**

**Adaptive Defense**
**Modo Learning**
No hay bloqueo, monitoriza todo lo ejecutado.

# DETECCIÓN MEJORADA

**Las compañías que utilizan una plataforma Threat Hunting tienen los siguientes beneficios:**

- **Mejore la velocidad de detección y respuesta** de amenazas.
- El 64% de las organizaciones obtiene una detección mejorada de amenazas avanzadas y **ataques sin guerra.**
- El 63% de las organizaciones reduce el tiempo de detección e investigación de amenazas.

***Grupo NCX, firma líder de consultoría en gestión de riesgos.**

panda

Panda Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

infosecurity MEXICO

¨El servicio Threat Hunting reduce drásticamente los riesgos y costos, mejora la detección de ataques y los tiempos de respuesta y reduce la superficie de ataque¨.

# CONCLUSIONES

## Tendencias

**Control de ejecución**
- Mercados de aplicaciones
- Modelos de atestación

**Número de hackers creciendo exponencialmente**
- Más ciber-expertos = más hackers.
- Adaptación a los modelos de seguridad.

## Consecuencias

**Evasión**
- Explotaciones
- Aplicaciones maliciosas haciéndose pasar por GW

**El robo de identidad**
- Los hackers se hacen pasar por administradores o usuarios corporativos.
- Ataques malvados

## Solución

**Panda Adaptive Defense 360**
Visibilidad sin Límites, Control Absoluto

- Servicio de attestation
- Tecnología anti-exploit

**Threat Hunting**
- Aplicaciones y modelos de comportamiento de usuarios y entidades.
- Detectar TTPs y ataques malwareless.

infosecurity MEXICO

# CASO DE USO

# Threat Hunting: Bondat – the invisible Worm

**Study of a threat, generation of hypotheses and validation**

infosecurity MEXICO

panda

# “El malware ya está bajo control con las capacidades de prevención de Adaptive Defense”

# “Con Threat Hunting buscamos hackers y empleados maliciosos”

Gartner peerinsights™

4.6 ★★★★★

131 Verified reviews

92% Recommend

Gartner peerinsights customers' choice 2019™

# Gracias.