LIVE
WEBINAR

xcitium

CONTENCIÓN INTELIGENTE

LA NUEVA ERA DE PROTECCIÓN ENDPOINT

SEGURIDADAMÉRICA.COM
Fortaleciendo Internet

xcitium + SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet

Hoy queremos destacar una alianza estratégica que marca un antes y un después en la forma en que protegemos las organizaciones: la colaboración entre Seguridad América y Xcitium, uno de los líderes mundiales en ciberseguridad Zero Trust y contención de amenazas.

Esta alianza no solo suma tecnologías; suma confianza, innovación y un compromiso real con elevar el nivel de protección de nuestros clientes frente a un panorama de amenazas cada vez más complejo.

¿QUÉ ES XCITIUM?

Xcitium es un líder global en ciberseguridad **Zero Trust**, reconocido por desarrollar una tecnología única en la industria: **ZeroDwell™ Containment**, un enfoque que evita que cualquier archivo desconocido o potencialmente malicioso cause daño en los sistemas. A diferencia de las soluciones tradicionales que dependen de “detectar para después bloquear”, **Xcitium** trabaja con un principio distinto: proteger primero, analizar después.

Su tecnología aísla automáticamente cualquier proceso o archivo extraño dentro de un entorno virtual seguro, permitiendo que la operación continúe sin interrupciones, mientras el sistema determina si es una amenaza real. Este enfoque reduce a cero el tiempo que un atacante puede “moverse” dentro del sistema, evitando ransomware, malware de día cero y ataques avanzados antes de que logren ejecutarse.

CAPAS DE CIBERSEGURIDAD

DURANTE ESTA SESIÓN USTED CONOCERÁ

01

Cómo las amenazas actuales superan los modelos tradicionales basados solo en detección.

02

El rol del New-Gen AntiVirus y el Firewall Control en la protección avanzada del endpoint.

03

Cómo la combinación de EDR + HIPS fortalece la prevención activa frente a comportamientos sospechosos.

04

El impacto estratégico de la tecnología Deception para detectar movimientos tempranos del atacante.

05

Cómo la Zero-Dwell Containment Architecture elimina el tiempo de permanencia del malware.

06

La evolución hacia un Enhanced XDR (Detection, Investigation & Remediation) con respuesta unificada.

07

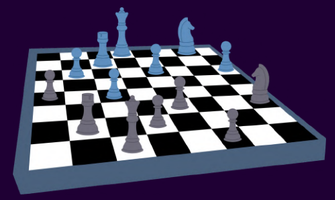
La integración con ITSM para alinear seguridad, operación y continuidad del negocio.

08

Cómo reducir el impacto financiero y operativo de un incidente antes de que escale.

CAPAS DE PROTECCIÓN

El capitán del barco tiene que ser como un ajedrecista.



APARICIÓN DE LA AMENAZA

RECONOCIMIENTO

PREPARACIÓN O ARMADO

ENTREGA

EXPLOTACIÓN

INSTALACIÓN O PERSISTENCIA

MOVIMIENTO LATERAL

TEMA 1

Cómo las amenazas actuales superan los modelos tradicionales basados solo en detección.

La ciber-protección proactiva consiste en adelantarse al atacante, reduciendo vulnerabilidades y detectando comportamientos anómalos antes de que generen impacto.

- Defensa Tradicional o Reactiva
- Defensa Moderna es proactiva
- Deficiencias de la defensa reactiva
- Por qué falla la defensa reactiva
- Implicación estratégica
- Premisa Central

TEMA 2

El rol del New-Gen AntiVirus y el Firewall Control en la protección avanzada del endpoint.

NGAV previene ataques modernos analizando comportamientos sospechosos en lugar de basarse solo en malware previamente identificado.

Firewall Control decide qué tráfico puede entrar o salir de una red según reglas de seguridad predefinidas. Reduciendo la superficie de ataque, evitando accesos no autorizados, y actuando como la "puerta de seguridad" de la red.

- ¿Qué lo hace diferente un NGAV del antivirus tradicional?
- ¿Qué implica un Firewall normalmente?
- Premisa Central

TEMA 3

Cómo la combinación de EDR + HIPS fortalece la prevención activa frente a comportamientos sospechosos.

EDR detecta y responde; HIPS previene y bloquea en tiempo real.

- Rol del EDR
- Rol del HIPS
- Operación conjunta EDR + HIPS
- Valor estratégico
- Premisa Central

TEMA 4

El impacto estratégico de la tecnología Deception para detectar movimientos tempranos del atacante.

Xcitium Deception detecta al atacante engañándolo para que interactúe con activos falsos plantados dentro de la red.

- Reducción del Tiempo de Exposición
- Visibilidad del comportamiento real del atacante
- Continuidad Operacional
- Complemento a EDR, XDR y Zero-Trust
- Ventaja frente a amenazas avanzadas
- Valor para Directorio y Gobierno Corporativo
- Premisa Central

TEMA 5

Cómo la Zero-Dwell Containment Architecture elimina el tiempo de permanencia del malware.

Zero-Dwell Containment asume que los archivos desconocidos podrían ser maliciosos y los ejecuta de forma aislada en contenedores virtuales en memoria para que no puedan causar daño, mientras determina su calidad.

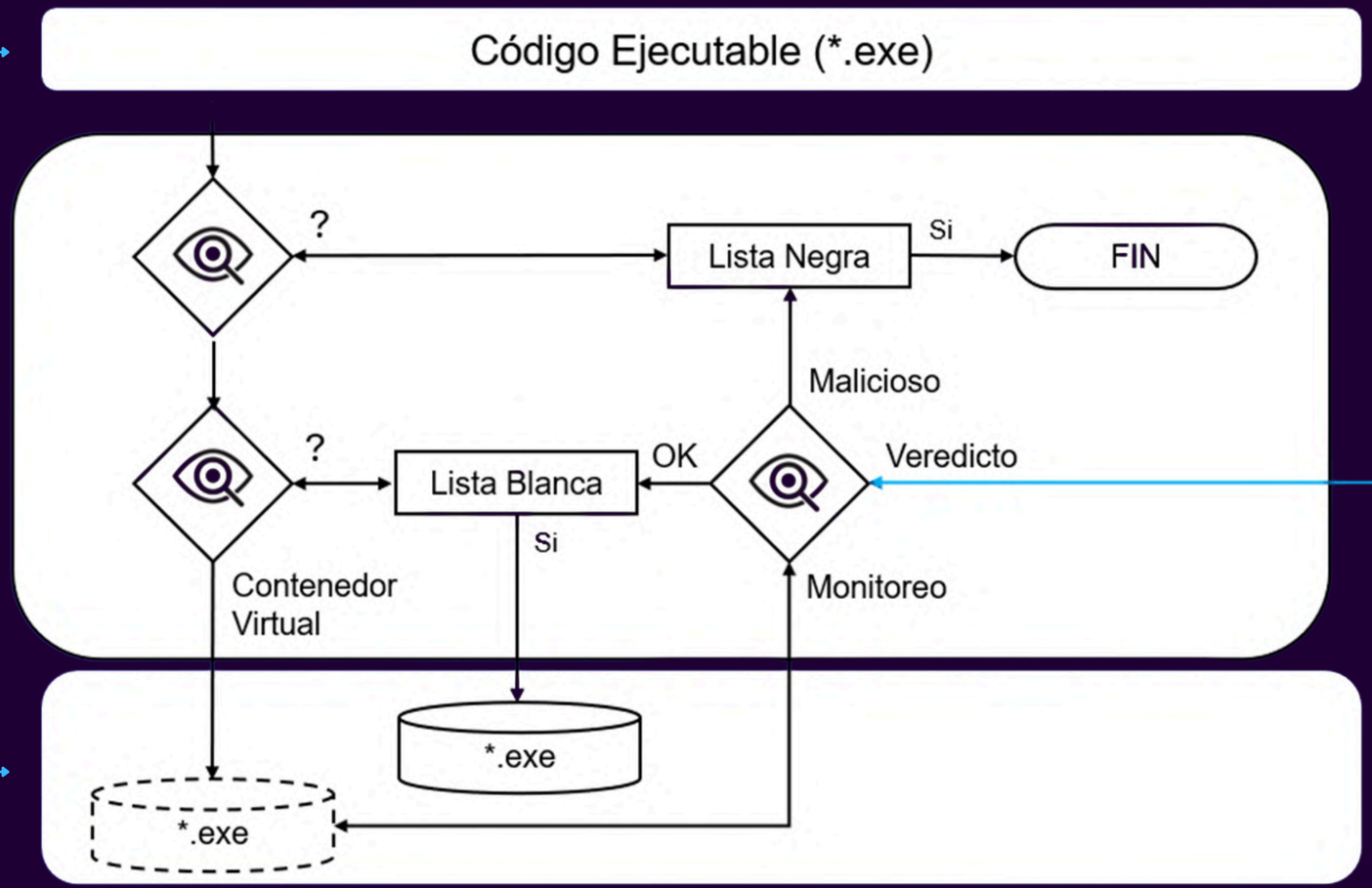
- Detección en tiempo real basada en comportamiento
- Contención automática inmediata
- Microsegmentación y Zero-Trust
- Automatización orquestada (XDR/SOAR)
- Reducción medible del dwell-time
- Impacto Estratégico
- Premisa Central

DIAGRAMA ZERO-DWELL

MEMORIA RAM

AGENTE XCITIUM

ENDPOINT



VERDICT - IA

CONSOLA XCITIUM

TEMA 6

La evolución hacia un Enhanced XDR (Detection, Investigation & Remediation) con respuesta unificada.

XDR mejorado unifica la visibilidad en todo el entorno para detectar y responder a ataques complejos desde una única plataforma.

- Detección unificada
- Investigación automatizada
- Remediación orquestada
- ¿Por qué es “Enhanced”?
- Impacto Estratégico
- Premisa Central

TEMA 7

La integración con ITSM para alinear seguridad, operación y continuidad del negocio.

Integración ITSM conecta herramientas técnicas con la mesa de ayuda para gestionar incidentes de forma automática y centralizada.

- Orquestación automática de incidentes
- Priorización basada en impacto
- Coordinación entre equipos
- Métricas ejecutivas unificadas
- Soporte a continuidad y resiliencia
- Beneficio Estratégico
- Premisa Central

TEMA 8

Cómo reducir el impacto financiero y operativo de un incidente antes de que escale.

Significa limitar pérdidas monetarias y evitar paralizar el negocio frente a un incidente de seguridad.

- Reducir la ventana de exposición
- Microsegmentación y principio de mínimo privilegio
- Automatización de respuesta (XDR + SOAR)
- Integración con ITSM y continuidad
- Respaldos inmutables y plan probado de recuperación
- Gestión ejecutiva del riesgo
- En términos estratégicos
- Premisa Central

PREGUNTAS Y RESPUESTAS

SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet

xcitium

¡GRACIAS POR ASISTIR A ESTE WEBINAR EDUCATIVO!

www.seguridadamerica.com / www.xcitium.com