xcitium

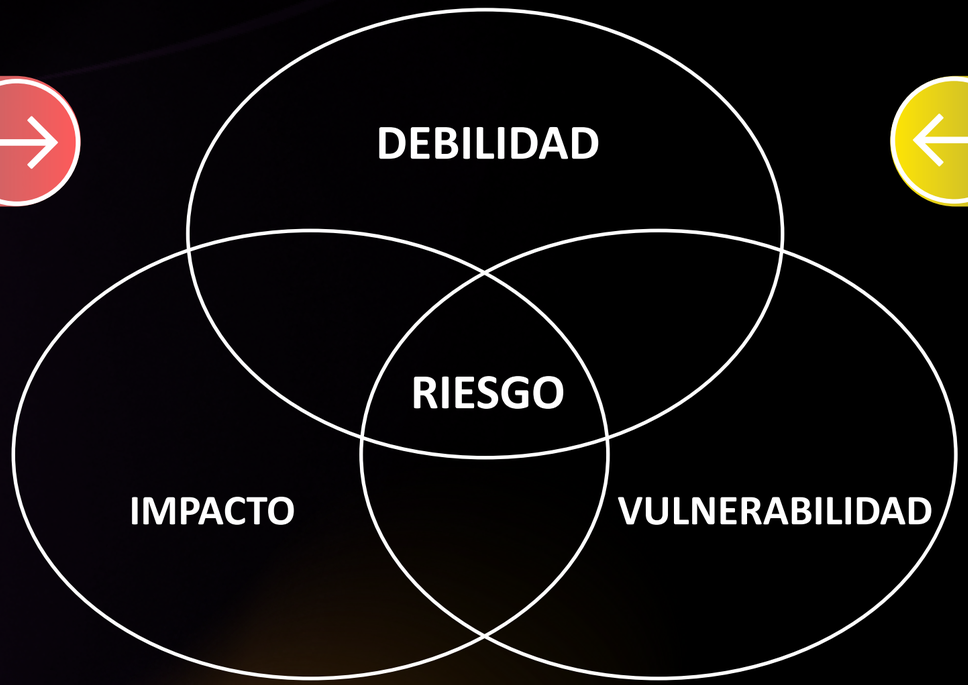
SEGURIDAD AMÉRICA.com

LA NUEVA ERA DE PROTECCIÓN DE DISPOSITIVOS

FACTORES CIBERSEGURIDAD

ATAQUE

AMENAZA



RIESGO = AMENAZA X VULNERABILIDAD X IMPACTO

xcitium

SEGURIDAD AMÉRICA.COM

CIBERSEGURIDAD

ENDPOINT SECURITY

Antes ——— Durante ——— Después

PROTECCIÓN

DETECCIÓN

RESPUESTA

xcitium

PROTECCIÓN → DETECCIÓN → RESPUESTA →

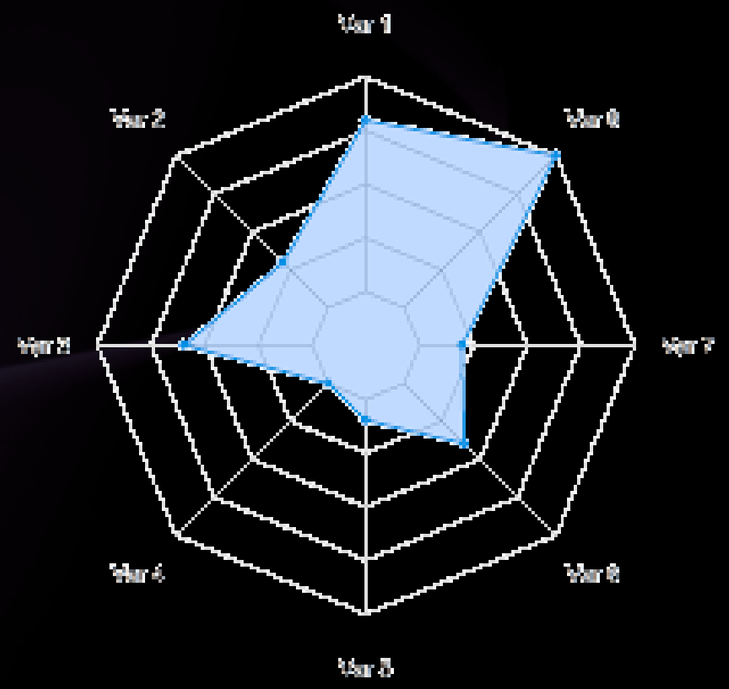
SEGURIDAD AMÉRICA.COM

PERSONAS	4,8
PERÍMETRO	4,4
RED	2,3
DISPOSITIVOS	3,4
APPs & APIs	1,1
DATOS	1,5
ACTIVOS CRÍTICOS	2,8

SOPORTE A USUARIOS / SOPORTE ARQUITECTURA

1 5

SUPERFICIE VULNERABLE (e.g.,)



PERSONAS | APPS & APIs | RED

DISPOSITIVOS | PERÍMETRO | DATOS

ACTIVOS CRÍTICOS

ENDPOINT SECURITY

ESTRATEGIA

ENFOQUE OPERATIVO PROACTIVO

ENFOQUE OPERATIVO REACTIVO

TÁCTICA

PROTECCIÓN INICIAL

PROTECCIÓN DISPOSITIVOS

DETECCIÓN AVANZADA

CONTENCIÓN PREVENTIVA

ANÁLISIS E INTELIGENCIA

MONITOREO ACTIVO

OPERACIÓN

FIREWALL + GESTIÓN VULNERABILIDADES

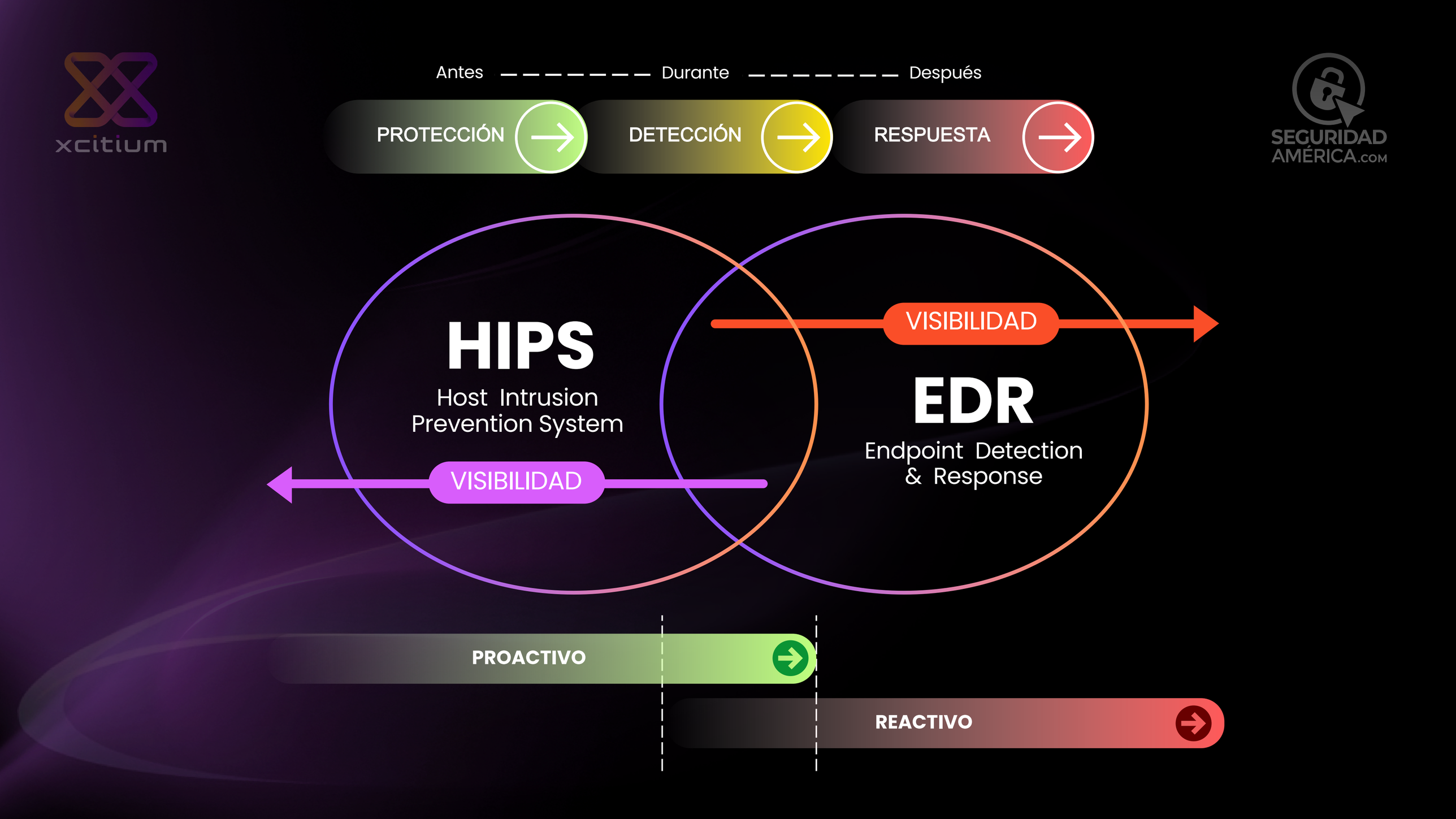
NGAV + HIPS

EDR + FILELESS MALWARE DETECTION

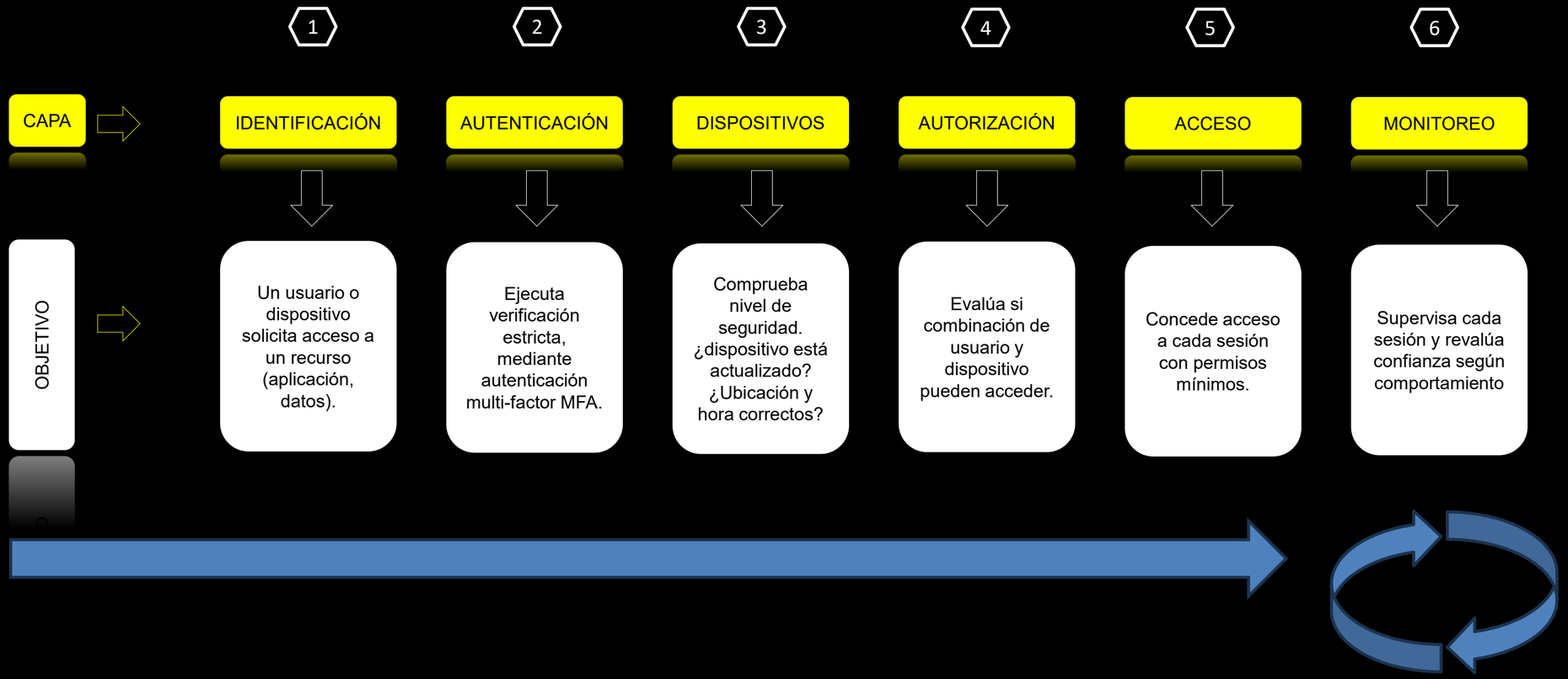
ZERO-DWELL + VERDICT CLOUD

TELEMETRÍA + ANÁLISIS + ADR

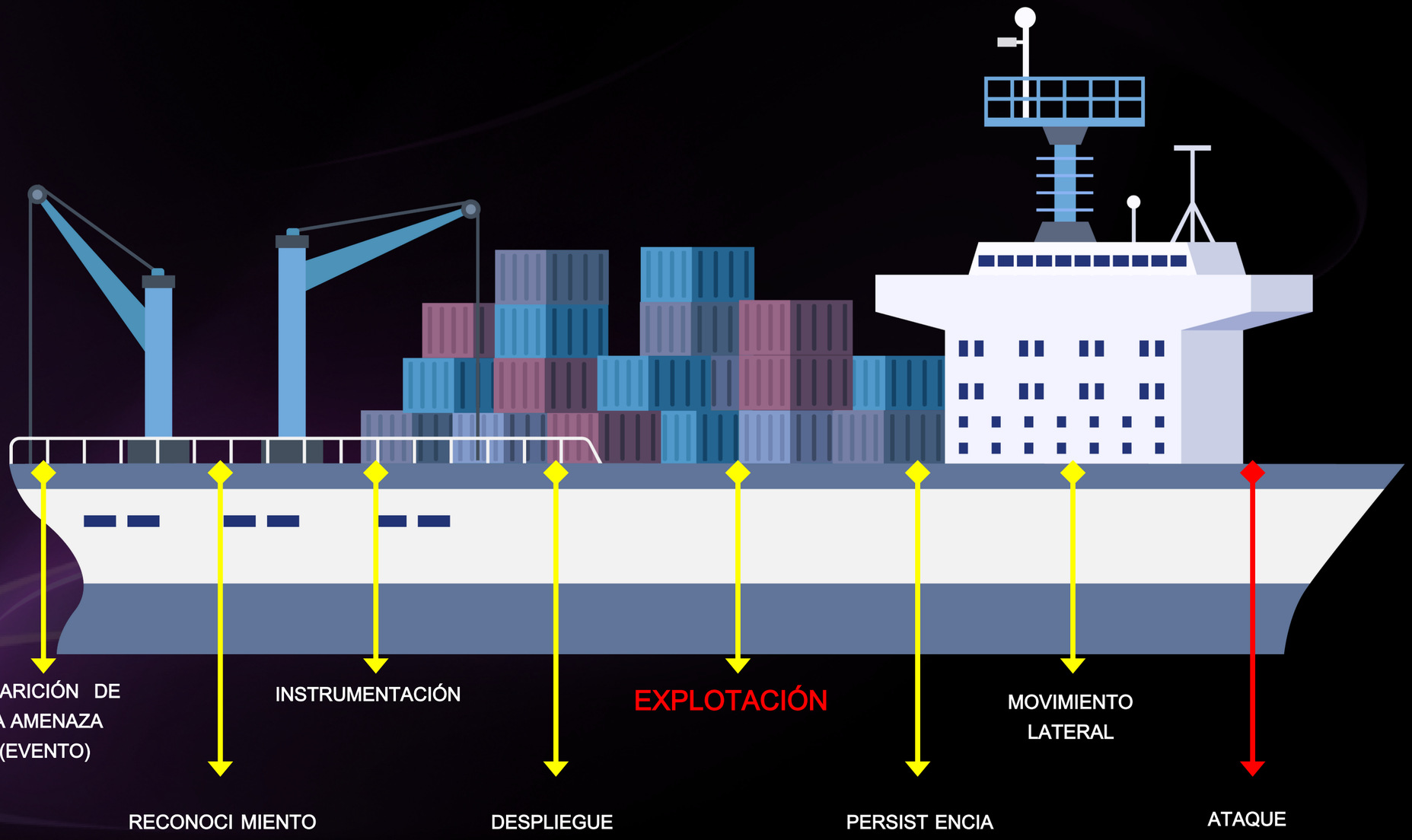
XDR + EXDR + ZERO-TRUST


Antes
Durante
Después
PROTECCIÓN
DETECCIÓN
RESPUESTA
HIPS
Host Intrusion Prevention System
VISIBILIDAD
VISIBILIDAD
EDR
Endpoint Detection & Response
PROACTIVO
REACTIVO

ZERO-TRUST SEQUENCE



SECUENCIA CIBERATAQUE



ENDPOINT SECURITY

ESTRATEGIA

ENFOQUE OPERATIVO PROACTIVO

ENFOQUE OPERATIVO REACTIVO

TÁCTICA

PROTECCIÓN INICIAL

PROTECCIÓN DISPOSITIVOS

DETECCIÓN AVANZADA

CONTENCIÓN PREVENTIVA

ANÁLISIS E INTELIGENCIA

MONITOREO ACTIVO

OPERACIÓN

FIREWALL + GESTIÓN VULNERABILIDADES

NGAV + HIPS

EDR + FILELESS MALWARE DETECTION

ZERO-DWELL + VERDICT CLOUD

TELEMETRÍA + ANÁLISIS + ADR

XDR + EXDR + ZERO-TRUST

ZERO-DWELL CONTAINMENT

Zero-Dwell Containment (ZDC) de Xcitium es una tecnología de seguridad basada en virtualización ligera a nivel del Kernel del Sistema Operativo, reforzada por la CPU, cuyo objetivo es eliminar en tiempo real, el riesgo asociado a la ejecución de archivos o procesos desconocidos mediante su contención virtual inmediata, y aislamiento completo.

ZDC opera bajo el principio de “default deny” aplicado dinámicamente, donde cualquier archivo o proceso no reconocido y acreditado por ZDC, es aislado y ejecutado de inmediato dentro de un contenedor virtual, sin interacción directa con recursos del sistema como File System, Registry, Memoria RAM, DCOM/RPC, Identidad y Credenciales, HDD/SSD, entre otros.

La Solución: Prevención Primero con ZeroDwell

Arquitectura Zero Trust:
"Culpable hasta que se demuestre su inocencia".

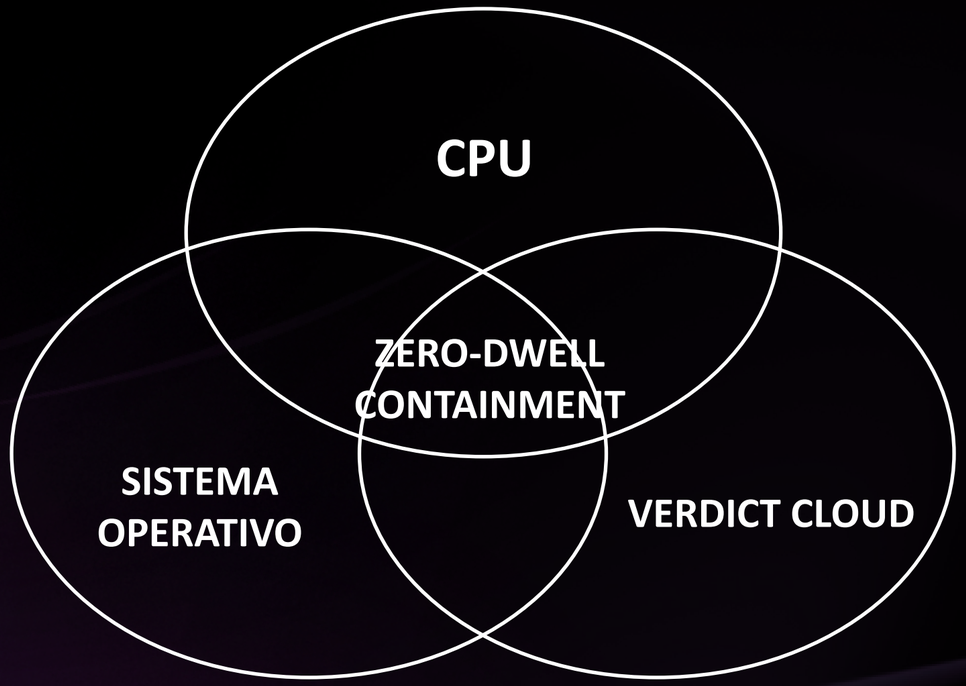
Auto-Contención Inmediata:
Los archivos desconocidos se virtualizan instantáneamente a nivel de API.

Uso Ininterrumpido:
El archivo opera normalmente dentro del prisma.
El usuario final sigue trabajando sin interrupciones, ajeno al proceso de análisis.

Ningún acceso a recursos del host.

xcitium

SEGURIDAD AMÉRICA.COM



ARCHIVOS Y PROCESOS →

NAVEGACIÓN WEB →

CONTENIDO EMAIL →

ACCESO A RECURSOS →

COMUNICACIÓN INTERPROCESOS →

PREPARACIÓN DEL ARCHIVO Y CLASIFICACIÓN EN TIEMPO-REAL

CONTENCIÓN AUTOMÁTICA Y EJECUCIÓN CONTROLADA

ANÁLISIS EN PARALELO Y DECISIÓN FINAL

RESPUESTA Y REGISTRO

← FILE SYSTEM

← MEMORIA RAM

← OS REGISTRY

← DCOM / RPC

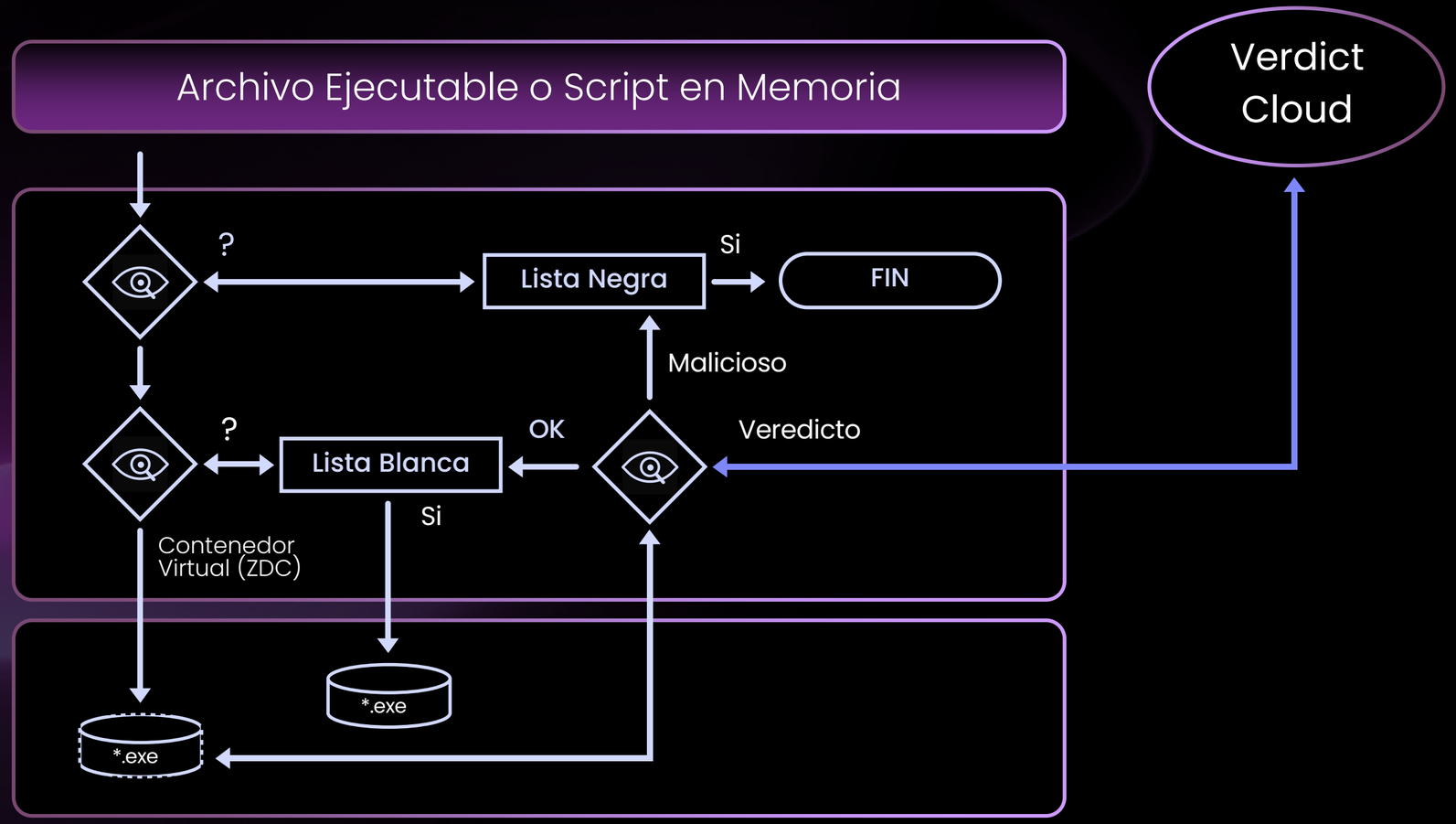
← IDENTIDAD & CREDENCIALES

ZERO-DWELL CONTAINMENT

Memoria RAM

Agente Xcitium

OS Kernel
API Virtualization

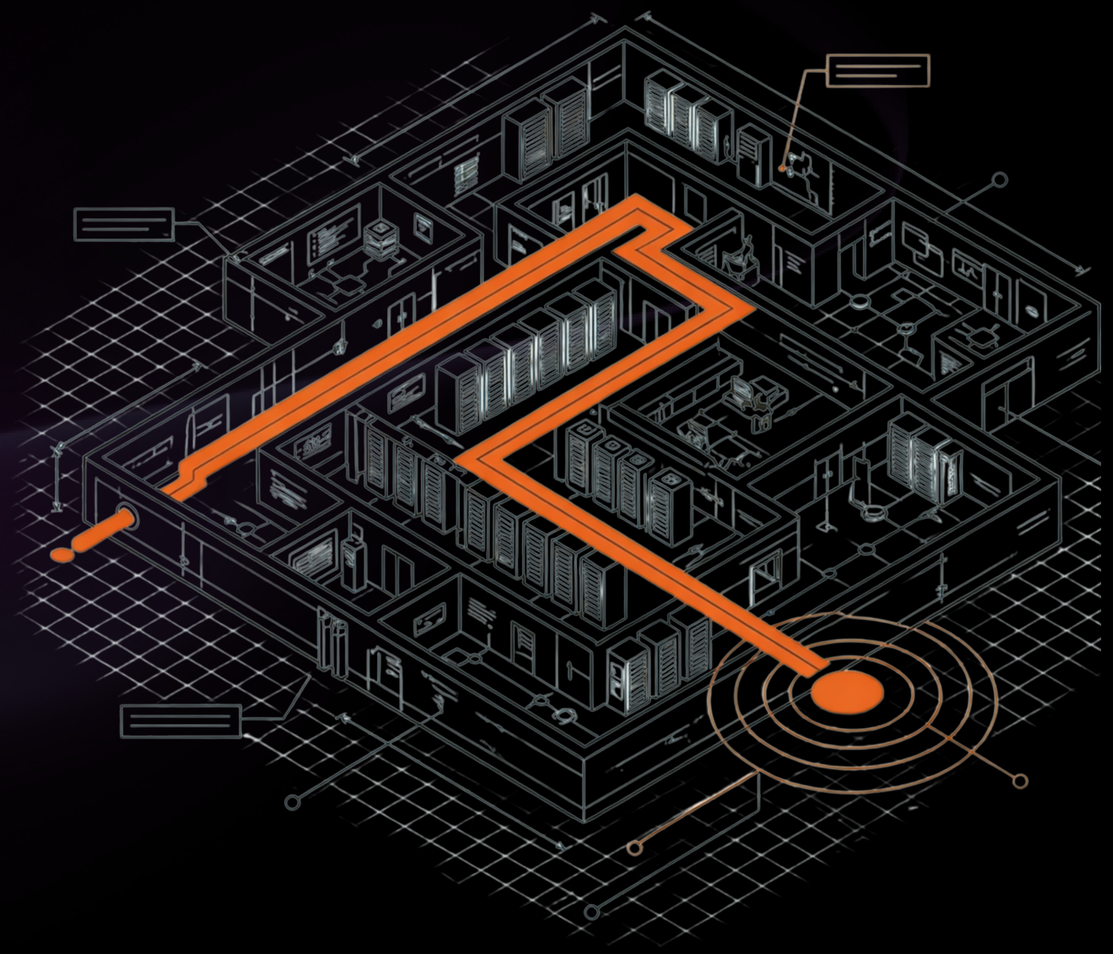


xcitium

VERDICT CLOUD

SEGURIDAD AMÉRICA.COM

1. AI + ML
2. DYNAMIC ANALYSIS + BEHAVIOR FILE LOOKUP SERVER GLOBAL
3. ANÁLISIS EQUIPO EXPERTO 24/7
4. RESPUESTA Y REGISTRO



xcitium

SEGURIDAD AMÉRICA.COM

CIBERSEGURIDAD

ITSM

PERSONAS

PROCESOS

TECNOLOGÍA

Sinergia Crítica: La Convergencia entre ITSM y Ciberseguridad

La ciberseguridad no es solo una cuestión de herramientas tecnológicas; es una disciplina integrada con la gestión de servicios de TI. Esta convergencia se articula en tres pilares (**Personas, Procesos y Tecnología**) que operan coordinadamente desde la estrategia hasta el soporte técnico.

PERSONAS

Personas: Del CISO al Service Desk

La estrategia es definida por líderes, mientras equipos capacitados ejecutan la vigilancia y respuesta.

PROCESOS

Procesos: Marcos de Trabajo Unificados

Integración de ITIL con ISO 27001 y NIST para gestionar riesgos, cambios y parches.

TECNOLOGÍA

Tecnología: Herramientas de Control y Visibilidad

Uso coordinado de SIEM, plataformas ITSM y herramientas de gestión de vulnerabilidades.

Áreas de Acción Estratégica: **Gestión y Monitoreo Proactivo**

El SOC y las herramientas GRC permiten detectar amenazas y gobernar riesgos continuamente.

Personas	Procesos	Tecnología
CISO y Analistas SOC	Riesgos y Gestión de Logs	Herramientas GRC y SIEM

Áreas de Acción Estratégica: **Operaciones y Soporte Integrado**

El Service Desk y los equipos de respuesta daben coordinar la resolución de incidentes.

Personas	Procesos	Tecnología
Administradores y Service Desk	Accesos (IAM) y Gestión de Tickets	Firewalls y Sistemas ITSM

"La seguridad no es solo tecnología". El éxito depende de la interacción fluida entre **personas, procesos y herramientas digitales.**

xcitium

IT SERVICE MANAGEMENT

SEGURIDAD AMÉRICA.COM

CIBERSEGURIDAD

DEVICE MANAGEMENT

PERSONAS → PROCESOS → TECNOLOGÍA

GESTIÓN → MANTENCIÓN → MONITOREO → OPERACIONES → SOPORTE

DEVICE & USERS + PROFILE	PATCH MGNT + APP STORE	ALERTS + AUDITING + REPORTS	REMOTE ACCESS + THUMBNAILS	TICKETS + CHAT

ITSM XCITIUM

CASO DE USO