

Un poderoso equipo de CTI, dentro de tu IA

Automatiza la detección de amenazas con el poder de la IA con CTI integrado

🔥 Crítico

📅 Zero Day

🦠 Malware

🕸 Cyber Attack

La actualización del sensor Falcon desencadena la crisis de BSOD de Windows 10

Creado el 19 de Julio de 2024 a las 04:15, última actualización el 20 de Julio de 2024

Una actualización reciente del sensor Falcon de CrowdStrike, lanzada el 19 de julio de 2024, provocó una interrupción global de la TI que afectó a los usuarios de PC en la nube con Windows 10, 11 y Windows 365 de varios sectores, incluidas instituciones financieras, hospitales, aerolíneas y cadenas minoristas. La actualización provocó un bucle de errores en el BSOD que afectó a los sistemas críticos. La causa principal fue un error humano en CrowdStrike, por el que se aprobó y distribuyó por error un archivo incorrecto lleno de ceros. CrowdStrike lo solucionó en un plazo de 24 horas, pero se recomienda a las organizaciones que permanezcan atentas a los intentos de suplantación de identidad que se aprovechan de la situación.

📁 8 MITRE ATT&CK TTPs

56 IoCs

🏢 Industria destinataria: **All**

🏢 Target organization: **CrowdStrike, Microsoft**

🏢 Organización destinataria: **Windows, Microsoft**

🏢 Malware: **Demons**

Historial

Se notifican actualizaciones sobre CVE e IOC.

🔄 **56** actualizaciones

07/20/2024 at 03:11 AM

CVEs agregados

CVE-2023-41443

CVE-2023-41432

MITRE ATT&CK TTPs

T1193

T1195

Los datos fragmentados y alertas constantes crean puntos ciegos para los ataques. La separación de actividades clave como escaneo de vulnerabilidades, inteligencia de amenazas y gestión de activos reduce la visibilidad del riesgo cibernético. La Inteligencia de Amenazas Cibernéticas (CTI) y la Gestión Externa de la Superficie de Ataque (EASM) de Axur cierran estas brechas, ofreciendo cobertura completa, información accesible y alta productividad. Este enfoque unificado permite priorizar vulnerabilidades, identificar riesgos críticos y responder rápidamente a las amenazas.



Visibilidad Unificada de Amenazas



Eficiencia Potenciada por IA



Inteligencia en Tiempo Real

Cobertura, velocidad y contexto **inigualables**

Ciberataques

Identifique y responda a los ataques en su superficie de ataque con alertas procesables para mantenerse por delante de las amenazas críticas.

Caza proactiva de Threat Hunting

Realice búsquedas avanzadas para investigar riesgos relacionados con credenciales, dominios y amenazas emergentes.

Vulnerabilidades

Priorice actualizaciones con alertas que destaquen vulnerabilidades, garantizando la aplicación eficiente de parches críticos.

Gestión de Exposición (EASM)

La inteligencia de amenazas integrada con EASM facilita la supervisión y respuesta a amenazas.

Deje que la **IA** haga el trabajo pesado **por usted**, buscando, analizando y priorizando alertas relevantes

Cada día, la solución CTI de Axur analiza cientos de fuentes, incluidas noticias, grupos, informes y feeds de amenazas.

Su modelo LLM altamente especializado resume cada ataque, amenaza o vulnerabilidad relevante.

Luego, filtra todo lo que es pertinente a tu mapa de superficie de ataque y a los temas de interés.

Así, envía alertas curadas y accionables con solo lo que realmente necesitas saber, nada más.



⊗ Antes

11,000 alertas
enfrentadas a diario por los
equipos de seguridad

30 min
tiempo promedio que un analista
gasta en cada alerta

✓ Con Axur

Gestión de amenazas 180x más rápida al
correlacionar alertas con su superficie de ataque.

Respuesta 3x más rápida, liberando a sus analistas
para que trabajen de manera estratégica.

Threat Landscape

Generar resumen ↗

Tendencias en los últimos 30 días relacionadas con mis activos

Ubicación más afectada

1ª Estados Unidos

2ª Canadá

3ª Brasil

4ª Rusia

5ª Ucrania

Activos

Identifique sus activos más vulnerables y frecuentemente atacados, ya sea en su entorno o a nivel global, para priorizar su protección.

Malware

Obtenga información sobre familias de malware e incidentes relacionados, lo que le permite responder más rápidamente a amenazas en evolución.

CVE's en Tendencia

Concéntrese en vulnerabilidades críticas que están siendo explotadas actualmente, con una vista priorizada para orientar la remediación.

Threat Actors

Acceda a perfiles de atacantes, incluyendo sus tácticas y vulnerabilidades explotadas, para anticipar riesgos.

TTPs

Rastree las tácticas y técnicas de adversarios en tendencia para anticipar sus estrategias de ataque y mejorar su postura defensiva.

Filtro por Industria

Filtre amenazas por industria para comparar riesgos específicos del sector y adaptar su estrategia de seguridad basada en información personalizada.

Transforme las alertas en información práctica

➔ Gestión de parches simplificada

Consolide los datos para simplificar la priorización de parches y actúe rápidamente sobre vulnerabilidades críticas.

➔ Datos estratégicos para CISOs y equipos de seguridad

Proporcione a los CISOs información procesable para prevenir ataques y fortalecer la postura de seguridad.

➔ Alertas curadas de primera mano

Manténgase por delante de las amenazas emergentes e informe de inmediato a la gerencia para tomar acciones rápidas.

➔ No más pestañas infinitas ni alertas sin contexto

Elimine el desorden de múltiples pestañas y reciba solo las alertas más relevantes y procesables.

Revólucione su ciberseguridad con EASM + CTI Unificados

Descubra una visibilidad completa de su huella digital externa, lo que le permitirá identificar y asegurar todos los activos expuestos a internet. Al integrar EASM con CTI, obtiene una capacidad inigualable para gestionar vulnerabilidades y responder a amenazas.

➔ Análisis de Vulnerabilidades

Compare sus activos con bases de datos de CVE para identificar brechas, evaluar la explotabilidad, proporcionar puntajes CVSS y verificar certificados digitales para autenticación.

➔ Descubrimiento de Activos

Identifique IPs, subdominios y servicios para dominios registrados, enriquezca con datos de Whois y detecte puertos abiertos con el software y los protocolos en ejecución.

The screenshot shows the Polaris interface with the title 'Monitored assets'. It includes a search bar with the placeholder 'Search assets...' and a '+ Add' button. Below the search bar, it indicates '1 - 50 of 1394 assets'. A table lists assets with columns 'Asset' and 'Type'. The assets listed are:

Asset	Type
one.ormus.com 14.123.412	Host
Safari	Technology
dev.ormus.com 123.123.321	Host
JQuery	Technology
nginx	Technology

El detector de phishing más potente

Impulse su inteligencia de amenazas con el Threat Hunting de Axur

➔ Investigaciones proactivas

Amplio lago de datos para cazar amenazas
15 millones de señales analizadas a diario

➔ Búsquedas asistidas por IA

Simplifica consultas complejas con IA

➔ Cobertura integral

Explore credenciales, tarjetas, dominios y URLs

The screenshot shows the Threat Hunting interface with the title 'Threat Hunting'. It includes a search bar with the placeholder 'emailDomain=ormus.com,ormuspay.com'. Below the search bar, there is a table with columns 'Credentials', 'Credit Cards', 'URLs & Domains', and 'Password'. The table lists credentials for various email addresses and their corresponding passwords.

	Credentials	Credit Cards	URLs & Domains	Password
06/18/24 at 09:25	alice.williams@ormus.com			galaxyway2024
01/15/ 24 at 08:30	bob.smith@ormus.com			T9r\$zQ8#IU4w
02/22/24 at 03:45	carol.jones@ormuspay.com			Q1u\$M6z#X4cY
03/09/24 at 11:56	david.brown@ormus.com			thunderstorm007
04/17/24 at 06:15	emma.davis@ormuspay.com			Mountain@peak99
05/03/24 at 12:00	frank.miller@ormuspay.com			sandcastle456!
06/26/24 at 04:30	hank.moore@ormus.com			D6r#Y3w!T4IZ
07/14/24 at 09:00	mia.hall@ormuspay.com			L7m@Q1b&N8pX

Proteja sus activos y mejore su postura de seguridad ahora.

INICIAR CON UNA DEMOSTRACIÓN

Descubra todas nuestras soluciones en axur.com



AXUR