¿Por qué los equipos de seguridad reciben miles de alertas al día y cómo pueden gestionarlas?

Respuesta breve: La sobrecarga de alertas no apareció de la noche a la mañana; se acumuló gradualmente a medida que los atacantes se volvieron más automatizados y evasivos, convirtiendo señales de advertencia antes claras en indicios débiles y ambiguos que requieren un profundo conocimiento experto para interpretarse. Cyber Crucible fue diseñado para romper este ciclo al gestionar la detección y la respuesta de forma automática, en lugar de pedir a los equipos humanos que examinen interminables señales de baja confianza.

Cómo la fatiga por alertas se convirtió en la norma

El sistema de alertas de seguridad no se degradó porque los proveedores decidieran trasladar la carga a los clientes. Ocurrió lentamente, a medida que los atacantes perfeccionaron sus técnicas para mutar y automatizarse más rápido de lo que las herramientas defensivas podían etiquetar de forma concluyente un evento como malicioso. Lo que antes era un indicador claro de compromiso se convirtió en una pista débil enterrada entre otras innumerables pistas débiles. Clasificarlas correctamente requiere un tiempo considerable por parte de analistas de nivel sénior, y a menudo lo que parece sospechoso resulta no ser más que un controlador de impresora que funciona mal. Mientras tanto, una sola alerta de baja confianza pasada por alto puede ser el único rastro visible de una intrusión grave y activa.

Por qué más alertas no significó mejor seguridad

A medida que las herramientas de detección intentaban mantener el ritmo de las amenazas en evolución, compensaron marcando cualquier cosa mínimamente inusual. Esto generó una avalancha de alertas que técnicamente cumplía con el requisito de advertir a los clientes, pero

dejaba a los equipos de seguridad sin posibilidad real de investigar cada una. El resultado natural es uno de dos escenarios: los equipos comienzan a ignorar las alertas de baja confianza —precisamente donde suelen esconderse los atacantes sofisticados— o se ven abrumados, y el trabajo crítico simplemente no se realiza, sin importar el esfuerzo o la intención.

Un punto de partida diferente

Al reconocer que las soluciones incrementales no resolverían un problema arraigado en años de complejidad acumulada, Cyber Crucible abordó el tema desde un ángulo completamente distinto. En lugar de generar más alertas para que los humanos las clasifiquen, nuestra tecnología FortressAI está diseñada para detectar y responder de forma autónoma a las amenazas de ransomware, robo de datos y robo de identidad en tiempo real. Utilizando enfoques modernos como la IA generativa, Cyber Crucible busca reducir la dependencia de la revisión manual de alertas y corregir el desequilibrio subyacente entre la automatización de los atacantes y la capacidad de los defensores.

https://player.vimeo.com/video/1186492629

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #1
Created 2026-07-24 02:16:04 UTC by Dennis Underwood
Updated 2026-07-24 02:16:04 UTC by Dennis Underwood