kiara

Seguridad Cognitiva

Brochure de Soluciones

info@kiara-tech.com

QUÉ DETECTAMOS

- EXFILTRACIÓN DE DATOS
- ENCUBRIMIENTO DE ACTIVIDAD Y SALTEO DE CONTROLES DE SEGURIDAD
- FRAUDE INTERNO
- USO DE APLICACIONES PIRATAS
- JUEGO ONLINE (GAMBLING)
- ESCALACIÓN DE PRIVILEGIOS
- MOVIMIENTOS LATERALES
- RANSOMWARE
- INFILTRACIÓN A LA RED CORPORATIVA
- CYBER-AMENAZAS
- ABUSO DE MARCA EN WEB Y DEEP WEB
- FRAUDE EXTERNO
- AMENAZAS DE SEGURIDAD EN CLOUD
- AMENAZAS DE SEGURIDAD ESPECÍFICAS A UNA DE TERMINADA INDUSTRIA

COMPORTAMIENTO DE USUARIOS

Monitoreamos el comportamiento dentro de su red que pone en riesgo a su organización mediante la detección de patrones avanzados de amenazas .

Tecnologías Cognitivas al Servicio de la Seguridad

NUESTRAS SOLUCIONES DE SEGURIDAD DETECTAN CON PRECISIÓN Y RAPIDEZ AMENAZAS CON BASE A ANALÍTICOS AVANZADOS DE COMPORTAMIENTO.

En KIARA tenemos un área de especialización: **la detección**. Esto es, a través de diversos mecanismos detectamos cualquier comportamiento anómalo o riesgoso, con un enfoque basado en el riesgo y construido con base en tecnologías de machine learning y big data, lo que nos permite aumentar drásticamente los niveles de precisión, reducir en tasas sin precedentes los falsos positivos y acortar la ventana de detección a períodos cercanos al tiempo real.

Las tecnologías digitales han logrado avances determinantes en materia de sistemas cognitivos que, aplicados a la seguridad informática, han logrado construir mecanismos que detectan patrones de comportamiento que se asocian a factores de riesgos y permiten incluso adelantarse a las intenciones de los atacantes. Las tecnologías tradicionales de detección necesitan complementarse con analistas de SOC que realicen investigaciones, sin embargo, no hay esfuerzo humano que pueda atender todas las alertas generados por los sistemas de seguridad, ni conocimiento que reconozca cualquier intento malintencionado, ni capacidad para hacerlo en los tiempos que el negocio requiere.

La información para detectar un ilícito reside en las organizaciones y requiere de analítica avanzada para cobrar sentido y propósito en la detección. Solo hace falta poner esa información a trabajar y hacer que los datos hablen. La tecnología y el conocimiento para hacer esto último realidad es lo que brindamos en KIARA: sistemas cognitivos, aplicados a la seguridad y la prevención del fraude, para llevar la detección a un siguiente nivel y habilitar en las organizaciones nuevas posibilidades de negocio aprovechando los avances de la tecnología digital.

Elimine Amenazas Internas de Seguridad

CUANDO LOS MECANISMOS DE PREVENCIÓN NO SON CAPACES DE DETENER LAS ACTIVIDADES MALICIOSAS, LA ÚLTIMA BARRERA DE DEFENSA ES LA DETECCIÓN .

Contamos con soluciones de monitoreo y detección de seguridad avanzadas que aumentan la precisión y acortan la ventana del atacante. Dichas soluciones están basadas en analíticos de comportamiento de usuarios y entidades (UEBA) y detectan patrones de amenazas asociados a usuarios negligentes, usuarios maliciosos o cuentas comprometidas con mínima intervención humana.

Nueva Generación de SIEM. Los SIEM son soluciones que generan alertas para notificar sobre problemas de seguridad al agregar y correlacionar registros de muchas fuentes. Ya sea que quiera renovar su plataforma SIEM o integrar a la ya existente capacidades de detección avanzadas, nuestra solución, basada en UEBA, detecta automáticamente patrones de riesgo nunca vistos con las soluciones tradicionales, como el movimiento lateral o la escalación de privilegios, entre otros.

Monitoreo de empleados. Todas las actividades que sus empleados realizan en los equipos de su organización, incluso fuera de su red interna, son registradas y almacenadas en un servicio central, donde se someten a analíticos avanzados que detectan patrones de comportamiento complejos y de riesgo como el robo avanzado de información o cualquier tipo de actividad ilegal.

Detección de infiltración. Descubra y prevenga inusual agregación de datos y escalación de privilegios por parte de atacantes externos que roban credenciales de sus empleados provocando un daño extenso en su organización. Adicionalmente, detecte herramientas de movimiento laterales y ransomware.

kiara

INTELIGENCIA DE AMENAZAS

Monitoreamos 24x7 su marca en la web y deep web.

AMENAZAS ONLINE

Protegemos su portal transaccional bloqueando cualquier actividad de bots (robots) asegurando que sus usuarios, aún infectados por malware, realicen transacciones seguras.

FRAUDE ONLINE

Detectamos sesiones y transacciones generadas por defraudadores sin afectar la experiencia del usuario.

Elimine Amenazas Externas de Seguridad

MITIGUE EL FRAUDE Y OTRAS AMENAZAS EXTERNAS SIN PERJUDICAR LA EXPERIENCIA DE SUS USUARIOS

En los últimos años hemos visto cómo las organizaciones se han digitalizado, creando nuevos canales a disposición de sus clientes para consumir sus productos y servicios, que hicieron más ágil la interacción entre ambos. Sin embargo, el fraude y otras amenazas comenzaron a crecer en paralelo, obligando a las mismas a buscar mecanismos que permitieran mitigar pérdidas monetarias al mismo tiempo que protegían a sus usuarios.

Para atender esta problemática, en KIARA tenemos una **plataforma integral** de detección y prevención del fraude en múltiples canales que, a través de mecanismos basados en inteligencia artificial, brinda precisión en la detección sin afectar de manera negativa la experiencia del usuario.

Inteligencia de amenazas. Nuestro servicio de monitoreo 7x24 detecta sitios de phishing y troyanos, aplicaciones maliciosas en repositorios móviles y ataques de abuso de marca. Además, realiza cyber-inteligencia en la deep web y redes sociales para detectar cualquier tipo de ataque.

Navegación Segura. Nuestra solución protege a los clientes y sus dispositivos de las actividades maliciosas ocasionadas por malware (ej. man-in-the-browser) permitiendo que, incluso clientes con dispositivos infectados ,realicen transacciones en línea de manera segura.

Monitoreo de Transacciones. Mediante modelos de inteligencia artificial monitoreamos y detenemos en tiempo real y de manera muy precisa, transacciones fraudulentas en múltiples canales (tarjetas de débito/crédito desde el lado emisor y adquirente, banca en línea y móvil, IVRs, ATMs y sucursales).

Autenticación multi-factor avanzada. Nuestro framework de autenticación de doble factor ofrece más de 14 mecanismos que pueden aplicarse en múltiples canales como la banca en línea y móvil, IVRs, ATMs y sucursales. Entre ellos se encuentran los soft tokens, códigos QR, identificación biométrica como reconocimiento facial o huella digital, tecnologías push al celular, SMS, entre otros.

Biometría de comportamiento. Cada persona utiliza su dispositivo móvil o computadora de escritorio de un modo único y particular. La velocidad con la que tecleamos, la manera en que movemos el mouse, el ángulo con el que sostenemos el móvil o los trazos que nuestros dedos realizan sobre una pantalla táctil nos identifican como si fuera un ADN de nuestro propio comportamiento. Nuestra tecnología de biometría de comportamiento permite detectar todos estos parámetros cuando interactuamos con un servicio digital e identificar si un defraudador intenta suplantar nuestra identidad.

kiara

ACERCA DE KIARA

Somos una compañía líder en el mercado de seguridad informática especializada en soluciones de detección.

Apoyados principalmente en la inteligencia artificial y consultoría de excelencia, ayudamos a las organizaciones a detectar comportamiento anómalo en sus sistemas o redes y les brindamos facilidades para responder a dichas anomalías mediante la investigación o el aseguramiento de la identidad del usuario.

kiara

+52 55 9155 9070
info@kiara-tech.com

www.kiara-tech.com