Vectra ITDR para Microsoft Azure AD | Detección de amenazas a la identidad basada en IA

Vea, comprenda y detenga los ataques dirigidos a servicios de identidad SaaS críticos

Con el creciente uso de servicios SaaS y el aumento del volumen de usuarios remotos, los equipos de seguridad deben hacer más para garantizar la identidad de los usuarios y las entidades que interactúan y acceden a los datos a través de dominios en la nube. Zero Trust sigue teniendo un gran alcance, ya que las organizaciones luchan con las complejidades de configuración y el apoyo de expertos para la gestión de identidades y accesos; lo que hace que los actores de amenazas cambien sus objetivos a los servicios IAM, incluido Microsoft Azure Active Directory (AD). Ante el aumento constante de los ataques, los equipos de seguridad necesitan una forma nueva y más fácil de identificar a los actores de amenazas que aprovechan las cuentas con privilegios de personas y máquinas. Vectra puede ayudar.

Principales retos

- Visibilidad limitada del SOC en Azure AD
- Conocimiento de los riesgos de las aplicaciones federadas
- Puesta en peligro de cuentas y actividad inadvertida de los usuarios
- Comprensión profunda de los ataques

Sepa cuándo sus cuentas Azure AD están comprometidas

Vectra Identity Threat Detection and Response (ITDR) para Azure AD es la defensa contra ataques basada en IA más avanzada del sector para cerrar la puerta a los ciberatacantes que acceden a Azure AD. Vectra ITDR para Azure AD aprovecha Security AI-driven Attack Signal Intelligence™ para descubrir y contrarrestar los compromisos de cuentas y cerrar la puerta a los ciberatacantes que acceden a aplicaciones y servicios federados, incluyendo: Azure AD M365, Salesforce, AWS y VPNs.

Integrada con la plataforma Vectra, Vectra ITDR enriquece las capacidades CDR con la perspectiva del usuario sobre las actividades en aplicaciones federadas y SaaS, donde la IA de seguridad da sentido a los inicios de sesión no autorizados, el acceso al motor de scripting, el abuso de aplicaciones de confianza, los cambios en la federación de dominios y el abuso general de privilegios en la nube. La IA se aplica para aprender de los datos, identificar patrones y tomar decisiones sin intervención humana, garantizando la visibilidad de los patrones cambiantes, los usuarios y los administradores, incluso cuando falla la MFA o la autenticación se realiza con cookies robadas.

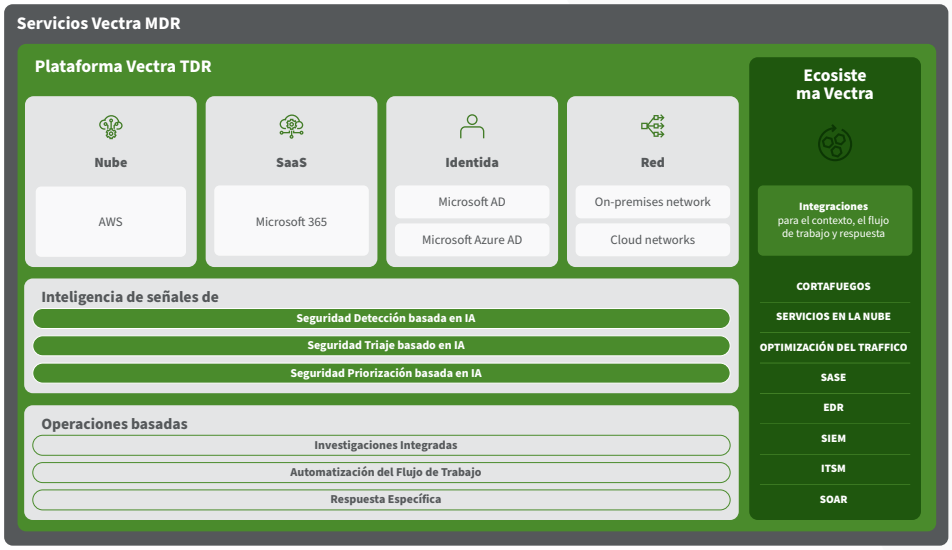
Principales funciones del producto

- **Detección basada en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de Seguridad, Vectra va más allá de las firmas y la simple detección de anomalías para exponer la narrativa completa de los ataques. Con un análisis exhaustivo de los datos de cuentas de Azure AD enriquecido con información sobre organizaciones y consorcios, Vectra ITDR descubre el uso malicioso de cuentas y credenciales comprometidas. Vectra revela un contexto de amenazas más profundo por cuenta para impulsar la atribución y detectar más del 90 % de las técnicas maliciosas de MITRE ATT&CK.
- **Triaje basado en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de Seguridad, Vectra comprende las amenazas previamente priorizadas y la actividad sospechosa de Azure AD. Mediante el análisis continuo de eventos, Vectra distingue los eventos maliciosos de los benignos basándose en el contexto y los puntos en común. A continuación, las detecciones benignas se clasifican automáticamente con la perspectiva de un analista experto.
- **Priorización basada en IA**
  Aprovechando la Inteligencia de Señales de Ataque basada en IA de seguridad, Vectra correlaciona, puntúa y clasifica automáticamente detecciones múltiples y concurrentes cuando se desarrollan los eventos. Los análisis de IA evalúan automáticamente los incidentes en comparación con los eventos existentes al nivel de un analista de seguridad altamente experimentado, revelando al instante los niveles de exposición al riesgo y la priorización relacionada para que SecOps pueda dedicar más tiempo a impulsar planes de acción.
- **Investigación avanzada**
  Vectra simplifica la investigación en profundidad y pone las respuestas al alcance de los analistas, reduciendo el esfuerzo y el tiempo necesarios para ejecutar consultas complejas, interpretar los resultados y sacar a la luz de forma proactiva señales para detener el avance de las amenazas. Las conclusiones extraídas de grandes cantidades de datos se interpretan automáticamente con detalles actualizados, de modo que los analistas de seguridad están mejor informados y pueden adoptar medidas de respuesta en el momento oportuno.
- **Cuadro de mandos del caos**
  Vea claramente el impacto y cualquier laguna en sus configuraciones de Azure AD. La postura activa muestra la actividad que realizan los usuarios normales y dónde podría estar dejando a tu organización abierta a futuros ataques, para que sepas qué riesgos mitigar.
- **Respuesta específica**
  Con un contexto de amenazas más profundo que el de las herramientas nativas de Microsoft, los equipos de seguridad adquieren amplias capacidades para responder, contener, investigar, comunicar y abordar los sistemas comprometidos en menos tiempo. La aplicación de la normativa por parte de los analistas pone a los humanos al mando con un enfoque flexible que permite flujos de trabajo automatizados o acciones activadas por los analistas en la interfaz de usuario. Los controles de respuesta “listos para usar” incluyen herramientas y guías ya existentes, lo que infunde confianza a todo el equipo, reduce el agotamiento y minimiza los costes.

Explore la plataforma Vectra

La plataforma Vectra Threat Detection and Response (TDR) combina una completa cobertura de la superficie de ataque en la nube pública, SaaS, identidad y red. Aprovechar la seguridad Señal de ataque basada en IA Intelligence™, obtén una claridad de señal inigualable que te permite tener el control mientras defiendes contra los ciberatacantes modernos, evasivos y avanzados.

- **Cobertura de ataques:** elimine las amenazas desconocidas en 4 de sus 5 superficies de ataque: nube, SaaS, identidad y redes.
- **Claridad de las señales:** aproveche la inteligencia de las señales de ataque para detectar, clasificar y priorizar automáticamente las amenazas desconocidas.
- **Control inteligente:** arme la inteligencia humana para cazar, investigar y responder a amenazas desconocidas.



Por qué las empresas eligen Vectra para Azure AD

- **Attack Signal Intelligence** proporciona señales enriquecidas que los analistas pueden utilizar para automatizar las tareas manuales relacionadas con la detección, el triaje y la priorización de amenazas.
- **Fácil proceso de configuración en 10 minutos** sin necesidad de hardware.
- **Cobertura sin agentes que se despliega en minutos** y activa la detección sin firmas, escuchas virtuales ni políticas estáticas.
- **Detecte amenazas a través de las tácticas de MITRE** que otras soluciones no pueden ver.
- **Investigación y respuesta integradas** que aceleran la detección de amenazas y amplían la cobertura para reducir significativamente el tiempo medio de respuesta (MTTR).
- **Elimina montañas de falsos positivos** para que los analistas dispongan de más tiempo para la investigación proactiva y estratégica.
- **Vista única de la actividad que vincula las detecciones o**riginadas en Azure AD, M365, on-premises y AWS.

Acerca de Vectra

Solo Vectra optimiza la IA de seguridad para comprender los comportamientos de los atacantes en la nube pública, la identidad, las aplicaciones SaaS y los centros de datos. Aprovechando la IA de seguridad, Vectra se compromete a capacitar a los equipos de seguridad para pasar a la ofensiva y evitar que los ciberataques se conviertan en brechas. Vectra proporciona la cobertura de amenazas, la claridad y los controles que los equipos de operaciones de seguridad necesitan para crear estrategias de seguridad más eficaces, eficientes y resistentes. Organizaciones de todo el mundo confían en la plataforma y los servicios gestionados de Vectra para obtener una mayor resistencia frente al ransomware, la cadena de suministro, el compromiso de cuentas y las amenazas internas. Más información en www.vectra.ai.

Si desea más información, póngase en contacto con nosotros:
Correo electrónico: info@vectra.ai | vectra.ai