Anomali Lens

La inteligencia artificial tiene el potencial de cambiar la forma en que los analistas de seguridad trabajan. También puede transformar la interfaz de comunicación entre las operaciones de seguridad y la empresa. Al incorporar inteligencia artificial (IA) dentro de la plataforma de operaciones de seguridad, Anomali mejora la experiencia de los analistas y la eficiencia operativa.

El uso de la IA por parte de Anomali se extiende a toda la interfaz hombre-máquina, aprovechando las capacidades de procesamiento de lenguaje natural (natural language processing, NLP) para transformar los datos generados por el ser humano en información legible para la máquina y convertir los datos generados por la máquina en información comprensible para el ser humano con generación de lenguaje natural (natural language generation, NLG). Anomali transforma y aumenta las operaciones de seguridad con el poder de la IA integrada en la plataforma.

BENEFICIOS

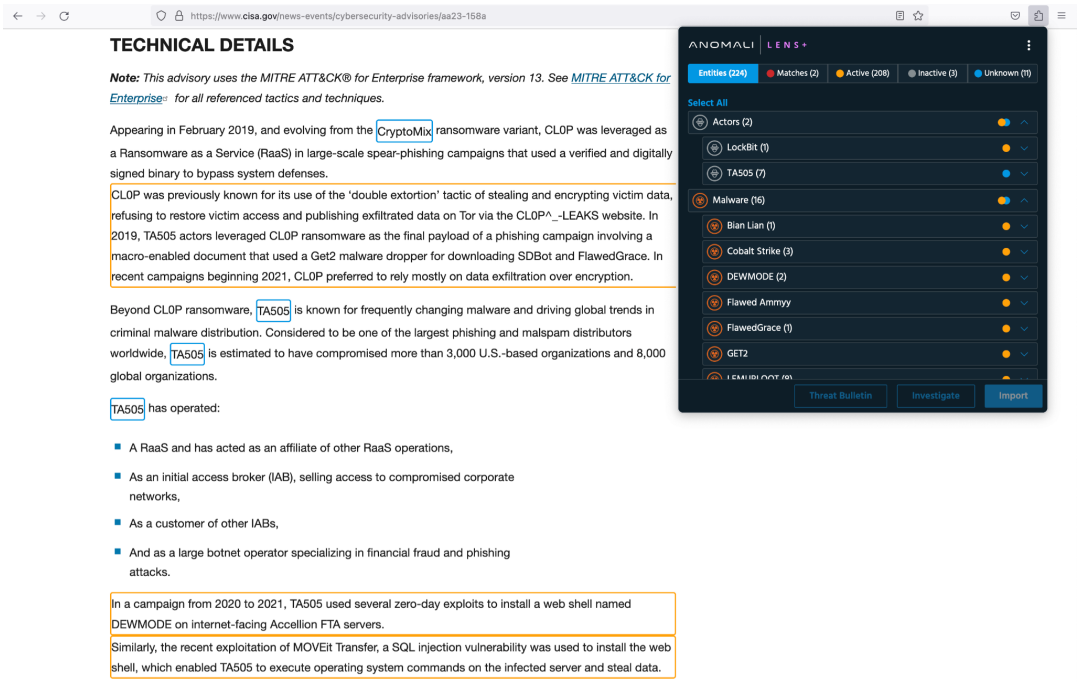
- Pase de datos no estructurados a inteligencia relevante en cuestión de segundos con procesamiento de lenguaje natural.
- Enriquezca de forma automática la inteligencia con actores, vulnerabilidades, industrias y más.
- Transforme los datos de máquina en información para ejecutivos y analistas con la generación de lenguaje natural.
- Acelere y simplifique la búsqueda de amenazas con contexto de inteligencia y la interfaz de lenguaje natural.
- Automatice los procesos manuales que requieren mucho tiempo para aumentar la productividad de los analistas.
- Mejore la comunicación y la colaboración interfuncional.

La arquitectura de Anomali correlaciona de manera automática la telemetría con los datos sobre amenazas externas a la velocidad de la IA

Procesamiento de lenguaje natural

La inteligencia no estructurada contra amenazas es un recurso vital para analistas y ejecutivos. Sin embargo, incorporar e interpretar estos datos en grandes cantidades para obtener información relevante puede ser una tarea ardua y requerir mucho tiempo. Esto es muy importante durante sucesos significativos, como un nuevo ataque informático o una filtración de datos.

Anomali Lens incluye un potente motor de procesamiento de lenguaje natural que ayuda a poner en funcionamiento la inteligencia contra amenazas mediante el análisis automático del contenido digital (PDF, HTML, Office 365 - Word, Excel, Outlook) para identificar amenazas relevantes y optimizar el ciclo de vida de la investigación y la generación de informes. Lens, que está disponible como extensión del navegador o complemento de Office 365, resalta de forma automática la información importante en artículos de noticias, boletines de amenazas, redes sociales, documentos de investigación, blogs, repositorios de codificación y fuentes de contenido interno, y ayuda a los analistas a comprender con rapidez todo el significado y contexto de una amenaza y a tomar medidas en toda la organización para reducir el riesgo. Los ejecutivos pueden obtener un contexto inmediato para los informes sobre los ataques informáticos en línea con visibilidad de la postura actual de sus organizaciones en un solo clic.

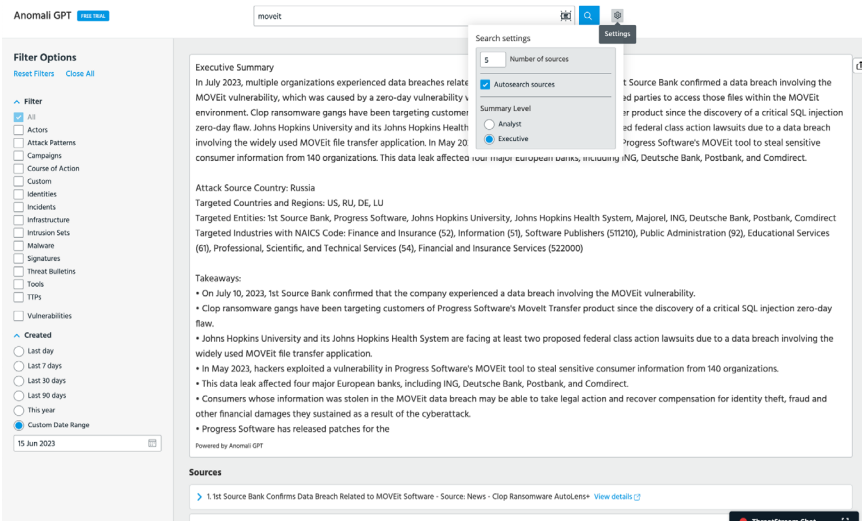


Examina de forma automática el contenido digital (PDF, HTML, OFFICE 365, etc.) para identificar las amenazas relevantes y simplificar la investigación y la generación de informes sobre esas amenazas.

Generación de lenguaje natural

Los datos son la esencia de la seguridad moderna e incluyen registros de varias fuentes de seguridad, inteligencia contra amenazas, incidentes, vulnerabilidades y más. La mayoría de las iniciativas de seguridad se saturan de información y a menudo carecen de contexto para la toma de decisiones en tiempo real. Anomali aprovecha el transformador generativo preentrenado (Generative Pretrained Transformer, GPT) para convertir las grandes cantidades de datos en información procesable y comprensible por el ser humano.

La capacidad de GPT de Anomali es un modelo privado de GPT, que se basa en el repositorio más grande del mundo de inteligencia exclusiva contra amenazas. Resume de forma automática los eventos importantes de varias fuentes de información, enriqueciéndolos con inteligencia exclusiva de Anomali para informar a los ejecutivos y analistas sobre los puntos clave y los riesgos comerciales asociados con los eventos de amenazas. También enriquece automáticamente la inteligencia con etiquetas y asociaciones de actores; malware; tácticas, técnicas y procedimientos (TTP) de MITRE; países; industrias; vulnerabilidades y más. Resuma los modelos de amenazas, busque en la base de conocimientos, busque amenazas, genere resúmenes de noticias para ejecutivos y muchas tareas más, utilizando lenguaje natural con GPT de Anomali.



Genere de forma automática resúmenes para ejecutivos y analistas para mejorar las comunicaciones entre equipos y acelerar los flujos de trabajo de los analistas

CAPACIDADES CLAVE

- **Obtenga inteligencia:** Transforme datos no estructurados de diferentes fuentes, como blogs, boletines de amenazas, Office 365, etc., en inteligencia en cuestión de segundos con procesamiento de lenguaje natural. Reconozca y etiquete los TTP de ATT&CK de MITRE para identificar y asociar las perspectivas de los actores.
- **Inteligencia exclusiva:** Pase de canales RSS tradicionales a canales RSS de alta calidad exclusivos y enriquecidos con resúmenes y conclusiones para ejecutivos generados por GPT con AutoLens+. Los canales incluyen Bleeping Computer, CISA Advisors, InfoSecurity Magazine y muchos más.
- **Automatice el enriquecimiento:** Agregue a la inteligencia etiquetas y asociaciones de actores, países, industrias, vulnerabilidades y más de forma automática con AutoLens+ a fin de traducir los indicadores técnicos en riesgo empresarial.
- **Ponga en funcionamiento la inteligencia**: Automatice la importación de un indicador de compromiso (Indicator of Compromise, IOC) en boletines de amenazas, investigaciones y detecciones en el entorno de pruebas, así como la creación de informes para exportar investigaciones como inteligencia terminada.
- **Obtenga información:** Proporcione paneles personalizables para obtener noticias identificadas sobre tendencias de malware, vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE), actores y más.
- **Resuma y colabore:** Resuma con rapidez la información de eventos importantes de varias fuentes mediante GPT/IA generativa para informar a los ejecutivos e impulsar una toma de medidas rápida.
- **Acelere la búsqueda:** Pase de boletines a la búsqueda de huellas de adversarios en su entorno con un solo clic. Busque años de datos en segundos.
- **Busque con lenguaje natural:** Almacene petabytes de datos a bajo costo en un lago de datos escalable y nativo de la nube, y búsquelo fácilmente en segundos utilizando un lenguaje natural.

Casos de uso clave

OBTENGA ACCESO A LA INTELIGENCIA DE FUENTES DE DATOS NO ESTRUCTURADOS

Analice correos electrónicos de fraude electrónico, direcciones de correo electrónico maliciosas, URL y hash desde un boletín de amenazas de origen, blog, Office 365, PDF o sitio web.

PONGA EN FUNCIONAMIENTO ATT&CK DE MITRE

Asocie de forma automática la inteligencia incorporada con técnicas escaneadas e importadas con los ID de ATT&CK de MITRE y, a continuación, exporte una investigación con solo pulsar un botón.

OBTENGA INFORMACIÓN SOBRE RIESGOS COMERCIALES A PARTIR DE LA INTELIGENCIA

Etiquete y asocie de forma automática nueva inteligencia con actores, países, industrias, vulnerabilidades, etc., para identificar el riesgo comercial y priorizar las medidas de respuesta.

BUSQUE AMENAZAS ACTIVAS

Con un solo clic se puede determinar si se observa un indicador de amenaza o TTP escaneado en su entorno, analizando años de datos en segundos.

GENERE INFORMES SOBRE INCIDENTES

Cree informes de calidad profesional para informar sobre la detección de amenazas, las respuestas y los esfuerzos de corrección, así como la gestión.

COLABORACIÓN Y TOMA DE DECISIONES INTERFUNCIONALES

Sintetice con rapidez información confidencial de varias fuentes de inteligencia en resúmenes que se pueden compartir para informarla.

REDUZCA EL CANSANCIO DE LOS ANALISTAS

Automatice las tareas repetitivas, incluida la extracción y el análisis de inteligencia, las investigaciones sobre incidentes, la generación de informes y las comunicaciones ejecutivas.

	LENS	LENS+	AUTOLENS+	GPT
ANÁLISIS E IDENTIFICACIÓN DE LAS ENTIDADES DE AMENAZAS				
Analice páginas web para identificar las entidades de amenazas	✔	✔		
Analice las consolas y los informes de productos web	✔	✔		
Analice documentos de MS O365 (Outlook, Word, Excel)		✔		
Analice documentos PDF		✔		
Analice de forma automática las páginas web		✔		
Analice y autogestione los canales RSS para obtener inteligencia				✔
ESTADO DE LAS ENTIDADES DE AMENAZAS, RELEVANCIA Y ETIQUETADO				
Resalte y vea información sobre las entidades dentro de los activos analizados	✔	✔		
Busque entidades de amenazas con un solo clic con Security Analytics	✔	✔		
Vea los detalles de las entidades de amenazas con un solo clic en ThreatStream	✔	✔		
Destaque los TTP de ATT&CK de MITRE		✔		
Automatice el etiquetado de países, industrias, actores, vulnerabilidades, TTP de MITRE, etc.			✔	
ANÁLISIS Y USO				
Proporcione resúmenes de GPT para los canales RSS			✔	
Resuma varios artículos de noticias para los ejecutivos y analistas				✔

	LENS	LENS+	AUTOLENS+	GPT
Importe las entidades de amenazas a ThreatStream		✔		
Cree o actualice investigaciones		✔		
Inspeccione las URL en el entorno de pruebas		✔		
Cree modelos de amenazas a partir de fuentes de inteligencia*				✔
Busque con lenguaje natural				✔
Búsqueda en la base de conocimientos				✔
USO				
Análisis de páginas	100	Ilimitado		
Usuarios	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Adquisición	Ninguna	Ilimitado	??	??
IMPLEMENTACIÓN				
Extensión del navegador (Chrome, Firefox, MS Edge)	✔	✔		
Complemento implementado en TI (Chrome, Firefox, MS Edge) Complemento de Microsoft O365	✔	✔		
Interfaz de usuario de la plataforma sde Anomali		✔	✔	✔

ANOMALI