Trend Micro Vision One™

XDR & ASRM

EDSI Trend Argentina

Asistencia técnica - octubre 2023

ACLARACIÓN

El siguiente documento tiene la finalidad de servir como guía para un breve recorrido por la consola de **Vision One**, abordando tanto su enfoque **reactivo** (XDR Threat Investigation) como su enfoque **proactivo** (Attack Surface Risk Management).

Además, compartimos con usted una breve explicación de aquellos módulos dentro de la consola, que permitirán gestionar los riesgos de los activos de la empresa de manera eficaz y visualizar las diversas alertas, eventos y detecciones generadas por la misma.

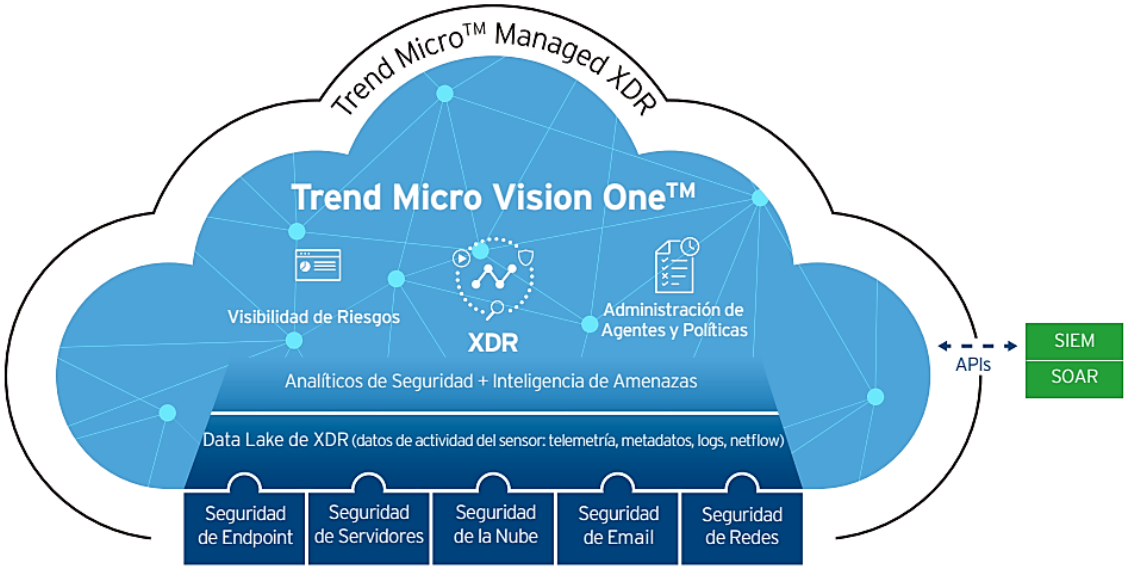
Cualquier duda o consulta, ¡comuníquese con nosotros!

INTRODUCCIÓN – Vision One™

Con un panorama de amenazas en constante evolución, se necesitan capacidades para ayudar con la detección y la respuesta ante las amenazas que puedan evadir sus defensas.

Vision One, es una plataforma de defensa frente a amenazas, que proporciona una **visibilidad centralizada de los riesgos**, y **prioriza las alertas**.

Ofreciendo entonces una tecnología de detección y respuesta extendidas, es decir de capacidades profundas y amplias de **XDR** que recopilan y **correlacionan** automáticamente los datos a lo largo de múltiples capas de seguridad (emails, endpoints servidores, workloads en la nube y redes).



Trend Micro Vision One previene la mayoría de los ataques gracias a una protección automatizada.

ENFOQUES

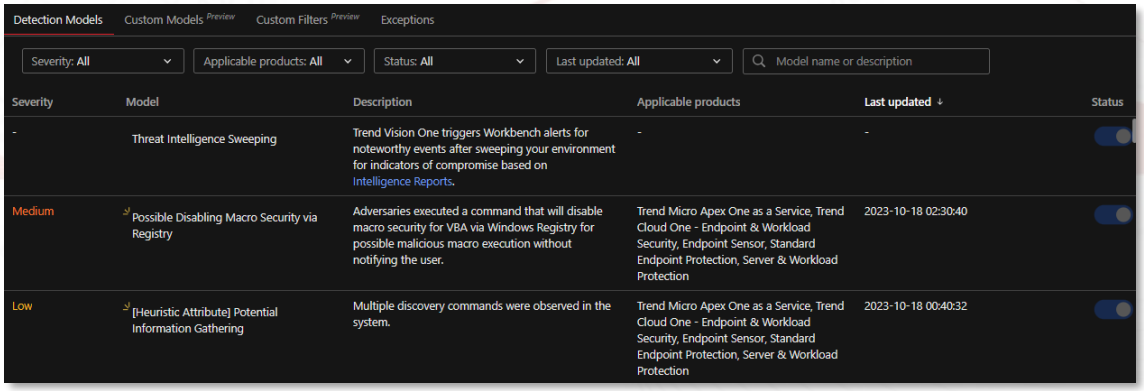
¿Qué tenemos en la parte re-activa de Vision One?

En el apartado de **XDR Threat Investigation**, hablamos de aquello que nos permite detectar e investigar en profundidad los distintos eventos. Dentro de este, destacamos los siguientes módulos para ir familiarizando y aprovechar las grandes funcionalidades de Vision One.

Detection Model Management

Hablamos de la inteligencia de Vision One de **correlacionar los datos**.

Este módulo cuenta con varios modelos de detección desarrollados por **Trend Micro**. Estos modelos, mediante la aplicación de diversas reglas, filtros y análisis de eventos, tienen la capacidad de identificar amenazas dentro de la infraestructura.

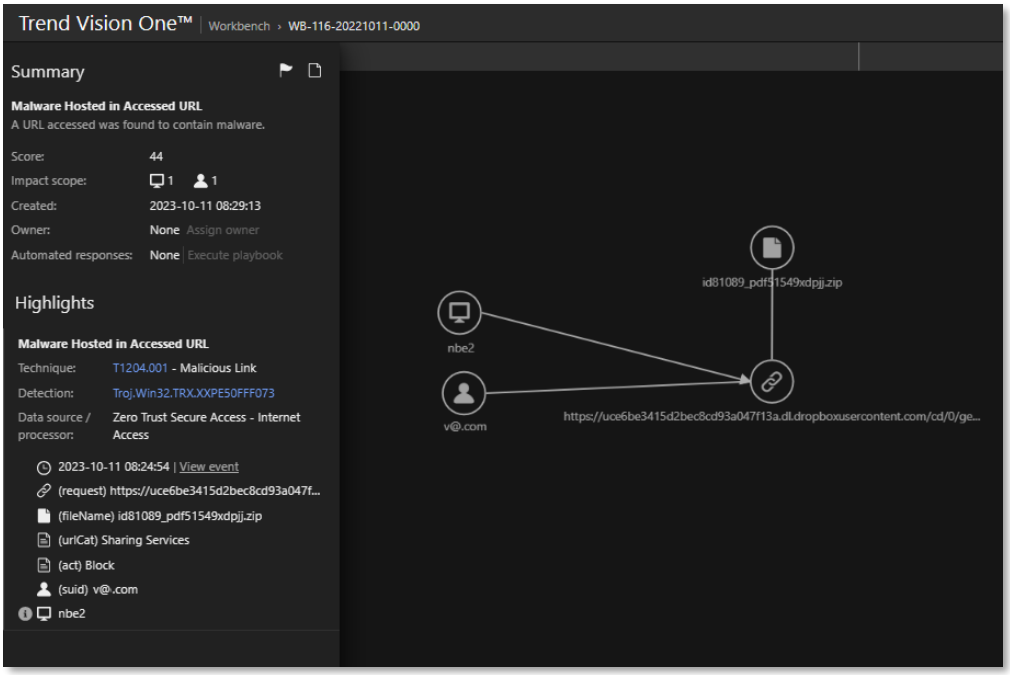


Las alertas vivas generadas por estos modelos de detección se presentan en forma de **Workbench**. Estas alertas correlacionadas resultan de alta fidelidad para definir cualquier actividad como maliciosa.

Workbench

Este módulo ofrece una lista detallada de alertas activadas por los modelos de detección, así como incidentes que están correlacionados con estas alertas.

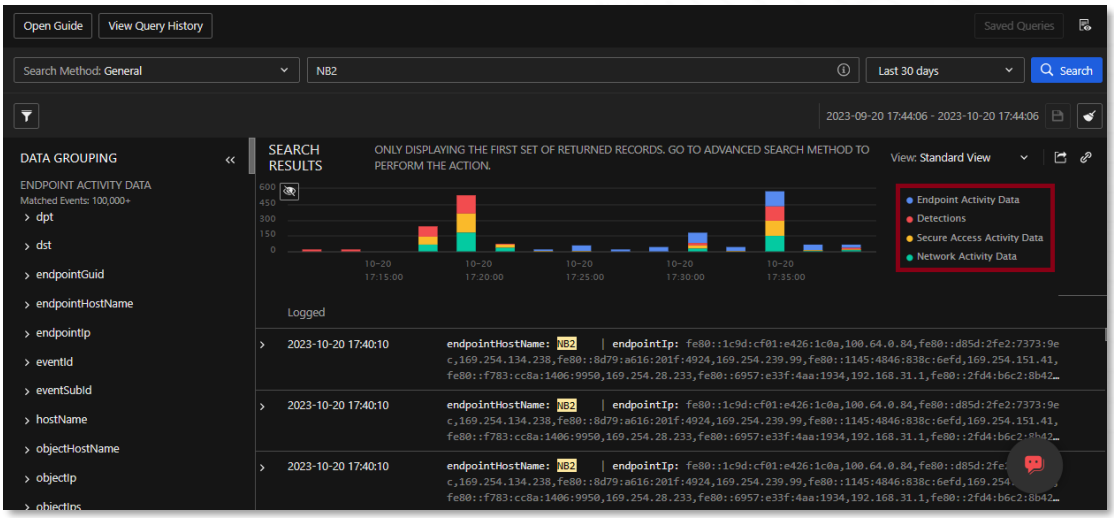
Además de proporcionar esta información crucial, el Workbench también identifica los equipos y/o cuentas específicas que se han visto afectados.



Esto permite una comprensión precisa del **alcance de la amenaza** y facilita la **toma de decisiones** informadas para abordar cada incidente.

Search

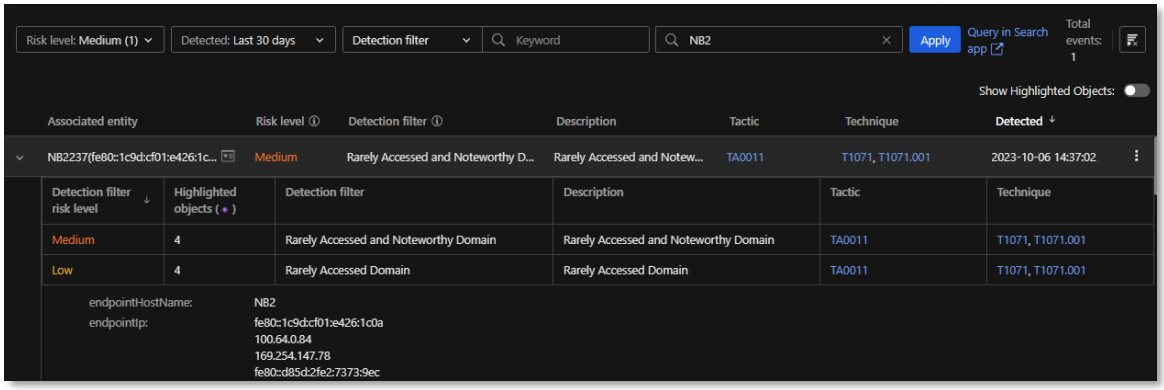
Dentro de este módulo, visualizamos toda la **telemetría en crudo** del equipo. Como puede ser cualquier creación, modificación, ejecución de un archivo, la modificación de llaves de registro, etc.



Además, ofrece diferentes métodos, filtros y un lenguaje de consulta (query) para identificar, clasificar y recuperar los resultados de la búsqueda.

Observed Attack Techniques

Nos muestra los eventos individuales detectados en su entorno que pueden activar una alerta y cualquier información de **MITRE** relacionada.



MITRE es una base de conocimientos que consta de las diferentes estrategias y técnicas específicas que utilizan los ciberdelincuentes para explotar las vulnerabilidades en su sistema.

Proporcionándonos entonces tácticas adversarias, técnicas ya conocidas, para identificarlas rápidamente y tomar acción desde Vision One.

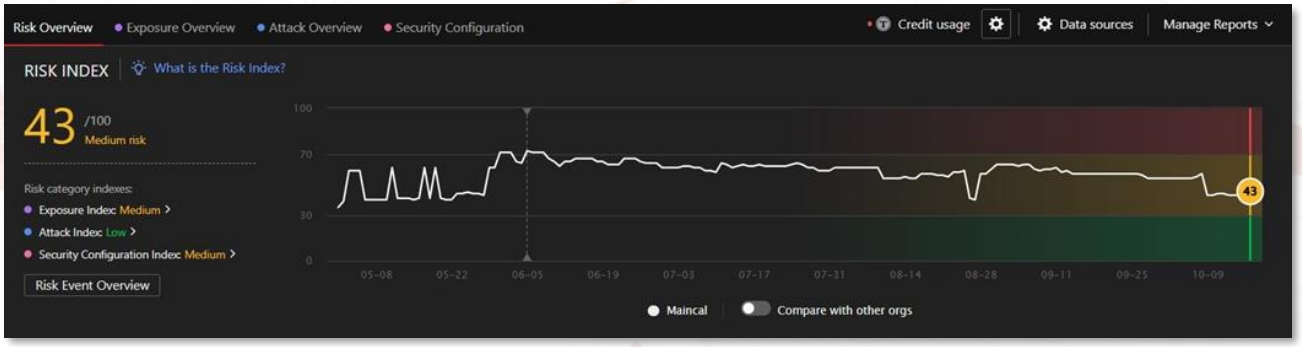
¿Qué tenemos en la parte proactiva de Vision One?

En primer lugar, tenemos el apartado de **Risk Insight**, el cual cuenta con diversos módulos que los ayudaran a **evaluar** y **gestionar** los diferentes **riesgos** de los activos de la empresa.

Executive Dashboard

Este apartado nos proporciona información sobre el índice de riesgo general de su empresa, que es una puntuación exhaustiva basada en la evaluación dinámica de los factores de riesgo, incluida la exposición, el riesgo de ataque y el riesgo de las configuraciones de seguridad.

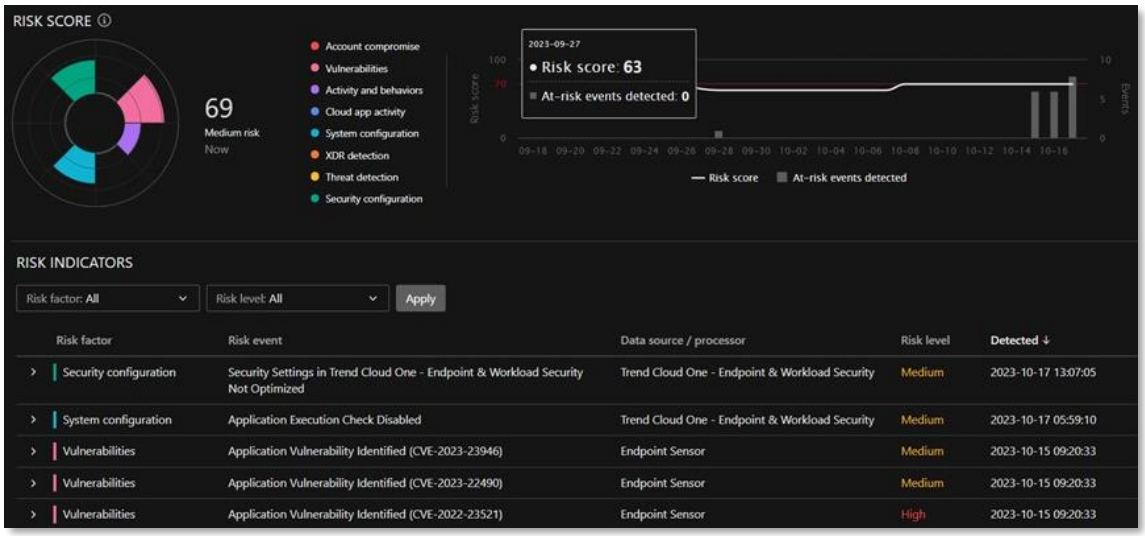
Permitiéndonos entonces tener una **cuantificación del riesgo** para evaluar rápidamente las condiciones en la que su empresa se encuentra, dando a entender que un puntaje lejano al 100 pasaría a ser nuestro nuevo objetivo.



Sumando entonces la porción de **ASRM**, contamos con los siguientes 2 módulos, que nos serán de gran utilidad a la hora de visualizar nuestro riesgo y profundizar nuestra investigación.

Attack Surface Discovery

Dentro de este módulo encontraremos información sobre diversos activos dentro de la organización, incluyendo a los endpoints, cuentas, dominios e IPs públicas a internet, así como las aplicaciones.

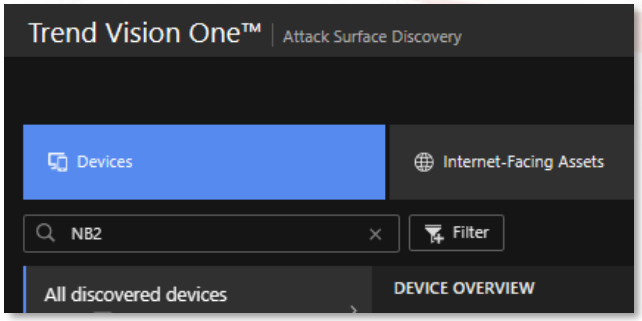


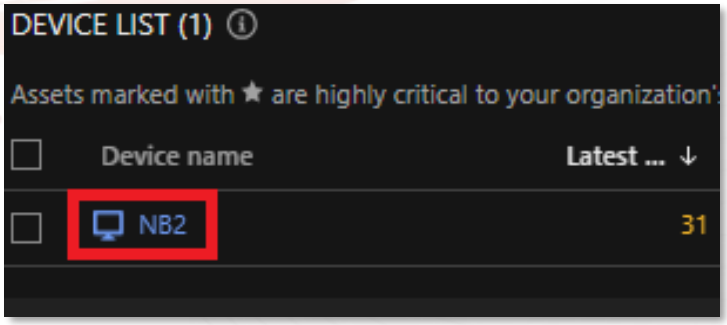
La característica fundamental de este módulo radica en la presentación de los distintos activos junto con su correspondiente puntaje de riesgo.

Al acceder a un elemento, podrán obtener información relacionada con vulnerabilidades, configuraciones del sistema y seguridad mal configurada, detección de amenazas, actividad y comportamiento, entre otros aspectos relevantes.

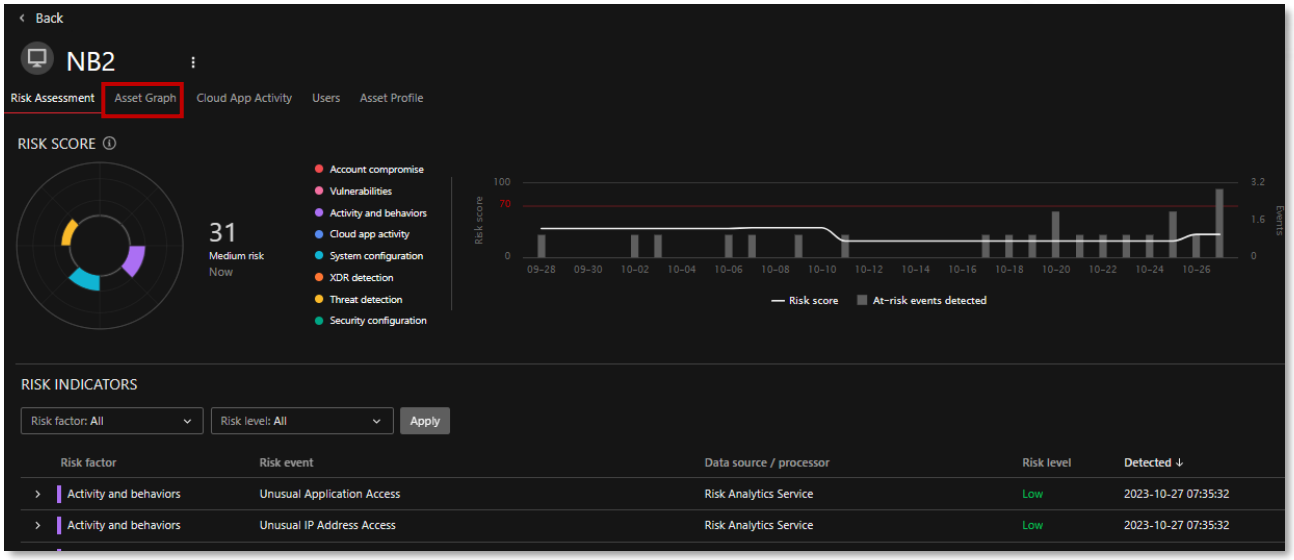
Además, podemos realizar la búsqueda de un endpoint/usuario en particular, devolviéndonos la información relacionada al mismo.

Para esto último en el apartado de **Attack Surface Discovery**, en el módulo de **Devices**, en el buscador indicamos el nombre del endpoint a encontrar y lo seleccionamos.





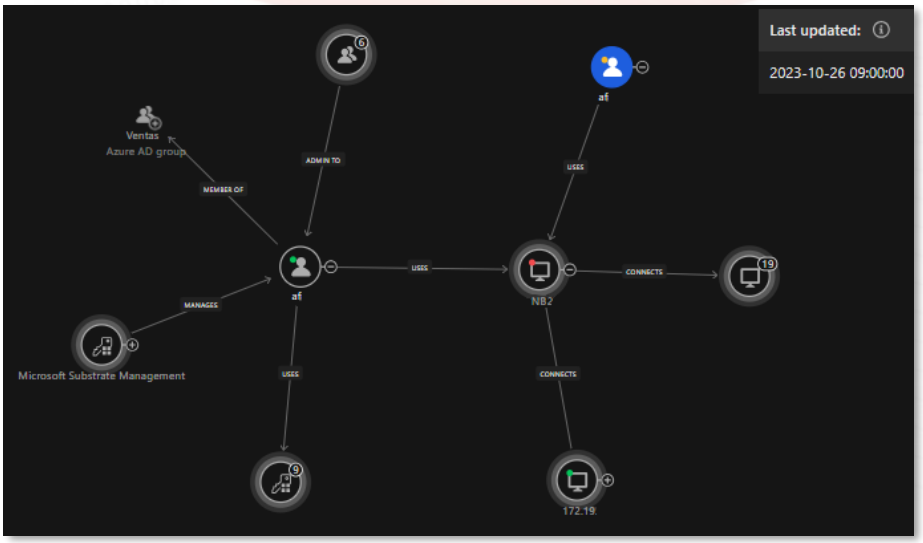
Nos brindará la siguiente información de cada una de la clasificación de riesgos de ese dispositivo.



Algo aún más interesante que nos brinda este apartado, es la capacidad de correlacionar la información de un usuario/dispositivo, si seleccionamos el módulo de **Asset Graph**.

Nos muestra esta 'ramificación' en la cual podemos identificar este tipo de datos:

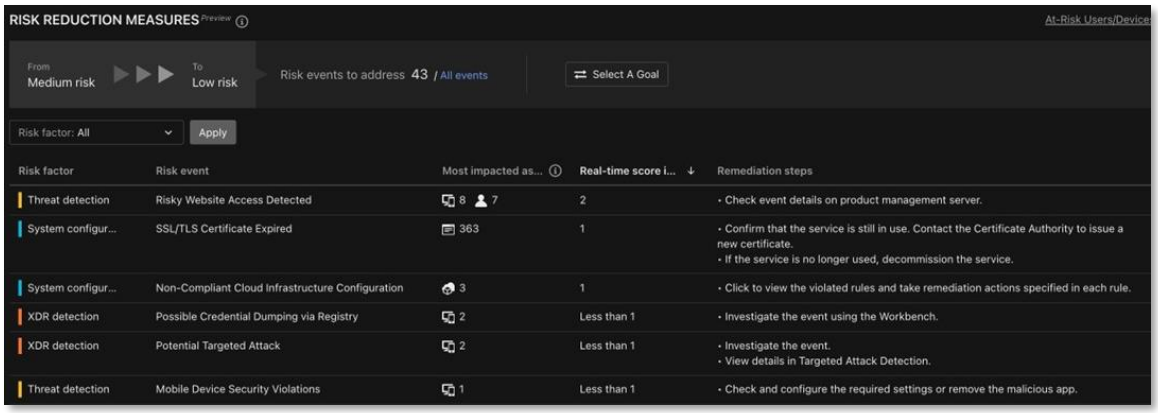
- El usuario en este dispositivo es “af”
- Utiliza el endpoint llamado “NB2”
- Pertenece al grupo de “Ventas” determinado por el Azure AD
- Visualizamos que dispone de ciertas credenciales
- Conexión con otros equipos, y más



Operations Dashboard

Nos permite ver información sobre factores de riesgo relevantes y tomar acciones correctivas para lograr objetivos específicos, como pueden ser el de reducción de riesgos.

Este widget identifica los eventos de riesgo con mayor impacto en el índice de riesgo, los activos a los que afectan estos eventos y los pasos de solución recomendados.



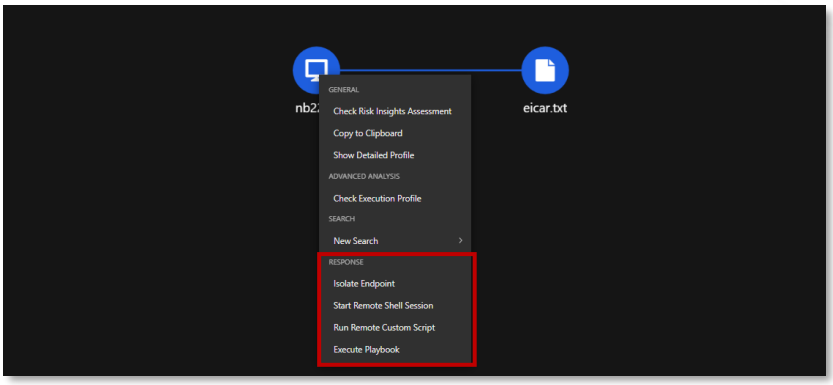
Nos brinda la capacidad de detectar e **investigar a fondo** una variedad de eventos, utilizando los datos recopilados de diversos componentes de la empresa, como los endpoints, servidores, redes y correos electrónicos.

¿Qué tenemos de respuesta en Vision One?

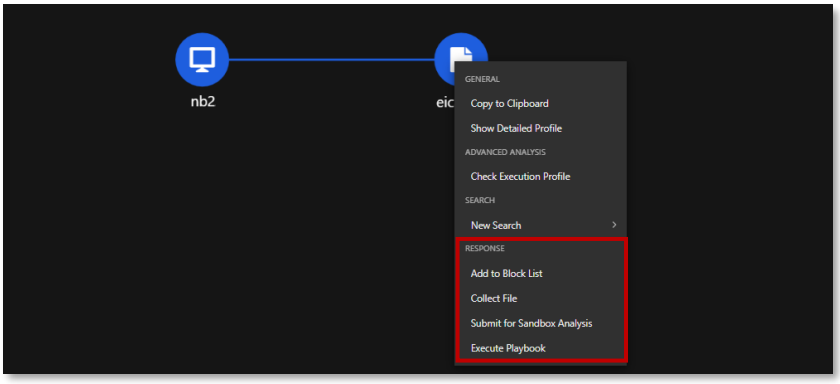
Teniendo en cuenta tanto la parte de **XDR** y los módulos que nos trae **ASRM**, la acciones a tomar frente aquello malicioso o sospechoso (como puede ser hasta con las casillas de correo) se vuelve aún más sencillo.

Desde la parte de los **Workbench**, podemos hacer *click derecho* en los ítems que nos proporciona esta alerta correlacionada y actuar.

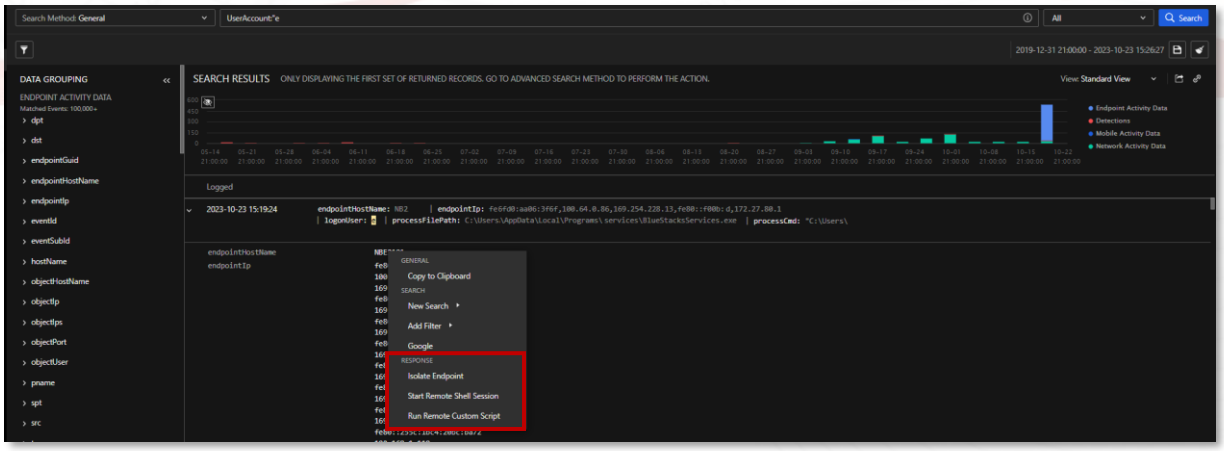
En este caso actuamos sobre el **dispositivo**, como puede ser aislarlo, correr un script, entre otras.



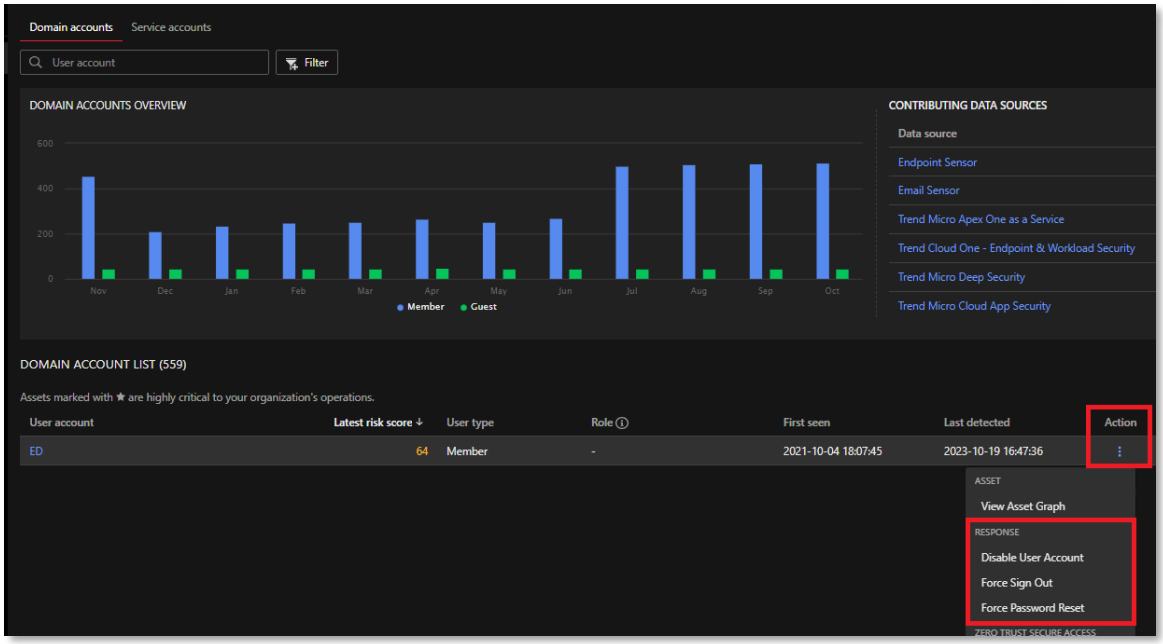
En este caso actuamos sobre el archivo, como puede ser añadirlo a la lista de objetos bloqueados, recolectarlo para una posterior investigación, entre otras.



También podemos tomar acción mediante el **Search**.



Y también podemos tomar acción desde **Attack Surface Discovery**, en este caso frente a un determinado usuario, podemos forzar un cierre de sesión, deshabilitar la cuenta del usuario, entre otras.

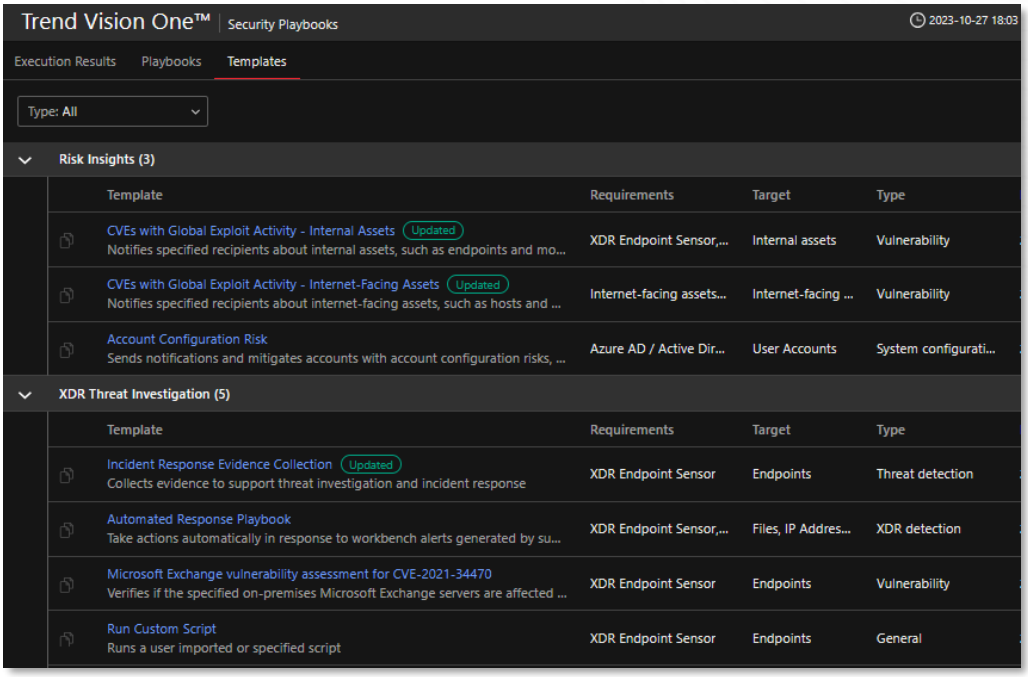


Security Playbooks

Vision One cuenta con **respuestas automatizadas**, conocidas como **Playbooks**, que como bien indicamos anteriormente en su nombre, facilitan la automatización de diversas acciones.

Esto no solo alivia la carga de trabajo, sino que también acelera significativamente las tareas e investigaciones de seguridad.

Los **Playbooks** están especialmente diseñados para guiar a los equipos de respuesta a través de las acciones esenciales necesarias para controlar, investigar y mitigar incidentes de seguridad.



Aclaramos que estos no son los únicos módulos disponibles en la consola de Vision One. Los mencionados anteriormente son los más utilizados en situaciones de amenaza, detecciones de eventos o evaluación de riesgo en la empresa. Como indicamos en la introducción es importante familiarizarse con los mismos.

En propósito de darle fin a este instructivo, les agradecemos su tiempo y esperamos les haya sido de ayuda.

Ante cualquier duda, consulta o inconveniente, pueden comunicarse con nuestro servicio de asistencia técnica: asistencia@edsitrend.com