



Vision One:

Guía rápida para usos específicos

Gerencia de cuentas
EDSI Trend Argentina



EDSI Trend

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 - 6000
www.trendargentina.com.ar

Página 1

Índice

Búsqueda de vulnerabilidades y cómo atenderlas.....	03
Búsqueda de equipos más comprometidos y cómo atenderlos.....	08
Búsqueda de usuarios más comprometidos y cómo atenderlos.....	12
Lectura de Workbench	15
Tratar falsos positivos	19
Agregar IoCs	22
Exceptuar IoCs.....	30
Verificar llegada de información por parte de productos integrados.....	26
Identificar en qué fase de un ataque se encuentra mi organización	28
Configuración de respuestas automáticas	30
Identificar cómo mejorar la postura de seguridad.....	33
Configuración de notificaciones.....	43
Configuración de reportes.....	43
Lectura de Observed Attack Techniques	23



Búsqueda de vulnerabilidades y cómo atenderlas

Búsqueda de vulnerabilidades

Para encontrar aquellas vulnerabilidades que se presentan mayormente en la organización podemos proceder de muchas formas y accederíamos a la misma información, pero desde distintas secciones de la consola.

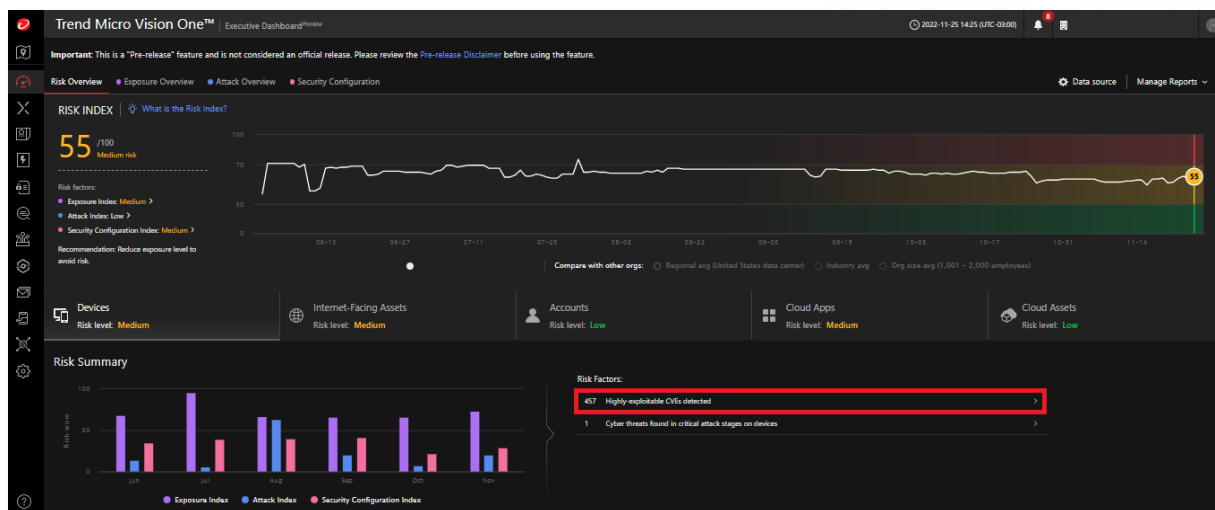
Para comenzar a reconocerlas y atenderlas, primero hay que diferenciarlas según la clasificación que se les da en Vision One. Estas son:

Internal Assets: aplica para activos como endpoints y servidores dentro de su red.

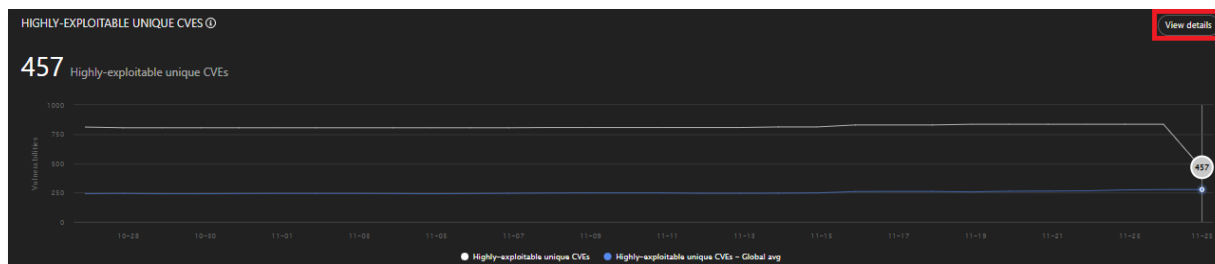
Internet-facing Assets: aplica para activos en la nube.

Desde la consola, podemos acceder a esta información de las siguientes formas:

1. Desde **Risk Insight > Executive Dashboard > Risk Overview** (pestaña seleccionada por defecto) > **Devices** (seleccionada por defecto) > “Highly-exploitable CVEs detected” para acceder a la información de Internal Assets. En caso de querer acceder a la información de Internet-facing Assets, en lugar de **Devices** debemos seleccionar **Internet-Facing Assets > “Highly-exploitable CVEs found on public assets”**:



Esto nos derivará a un gráfico que muestra el historial de nuestra organización en el último mes en cuanto a la cantidad de vulnerabilidades que presentan:



También es posible acceder a este gráfico desde **Risk Insight > Executive Dashboard > Exposure Overview > Vulnerabilities** (seleccionada por defecto).

Haciendo click en el botón de “View details”, como se ve en la imagen de arriba, finalmente nos derivará al listado de las vulnerabilidades:

457
Highly-exploitable Unique CVEs

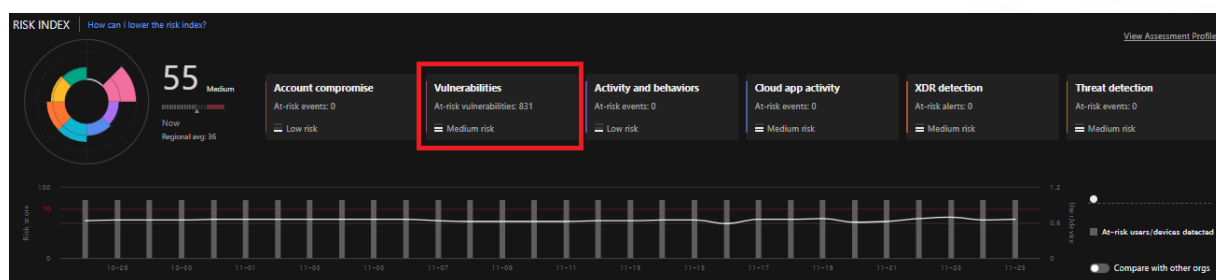
Remediation Actions
Automate your vulnerability management workflow by implementing playbooks that contain ticketing system and customized notifications.
[Create Playbook](#)

HIGHLY-EXPLOITABLE UNIQUE CVEs | Powered by Zero Day Initiative ⓘ

Status: Select value... Vulnerability ID [Apply](#) [Manage Reports](#) Preview

Vulnerability ID	Global exploit activity ↓	CVSS score	OS/Application	Devices	Prevention rule	Exploit attempts ⓘ	Published
▶ CVE-2017-0143	High	8.1	Windows Server 2016	1	5	0	2017-03-16
▶ CVE-2019-0797	High	7.8	Windows Server 2016	5	2	0	2019-04-08
▶ CVE-2019-0803	High	7.8	Windows Server 2016	5	8	0	2019-04-08
▶ CVE-2019-0859	High	7.8	Windows Server 2016	5	7	0	2019-04-08
▶ CVE-2019-0863	High	7.8	Windows Server 2016	5	4	0	2019-05-15
▶ CVE-2019-1214	High	7.8	Windows Server 2016	5	0	0	2019-09-10
▶ CVE-2019-1215	High	7.8	Windows Server 2016	5	0	0	2019-09-10
▶ CVE-2020-0601	High	8.1	Windows Server 2016	6	10	0	2020-01-13
▶ CVE-2020-0683	High	7.8	Windows Server 2016	6	1	0	2020-02-10

- Otra forma de encontrar el listado de vulnerabilidades es dirigirse a **Risk Insight > Operations Dashboard > Risk Factors** (pestaña seleccionada por default) > **Vulnerabilities**:



La misma sección pasará a mostrar el listado de vulnerabilidades separándolas por los dos tipos mencionados anteriormente:

HIGHLY-EXPLOITABLE UNIQUE CVEs | Powered by Zero Day Initiative ⓘ

Internal Assets Internet-facing Assets

Status: Select value... Vulnerability ID [Apply](#) [Manage Reports](#) Preview

Vulnerability ID	Global exploit activity ↓	CVSS score	OS/Application	Devices	Prevention rule	Exploit attempts ⓘ	Published
▶ CVE-2017-0143	High	8.1	Windows Server 2016	1	5	0	2017-03-16
▶ CVE-2019-0797	High	7.8	Windows Server 2016	5	2	0	2019-04-08
▶ CVE-2019-0803	High	7.8	Windows Server 2016	5	8	0	2019-04-08
▶ CVE-2019-0859	High	7.8	Windows Server 2016	5	7	0	2019-04-08
▶ CVE-2019-0863	High	7.8	Windows Server 2016	5	4	0	2019-05-15
▶ CVE-2019-1214	High	7.8	Windows Server 2016	5	0	0	2019-09-10
▶ CVE-2019-1215	High	7.8	Windows Server 2016	5	0	0	2019-09-10
▶ CVE-2020-0601	High	8.1	Windows Server 2016	6	10	0	2020-01-13
▶ CVE-2020-0683	High	7.8	Windows Server 2016	6	1	0	2020-02-10

- Otra manera de encontrar las vulnerabilidades más presentes es dirigirse a **Risk Insight > Security Dashboard** y, según la customización que hicimos, las podremos ver en la tabla “TOP 10 AT RISK VULNERABILITIES”, la cual las ordena según la Global exploit activity:

TOP 10 AT RISK VULNERABILITIES			Go to App	Last 30 days	
App: Operations Dashboard					
Vulnerability ID (CVSS)	Devices	Global exploit activity			
CVE-2020-1350 (10)	6	High			
CVE-2020-1472 (10)	15	High			
CVE-2022-34718 (9.8)	20	Medium			
CVE-2022-24497 (9.8)	20	Medium			
CVE-2021-31962 (9.8)	19	Medium			
CVE-2021-28476 (9.9)	18	Medium			
CVE-2021-34448 (8.8)	19	High			
CVE-2020-1020 (8.8)	7	High			
CVE-2019-1181 (9.8)	5	Medium			
CVE-2021-33742 (8.8)	19	High			

Atender vulnerabilidades

Para atender aquellas vulnerabilidades que se presentan en la organización podemos proceder según dos criterios que determinan la criticidad de la vulnerabilidad y se muestra en dos columnas:

Vulnerability ID	Global exploit activity ↓	CVSS score	OS/Application
CVE-2019-0797	High	7.8	Windows Server 2016

Global exploit activity: clasificación determinada por la frecuencia con la que la vulnerabilidad se explota globalmente y la expectativa de que la vulnerabilidad pueda ser explotada en el futuro.

CVSS score: es un estándar industrial libre y abierto para evaluar la gravedad de las vulnerabilidades de seguridad de los sistemas informáticos. Las puntuaciones se calculan en base a una fórmula que depende de varias métricas que aproximan la facilidad y el impacto de un exploit. Las puntuaciones van de 0 a 10, siendo 10 la más grave.

Si hacemos click en alguna de estas dos columnas, las vulnerabilidades pasarán a ordenarse según el criterio clickeado.

Una vez hecho esto, elegimos la de máxima criticidad e ingresamos en ella haciendo click en el nombre – en este caso, hacemos click en “CVE-2019-0797”. El link directamente nos llevará a toda la información vinculada a la CVE y por defecto nos situará en la pestaña **Basic**.

Dentro, lo primero que debemos hacer es leer la descripción de la vulnerabilidad, y, en caso de que sea necesario, podemos apoyarnos en la información complementaria que está disponible en el link con la fecha de publicación de la vulnerabilidad – en este caso, “Published: 2019-04-08” -.



CVE-2019-0797

Basic Devices

- Global exploit activity: **High** | Published: 2019-04-08
- An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0808.
- CVSS: v3.0 7.8(AVL/ACL/PR/L/UN/SU/CH/EH/AH), v2.0 7.2(AVL/ACL/Au:N/CC/IC/AC)

ATTACK PREVENTION / DETECTION RULES

Product	Rule ID / Malware Name
Trend Micro Cloud One - Endpoint & Workload Security, Deep Security Software	1009583
Trend Micro Cloud One - Network Security	36854
TipingPoint - Intrusion Prevention System	36854

MITIGATION OPTIONS

Method

Remediation: Please follow vendor's guidance to apply the official patch.

Minimal KB ID and released date: 4489868, released date: 2019-03-11 OS / Application version
 4489882, released date: 2019-03-11 OS / Application version
 4489899, released date: 2019-03-11 OS / Application version

For the latest KB, please visit Microsoft support website: Windows 10, Windows 11, or Windows Server 2022

Recommended action: Enable all available Trend Micro prevention/detection rules, enable real-time malware services, and apply any official patches.

REFERENCE

Sources (Type)	Link
in_the_wild_reference	https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Lo siguiente a saber es el scope de equipos que tienen esta vulnerabilidad para luego trabajar en ellas. Para ello hacemos click en la pestaña **Devices**. Además de obtener el host o IP de estos equipos, obtendremos información como el sistema operativo, el usuario y el risk score (de cada equipo) que, luego, podemos utilizar para seguir trabajando en reducir el score de la organización:

CVE-2019-0797

Basic **Devices**

Device

Device name	Operating system	IP address	User name	Latest risk score
TAHQ004vw0462	Windows Server 2016 10.14393	172.25.6.37, 169.254.225.92	seg-900212947, adm-900214106, C...	80
TAHQ002VW0706	Windows Server 2016 Standard (64 bit) build ...	172.25.2.159, 169.254.104.79	seg-900212947	63
SMILAPRT01	Windows Server 2016 10.0.14393	172.25.0.185	Administrator	62
TAHQ004vw0668	Windows Server 2016 Standard (64 bit) build ...	172.25.6.42, 169.254.225.92	ColegaAgenciasExt, seg-900212947, ...	58
SMILAVDI05	Windows Server 2016 10.0.14393	172.25.0.184	Administrator	54

Conociendo el scope, volvemos a **Basic** para seguir leyendo las remediaciones o recomendaciones para atender a la vulnerabilidad:



En “ATTACK PREVENTION / DETECTION RULES” debemos identificar los productos de Trend Micro con los que contamos y verificar que en ellos tengamos las reglas de IPS que protegen a la organización de esta vulnerabilidad:

ATTACK PREVENTION / DETECTION RULES	
Product	Rule ID / Malware Name
Trend Micro Cloud One - Endpoint & Workload Security, Deep Security Software	1009583
Trend Micro Cloud One - Network Security	36854
TippingPoint - Intrusion Prevention System	36854

Nos dirigimos a Trend Micro Cloud One – Endpoint & Workload Security para agregar esta regla en el módulo de **Intrusion Prevention** en la o las políticas de los equipos que correspondan. Hacer click en el botón “Assign/Unassign” para poder habilitar la regla en caso de que haga falta:

IPS Rules All rule availabilities All All By Application Type 1009583

New Delete... Properties... Duplicate Export Application Types... Columns...

Rule Selection

	NAME ^	PRIORI...	SEVERI...	MODE	TYPE	CATEGORY	RULE AVAIL.
Web Client Common (1)							
<input checked="" type="checkbox"/>	1009583 - Microsoft Windows Win32k Elev...	2 - Normal	Medium	Prevent	Exploit	Vulnerabilities and Ex...	Workload

Luego, en “MITIGATION OPTIONS”, debemos apoyar el mouse sobre el texto en azul “OS / Application version” para saber cuál de los KB de Microsoft corresponden para los sistemas operativos que debemos parchear.

IMPORTANTE: no es necesario instalar todos los KB presentados en el detalle, por eso es importante reconocer el scope de equipos y sus sistemas operativos para luego buscar el KB indicado como se explicó recientemente:

MITIGATION OPTIONS

Method

Remediation: Please follow vendor's guidance to apply the official patch.

Minimal KB ID and released date:	4489868, released date: 2019-03-11 OS / Application version	<ul style="list-style-type: none"> Windows 10 Version 1607 for x64-based Systems Windows Server 2016 Windows 10 Version 1607 for 32-bit Systems Windows Server 2016 (Server Core installation)
	4489882, released date: 2019-03-11 OS / Application version	
	4489899, released date: 2019-03-11 OS / Application version	

For the latest KB, please visit Microsoft support website: [Windows 10](#), [Windows 11](#), or [Windows Server 2016](#)

Recommended action: Enable all available Trend Micro prevention/detection rules, enable real-time malware services, and apply any official patches.

Habiendo hecho todas las acciones indicadas o si se están trabajando en las mismas es necesario categorizar a la vulnerabilidad. Para hacer esto debemos volver al listado de vulnerabilidades y hacer click en la bandera a la izquierda del nombre de esta:



🚩	CVE-2019-0797	High	7.8
🚩 New	9-0803	High	7.8
🔄 In progress	9-0859	High	7.8
✓ Closed	9-0863	High	7.8
🚩	CVE-2019-1214	High	7.8

La categorización por defecto en todas las vulnerabilidades es “New”, por lo que al finalizar con la atención de la CVE debemos marcarla como “Closed”. **Esto favorecerá a que el risk score del equipo y de la organización comiencen a bajar.** Por otro lado, recomendamos usar la categoría “In progress” cuando la atención de la vulnerabilidad está en proceso, tanto como una ayuda para la memoria, así como también para en el caso en que más de un usuario esté usando la consola y estén trabajando en conjunto en la reducción del risk score.

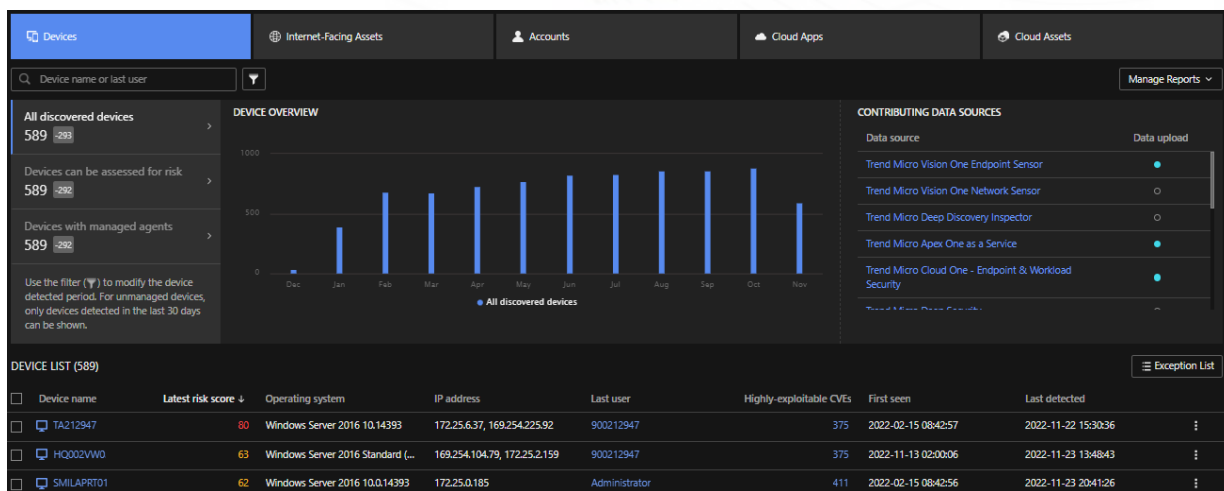


Búsqueda de equipos más comprometidos y cómo atenderlos

Búsqueda de equipos más comprometidos

Para encontrar aquellos dispositivos que se encuentran más comprometidos en la organización podemos proceder de las siguientes formas:

1. Desde **Risk Insight > Attack Surface Discovery > Devices** (pestaña seleccionada por defecto):



En la parte inferior, encontraremos el “DEVICE LIST”, que por defecto tiene ordenado a los dispositivos según su último risk score.

2. También para encontrar los endpoints más comprometidos podemos dirigirnos a **Risk Insight > Security Dashboard** y, según la customización que hicimos, las podremos ver en la tabla “AT-RISK DEVICES”:

AT-RISK DEVICES			
App: Operations Dashboard			
Device	Operating system	Vulnerabilities	Latest risk score
TA212947	Windows Server 2016 10.14393	375	93
vw0462	Windows Server 2016 10.14393	75	80
HQ004	Windows Server 2016 10.14393	80	80

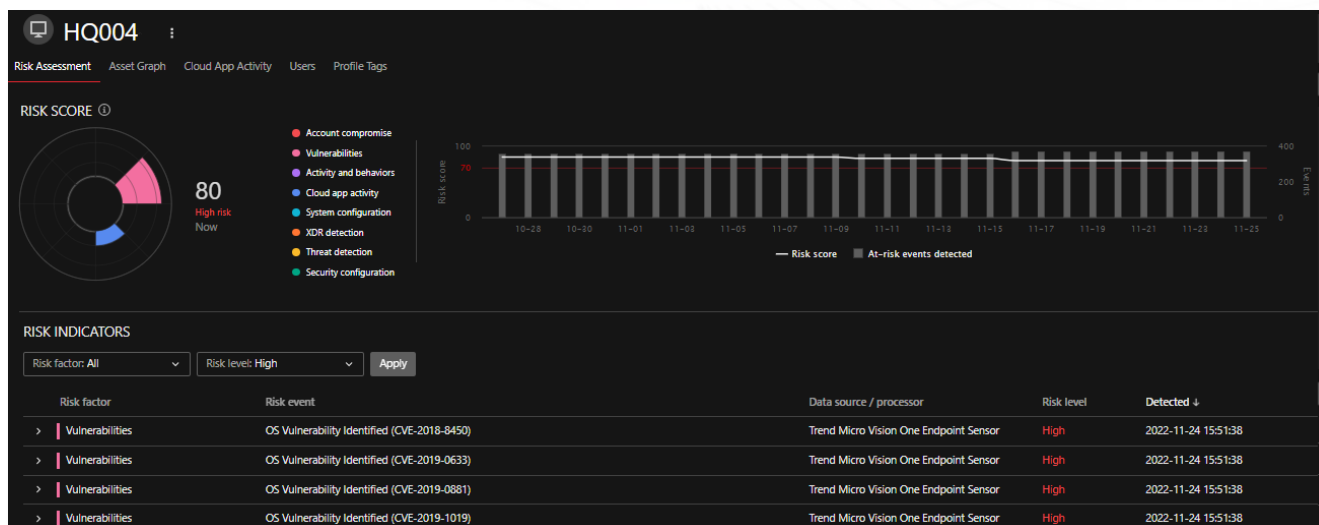
3. Desde **Risk Insight > Operations Dashboard > Risk Factors** (pestaña seleccionada por defecto), en la parte inferior tendremos el listado de equipos y usuarios más comprometidos en “AT-RISK USERS/DEVICES”. Aquí debemos diferenciar cual es un usuario y cual es un equipo prestando atención en el ícono que está a la izquierda de su nombre en la columna “User / Device name”:



AT-RISK USERS/DEVICES ①				
Status: New	Risk factor: All	Risk event: All	Q User / Device name	Apply
Configure Alert Notifications				
Latest risk ... ↓	User / Device name	Risk event	Risk factor	Detected
80	TAHQ004w0462	OS Vulnerability Identified, Risky Cloud App Access	Vulnerabilities Cloud app activity	2022-11-22 15:30:36

Atender risk score del equipo

Para comenzar a trabajar en el descenso del risk score debemos ingresar al equipo elegido:



Por defecto en “RISK INDICATOR”, el “Risk level” seleccionado es “High” por lo que debemos poner “All” o algún otro según la necesidad que tengamos.

Luego, ingresamos a los indicadores que hacen subir el risk score del equipo y comenzamos a seguir las indicaciones de este:

Cloud app activity	Risky Cloud App Access	Trend Micro Vision One Endpoint Sensor	Medium	2022-11-09 04:32:41
Access to a cloud app (Microsoft Live) with a (medium) risk reputation score (50) detected.				
Suggested Actions: <ul style="list-style-type: none">Create a Zero Trust Secure Access rule to block unsanctioned apps.If the app is permitted, Sanction the app.				
request:	login.live.com			
riskLevel:	medium			
appName:	Microsoft Live			
deviceOs:	Windows Server 2016 Standard (64 bit) build 14393 10.0.14393			
appCategory:	IT Services & Support			
endpointIp:	69.254.225.92, 172.25.6.3			
loginUser:	5019			
aggregateAccessCount:	1			
endpointHostName:	HQ004			
clientApp:	C:\Windows\System32\svchost.exe			
riskScore:	50			

Habiendo trabajado en los indicadores, nos dirigimos a **Risk Insight > Operations Dashboard** y categorizamos al dispositivo según el estado en que se encuentre:



AT-RISK USERS/DEVICES ⓘ

Status: **New**
Risk factor: **All**

Latest risk ... ↓
User / Device name

80	HQ004
----	-------

New
In progress
Issues resolved
Closed - false positive

IMPORTANTE: por el momento, esto es solo es posible con aquellos equipos que figuren como “AT-RISK”. De no haber ningún equipo clasificado como “AT-RISK”, nos aparecerá el siguiente mensaje con el siguiente botón:

No at-risk user/device found.

View All Asset Risks

or

Configure data sources for risk analysis

Haciendo click en **View All Asset Risks**, se nos habilitará el listado completo de dispositivos y usuarios para atenderlos tal como se comento sobre los dispositivos y usuarios clasificados como “AT-RISK”:

ALL ASSET RISKS ⓘ						
<div> Devices Domain Accounts Service Accounts Domains Public IPs Cloud Assets </div>						
<div> Status: New Latest risk score: All Risk factor: All Risk event: All <input type="text" value="Asset name"/> Apply </div>						
Latest risk score ↓	Asset name	Risk event			Risk factor	Detected
62	55201	OS Vulnerability Identified, Security Settings in Trend Micro Apex One as a Service Not Optimized, Depre...			Vulnerabilities	2023-01-02 09:45:25
59	ABWP	OS Vulnerability Identified, Application Vulnerability Identified, Application Execution Check Disabled, Ma...			Vulnerabilities	2023-01-02 05:04:51
58	55578	OS Vulnerability Identified, Deprecated OS Version Identified, Disk Encryption Disabled, Application Exec...			Vulnerabilities	2022-12-31 11:04:30
58	57002	OS Vulnerability Identified, Application Vulnerability Identified, Deprecated OS Version Identified, Applica...			Vulnerabilities	2023-01-02 05:28:09



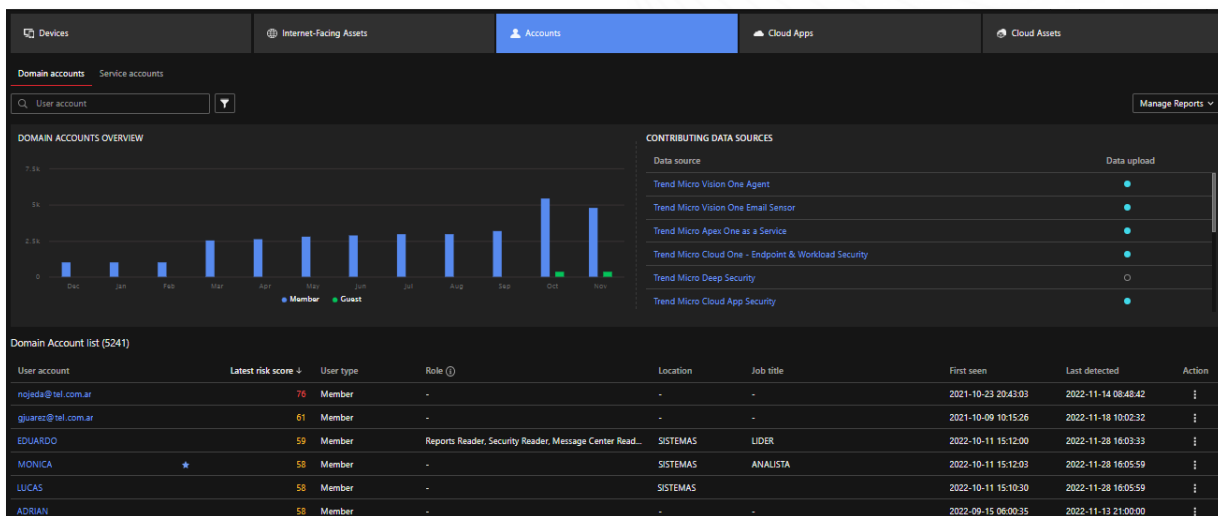
Búsqueda de usuarios más comprometidos y cómo atenderlos

Búsqueda de usuarios más comprometidos

Para encontrar aquellos usuarios que se encuentran más comprometidos en la organización podemos proceder de las siguientes formas:

IMPORTANTE: no se verá ningún usuario si aún no se ha integrado algún servicio de LDAP, como por ejemplo Azure AD o Active Directory (on-premise).

1. Dirigirse a **Risk Insight > Attack Surface Discovery > Accounts** y bajar hasta encontrar en “Domain Account list”:



Los usuarios, por defecto, aparecerán ordenados según su último risk score (los scores más altos figuran primero).

2. También para encontrar los endpoints más comprometidos podemos dirigirnos a **Risk Insight > Security Dashboard** y, según la customización que hicimos, las podremos ver en la tabla “AT-RISK USERS”:

The screenshot shows the 'AT-RISK USERS' table in the Trend Micro Risk Insight interface. The table has columns for 'User name', 'Email address', and 'Latest risk score'. The user 'LUCAS' is highlighted with a risk score of 76. The interface also includes a 'Go to App' button and a 'Last 30 days' filter.

User name	Email address	Latest risk score
LUCAS	lojeda@tel.com.ar	76

3. Otra manera, y hasta el momento la mejor opción, es dirigirse a **Risk Insight > Operations Dashboard > Risk Factors** (pestaña seleccionada por defecto). Debajo encontraremos el listado “AT-RISK USERS/DEVICES” donde encontraremos tanto a los usuarios como a los dispositivos más comprometidos. Los diferenciamos prestando atención al icono que se sitúa en la columna “User / Device name”:



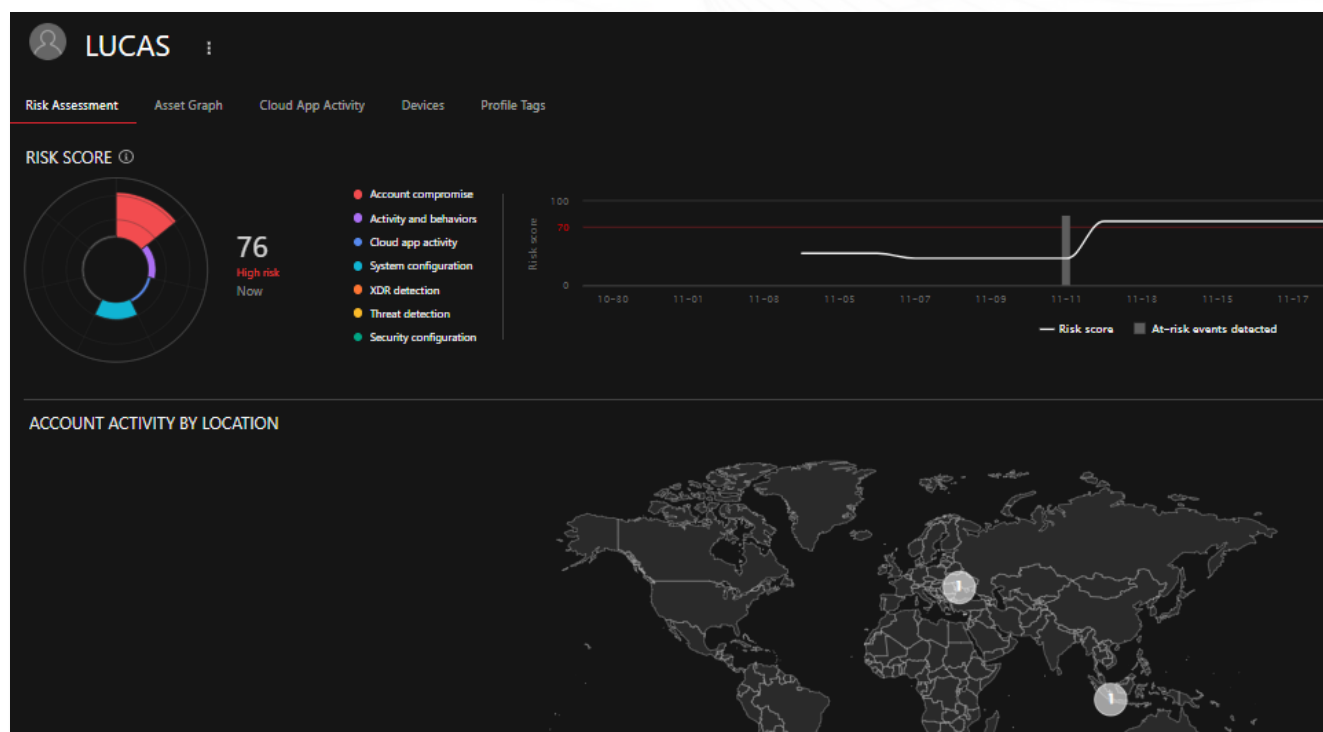
AT-RISK USERS/DEVICES ①

Status: New Risk factor: All Risk event: All User / Device name Apply Configure Alert Notifications

Latest risk score ↓	User / Device name	Risk event	Risk factor	Detected
76	LUCAS	Azure AD Identity Protection Risk Detection, Account with Weak Sign-In Security Policy: MFA Disabled, U...	Account com...	2022-11-14 08:48:42
72	54495	OS Vulnerability Identified, Application Vulnerability Identified, Deprecated OS Version Identified, Disk En...	Vulnerabilities	2022-11-28 04:12:38

Atender risk score de los usuarios

Ingresamos al detalle de alguno de los usuarios haciendo click en su nombre:



Una vez dentro, bajamos hasta encontrar el listado “RISK INDICATORS” y comenzamos a trabajar siguiendo las recomendaciones que hay por cada indicador

RISK INDICATORS

Risk factor: All Risk level: High Apply

Risk factor	Risk event	Data source / processor	Risk level	Detected ↓
Account compromise	Azure AD Identity Protection Risk Detection	Azure AD	High	2022-11-11 18:25:32

Azure AD Identity Protection detected a sign-in attempt with a (high) risk.
Remediation: Disable or reset this account with a strong password.
Suggested Actions: Create a Zero Trust Secure Access rule to block access to company resources if the same risk is detected.
Location: Indonesia - Jakarta

Una vez que ya hayamos trabajado en los indicadores nos dirigimos a **Risk Insight > Operations Dashboard > Risk Factors** y buscamos el listado “AT-RISK USERS/DEVICES” para categorizar al o a los usuarios según el estado de sus indicadores. Si sus indicadores se dispararon por falsos positivos utilizamos esa opción; “Issues resolved” en caso de haber trabajado en todos los indicadores; y “In progress” si aún estamos trabajando en bajar el risk score:



AT-RISK USERS/DEVICES ⓘ

Status: **New** ▼ Risk factor: **All** ▼

Latest risk score ↓	User / Device name
76	LUCAS
	54498

New

In progress

Issues resolved

Closed - false positive

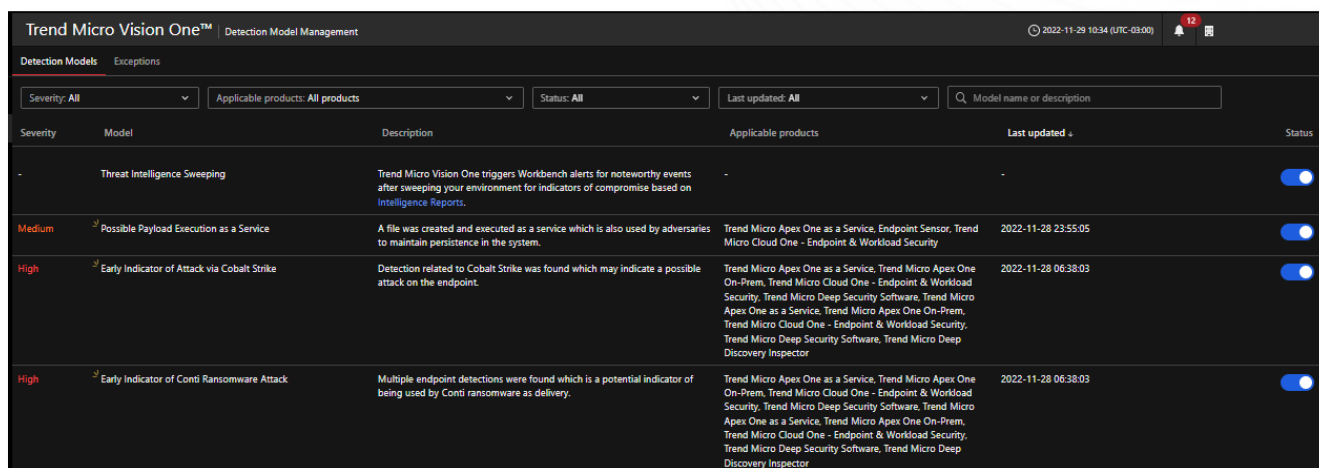


Lectura de Workbench

Lo primero a saber sobre Workbench es que se trata de una aplicación que proporciona una lista de alertas activadas/disparadas por modelos de detección, así como incidentes que agrupan alertas relacionadas. La aplicación Workbench le permite investigar y responder a cada alerta e incidente.

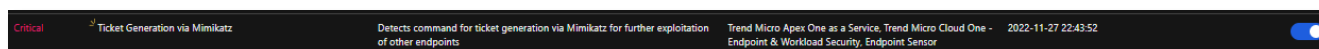
Modelos de detección

Cada modelo de detección está especializado en descubrir un tipo concreto de amenazas. Para encontrar los modelos disponibles diríjase a **XDR Threat Investigation > Detection Model Management > Detection Models** (pestaña seleccionada por defecto):



Severity	Model	Description	Applicable products	Last updated	Status
-	Threat Intelligence Sweeping	Trend Micro Vision One triggers Workbench alerts for noteworthy events after sweeping your environment for indicators of compromise based on Intelligence Reports.	-	-	<input type="checkbox"/>
Medium	Possible Payload Execution as a Service	A file was created and executed as a service which is also used by adversaries to maintain persistence in the system.	Trend Micro Apex One as a Service, Endpoint Sensor, Trend Micro Cloud One - Endpoint & Workload Security	2022-11-28 23:55:05	<input type="checkbox"/>
High	Early Indicator of Attack via Cobalt Strike	Detection related to Cobalt Strike was found which may indicate a possible attack on the endpoint.	Trend Micro Apex One as a Service, Trend Micro Apex One On-Prem, Trend Micro Cloud One - Endpoint & Workload Security, Trend Micro Deep Security Software, Trend Micro Apex One as a Service, Trend Micro Apex One On-Prem, Trend Micro Cloud One - Endpoint & Workload Security, Trend Micro Deep Security Software, Trend Micro Deep Discovery Inspector	2022-11-28 06:38:03	<input type="checkbox"/>
High	Early Indicator of Conti Ransomware Attack	Multiple endpoint detections were found which is a potential indicator of being used by Conti ransomware as delivery.	Trend Micro Apex One as a Service, Trend Micro Apex One On-Prem, Trend Micro Cloud One - Endpoint & Workload Security, Trend Micro Deep Security Software, Trend Micro Apex One as a Service, Trend Micro Apex One On-Prem, Trend Micro Cloud One - Endpoint & Workload Security, Trend Micro Deep Security Software, Trend Micro Deep Discovery Inspector	2022-11-28 06:38:03	<input type="checkbox"/>

Dentro, encontraremos el listado con los diferentes modelos que se encuentran activados o desactivados según lo indique la columna “Status”. Se recomienda tener activos, en caso de no estarlo, aquellos modelos que apliquen para los productos que tenemos integrados a Vision One y que coincidan con los productos descritos en la columna “Applicable products”. Por ejemplo:



Critical	Ticket Generation via Mimikatz	Detects command for ticket generation via Mimikatz for further exploitation of other endpoints	Trend Micro Apex One as a Service, Trend Micro Cloud One - Endpoint & Workload Security, Endpoint Sensor	2022-11-27 22:43:52	<input type="checkbox"/>
----------	--------------------------------	--	--	---------------------	--------------------------

Este modelo aplica para “Apex One SaaS” y para “Cloud One – Endpoint & Workload Security”; si su organización cuenta con alguno de estos productos integrado a Vision One, corresponde tener activo este modelo de detección. De esta forma se podrán generar Workbenches (correlación de información entre los distintos productos) vinculados a amenazas concretas.

Cabe destacar que esta acción no es una tarea que se deba hacer rutinariamente. Basta con hacer una primera configuración y, luego, ajustarla en caso de que los Workbench que dispare no correspondan a una situación que amerite interceder o que sea notificada por Vision One.

Lectura de Workbench

Sabiendo esto, encontramos los Workbenches generados dirigiéndonos a **XDR Threat Investigation > Workbench**. Dentro encontramos dos secciones:



Alert View: Muestra las alertas que se pueden investigar a través de un análisis en profundidad de la causa raíz y el impacto para comprender el alcance y la gravedad de la alerta y determinar más acciones para responder a las alertas.

Incident View: Muestra incidentes que agrupan alertas relacionadas (las mismas de Alert View) entre sí para ayudarle a identificar y mitigar rápidamente las posibles brechas del sistema en su entorno de red.

Por defecto, la aplicación nos situará en la pestaña **Alert View**:

Alert View		Incident View						Automated Response Playbook <small>Preview</small>	
Status: All	Created: Last 30 days	Model: All	Q Workbench ID, Endpoint, User, Email	Apply					View: All
Score	Workbench ID	Model	Model severity	Impact scope	Created	Associated incident			
29	WB-15387-20221129-00002	Internal Network Scanner	Low	2 1	2022-11-29 10:55:12	IC-15387-20221129-00000			
26	WB-15387-20221129-00001	Internal Network Scanner	Low	1 1	2022-11-29 10:52:09	IC-15387-20221129-00000			
20	WB-15387-20221129-00000	Spear Phishing Email with Known Phishing Behaviors	Low	2	2022-11-28 23:58:03				
21	WB-15387-20221127-00000	Cybercrime Malware Mitigation	Low	1	2022-11-27 09:31:46				
20	WB-15387-20221126-00000	Possible Spear Phishing Attack via Link	Low	2	2022-11-26 03:40:01	IC-15387-20221124-00000			
20	WB-15387-20221125-00004	Possible Spear Phishing Attack via Link	Low	2	2022-11-25 01:53:38	IC-15387-20221124-00000			
20	WB-15387-20221125-00003	Possible Spear Phishing Attack via Link	Low	2	2022-11-25 01:53:37	IC-15387-20221124-00000			
20	WB-15387-20221125-00002	Possible Spear Phishing Attack via Link	Low	2	2022-11-25 01:52:38				
20	WB-15387-20221125-00000	Possible Spear Phishing Attack via Link	Low	2	2022-11-25 01:52:38	IC-15387-20221124-00000			

Sabiendo las posibilidades de cada uno, lo aconsejable sería comenzar ingresando a la solapa **Incident View**, para poder entender si estas alertas vistas en **Alert View** están relacionadas entre sí. Además, tendremos la posibilidad de leer rápidamente la descripción de este incidente al mismo tiempo que, desde los links que aparecen al final de la descripción, podemos acceder a las URL de MITRE que describen más en profundidad técnicas de ataque relacionados a estos incidentes:

Trend Micro Vision One™		Workbench - IC-18846-20221201-00000		2022-12-30 16:47 (UTC-03:00)			
Alerts (15)	Incident Timeline	Impact Scope (18)	Highlighted Objects (47)				
<div> <div>21</div> <div>Repetitive alerts (15).</div> <div> <p>It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. Key attack techniques: T1566.002, T1192</p> </div> </div>		<div>Created: 2022-12-01 02:39:24</div> <div>Last updated: 2022-12-01 02:48:41 (New alert correlated)</div>					
Status: All	Created: All	Model: All	Q Workbench ID, Endpoint, User, Email	Apply			
Score	Workbench ID	Model	Model severity	Relationship	Impact scope	Created	
20	WB-18846-20221201-00001	Possible Spear Phishing Attack via Link	Low	Same email sender, SimilarUrlAccess, Simil...	2	2022-12-01 02:42:17	
20	WB-18846-20221201-00002	Possible Spear Phishing Attack via Link	Low	Same email sender, SimilarUrlAccess, Simil...	2	2022-12-01 02:42:26	
20	WB-18846-20221201-00003	Possible Spear Phishing Attack via Link	Low	Same email sender, SimilarUrlAccess, Simil...	2	2022-12-01 02:42:18	
20	WB-18846-20221201-00004	Possible Spear Phishing Attack via Link	Low	Same email sender, SimilarUrlAccess, Simil...	2	2022-12-01 02:42:16	
20	WB-18846-20221201-00005	Possible Spear Phishing Attack via Link	Low	Same email sender, SimilarUrlAccess, Simil...	2	2022-12-01 02:42:30	

En este caso, el incidente describe:

"It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing."

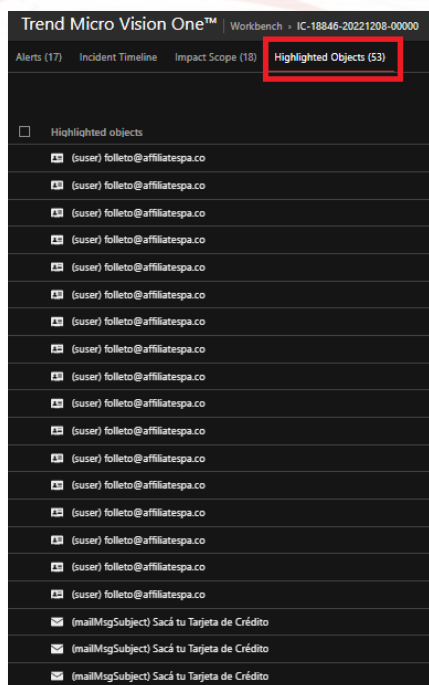
Al español:

Se diferencia de otras formas de spearphishing en que emplea el uso de enlaces para descargar malware contenido en el correo electrónico, en lugar de adjuntar archivos maliciosos al propio correo, para evitar las defensas que pueden inspeccionar los archivos adjuntos al correo electrónico. Los delincuentes pueden enviar correos electrónicos de



spearphishing con un enlace malicioso para intentar acceder a los sistemas de las víctimas. El spearphishing con enlace es una variante específica del spearphishing.

Ante esto lo que podemos hacer es informarnos sobre la procedencia de este correo, para esto nos dirigimos a la solapa **Highlighted Objects** y buscamos al objeto “(user)”:



De esta forma identificamos que la casilla en cuestión ha sido la que ha enviado los correos con contenido malicioso que ha disparado, en este caso, las 17 alertas.

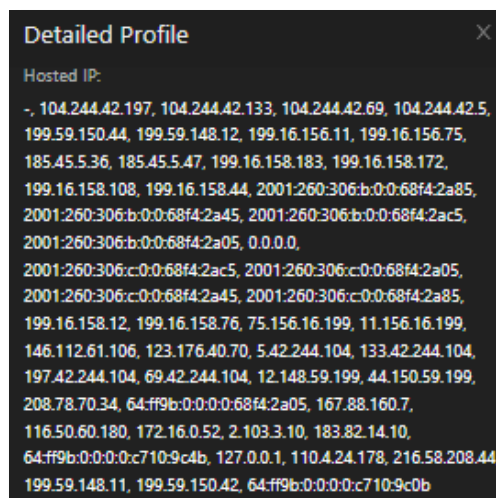
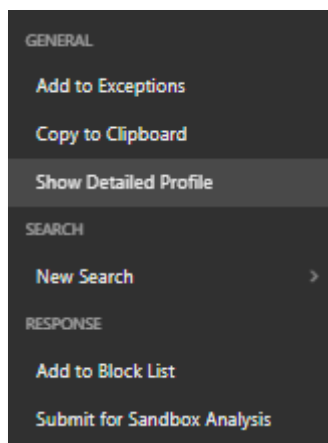
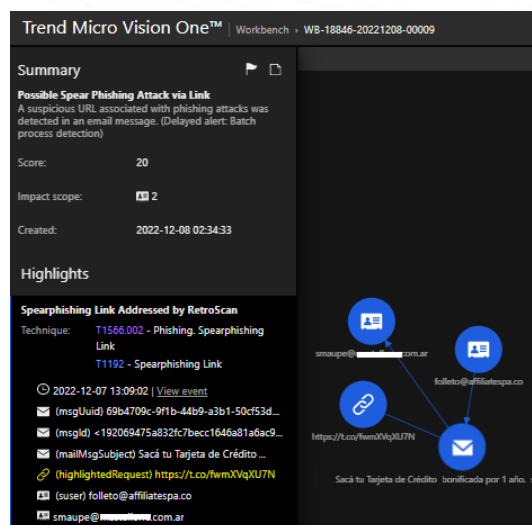
Por lo tanto, después de ver esto, en nuestra solución para la capa de correos, debemos agregar esta casilla o dominio a blacklist o contemplar una política que bloquee a esta casilla o dominio.

Otra tarea para realizar es ingresar a las alertas para obtener el link en cuestión y agregarlo a la lista de URL a bloquear para nuestras soluciones de proxy y firewall.

Para ello debemos ingresar a las alertas y sobre el objeto

“(highlightedRequest)”, en la imagen de la derecha hacemos click derecho para que la consola nos de más opciones para avanzar. Dentro tendremos la

opción **Copy to Clipboard**. De esta forma ya contaremos con el link. Si por algún motivo no es posible agregar esta URL como tal, podremos obtener las IP en la que esta hosteada esta URL. Para ello también hacemos click en el objeto “(highlightedRequest)” pero esta vez seleccionamos **Show Detailed Profile**, donde además de lo mencionado, encontramos otros detalles que nos pueden servir:



Otras tareas que se pueden realizar son agregar como IoC alguno de los objetos que conforman a la alerta. Para ello debemos hacer click en el objeto y, luego, click en **Add to Block List**.

Hay que remarcar que añadir un objeto a la lista de objetos sospechosos definida por el usuario no finaliza ningún proceso activo ni ninguna conexión al objeto. Para terminar procesos activos, asegúrese de que también configuró y activó una **Terminate Process task** desde **Workflow and Automation > Response Management**.

Más información en los siguientes links:

<https://docs.trendmicro.com/en-us/enterprise/trend-micro-vision-one-olh/common-apps/response-management/response-actions/blocking-objects.aspx>

<https://docs.trendmicro.com/en-us/enterprise/trend-micro-vision-one-olh/common-apps/response-management/response-actions/terminating-processes.aspx>



Tratar falsos positivos

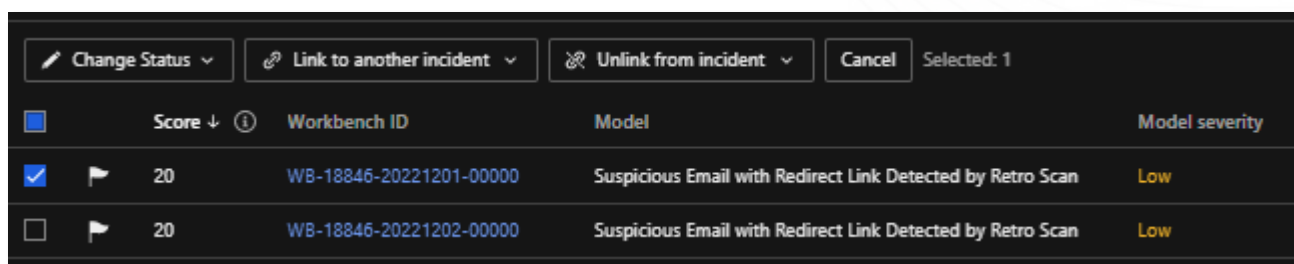
Tratar falsos positivos desde la alerta o incidente

Los falsos positivos a tratar son aquellos Workbench que se han generado y que no corresponden con un incidente o ataque. Teniendo en cuenta esto podemos avanzar con esta tarea de manera granular o más abarcativa, es decir, desde **Alert View** o desde **Incident View** respectivamente.

Lo primero a saber son los objetos que integran a cada alerta e identificar si estos son válidos. En caso de que esto sea así la próxima decisión para tomar es lo comentado con anterioridad, tratar estos falsos positivos de manera granular entrando a cada alerta o de manera más abarcativa ingresando al incidente que integra a todas estas alertas.

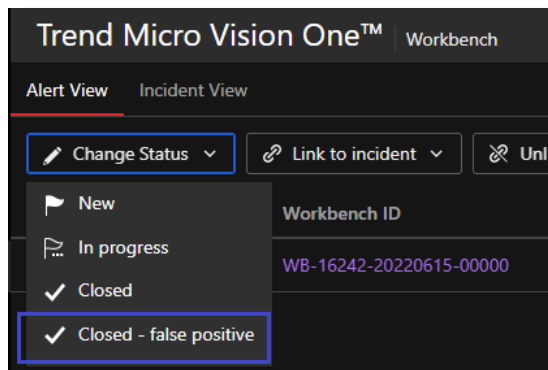
El modo para clasificar los Workbench como falsos positivos es el mismo en ambos casos:

Ingresamos a **XDR Threat Investigation > Workbench**. Luego seleccionamos el checkbox de la alerta o incidente correspondiente (también podemos seleccionar más de uno en caso de que sea necesario) y hacemos click **Change Status**.



<input type="checkbox"/>	Score ↓ ⓘ	Workbench ID	Model	Model severity
<input checked="" type="checkbox"/>	20	WB-18846-20221201-00000	Suspicious Email with Redirect Link Detected by Retro Scan	Low
<input type="checkbox"/>	20	WB-18846-20221202-00000	Suspicious Email with Redirect Link Detected by Retro Scan	Low

Al hacer click en **Change Status**, se despliegan -sobre el mismo botón- las opciones que tenemos a disposición:



Luego, introduzca la razón por la que cree que se trata de una alerta de falso positivo:



Mark as False Positive

Alerts: 1 selected

Specify why you are marking this alert as a false positive:

- ☐ Turned out to be false but was an interesting case
- ☐ Resulted from a penetration test
- ☐ Not an attack but was a business policy violation
- ☐ Background noise
- ☐ Obvious false positive
- ☒ Others

Leave your comments here

Submit Close

ACLARACIÓN: Esta acción no puede evitar que se vuelvan a activar alertas similares. No obstante, el equipo de backend de Trend Micro revisará esta alerta de falso positivo y mejorará nuestro modelo de detección si realmente se trata de una alerta falsa.

Tratar falsos positivos agregando a los objetos destacados como excepciones:

Otra forma de tratar a los falsos positivos es añadiendo a los *highlightned-objects* -que conforman a los Workbench- y agregarlos como excepciones.

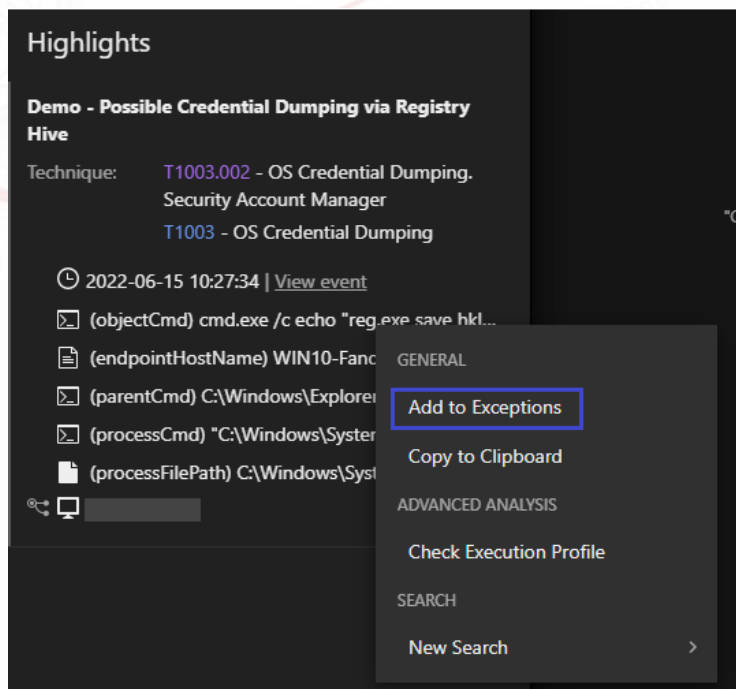
Para ello, ingresamos a **XDR Threat Investigation > Workbench**. Por default, nos situaremos en la pestaña **Alert View**. Haga clic en el link de Workbench ID correspondiente a la alerta que desee investigar.

Alert View Incident View				
Status: All		Created: Last 30 days	Model: All	Workbench ID, Endpoint, User, Email
<input type="checkbox"/>	Score ↓ ⓘ	Workbench ID	Model	Model severity
<input type="checkbox"/>	43	WB-18846-20221220-00000	Suspicious Mailbox Rule Forwards All Email to an External Location	Medium

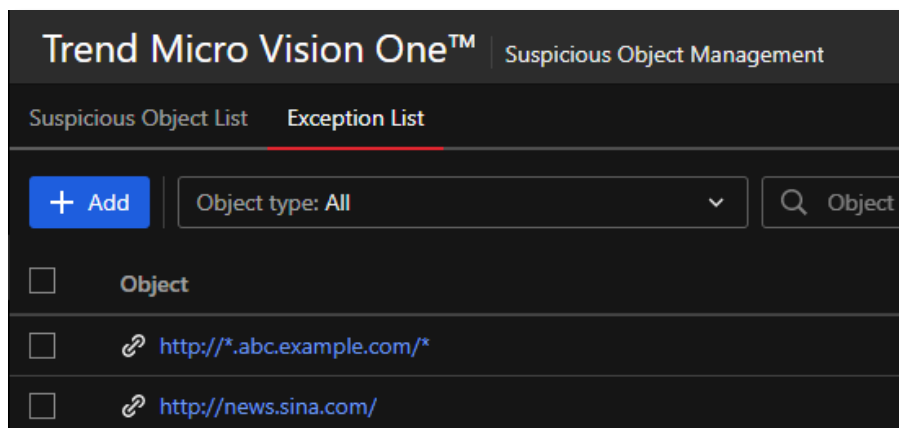
Al hacer click aparecerá la pantalla de detalles de la alerta.

En el panel “Highlights”, compruebe los objetos implicados en cada evento y elija un objeto para añadirlo como excepción. Tenga en cuenta que sólo puede añadir objetos destacados (*highlightned-objects*) a excepciones. Dado que las entidades de ámbito de impacto no son los criterios de activación de alertas, no pueden añadirse como excepciones.





Al agregar estos objetos como excepciones, estos se pueden ver en el listado definido por el usuario, al cual se puede acceder dirigiéndose a **Threat Intelligence > Suspicious Object Management > Exception List**:



Desde aquí, también podríamos agregar los objetos si así lo quisiéramos.

Fuente: https://success.trendmicro.com/dcx/s/solution/000291349?language=en_US



Agregar IoCs

Cómo funciona la adición de IoCs

Puede especificar acciones para que los productos conectados las lleven a cabo tras detectar objetos sospechosos específicos. Trend Micro Vision One se conecta a diferentes productos y envía la lista de objetos sospechosos a los productos conectados para su detección. A continuación, los productos conectados aplican la acción especificada en función de su capacidad.

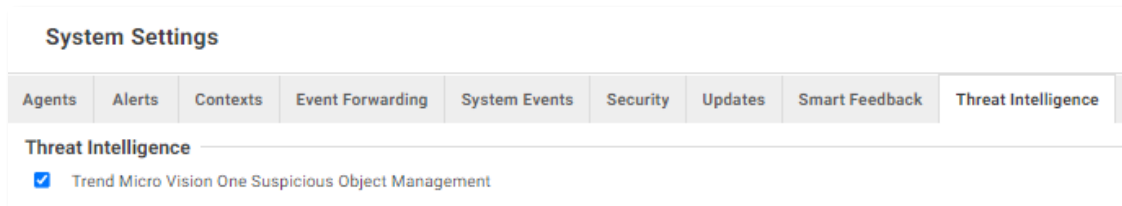
Trend Micro Vision One admite actualmente el envío de la lista de objetos sospechosos a los siguientes productos si están conectados correctamente:

- Trend Micro Apex One as a Service
- Trend Micro Cloud App Security:
 - Por defecto, la sincronización de la lista de objetos sospechosos está desactivada en la consola de Cloud App Security. Por lo tanto, asegúrese de haber habilitado la sincronización de Suspicious Object List para que Cloud App Security reciba información sobre objetos sospechosos.



Procedimiento: <https://docs.trendmicro.com/en-us/enterprise/cloud-app-security-online-help/administration/global-settings/configuring-suspicio.aspx>

- Trend Micro Cloud One - Endpoint & Workload Security:
 - De forma predeterminada, Trend Micro Vision One Suspicious Object Management está deshabilitada en Threat Intelligence de Cloud One - Workload Security. Por lo tanto, asegúrese de haber habilitado la opción en la consola Cloud One - Workload Security para recibir información de objetos sospechosos.



Procedimiento: <https://cloudone.trendmicro.com/docs/workload-security/threat-intelligence/>

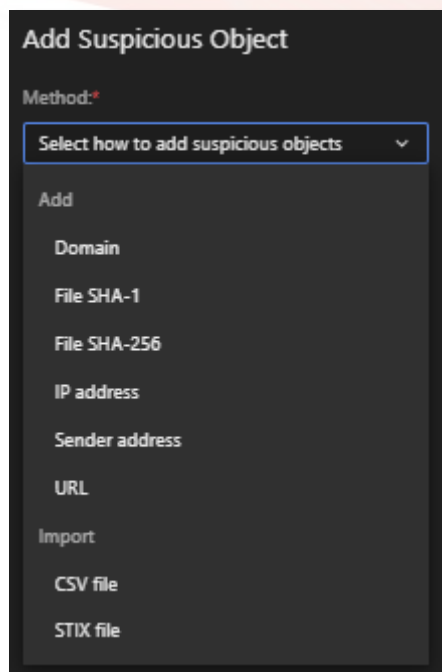
- Service Gateway Management



Cómo agregar IoCs

Para agregar IoCs en la consola de Vision One hay que dirigirse a **Threat Intelligence > Suspicious Objects Management > Suspicious Objects List** (pestaña por defecto).

Dentro hacer click en el botón **Add**. Al hacer click se nos desplegará un panel desde la derecha en el que debemos indicar el tipo de IoC del cual se trata:



A su vez, podemos agregar IoCs desde archivos con extensión CSV siempre y cuando sigan el siguiente formato -la consola nos permite descargar un ejemplo para este archivo-:

	A	B	C	D	E	F	G
1	Type, Object, Description						
2	domain, example.com, test domain						
3	url, http://www.example.com, test url						
4	ip, 1.1.1.1, test ipv4						
5	ip, 0:0:0:0:0:0:1, test ipv6						
6	sha1, 3395856CE81F2B7382DEE72602F798B642F14140, test sha1						
7	sha256, AEC070645FE53EE3B3763059376134F058CC337247C978ADD178B6CCDFB0019F, test sha256						
8	email_sender, example@gmail.com, test email sender						

Al elegir la opción de importar un archivo CSV, el panel de la derecha suma más opciones que nos permite indicar que acción pretendemos que se ejecute sobre cada tipo de indicador dentro del archivo que agreguemos y cual será el nivel de riesgo que se le adjudicará al momento de encontrar detecciones:



Method: ▼
CSV file

File: ▼
Select File...

Tip: Click "Download sample CSV" to obtain a properly formatted example CSV file. Populate the file with properly-formatted objects and import the file.

[Download sample CSV](#)

Risk level: ▼
High

Specify the actions to apply after detecting the specific objects.

Domain: ▼
Block / Quarantine

File SHA-1: ▼
Block / Quarantine

File SHA-256: ▼
Log

IP address: ▼
Block / Quarantine

Sender address: ▼
Log

URL: ▼
Block / Quarantine

Expiration:
☐ Automatically expire in 30 ▼ days
☒ Never expire

Submit Cancel

Por último, confirmamos haciendo click en **Submit**.

ACLARACIÓN: Al agregar IoCs mediante un archivo CSV, no es posible asignar diferentes acciones para diferentes indicadores de un mismo tipo. Es decir que si para los indicadores del tipo URL, la acción elegida fue "Block / Quarantine" no podremos elegir que a una URL la bloquee y a otro solo la registre (log).

Agregar IoCs desde Workbench

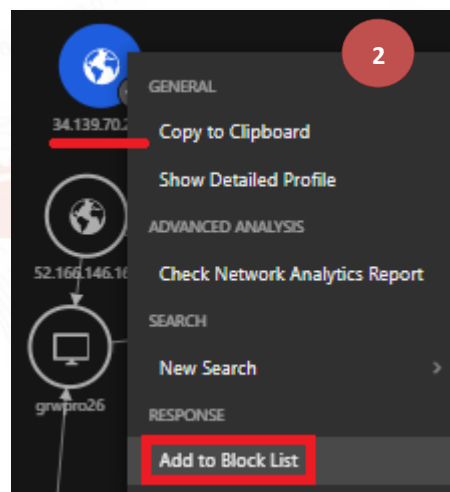
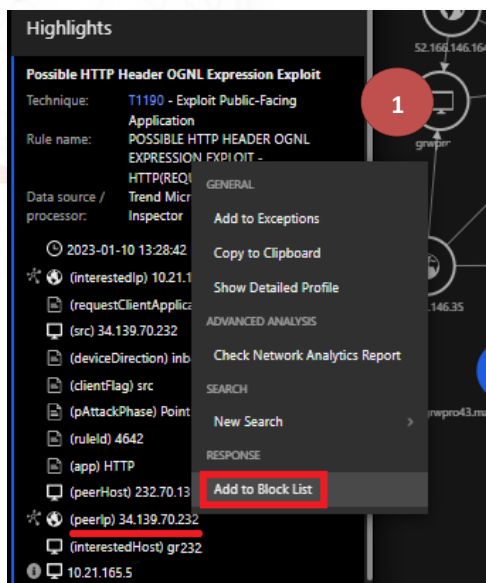
Al ingresar en un Workbench podemos observar algunos objetos destacados que corresponden con indicadores que podemos agregar a la lista de objetos sospechosos.

Lo importante es saber distinguir cuales objetos pertenecen a nuestra infraestructura y cuales no. Vision One no puede distinguir unos de otros, por lo tanto, por error, podríamos agregar como objeto sospechoso un objeto que es completamente válido y que pertenece a nuestra infraestructura.

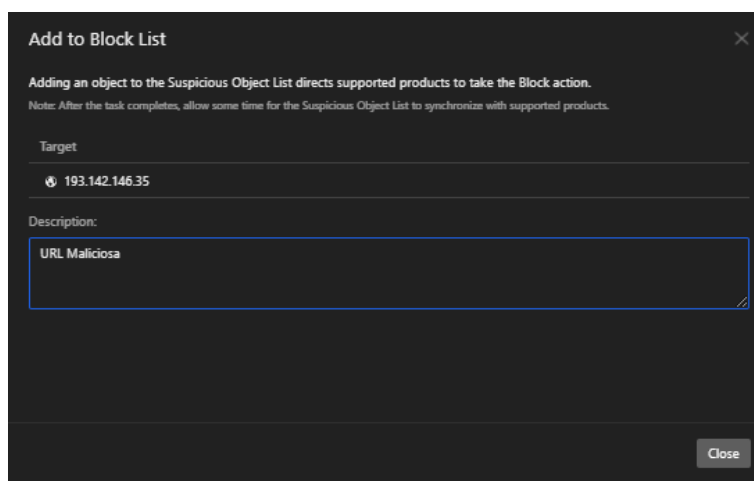
Para agregar los objetos desde el Workbench podemos hacerlo desde las dos siguientes formas:

1. Haciendo click derecho sobre el objeto destacado en **Highlights**
2. Haciendo click derecho sobre el objeto destacado en el panel interactivo.





Al hacer click en **Add to Block List**, nos aparecerá la siguiente ventana emergente donde se nos dará la opción de agregar una descripción del indicador que vamos a agregar:



Por defecto, al agregar un indicador, la expiración de este es de 30 días de haber sido agregado por lo que si queremos que este nunca expire debemos editar esta configuración:

Trend Micro Vision One™

Suspicious Object Management

Suspicious Object List

Exception List

+ Add



Last updated: All

Object type: All

Source: All

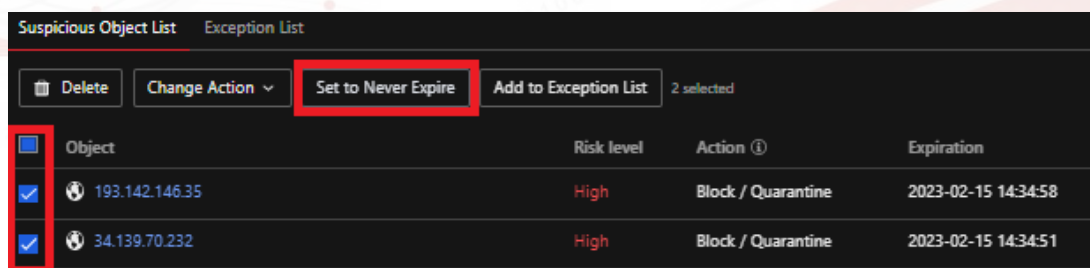
Q

Object, Source d...

<input type="checkbox"/>	Object	Risk level	Action ①	Expiration	Source	Source details
<input type="checkbox"/>	 193.142.146.35	High	Block / Quarantine	2023-02-15 14:34:58	User defined	Workbench
<input type="checkbox"/>	 34.139.70.232	High	Block / Quarantine	2023-02-15 14:34:51	User defined	Workbench

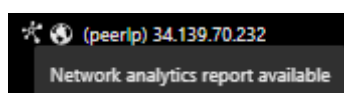


Para ello, desde **Threat Intelligence > Suspicious Object List**, hacemos click en el o los indicadores en cuestión y luego hacemos click en **Set to Never Expire** y luego confirmamos haciendo click en **Ok** dentro de la ventana emergente que nos aparecerá:



Agregar IoCs desde Network Analytics Report

Dentro de los Workbench, en algunos casos, se generan estos reportes que detallan las diferentes transacciones o envíos de paquetes/solicitudes entre un nodo y otro. En estos reportes también se detallan estos objetos destacados con la diferencia de que aquí obtendremos más información al respecto. Para ingresar al Network Analytics Report, primero debemos ingresar a un Workbench, y en la sección **Highlights** debemos buscar a algún objeto que tenga el siguiente ícono a su izquierda:



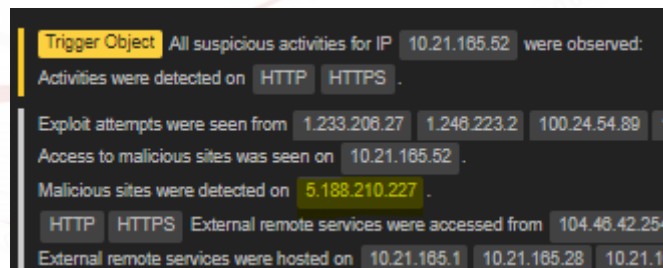
Al hacer click sobre este ícono se nos abrirá una nueva pestaña en la cual se nos mostrará este reporte:



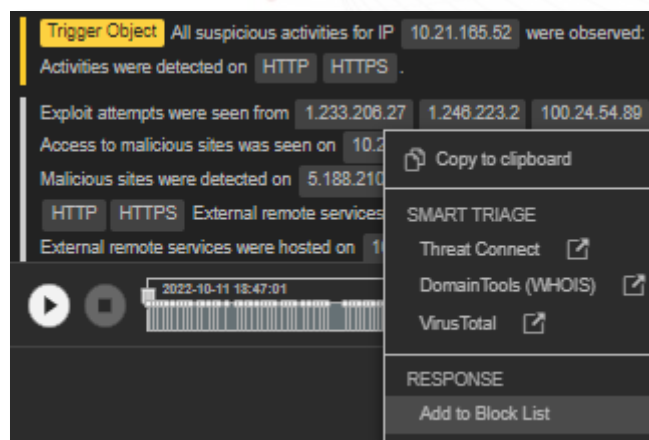
Aquí podremos agregar los indicadores desde dos de las tres secciones que tiene el Network Analytics Report:

1. El primer lugar es desde el **Summary**, donde tendremos más detallado cuales son las IP maliciosas y desde cuales se hicieron intentos de exploit.

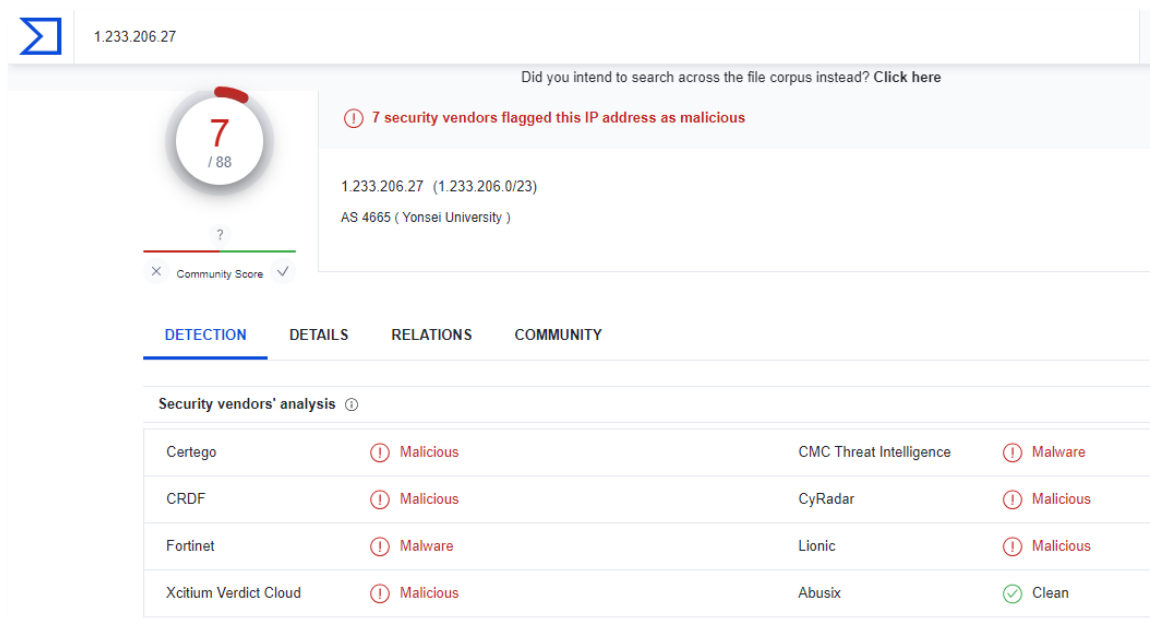




Desde cualquiera de estas podemos hacer click derecho y agregarla al listado de objetos sospechosos:



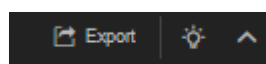
Como se puede ver en la imagen anterior, tanto en las IP que ya figuran como maliciosas, así como también en aquellas IP que figuran que han realizado intentos de exploit, se nos brinda la opción de corroborar su categorización en otros vendors como es el caso de VirusTotal. Al hacer click, se nos derivará a la página en cuestión. En la siguiente imagen, vemos la redirección a VirusTotal en la IP que figura con intento de exploit:



Esta información nos permite confirmar si es conveniente o no agregar esta IP a la lista de objetos sospechosos a fin de evitar un falso positivo.

2. También, es posible agregar estos indicadores a lista de objetos sospechosos desde la sección de **Transactions/IOCs**. Por defecto esta sección nos sitúa en **IOCs** pero este procedimiento lo podríamos hacer, también, desde **Transactions** dependiendo cual nos sea más cómodo para entender la detección. El procedimiento sería exactamente el mismo al mencionado anteriormente:

3. Otra forma de añadir los indicadores es realizando una exportación de los detalles del Network Analytics Report. Este procedimiento nos permitirá añadir IoCs de manera masiva, para ello hacemos click en **Export**, botón situado en la parte superior derecha:



Luego, elegimos el formato CSV. Al hacer la exportación, obtendremos un archivo “.zip” que contiene diferentes CSVs:


AttackPatterns.csv	100
Hosts.csv	34.308
IOC.csv	23.927
MitreTactics.csv	80.855
Risk&Counts.csv	56
RulesTriggered.csv	135.687
Summary.csv	13.174
Transactions.csv	374.750



El archivo que necesitamos es el llamado "IOC.csv", por lo cual ingresamos en el para ajustarlo según los requerimientos de formato que tiene Suspicious Object List:

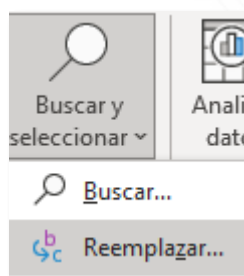
El archivo debe pasar del formato de la imagen de la izquierda:

	A	B
1	IOC Type,"IOC"	
2	IP Addresses,"1.233.206.27"	
3	IP Addresses,"1.246.223.2"	
4	IP Addresses,"2.32.254.133"	



	A	B
1	Type,Object,Description	
2	ip,1.233.206.27,test	
3	ip,1.246.223.2,test	
4	ip,2.32.254.133,test	

Para ello en el CSV, desde Excel -o algún otro editor para este formato- debemos reemplazar algunos valores:



Los valores a reemplazar son:

- IOC Type,"IOC" por Type,Object,Description
- IP Addresses," por ip,
- " por ,test

ACLARACIÓN 1: La palabra "test" está a modo de ejemplo, en su lugar debe ir la descripción que el usuario crea conveniente.

ACLARACIÓN 2: Se aconseja revisar el listado en cuestión para evitar falsos positivos ya que puede llegar a incorporar indicadores que pertenecen a la infraestructura o son objetos válidos.

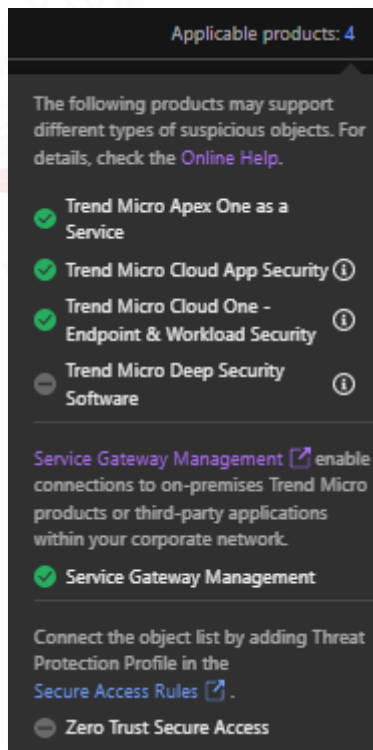
Una vez adaptado el archivo CSV, se debe guardar e importar en **Suspicious Object List** e importarlo como se indicó anteriormente.

Sincronización de IoCs agregados a Vision One con otros productos

Los IoCs agregados a Suspicious Object List se sincronizan con las integraciones que hayamos hecho hacia esta consola, tanto para los productos de Trend Micro como para los productos de terceros.

En el caso de los productos de Trend Micro, aquellos productos que recibirán este listado son los primeros que figuran en la siguiente imagen:





Productos que importarán el listado y actualizaciones de Suspicious Object List

En este ejemplo vemos que hay 3 productos que importarán a su listado de objetos sospechosos los mismos indicadores que se han agregado en Vision One. Por otro lado, los productos de terceros recibirán los indicadores a través del Service Gateway.

En **Apex One/Central SaaS**, podemos ver estos IoCs importados dirigiéndonos a **Threat Intel > Custom Intelligence**. Por defecto, nos sitúa en la pestaña de **User-Defined Suspicious Objects** que es el lugar donde veremos estos IoCs. La manera de diferenciar si fueron importados desde Vision One es observando el detalle de “Source Added By” donde veremos que nos indica que fue “Trend Micro Vision One”:

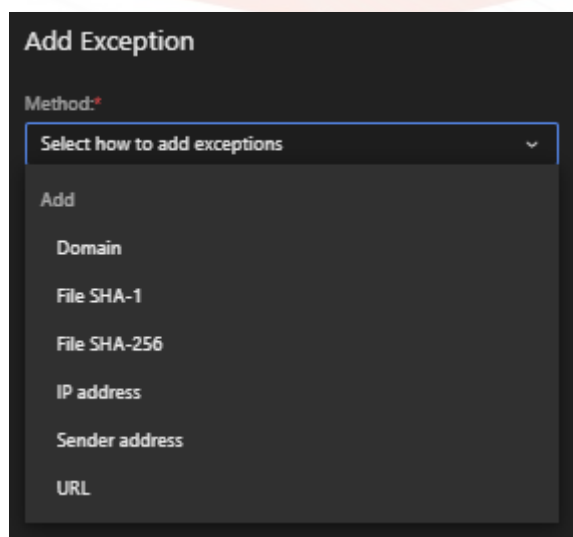
Trend Micro Apex Central™																																							
Dashboard	Directories	Policies	Threat Intel	Response	Detections	Administration	Help	Trend Micro Vision One																															
Custom Intelligence																																							
Protect against objects not yet identified on your network by manually adding suspicious objects to the list.																																							
User-Defined Suspicious Objects STIX OpenIOC																																							
View: All [Search]																																							
<div> Add Import Edit Export All Delete </div> <table> <thead> <tr> <th><input type="checkbox"/></th><th>Object</th><th>Type</th><th>Affected Endpoints/Recipients</th><th>Scan Action</th><th>Source</th><th>Source Added By</th><th>Notes</th><th>Last Modified ▼</th><th>Expiration Date</th></tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td><td>219.156.78.40</td><td>IP address</td><td>0 / 0</td><td>Block</td><td>API</td><td>Trend Micro Vi...</td><td></td><td>01/12/2023 11:50:43</td><td></td></tr> <tr> <td><input type="checkbox"/></td><td>209.141.54.195</td><td>IP address</td><td>0 / 0</td><td>Block</td><td>Manual</td><td></td><td></td><td>12/14/2021 14:08:48</td><td></td></tr> </tbody> </table>										<input type="checkbox"/>	Object	Type	Affected Endpoints/Recipients	Scan Action	Source	Source Added By	Notes	Last Modified ▼	Expiration Date	<input type="checkbox"/>	219.156.78.40	IP address	0 / 0	Block	API	Trend Micro Vi...		01/12/2023 11:50:43		<input type="checkbox"/>	209.141.54.195	IP address	0 / 0	Block	Manual			12/14/2021 14:08:48	
<input type="checkbox"/>	Object	Type	Affected Endpoints/Recipients	Scan Action	Source	Source Added By	Notes	Last Modified ▼	Expiration Date																														
<input type="checkbox"/>	219.156.78.40	IP address	0 / 0	Block	API	Trend Micro Vi...		01/12/2023 11:50:43																															
<input type="checkbox"/>	209.141.54.195	IP address	0 / 0	Block	Manual			12/14/2021 14:08:48																															



Exceptuar IoCs

Para agregar IoCs en la consola de Vision One hay que dirigirse a **Threat Intelligence > Suspicious Objects Management > Exception List**.

Dentro hacer click en el botón **Add**. Al hacer click se nos desplegará un panel desde la derecha en el que debemos indicar el tipo de IoC del cual se trata:



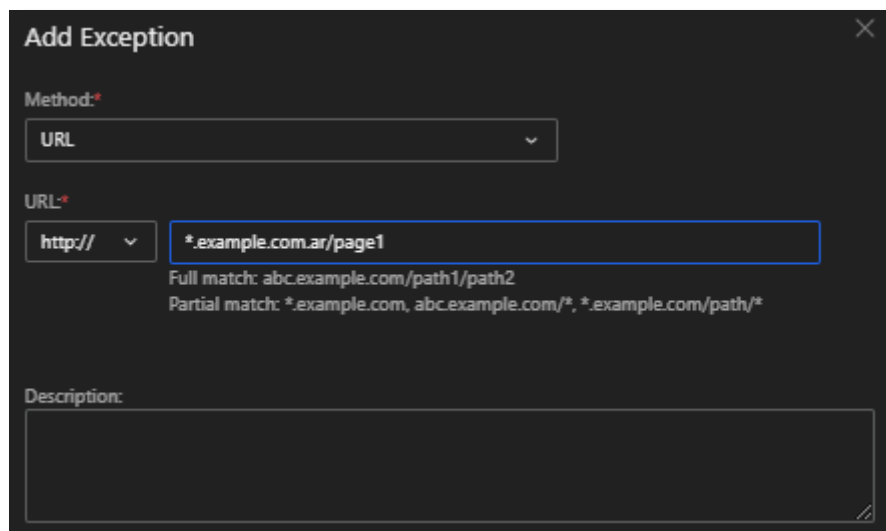
Add Exception

Method:*

Select how to add exceptions

- Add
- Domain
- File SHA-1
- File SHA-256
- IP address
- Sender address
- URL

Luego, agregamos los datos correspondientes y confirmamos haciendo click en **Submit**.



Add Exception

Method:*

URL

URL:*

http:// *example.com.ar/page1

Full match: abc.example.com/path1/path2
Partial match: *.example.com, abc.example.com/*, *.example.com/path/*

Description:

Una vez agregada los IoCs como excepciones se verán reflejados de la siguiente manera:



Trend Micro Vision One™

Suspicious Object Management

Suspicious Object List

Exception List

+ Add

Object type: All



Object



Object



http://*.abc.example.com/



<http://news.sina.com/>



EDSI Trend

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 - 6000
www.trendargentina.com.ar

Página 32