

CII CYBERPEACE

INFORME MENSUAL

PAVISA LUXE



www.cyberpeace.tech

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

SGSI-DOC-SOC-06 PAVISA-INFORME MENSUAL

Elaborado por:	Eliud Hernández Tapia Vilmerth Daniel Carrizosa Ceron Raziel Mata						
Aprobado por:	Iván Hernández						
Fecha:	05/07/23						
Objetivo del informe:	Dar a conocer la información relevante sobre los hallazgos en materia de seguridad obtenidos en este periodo de operación.						
Contexto:	Informe emitido como parte de las alertas de seguridad mostrados en el SOC.						
Alcance:	INICIO			FIN			
	01	06	2023		30	06	2023

Contenido

Contenido	2
Confidencialidad	4
Aviso de Restricción	4
Introducción.....	5
Eventos de seguridad Endpoint Apex Central.....	6
Actividad Sospechosa.....	6
Top de endpoints con actividad maliciosa	7
Dominios reportados por reputación de sitio.....	10
Top de usuarios con más detecciones	14
Eventos de seguridad en servidores Cloud One (Workload Security).....	15
Estatus de los agentes y consola de administración	15
Detecciones por Anti-Malware	16
Detecciones por Log Inspection	17
Detecciones por Integridad	20
Detecciones por Firewall	22
Reporte de Vision One	24
Detección de Vulnerabilidades.....	25
Postura de seguridad de PAVISA Luxe.....	26

Reporte de SIEM28

Reporte de Dark Trace29

Conexión nueva sospechosa 30

Conexión por puertos no estándares 31

Conexión Remota 32

Dominios Sospechosos 34

Movimiento Lateral 35

Peticiones DNS 36

Recomendaciones.....37

Acuse de recibido38

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Confidencialidad

Para efectos de este documento, el término “Material Confidencial” significa toda información, escrita, gráfica o contenida en cualquier medio tangible o intangible que Cyberpeace entregue a **PAVISA LUXE** para la prestación de los Servicios y la identifique como confidencial.

El término Material Confidencial no incluye aquella información que (I) está disponible al público en general, (II) se puso a disposición de Cyberpeace sin el carácter de confidencial antes de lo aquí establecido, o (III) se puso a disposición de Cyberpeace, sin el carácter de confidencial, por otra fuente sin obligación de confidencialidad.

Para mantener la confidencialidad de este material, FDFLA conviene en: (I) no usar el Material Confidencial, excepto para la prestación de los Servicios; (II) no revelar, -excepto por orden de una autoridad judicial o administrativa- el Material Confidencial a cualquier persona excepto a sus directores, empleados, asesores y representantes (conjuntamente los “Representantes”) que necesiten conocer la información; dichos Representantes se obligan a mantenerla como confidencial, y (III) no usar el Material Confidencial para fines propios y de terceras partes.

Aviso de Restricción

Restricciones de uso, divulgación del contenido

La información contenida en este reporte de servicio o cotización constituye un secreto industrial por lo que está clasificado como confidencial. Es revelada al cliente con la restricción de que no será usada o divulgada, sin el permiso de Cyberpeace, para otros propósitos que no sean su evaluación; obligándose a proteger la Información Confidencial recibida, usando un razonable grado de cuidado, pero no menor al grado de cuidado utilizado para proteger su información o material similar. Esta restricción no limita al derecho del cliente para usar o divulgar esta información si se obtuvo de otra fuente sin obligación de confidencialidad.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Introducción

El presente informe se encarga de documentar y reportar la actividad sospechosa o potencialmente crítica que se registró tanto en la plataforma de Trend Micro Apex Central, Trend Micro Cloud One, Trend Micro Vision y DarkTrace.

Al final de este reporte se anexan recomendaciones por parte de Cyberpeace que se espera sean atendidas para poder robustecer la infraestructura de **PAVISA LUXE** tanto en la red empresarial como en la plataforma en la nube. Realizando estas recomendaciones se ayuda a mitigar las vulnerabilidades que pudiese presentarse en los equipos o en la red de **PAVISA LUXE**.

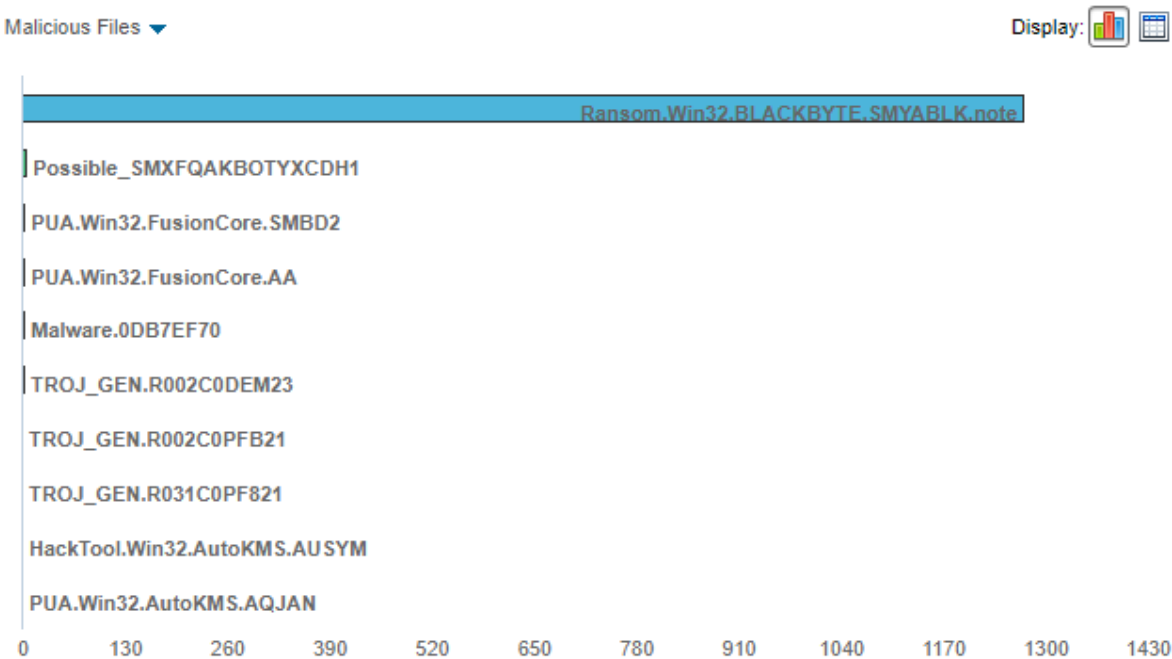
Algunas de estas recomendaciones deberán realizarse periódicamente en los equipos que los usuarios utilizan por lo cual se solicita el apoyo de los administradores para alentar a los usuarios a que las realicen.

Eventos de seguridad Endpoint Apex Central

En este apartado se muestran los eventos de seguridad que se presentan en el periodo reportado.

Actividad Sospechosa

Durante el análisis que se realizó a través de la herramienta Apex Central, se muestra el siguiente top con las actividades sospechosas registradas este mes.




Gráfica 1. Top de actividad sospechosa en el último mes.




La actividad presentada en la imagen anterior se detalla en la tabla 1.

Top de endpoints con actividad maliciosa

A continuación, se enlistan los endpoints con mayor actividad registrada durante el presente periodo, así como con el número de detecciones y los endpoint con la ruta donde se encontró la actividad maliciosa.

Tabla 1. Actividad sospechosa con número de eventos y endpoints donde se detectó.

Nombre de la actividad	Descripción	Número de Detecciones	Endpoint y Ruta
Ransom.Win32.BLACKBYTE.SMYABLK.note	El ransomware como servicio se puede entregar de muchas maneras, lo que depende del afiliado que está implementando el ransomware. Por ahora, Ransom.BlackByte parece usar una vulnerabilidad conocida de Microsoft Exchange Server para establecer una primera base y usar capacidades similares a gusanos para extenderse a través de una red.	1273	D33510PROYTC  Ransom.Win32.BLA CKBYTE.SMYABLK.no
Possible_SMXFQAKBOTYXCDH1	Possible_SMXFQAKBOTYXCDH1, es una detección heurística de un descargador QAKBOT.	4	 Possible_SMXFQAKB OTYXCDH1.pdf
PUA.Win32.FusionCore.SMBD2	Esta aplicación potencialmente no deseada llega a un sistema como un archivo eliminado por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos.	3	L00210ADMINI  PUA.Win32.FusionC ore.SMBD2.pdf

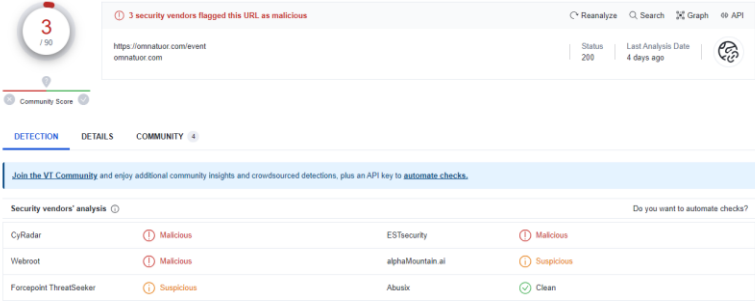
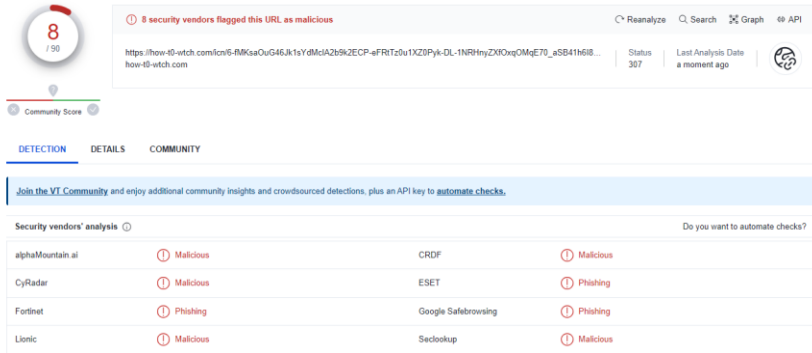
Nombre de la actividad	Descripción	Número de Detecciones	Endpoint y Ruta
PUA.Win32.FusionCore.AA	Este troyano llega a un sistema como un archivo caído por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos. Puede ser instalado manualmente por un usuario.	2	L00210ADMINI  PUA.Win32.FusionCore.AA.pdf
Malware.0DB7EF70	El malware abarca virus informáticos, troyanos, gusanos, spyware, puertas traseras y otro software malicioso. El malware puede diseñarse para cualquier sistema informático y, por lo tanto, cualquier dispositivo como teléfonos inteligentes, tabletas o incluso controladores lógicos programables en plantas industriales, puede verse afectado. Los ciberdelincuentes crean malware principalmente con fines de lucro, como parte de una próspera economía subterránea digital.	2	L00210ADMINI  Malware.0DB7EF70.pdf
TROJ_GEN.R002C0DEM23	Este troyano llega a un sistema como un archivo caído por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos. Requiere ser ejecutado con un argumento/parámetro específico, un componente adicional o en un entorno	2	D36010CAPHUM  TROJ_GEN.R002C0DEM23.pdf

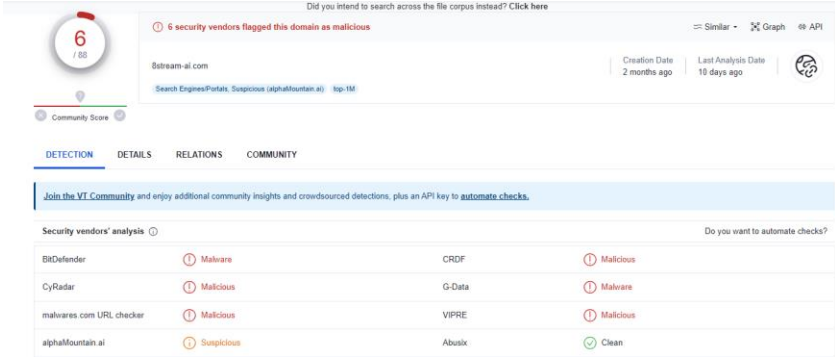
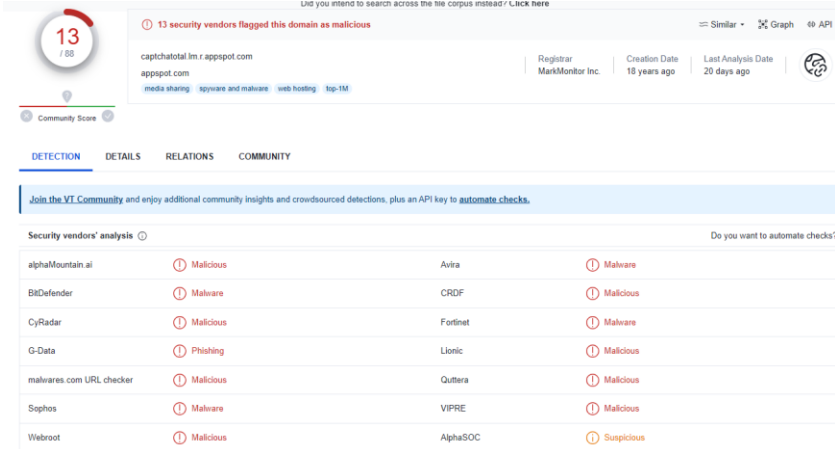
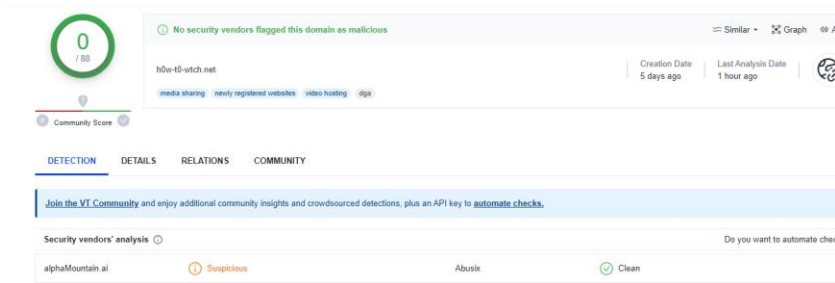
Nombre de la actividad	Descripción	Número de Detecciones	Endpoint y Ruta
	específico para continuar con su rutina prevista.		
TROJ_GEN.R002C0PFB21	Los troyanos suelen llevar cargas útiles u otras acciones maliciosas que pueden ir desde lo ligeramente molesto a lo irreparablemente destructivo. También pueden modificar la configuración del sistema para iniciar automáticamente	1	L00210ADMINI  TROJ_GEN.R002C0PFB21.pdf
TROJ_GEN.R031C0PF821	Los troyanos suelen llevar cargas útiles u otras acciones maliciosas que pueden ir desde lo ligeramente molesto a lo irreparablemente destructivo. También pueden modificar la configuración del sistema para iniciar automáticamente	1	L11312DISNOU  TROJ_GEN.R031C0PF821.pdf
HackTool.Win32.AutoKMS.AUSYM	Esta herramienta de piratería llega a un sistema como un archivo caído por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos.	1	L17413MOLDIT  HackTool.Win32.AutoKMS.AUSYM.pdf
PUA.Win32.AutoKMS.AQJAN	Esta aplicación potencialmente no deseada llega a un sistema como un archivo eliminado por otro malware o como un archivo descargado sin saberlo por los usuarios cuando visitan sitios maliciosos.	1	L17413MOLDIT  PUA.Win32.AutoKMS.AQJAN.pdf

Dominios reportados por reputación de sitio

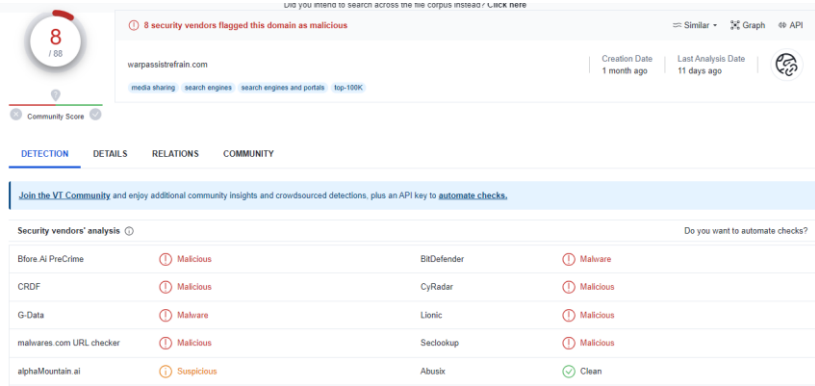
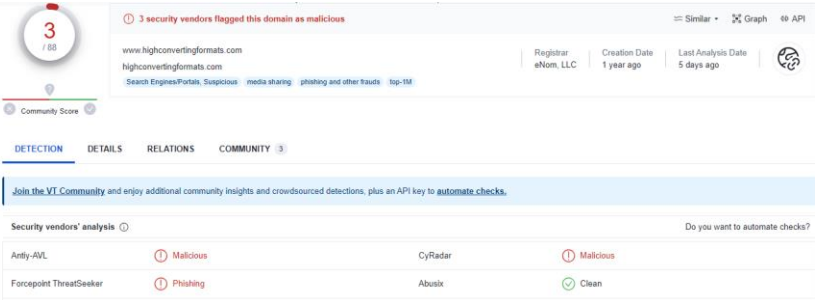
A continuación, dentro de la tabla 4 se llevará a cabo el registro de los 10 principales dominios reportados por el Apex Central los cuales han sido analizados en la herramienta de Virus Total, y en ellos se encontraron relaciones con malware y archivos maliciosos por lo que son catalogados como sitios potencialmente maliciosos. así mismo es posible observar los indicadores de compromiso de cada sitio por el cual fue reportado.

Tabla 4. Reputación de principales sitios bloqueados

ID dominio	Dominio	Tipo de bloqueo Apex Central	Reputación del sitio
1	omnatuor.com	Web reputation	 <p><i>Imagen 1. Sitio potencialmente malicioso 1</i></p>
2	how-t0-wtch.com	Web reputation	 <p><i>Imagen 2. Sitio potencialmente malicioso 2</i></p>

ID dominio	Dominio	Tipo de bloqueo Apex Central	Reputación del sitio
3	8stream-ai.com	Web reputation	 <p>Imagen 3. Sitio potencialmente malicioso 3</p>
4	captchatotal.lm.r.appspot.com	Web reputation	 <p>Imagen 4. Sitio potencialmente malicioso 4</p>
5	h0w-t0-wtch.net	Web reputation	 <p>Imagen 5. Sitio potencialmente malicioso 5</p>

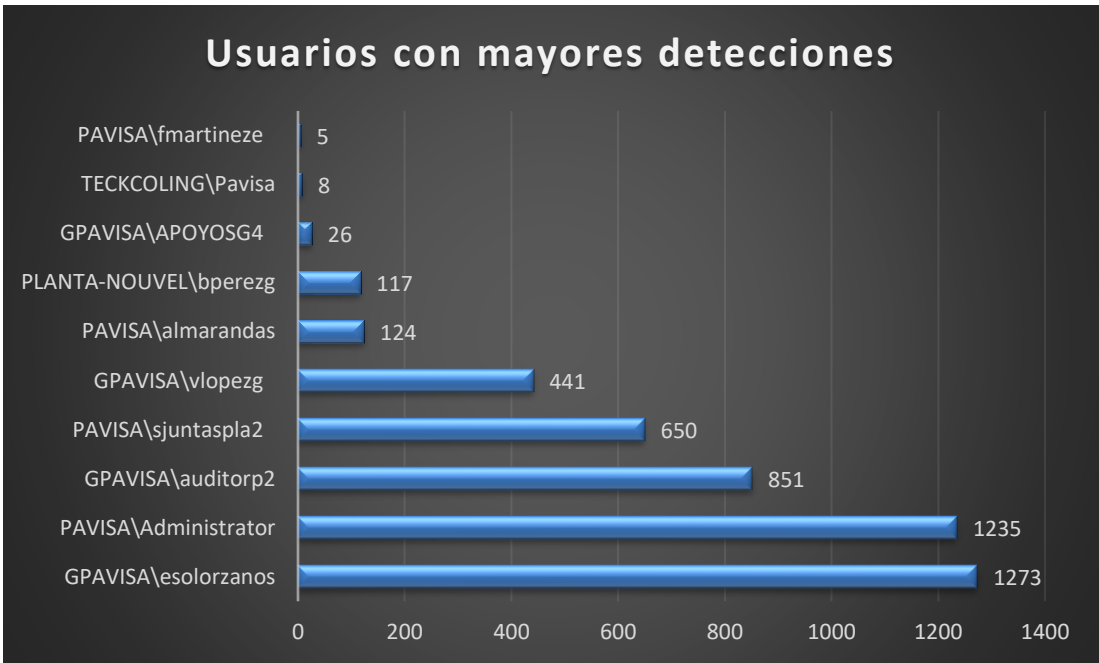
ID dominio	Dominio	Tipo de bloqueo Apex Central	Reputación del sitio
6	pogothere.xyz	Web reputation	
7	srxlpdfmxntetflx.com	Web reputation	
8	reallyindepende ncehated.com	Web reputation	

ID dominio	Dominio	Tipo de bloqueo Apex Central	Reputación del sitio
9	warpassistrefrain.com	Web reputation	 <p>Imagen 9. Sitio potencialmente malicioso 9</p>
10	www.highconvertingformats.com	Web reputation	 <p>Imagen 10. Sitio potencialmente malicioso 10</p>

Los anteriores dominios fueron bloqueados por la herramienta de seguridad por web reputation.

Top de usuarios con más detecciones

Durante este periodo el usuario que presentó mayores detecciones maliciosas fue el usuario **GPAVISA\esolorzanos**, tal como se muestra en la siguiente ilustración.



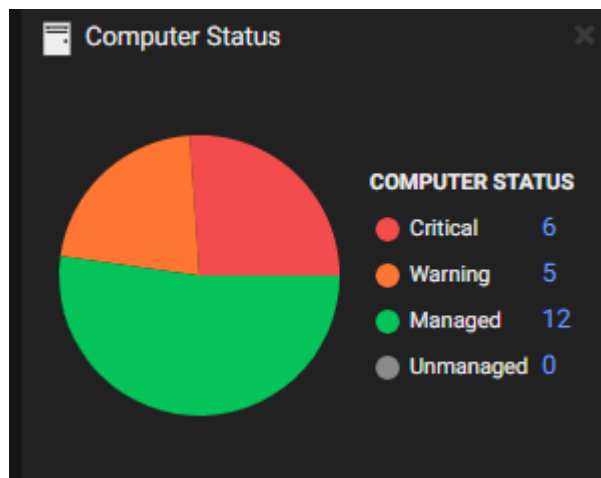
Gráfica 3. Usuarios con mayores detecciones

Las detecciones sobre los usuarios ocurren en mayor medida por los eventos acerca de la administración de endpoints, los cuales han sido descritos anteriormente dentro de la tabla 1, en donde se puede observar una breve descripción sobre el tipo de infección o virus con el que cuenta el dispositivo, así como también la cantidad de veces que fue detectado este evento al igual que nos brinda información acerca de los dispositivos involucrados.

Eventos de seguridad en servidores Cloud One (Workload Security)

Estatus de los agentes y consola de administración

Desde la herramienta de Trend Micro Cloud One se visualizó el estado de los agentes en los últimos 30 días, donde se pueden observar **6 servidores** en estado crítico, **5 servidores** en estado de warning y **12 en estado administrado**.



Gráfica 4. Estado de los servidores

Las alertas en los servidores de tipo *critical* se deben a que están en un estado offline, por parte de PAVISA nos han indicado que los servidores se encuentran encendidos y con el agente de Trend Micro instalado, también que se han hechos cambios en el firewall de la compañía para garantizar la comunicación con Trend Micro.

Computers (6)					
SAPQA.Pavisa.Local	10.11.10.13	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Errors	●
niquel.Pavisa.Local	192.168.200.225	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Errors	●
CRISTAL01	192.168.2.247	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Errors	●
ARCILLA.Pavisa.Local	192.168.2.68	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Errors	●
EMPAK.Pavisa.Local	192.168.200.113	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Unresolved s...	●
BACKUP_GPAVISA	192.168.200.55	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Unresolved s...	●

Imagen 8. Servidores con alerta critical.

En cuanto los servidores que presentan múltiples errores en el caso de **SAPQA**, **niquel**, **CRISTAL01** y **ARCILLA**, podemos observar que los errores se deben a el estado offline, la actualización del agente que fallo al instalarse, actualizaciones de configuración pendientes y el escaneo de malware que está pendiente.



	 Agent
Warnings/Errors	 Multiple Errors Software Update: Agent Software Upgrade Failed (Send software failed) Offline
Task(s)	Update of Configuration Pending (Offline) Scheduled Malware Scan Pending (Offline)

Imagen 9. Servidores ARCILLA e IMÁGENES con múltiples errores.

En cuanto a las alertas de tipo *warning* se debe al tema de actualizaciones pendientes que muestran los servidores con el agente de Trend Micro, de las cuales se han enviado desde la consola para que se aplique la actualización.





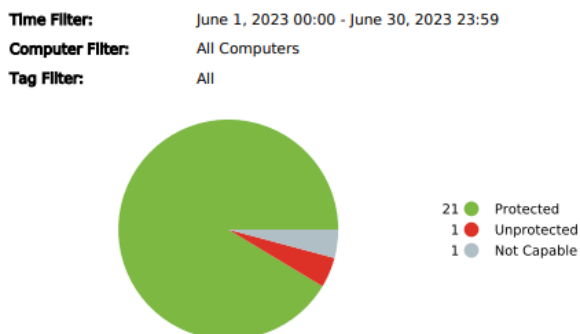
Computers (5)					
	GPAVHV03.Pavisa.Local	192.168.207.250	Microsoft Windows Server 2022 (64 bit)	WIN-PAVISA	Multiple Warn... 
	GPAVHV02	192.168.200.219	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Warn... 
	GPAVHV01	192.168.200.220	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Multiple Warn... 
	SODA.Pavisa.Local	10.11.10.5	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Software Upd... 
	PAVIFACT	192.168.207.47	Microsoft Windows Server 2016 (64 bit)	WIN-PAVISA	Smart Protect... 

Imagen 10. Servidores con alerta de warning.

Detecciones por Anti-Malware

El estado del módulo para conocer si los servidores están protegidos con Anti-Malware podemos observar que **21 servidores** se encuentran en estado de protegido, **1** es marcado como desprotegido debido al tema de actualizaciones, sin embargo, cuenta con la protección del agente, pero no en su última versión y **1 servidor en estado de not capable** esto se debe al estado de offline o problema de comunicación, el cual se está revisando para solucionarlo.

Anti-Malware Report



Gráfica 5. Estado del módulo Anti-Malware

El módulo de anti-malware no presenta datos durante este periodo.

Top 25 Infected Computers

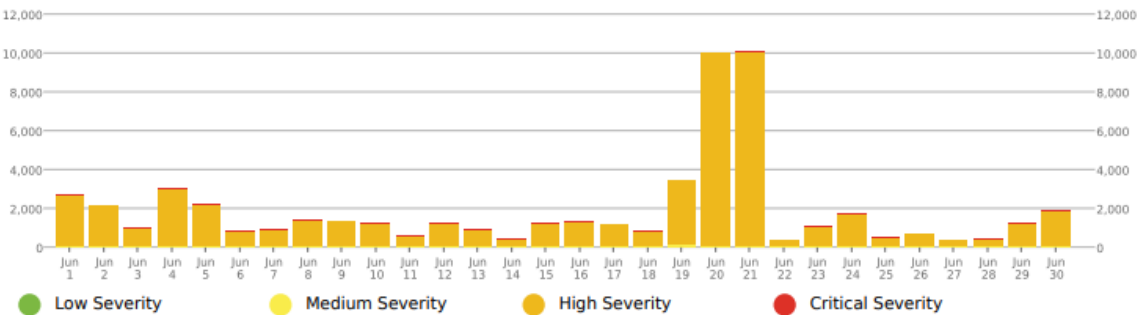
# of Malware	Computer
No Information	

Imagen 11. Eventos de la semana relacionados a Malware

Detecciones por Log Inspection

El módulo de inspección de logs en los últimos 30 días contó con actividad como se puede observar en la imagen siguiente.

Log Inspection Event History



Gráfica 6. Evento de la semana relacionados a la inspección de logs

En la siguiente tabla se describen los eventos relacionados a la inspección de logs.

Tabla 5. Desglose de logs inspection

Numero de eventos	Regla	Detalle
34,983 eventos correspondientes al 64.3%	1002795 - Microsoft Windows Events	Inspecciona los registros de eventos de los sistemas operativos Microsoft Windows (2000, XP, 2003) en busca de eventos.
18,136 eventos correspondientes al 33.3%	1003987 - Eventos de seguridad de Microsoft Windows - 2	Inspeccione los registros de eventos de los sistemas operativos Microsoft Windows en busca de eventos de Seguridad.

1,247 eventos correspondientes al 2.3%	1004057 - Eventos de seguridad de Microsoft Windows - 1	<p>inspección de los registros de eventos de los sistemas operativos de Microsoft Windows en busca de eventos de seguridad.</p> <p>Plataforma: Microsoft Windows 2016, Windows 10, Windows 2012, Windows 2008, Windows 7, Windows 2008, Windows 2008, Windows 2008, Windows 2008, Windows 2008 y Windows Vista.</p>
34 eventos correspondientes al 0.1%	1004488 - Servidor de base de datos - Microsoft SQL	Inspeccione los registros de eventos de Microsoft SQL Server.
30 eventos correspondientes al 0.1%	1003835 - Servidor Web - Seguridad del servidor Microsoft IIS	Inspeccione los registros de eventos IIS del Servidor Web en busca de eventos.

Los servidores que generan la mayor cantidad de los eventos de logs anteriores durante el periodo semanal son; **YSOFT, SRVPLANTA2, GPAVHV03, SRVPlanta01 y BACKUP_GPAVISA.**














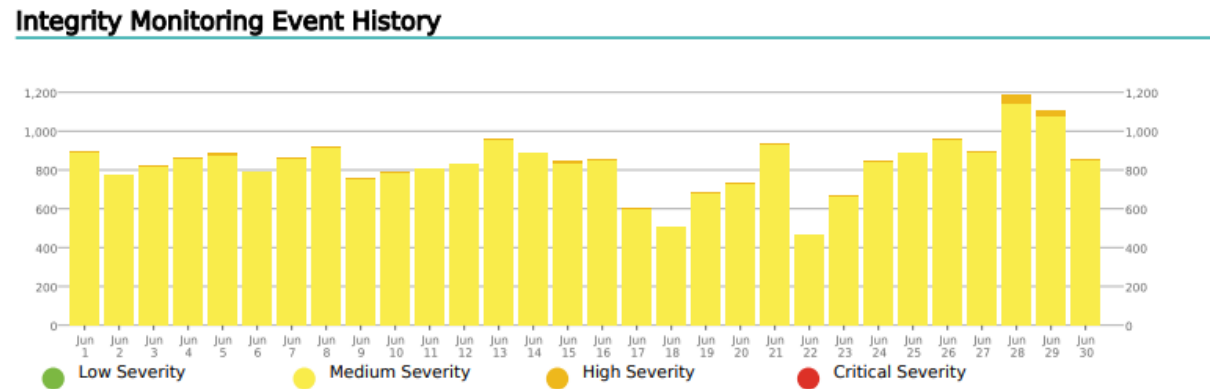
Top 25 Computers Ranked by Number of Log Inspection Events			
# of Events		Computer	
16,998	(31.2%)	 YSOFT.Pavisa.Local (192.168.207.55)	Last Update: July 1, 2023 01:35
		Policy: WIN-PAVISA	
13,734	(25.2%)	 SRVPLANTA2.Pavisa.Local (192.168.2.171)	Last Update: July 1, 2023 22:17
		Policy: WIN-PAVISA	
8,124	(14.9%)	 GPAVHV03.Pavisa.Local (192.168.207.250)	Last Update: July 2, 2023 23:09
		Policy: WIN-PAVISA	
4,156	(7.6%)	 SRVPlanta01.Pavisa.Local (192.168.200.202)	Last Update: June 28, 2023 15:41
		Policy: WIN-PAVISA	
3,469	(6.4%)	 BACKUP_GPAVISA (192.168.200.55)	Last Update: June 29, 2023 05:18
		Policy: WIN-PAVISA	
3,021	(5.5%)	 NiquelDC.Pavisa.Local (192.168.200.226)	Last Update: July 1, 2023 21:44
		Policy: WIN-PAVISA	
1,321	(2.4%)	 NITRATODC.Pavisa.Local (192.168.207.181)	Last Update: July 1, 2023 22:45
		Policy: WIN-PAVISA	
986	(1.8%)	 BARIO.Pavisa.Local (192.168.200.54)	Last Update: July 1, 2023 02:37
		Policy: WIN-PAVISA	
613	(1.1%)	 GPAVCRM01.Pavisa.Local (192.168.200.197)	Last Update: July 1, 2023 19:08
		Policy: WIN-PAVISA	
568	(1%)	 GPAVSQL01.Pavisa.Local (192.168.200.232)	Last Update: July 2, 2023 23:33
		Policy: WIN-PAVISA	
478	(0.9%)	 GPAVHV02 (192.168.200.219)	Last Update: July 2, 2023 06:30
		Policy: WIN-PAVISA	
453	(0.8%)	 GPAVHV01 (192.168.200.220)	Last Update: July 2, 2023 11:48
		Policy: WIN-PAVISA	
448	(0.8%)	 EMPAK.Pavisa.Local (192.168.200.113)	Last Update: June 29, 2023 08:03
		Policy: WIN-PAVISA	

Imagen 12. Tops servidores que generan los eventos de logs.

Detecciones por Integridad

Para el módulo de integridad la actividad fue como se puede observar en la imagen siguiente.



Gráfica 7. Eventos de la semana relacionados con integridad

En la siguiente tabla se observa el detalle sobre los eventos del monitor de integridad.

Tabla 6. Desglose del monitor de integridad.

Número de eventos	Regla	Detalle
15,542 eventos correspondientes al 62.5%	1002781 - Microsoft Windows - Atributos de servicios modificados (ATT&CK T1036.004)	Esta regla está destinada a alertar cuando se modifican los atributos de ciertos servicios de Microsoft.
9,029 eventos correspondientes al 36.3%	1006076 - Microsoft Windows - Entradas del programador de tareas modificadas (ATT&CK T1053.005)	Un adversario puede utilizar la programación de trabajos para ejecutar programas al inicio del sistema o de forma programado para la persistencia, para llevar a cabo la ejecución como parte del movimiento lateral, para obtener privilegios de root, o para ejecutar un proceso bajo el contexto de una cuenta específica.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

136 eventos correspondientes al 0.5%	1002780 - Microsoft Windows - Atributos del software instalado modificados (ATT&CK T1195.002, T1554)	Esta regla alerta cuando hay algún cambio en los atributos del software instalado o en los atributos del programa instalados. También avisa cuando se instala o desinstala un programa en el host de Windows.
93 eventos correspondientes al 0.4%	1003019 - Aplicación - Trend Micro Deep Security Agent / Relay	Esta alerta de regla indica que los archivos / claves de registro / servicios creados por Deep Security Agent / Relay fueron modificados. Esto podría indicar que el software fue actualizado o instalado / desinstalado.
30 eventos correspondientes al 0.1 %	1002999 - Aplicación - Microsoft SQL Server	Esta alerta indica que los archivos / claves de registro / servicios creados por Microsoft SQL Serve han sido modificados. Esto podría indicar que el software fue actualizado o instalado / desinstalado.
18 eventos correspondientes al 0.1%	1002778 - Microsoft Windows - Archivos .dll o .exe del sistema modificados (ATT&CK T1036.003, T1222.001)	Esta regla alerta cuando hay un cambio en los archivos .dll o .exe en la ruta %WINDIR%\system32. Para obtener información adicional, consulte la pestaña Detalles.

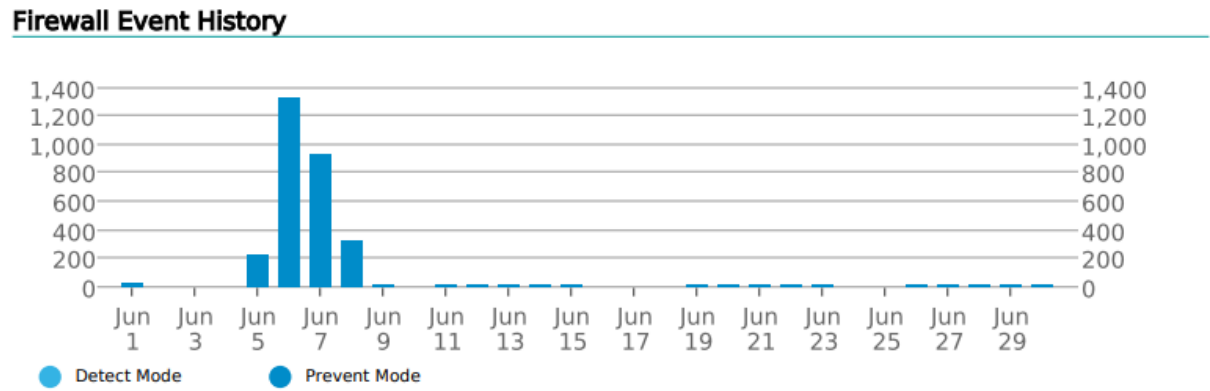
Los servidores que generan la mayor cantidad de los eventos de detecciones por integridad durante el periodo semanal son; **SODA, BACKUP_GPAVISA, NITRATO, silica y CLOUDQAS.**

Top 25 Computers Ranked by Number of Integrity Monitoring Events			
# of Events	Computer		
2,528 (10.2%)	<div> <div></div> <div>SODA.Pavisa.Local (10.11.10.5)</div> <div>Last Update: June 27, 2023 22:49</div> <div>Policy: WIN-PAVISA</div> </div>		
2,088 (8.4%)	<div> <div></div> <div>BACKUP_GPAVISA (192.168.200.55)</div> <div>Last Update: June 29, 2023 05:18</div> <div>Policy: WIN-PAVISA</div> </div>		
1,803 (7.3%)	<div> <div></div> <div>NITRATO.Pavisa.Local (10.11.10.21)</div> <div>Last Update: June 28, 2023 15:19</div> <div>Policy: WIN-PAVISA</div> </div>		
1,609 (6.5%)	<div> <div></div> <div>silica.Pavisa.Local (10.11.10.11)</div> <div>Last Update: July 2, 2023 14:36</div> <div>Policy: WIN-PAVISA</div> </div>		
1,537 (6.2%)	<div> <div></div> <div>CLOUDQAS.Pavisa.Local (10.11.10.12)</div> <div>Last Update: June 28, 2023 15:20</div> <div>Policy: WIN-PAVISA</div> </div>		
1,474 (5.9%)	<div> <div></div> <div>GPAVHV01 (192.168.200.220)</div> <div>Last Update: July 2, 2023 11:48</div> <div>Policy: WIN-PAVISA</div> </div>		
1,359 (5.5%)	<div> <div></div> <div>SRVPLANTA2.Pavisa.Local (192.168.2.171)</div> <div>Last Update: July 1, 2023 22:17</div> <div>Policy: WIN-PAVISA</div> </div>		

Imagen 13. Tops servidores que generan eventos de integridad.}

Detecciones por Firewall

Durante este periodo las detecciones en modo preventivo del firewall fueron como se observa en la imagen siguiente.



Gráfica 8. Eventos de la semana relacionados con el Firewall

En el apartado de las direcciones IP más comunes para los eventos del firewall durante este periodo no se presenta información.

25 Most Common Source IPs for Firewall Events (Detect Mode)

# of Packets	IP Address
No information	

Imagen 14. Top IPs detectadas por firewall en modo detect

En este periodo en el apartado de puertos, no se presenta información.

25 Most Common Destination Ports for Firewall Events (Detect Mode)

# of Packets	Port
No information	

Imagen 15. Top puertos detectadas por firewall

Mientras que en el modo prevención las direcciones IP detectadas fueron:

25 Most Common Source IPs for Firewall Events (Prevent Mode)

# of Packets	IP Address
2,612 (93.1%)	IP 10.1.8.230
151 (5.4%)	IP 10.1.8.30
25 (0.9%)	IP 10.1.8.204
8 (0.3%)	IP 192.168.207.140
6 (0.2%)	IP 192.168.200.114
3 (0.1%)	IP 192.168.200.8
1 (0%)	IP 192.168.2.171
1 (0%)	IP 192.168.207.181

Imagen 16. Top IPs detectadas por firewall en modo prevent

En este periodo en el apartado de puertos, se presenta que el puerto más común fue el puerto (49667), el cual se trata de un puerto no estándar, dinámico por lo cual la actividad podría tratarse de alguna aplicación interna.

25 Most Common Destination Ports for Firewall Events (Prevent Mode)

# of Packets	Port
1,868 (90.5%)	49667
194 (9.4%)	445
1 (0%)	3268
1 (0%)	443
1 (0%)	57848

Imagen 17. Top puertos detectadas por firewall

Los eventos detallados en la sección anterior fueron catalogados en modo detección, esto porque la política de prevención de amenazas a nivel firewall no se ha configurado para "Prevenir" esos eventos, es decir bloquearlos, cuando los eventos solo son detectados sólo se registrarán y alertarán de la ocurrencia de un evento, pero el Gateway no impedirá realmente que ocurra nada. Este modo es bueno para darle una idea de lo que está sucediendo en su entorno.

Reporte de Vision One

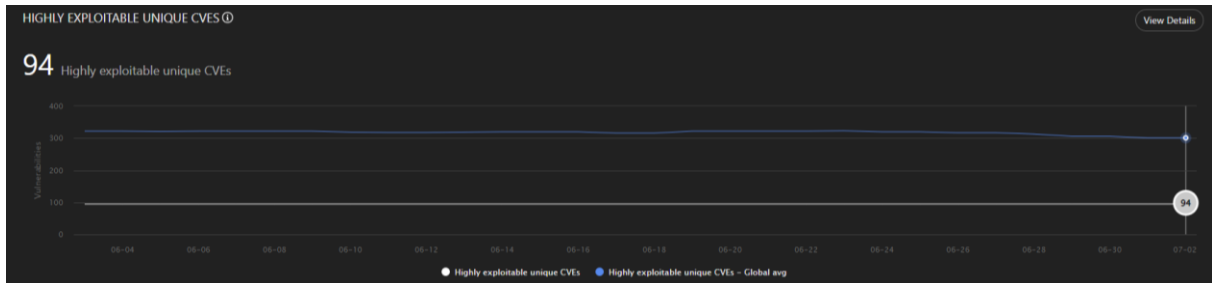
Durante el periodo Vision One detectó 1,072 eventos de ransomware y 690 eventos de malware, los cuales la herramienta Apex Central tomo la acción de bloquear el 100% de eventos de ransomware y el 99.38% de los eventos de malware, a lo que el otro 0.31% de eventos de malware fueron detectados en:

- D29940VTSNAC (IP: 192.168.1.68) en la ruta C:\Users\immiranda\Downloads\Summary-1517036838-Feb-15.zip
- D29940VTSNAC (IP: 192.168.1.68) en la ruta C:\Users\immiranda\Downloads\Summary-2106050159-Feb-15.zip
- D36010CAPHUM (IP: 192.168.200.35) en la ruta C:\Users\Pavisa\Desktop\angel\Desktop\Speed-Hack 2018 by LevelMaster GD\
- L00210ADMINI (IP: 10.1.8.240) en la ruta D:\angel\Desktop\Speed-Hack 2018 by LevelMaster GD\

Cabe destacar que estos eventos por la detección de archivos de texto dejados por la infección de ransomware del año pasado, lo que se recomienda eliminar dichos archivos para descartar alertas falsas positivas.

Detección de Vulnerabilidades

Durante el último periodo de evaluación (01 de junio al 30 de junio 2023) se han detectado la cantidad **88** de **CVE** únicos.



Grafica 9. Vulnerabilidades detectadas en la infraestructura.

Los dispositivos afectados son sistemas operativos Windows Server 2016, Windows Server 2019 y Windows 10, dado que se detectan sin los parches de seguridad correspondientes. Así mismo se identifica que los dispositivos rastreados como: SAPQA con 53 CVE, MANGANESO con 56 CVE, NITRATO 56 con CVE, NITRATODC con 56 CVE, BACKUP_GPAVISA con 56 CVE, silica con 56 CVE y GPAVHV03 con 51 CVE. Entre ellas podemos destacar **CVE-2023-21674**, la cual tiene un puntaje de impacto CVE de 74 y clasificado como crítico dada su fácil explotación, lo que ocasiona que afecte completamente a la disponibilidad, confidencialidad e integridad.

Se recomienda habilitar todas las reglas de prevención/detecciones disponibles de Trend Micro, habilitar los servicios de malware en tiempo real y aplique cualquier parche oficial.

CVE-2023-21674				
Basic Devices				
<input type="text" value="Device"/> <input type="button" value="Apply"/>				
Device name	Operating system	IP address	User name	Latest risk score
MANGANESO	Microsoft Windows Server 2016 10.0 (Bui...	10.11.10.1	SYSTEM	56
NITRATO.Pavisa.Local	Microsoft Windows Server 2016 10.0 (Bui...	10.11.10.21	quadm	56
NITRATODC.Pavisa.Local	Microsoft Windows Server 2022 10.0 (Bui...	192.168.207.181	NETWORK SERVICE	56
silica.Pavisa.Local	Microsoft Windows Server 2016 10.0 (Bui...	10.11.10.11.10.10.30.48	SYSTEM	56

Imagen 18. Vulnerabilidad de elevación de privilegios

Así mismo se detecta que dichas vulnerabilidades contienen una alta actividad de explotación en campañas maliciosas externas a Pavisa.

- CVE-2023-21674:** Es una vulnerabilidad en la llamada de procedimiento local avanzado (ALPC) de Windows que podría conducir a un escape del espacio aislado del navegador y permitir a los atacantes obtener privilegios de SISTEMA en una amplia variedad de instalaciones de Windows y Windows Server.

TOP 10 AT RISK VULNERABILITIES			Go to App	
App: Operations Dashboard				
Vulnerability ID	CVE impact score ↓ ⓘ	Impact scope		
CVE-2023-21674	74	4		
CVE-2022-41128	73	3		
CVE-2023-21768	71	1		
CVE-2023-21823	71	4		
CVE-2022-41033	70	1		
CVE-2022-41073	70	3		
CVE-2022-41125	70	3		
CVE-2023-23376	70	4		
CVE-2023-28252	70	4		
CVE-2023-29336	70	3		

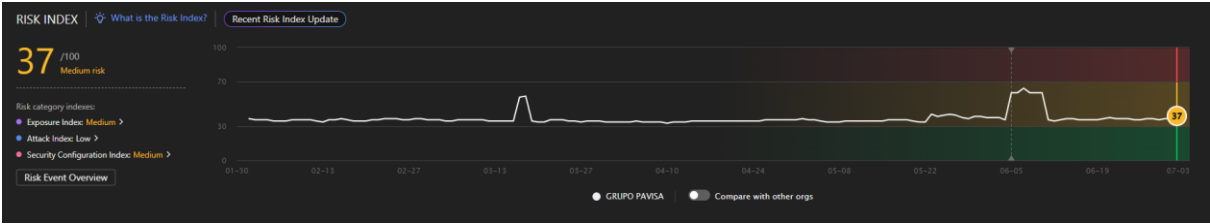
Imagen 19. Top de vulnerabilidades detectadas.

Se recomienda ampliamente realizar evaluaciones y gestión de riesgos con el fin de aplicar los parches de seguridad de los diversos dispositivos utilizados para la operación del negocio, con el fin de reducir el riesgo de explotación de estas. Asimismo, se recomienda el bloqueo de los programas conocidos como “Activadores” para el uso de herramientas comerciales. Dado que estos pueden llegar a contener artefactos maliciosos que provoquen la infección de un malware y/o la interrupción del negocio.

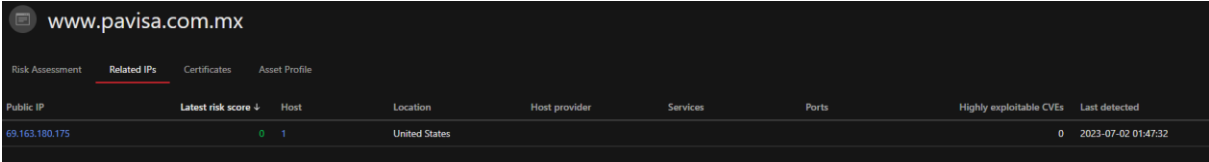
Realizar campañas de concientización con el fin de comunicar y concientizar a todos los colaboradores de los riesgos presentes en el ciber espacio y en el uso adecuado de las herramientas de trabajo.

Postura de seguridad de PAVISA Luxe

El host utilizado por PAVISA con IP 69.163.180.175 cuenta con un riesgo medio promedio del **37%** en el periodo de junio con un pico del 64%. Esto es el resultado del análisis de Vision One, el cual es realizado mediante métricas de riesgo de la propia herramienta que hace uso de la información recopilada de las campañas maliciosas activas e inactivas alrededor del mundo y la información recolectada de la infraestructura de Pavisa Luxe, asimismo se recomienda gestionar las vulnerabilidades presentes en los activos utilizados, generar campañas de *awareness* o *concientización*, dirigidas a todos los niveles, con el fin de disminuir el riesgo de infección de ransomware o malware, suplantación de identidad, secuestro de información, entre otras amenazas latentes en el ciber espacio en relación a las características similares entre el tipo de negocio y PAVISA.



Grafica 10. Riesgo de seguridad en el negocio.



www.pavisa.com.mx								
Risk Assessment		Related IPs		Certificates		Asset Profile		
Public IP	Latest risk score ↓	Host	Location	Host provider	Services	Ports	Highly exploitable CVEs	Last detected
69.163.180.175	0 1		United States				0	2023-07-02 01:47:32

Imagen 20. Dirección IP asignada al dominio pavisa.com.mx.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Reporte de SIEM

Debido a la intermitencia presentada sobre la instancia del Wazuh no se logra visualizar la herramienta y obtenemos el siguiente mensaje. Se tiene entendido que el tema actualmente se debe a cuestiones de infraestructura de PAVISA, quedamos en espera para llevar a cabo la reinstalación de la herramienta cuando se cuenten con lo enviado en el documento de requerimientos.

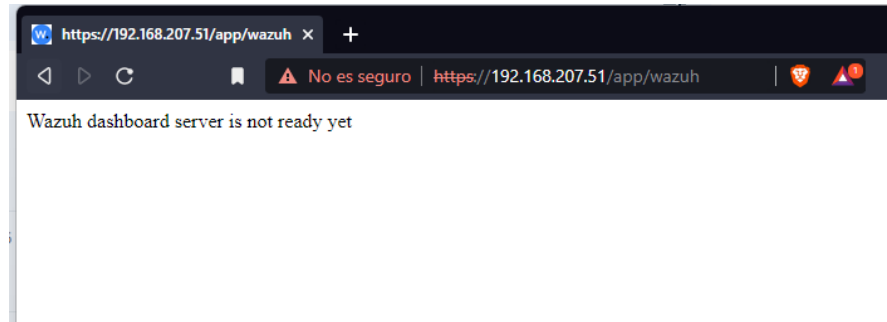


Imagen 21. Error Wazuh.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

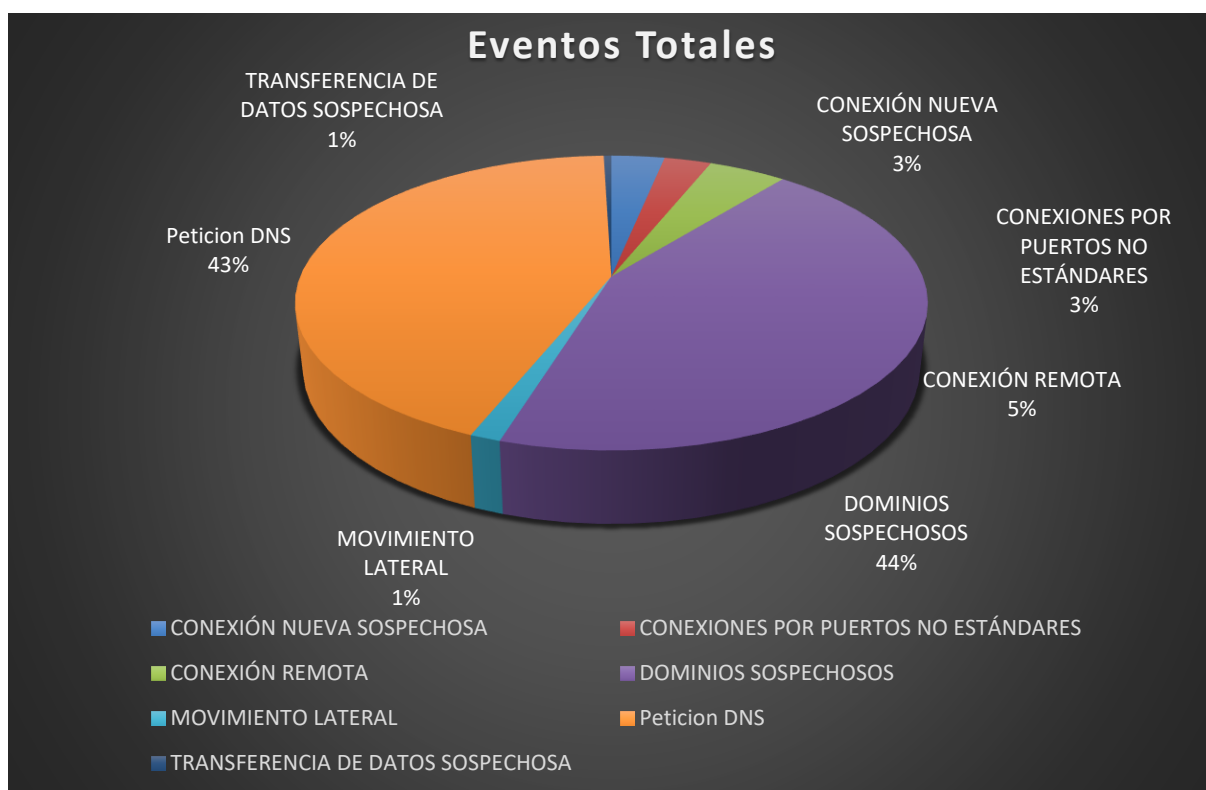
Reporte de Dark Trace

En el periodo de análisis se realizaron detecciones que mostraron una actividad alta en la red de Pavisa Luxe. Las detecciones fueron catalogadas como conexiones por puertos no estándares, conexiones remotas, dominios sospechosos, movimientos laterales, conexiones internas, peticiones de DNS y transferencia de datos sospechosa.

Se tuvo un total de **1,764 detecciones** en este periodo, en el cual, para las actividades internas detectadas como sospechosas se solicitó la validación de la actividad o se actuó de manera proactiva bloqueando las conexiones.

Es importante denotar que en este periodo se detectaron un gran número de peticiones a sitios que contaban con un historial de dominios sospechoso. Muchos de estos sitios no tienen ninguna relación con el sector en donde se desenvuelve Pavisa Luxe y presentaban indicadores de compromiso como puertos no seguros (http), certificados sin validar o contaban con relación con otros sitios maliciosos.

Finalmente, más del 95% de las detecciones se realizaron dentro del horario laboral, por lo que no se presentaron detecciones con cantidades anómalas en horarios inusuales. A continuación, se describen los hallazgos.



Gráfica 9. Eventos Totales

Conexión nueva sospechosa

Se detectaron **70 eventos** de conexión nueva sospechosa lo que representa un **3%** de los eventos totales del mes reportado, mismos que se presentaron al identificar conexiones que no se realizan comúnmente por parte de los hosts. Las conexiones detectadas fueron movimientos entre host internos o sitios sin indicadores de compromiso reportados en los informes semanales y corresponden a conexiones vía puerto 88 TCP relacionado a protocolo Kerberos, 389 LDAP, así como de otros puertos relacionados a servicios como, POP3, IMAP, XMPP Client Connection entre otros.



Gráfica 10. Eventos Totales de conexión nueva sospechosa

A lo largo del mes, estas conexiones se reportaron en su mayoría sobre los host **D00310ADMINI**, **D02210ADMINI** y **192.168.200.184**, esta actividad indica que dichos hosts albergan un sistema de autenticación (Directorio Activo, Kerberos, LDAP) que se encarga de permitir la autenticación recíproca entre un cliente y un servidor y se utiliza principalmente para centralizar la autenticación de usuarios y equipos en una red, lo que denota una actividad normal para este tipo de sistemas.

Conexión por puertos no estándares

Se detectaron **62 eventos de conexión por puertos no estándares** lo que representa un **3%** de los eventos totales del mes reportado, mismos que se presentaron al identificar conexiones mediante puertos no comunes o puertos dinámicos, este tipo de intento de conexiones pueden suceder por alguna configuración específica del usuario o algún tipo software. Se destaca que la mayoría de estos sitios de conexión no cuentan con un histórico maliciosos. Sin embargo, se mantiene seguimiento a este tipo de conexiones, a fin de detectarse reincidencias en las mismas y de igual forma de identificarse algún histórico malicioso sobre las mismas, se bloquearon de manera proactiva las conexiones al sitio.

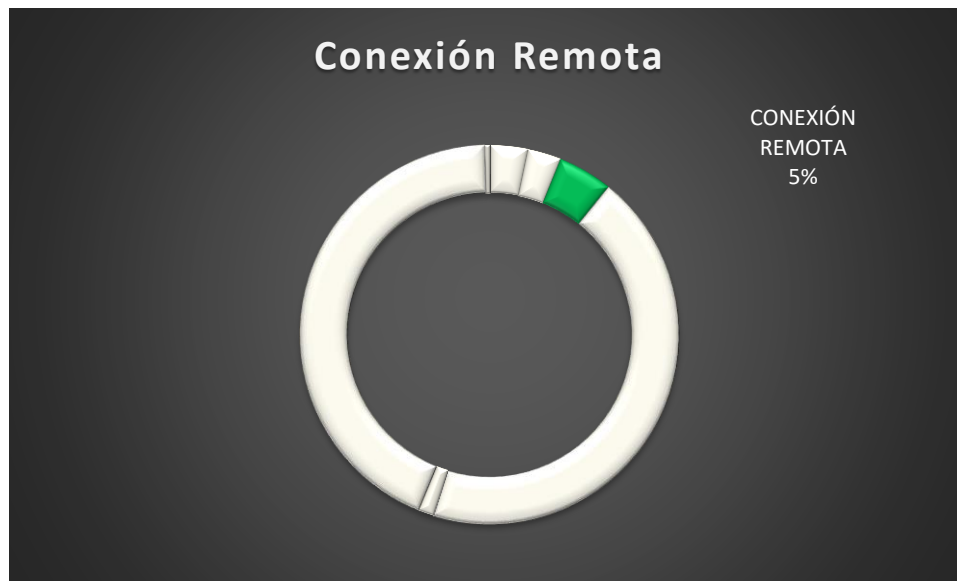


Gráfica 11. Eventos Totales de conexión por puertos no estándares

Se destaca que la mayoría de estos movimientos fueron originados desde host internos hacia IPs externas a la red de Pavisa, algunos de los hosts con mayor número de visualizaciones fueron **192.168.200.184**, **189.216.151.68**, **REDMI-9** y mismos que se conectaron a IPs/Sitios externos mediante puertos identificados como dinámicos por la IANA, cabe destacar que en la revisión de las conexiones no se visualizaron movimientos anómalos debido a que las conexiones correspondían a movimientos sobre las direcciones IP asociadas a dominios como **Telmex**, **Megacable**, **Cablevisión**, **Totalplay**, **Amazon**, **Google**, **Uninet**, **Alestra**, **Telcel** entre otros por lo que correspondían principalmente a movimientos sobre los servicios del sitio. Se debe validar si los hosts tienen permitido realizar este tipo de actividades o si las mismas son afines para el cliente.

Conexión Remota

Se detectaron **102** eventos de **conexión remota** lo que representa un **5%** de los eventos totales del mes reportado, mismos que se presentaron al identificar conexiones mediante el uso de algún software de control remoto de terceros o mediante escritorios remotos. Dichas conexiones fueron validadas por el equipo de Pavisa Luxe anteriormente o durante su revisión



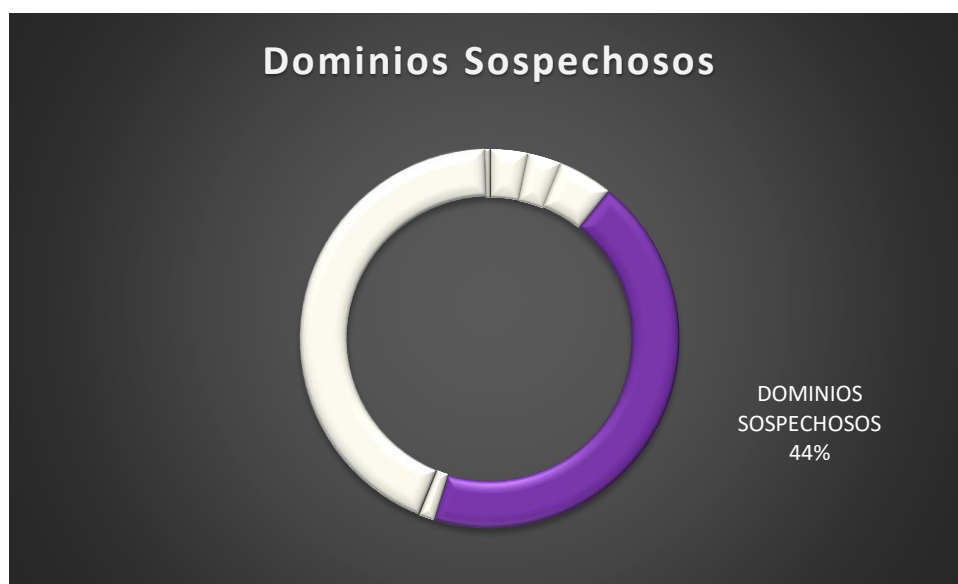
Gráfica 12. Eventos totales conexión remota

Estos eventos se realizaron en su mayoría sobre las direcciones IP **L00210ADMINI**, **192.168.200.43**, **D00310ADMINI**, **L14710ADMIN** y **SISTEMAS0001** entre otras realizando conexiones remotas sobre el dominio **divetro.home.linux**, **anydesk**, así como **RDP de Microsoft Windows** vía puerto **3389**, actividad validada por el equipo de Pavisa Luxe con anterioridad.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Dominios Sospechosos

Se detectaron **953 eventos** de dominios sospechosos lo que representa un **44%** de los eventos totales del mes reportado, mismos que se refieren a la conexión desde la infraestructura de Pavisa Luxe hacia sitios web sospechosos por protocolos como https y http. En la mayoría de los eventos, los sitios web no presentaron indicadores de compromiso actuales, pero si un antecedente o reputación negativa o bien relación con algunos otros sitios que presentan indicadores de phishing o malware, en los casos anteriores se actuó de manera proactiva el 100% de las ocasiones bloqueando los dominios mediante la Watch List de Dark Trace o en su caso el propio sistema de Respond Action bloqueo la conexión, solicitando posteriormente de nuestro lado la respectiva validación a fin de mantener o liberar los bloqueos en alguno de los sitios.



Grafica 17. Eventos totales por dominios sospechosos

Los dominios donde se reportan más interacciones son: **objects.githubusercontent.com**, **ipify.org**, y **retcode-us-west-1.arms.aliyuncs.com**. Los dominios previamente presentados se analizaron durante el periodo de monitoreo y en dado caso de actividad sospechosa o relación con indicadores de compromiso se procedió al bloqueo de estos por medio del watched domains de la herramienta.

Movimiento Lateral

Se detectaron **29 eventos** de movimiento lateral lo que representa un **1%** de los eventos totales del mes de reportado, mismos que se derivaron de la conexión de usuarios quienes inician sesión mediante conexiones por SMBv2 para la lectura/escritura de archivos o mediante el protocolo DCE RPC para el acceso a un recurso o aplicaciones las cuales se usan para la comunicación entre equipos.

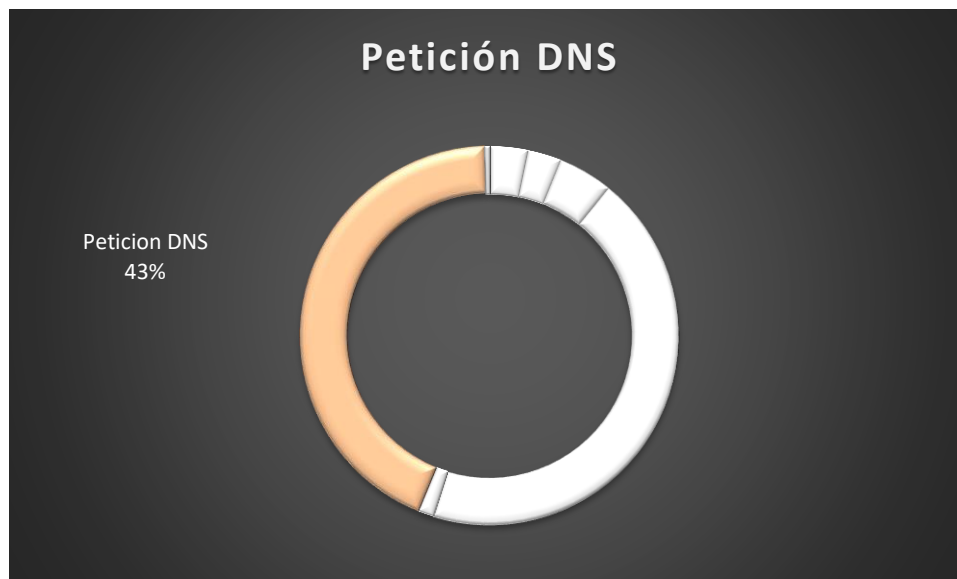
Estos eventos fueron alertados y en algunos casos validados por el equipo de Pavisa Luxe, donde se analizaron los eventos y ninguno de ellos presentó persistencia o algún otro indicador que sugiera la presencia de un artefacto malicioso o malware. Teniendo mayor visibilidad en los eventos los hosts **L16810SISGES**, **L07910SISGES**, **L11910TECINF**, **L02910CAPHUM**, entre otros donde se visualizó durante el mes lectura y escritura por parte de diversos usuarios, en su mayoría administradores.



Gráfica 15. Eventos totales movimiento lateral

Peticiones DNS

Se detectaron **940 eventos** de peticiones de DNS por el puerto 53 entre varios dispositivos internos de la red de Pavisa Luxe lo que representa un **36%** de los eventos totales del mes reportado. Estas peticiones fueron detectadas ya que el dominio al que se intenta tener conexión se encuentra en la lista de dominios sospechosos en Dark Trace debido a que presentó un histórico de actividad maliciosa durante las revisiones de este. Se destaca que ninguna de estas peticiones de resolución de nombres fue exitosa debido a que el sistema de Antigena bloqueó cada una de estas, así mismo esto debido a que se encuentra en la lista de Watch Domains.



Grafica 16. Hosts de origen

Cabe destacar que durante este periodo los dominios principales donde se reportan más peticiones DNS son, **ipify.org**, **s-onetag.com** es importante realizar el bloqueo mediante los equipos de seguridad perimetral de la red esto con el fin de robustecer la seguridad de la red.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Recomendaciones

- Es de vital importancia mantener actualizado los sistemas operativos, las aplicaciones instaladas en los equipos a las últimas versiones disponibles. Esto con el fin de evitar cualquier tipo de incidente de seguridad que pudiera producirse por este medio.
- Realizar una investigación sobre los usuarios que se conectan desde lugares no identificados e identificar si es un inicio de sesión válido.
- Analizar cuáles de las recomendaciones dada por las plataformas de Trend Micro es posible implementar sin que genere un costo y afecten las operaciones de Pavisa Luxe.
- Fortalecer las políticas de restricción a sitios no deseados para evitar la descarga de artefactos maliciosos que pueden estar contenidos en las herramientas catalogadas como hacktools las cuales suelen alertarse por parte del SOC y que aparecen reportadas a lo largo de los informes mensuales y semanales.
- Reforzar las políticas de acceso o restricciones que se tienen configuradas en el o los firewalls o IPS/IDS de la organización (seguridad perimetral).
- Realizar el cambio periódico de las contraseñas de los equipos y de los usuarios que laboran en la organización.
- Realizar la configuración e instalación del Gateway en Vision One y agentes con el fin de tener una mayor visibilidad de eventos sospechosos, así como un mejor control ante su detección.
- Habilitar el servicio de SIEM (Wazuh) para centralizar eventos de seguridad distintos a las herramientas de Trend Micro lo cual ayudará a complementar la visibilidad de eventos que actualmente tenemos con la herramienta de Trend Micro Vision One y realizar notificaciones proactivas o tempranas.
- Fortalecer las listas negras para evitar la conexión con dominios sospechosos en internet y crear una lista blanca que contenga actividad legítima de servidores como respaldos y otras actividades válidas a fin de prevenir y liberar bloqueos que pudieran impactar en la actividad del cliente.
- Realizar el bloqueo vía Firewall del dominio **s-onetag.com** y **ipify.org**, con el fin de ya no presentar este tipo de conexiones que a pesar de que la herramienta de DarkTrace está bloqueando, robustecería la seguridad un bloqueo desde otra capa de seguridad como la perimetral.

	Informe mensual	Versión:	01
		Clasificación:	Reservado
		Etiqueta:	TLP: AMBER

Acuse de recibido

Leído y analizado el presente informe, se firma de conformidad para todos los efectos.

José Roberto Segundo G.

SOC Manager - Ivan Hernández Cortés

Observaciones



CII