INFORME DE GESTION DE LA PLATAFORMA DE SEGURIDAD TRELLIX EPO

Preparado para:

AERONÁUTICA CIVIL
Unidad Administrativa Especial

BOGOTÁ
2022

CONTENIDO

INTRODUCCIÓN 3
EQUIPOS GESTIONADOS 4
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS NOVIEMBRE 2022. 4
MCAFEE ENDPOINT SECURITY 5
VERSIONES DE PRODUCTOS MCAFEE DEL MES DE NOVIEMBRE 6
McAfee Agent 6
Endpoint Security Platform 6
Endpoint Security Threat Prevention 7
Endpoint Security Adaptive Threat Protección 7
Endpoint Security Web Control 8
INFORMACIÓN DE ATAQUES E INFECCIONES 9
ENDPOINT SECURITY 9
Top 10 de equipos con más detecciones durante el mes de noviembre 9
Top 10 de las principales amenazas detectadas durante el mes de noviembre. 11
ENS: 10 principales amenazas por categoría de amenaza noviembre 2022 11
Amenazas por categoría 11
Acciones realizadas 12
INFORMACION DE ACTUALIZACIONES 14
ENS: Top 10 de las actualizaciones DAT 14
Observaciones 14

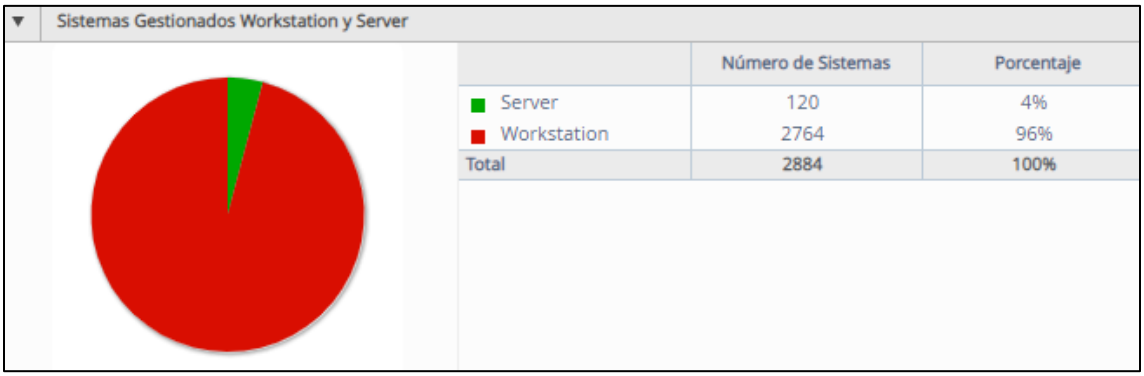
INTRODUCCIÓN

El presente informe tiene como objeto realizar una entrega de información detallada de la manera en la que actualmente opera la consola de administración Trellix ePO MVISION, la forma en la que en este momento se encuentran los productos administrados por esta, en temas relativos a estado de la protección de antivirus, estado de actualización de versiones de producto y estado de las actualizaciones de seguridad. También entregar el top 10 de los equipos que presentaron amenazas, principales amenazas detectadas, entre otros, correspondiente al mes de noviembre de 2022.

EQUIPOS GESTIONADOS

A continuación, se relaciona el número de equipos actualmente gestionados por la consola de administración Trellix ePO, en donde se realiza una comparativa del número de equipos gestionados del mes de octubre de 2022.

ITEM	Octubre - 2022		Noviembre - 2022	
	No Sistemas Gestionados	Porcentaje	No Sistemas Gestionados	Porcentaje
Workstation	2853	96%	2761	96%
Servidores	119	4%	120	4%
Total	2972	100%	2881	100%



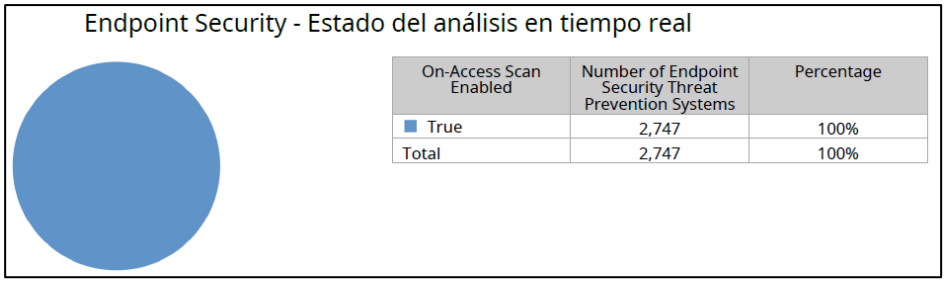
En el mes de noviembre y parte de diciembre se continuó con la migración de equipos a consola en la nube. Se realizo depuración con base en la revisión de equipos que presentaban una versión de firma desactualizada, más concretamente equipos con versión 46, 47 y 48. Es de aclarar, que aún siguen apareciendo nuevos equipos en consola local. A la fecha queda un reporte de **3 equipos** en consola **On-Premise**. Algunos equipos migran automáticamente, en otros casos se tiene que hacer la actualización en sitio debido a que no se aplican las directivas y tareas de manera correcta. Se evidencia una disminución de equipos considerable debido a un último informe de **L3000** que presentaba mas de **140 equipos duplicados**.

ESTADO ACTUAL PROTECCIÓN ANTIVIRUS NOVIEMBRE 2022.

Es importante indicar que actualmente los equipos de cómputo de la AERONÁUTICA CIVIL (estaciones de trabajo y servidores) se encuentran netamente monitoreados por **McAfee Endpoint Security.**

TRELLIX ENDPOINT SECURITY

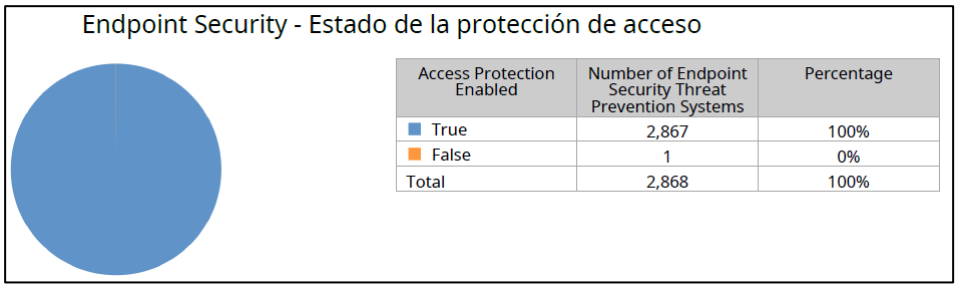
Estado del análisis en tiempo real.



On-Access Scan Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,747	100%
Total	2,747	100%

Este análisis es correspondiente al módulo de **Adaptive Threat Prevention** como detección temprana de amenazas que se puedan catalogar como amenaza en el sistema.

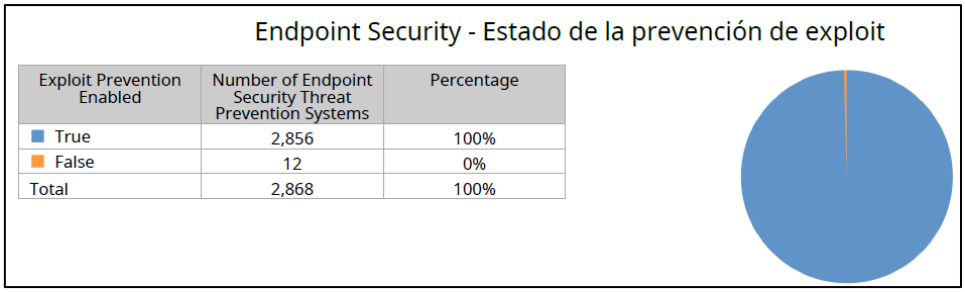
Estado de la Protección de Acceso.



Access Protection Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,867	100%
False	1	0%
Total	2,868	100%

Estos eventos corresponden al módulo de **Threat Prevention** en el momento de ejecución de aplicaciones que no están permitidas.

Estado de la Prevención de Exploit.



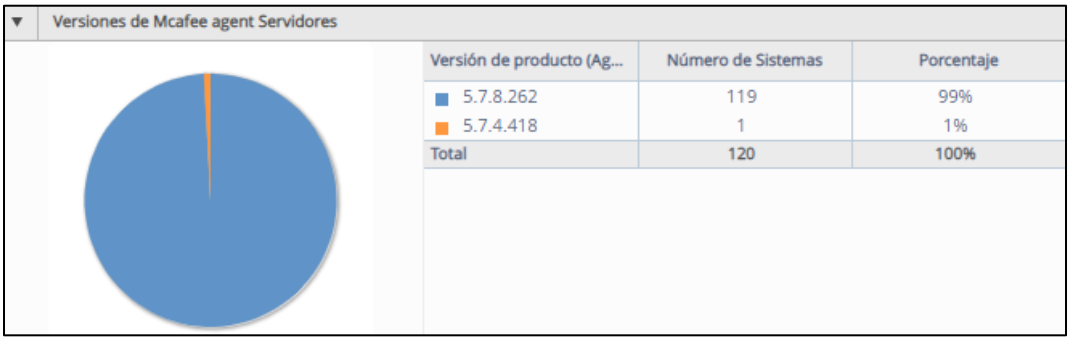
Exploit Prevention Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,856	100%
False	12	0%
Total	2,868	100%

Este gráfico nos muestra el estado de explotación y minería de datos los cuales están en el módulo de **Exploit Prevention**.

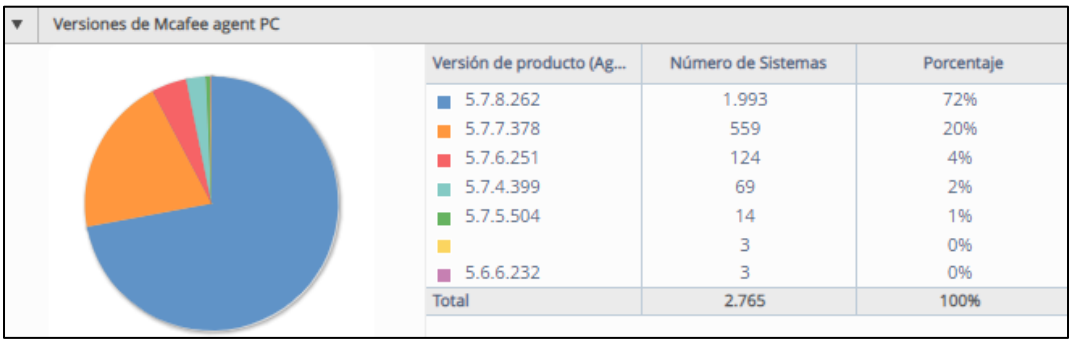
VERSIONES DE PRODUCTOS TRELLIX DEL MES DE NOVIEMBRE

A continuación, serán mostrados los datos relativos a las versiones de producto de los principales componentes Trellix utilizados en la AERONÁUTICA CIVIL, con el fin de dar a conocer las diferentes versiones que se encuentran instaladas en la red.

Trellix Agent.



Versión de producto (Ag...	Número de Sistemas	Porcentaje
5.7.8.262	119	99%
5.7.4.418	1	1%
Total	120	100%

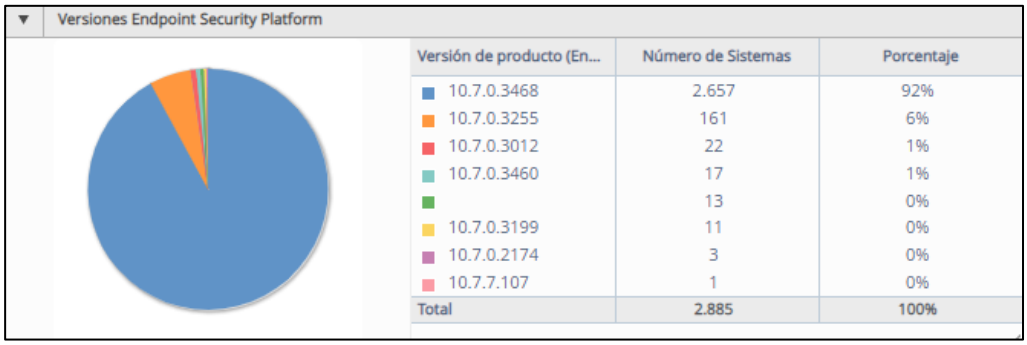


Versión de producto (Ag...	Número de Sistemas	Porcentaje
5.7.8.262	1.993	72%
5.7.7.378	559	20%
5.7.6.251	124	4%
5.7.4.399	69	2%
5.7.5.504	14	1%
	3	0%
5.6.6.232	3	0%
Total	2.765	100%

A partir del mes de diciembre, se generó una nueva versión del agente **5.7.8.262**, actualmente se sigue en una tarea constante para actualizar en su totalidad y a la última versión los equipos de la AC. Es de aclarar que los nuevos equipos que sean instalados a través de la **URL** van a subir con la versión **5.7.8.262.** Esta versión incluye una mejora y resuelve varios problemas, incluidos los de seguridad. Por otro lado, los productos se han estado revisando constantemente en busca de cualquier novedad en el cambio de su versionamiento.

Endpoint Security Platform

ENS Platform es la interfaz gráfica donde van integrados todos los módulos de ENS.

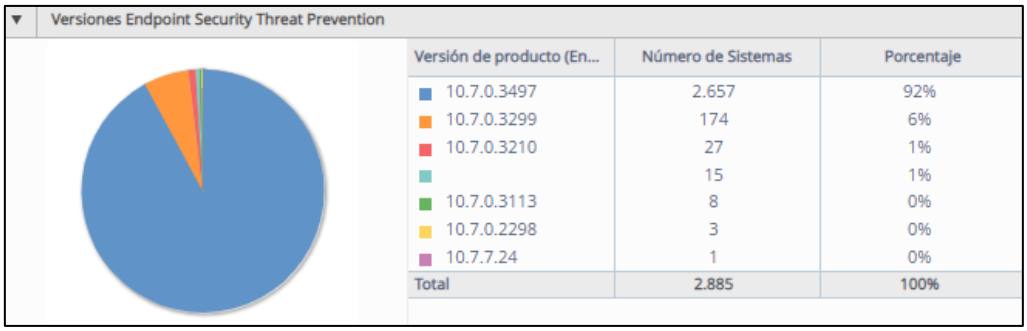


Versiones Endpoint Security Platform

Versión de producto (En...	Número de Sistemas	Porcentaje
10.7.0.3468	2.657	92%
10.7.0.3255	161	6%
10.7.0.3012	22	1%
10.7.0.3460	17	1%
	13	0%
10.7.0.3199	11	0%
10.7.0.2174	3	0%
10.7.7.107	1	0%
Total	2.885	100%

Endpoint Security Threat Prevention

ENS Threat Prevention es el módulo protección y el antivirus del sistema.

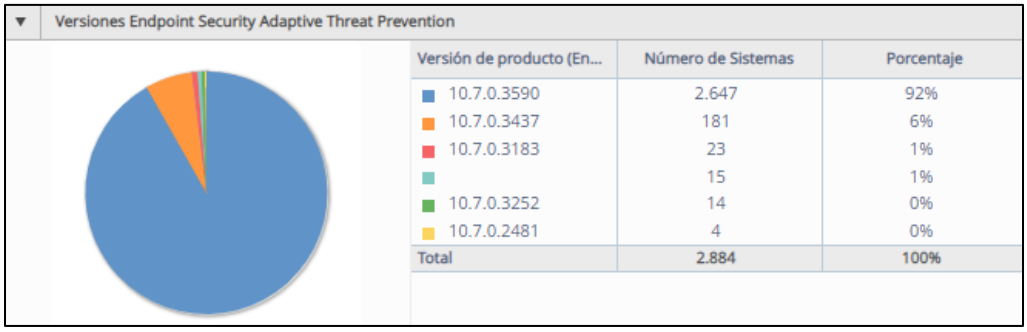


Versiones Endpoint Security Threat Prevention

Versión de producto (En...	Número de Sistemas	Porcentaje
10.7.0.3497	2.657	92%
10.7.0.3299	174	6%
10.7.0.3210	27	1%
	15	1%
10.7.0.3113	8	0%
10.7.0.2298	3	0%
10.7.7.24	1	0%
Total	2.885	100%

Endpoint Security Adaptive Threat Prevention

ENS ATP es el módulo de protección en tiempo real y detección temprana.

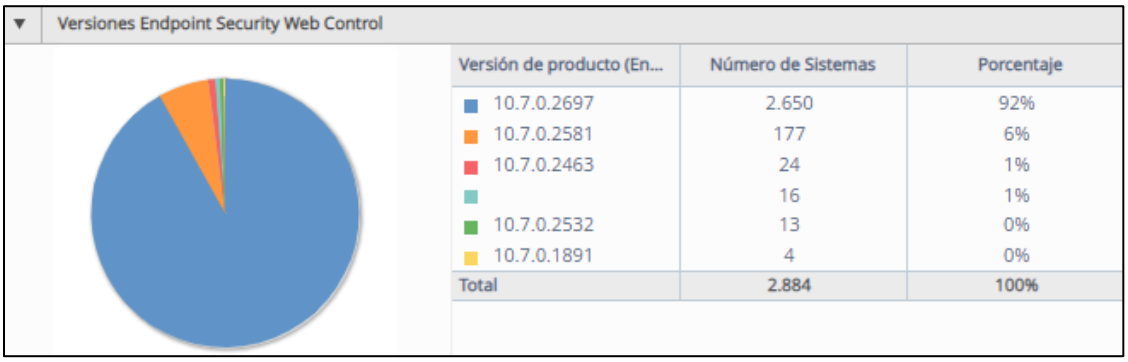


Versiones Endpoint Security Adaptive Threat Prevention

Versión de producto (En...	Número de Sistemas	Porcentaje
10.7.0.3590	2.647	92%
10.7.0.3437	181	6%
10.7.0.3183	23	1%
	15	1%
10.7.0.3252	14	0%
10.7.0.2481	4	0%
Total	2.884	100%

Endpoint Security Web Control

Es el módulo de control en la navegación acá podemos ver los equipos que navegan en páginas que pueden ser potencialmente peligrosas para el sistema.



Se evidencia que aproximadamente el **98%** de los equipos ya están actualizados con las últimas dos versiones de Endpoint Security, se encuentra en ejecución un despliegue automático para que siempre ejecute el **ENS** en los equipos que no posean estos productos. En algunos equipos no fue posible realizar la actualización, por lo cual se realizó un correo para la apertura de casos a la **L3000** para que realicen la correcta instalación en sitio, por esta razón se evidencian sistemas sin versionamiento de los productos, debido a la corrupción que presentan actualmente en el agente y los equipos que aún están en proceso de migración desde la consola local.

Las versiones de productos que se están instalando actualmente en los nuevos equipos son:

Productos	Versión
Agente McAfee	*5.7.8.262*
Plataforma de Endpoint Security	*10.7.0.3468*
Módulo Prevención de amenazas	*10.7.0.3497*
Módulo Protección adaptable frente amenazas	*10.7.0.3590*
Módulo Control Web	*10.7.0.2697*

INFORMACIÓN DE ATAQUES E INFECCIONES

A continuación, se presenta una relación de los eventos de amenazas, detecciones y acciones realizadas por los productos **McAfee ENS Threat Prevention**, así como de los apoyos en detección realizados por el producto **ENS Adaptive Threat Protection**.

ENDPOINT SECURITY

Top 10 de equipos con más detecciones durante el mes de noviembre.

En la tabla se muestra el top 10 de las máquinas que tuvieron más detecciones de amenazas durante el mes de octubre, en total se detectaron **17.181** amenazas.

ENS: Los 10 equipos con más detecciones mes Noviembre - 2022

Nombre de sistema	Número de Eventos de amenaza
BO0991CEA	7.407
RG0963STE	6.347
BO7463ATS	948
BO004SAR	771
BOG130	593
PT9440INF	340
PP6170ADM	308
BO0162CEA	211
BOG120	171
LT0773ADM	85
Total	17.181

Se evidencia que las dos principales amenazas detectadas son de tipo **Protección de acceso**, estas se presentan debido a que los equipos **BO0991CEA** y **RG0963STE** tienen el intento de creación de un archivo **Autorun.inf** en proceso, esta acción se ejecuta cada cinco minutos, de allí el resultado de una suma considerable de eventos. Del equipo **RG0963STE** el requerimiento fue solucionado por el técnico en sitio. La ruta en la que se presenta este tipo de novedad en ambos equipos apunta al aplicativo **OneDrive**. Persisten los eventos de amenaza en el equipo **BO0991CEA.** Por otro lado, el equipo **BO7463ATS** presenta eventos de amenaza tipo **Protección de acceso,** se realiza un caso a L3000 **RQ160871** para la eliminación del aplicativo **USB.Ink** el cual se encuentra alojado desde un dispositivo Pendrive con partición **F:**.

ENS: Detecciones de malware por Grupo Aerocivil.

Nombre de grupo	Número de Eventos de amenaza
CEA	455
Portatiles	429
Piso-1 y Sotano	385
CNA	375
Piso-4	271
Leticia	259
Cali	233
Medellin	230
CGAC	190
Piso-2	188
Piso-3	117
Rionegro	97
Barranquilla	93
Cartagena	71
Villavicencio	58
Pereira	48
Cucuta	45
Piso-5	43
Santa Marta	41
Tame	31
Bucaramanga	28
Arauca	26
Guaymaral	24
Pto Asis	21
ARANDA	20
Popayan	19
Yopal	18
Ibague	17
BOGOTA	16
Barrancabermeja	13
Monteria	11
Armenia	10
San Andres	9
Pasto	8
Quibdo	7
ALMACEN	6
Maniquita	6
Neiva	6
Otros Aeropuertos	5
DE ARCHIVOS	4
Girardot	4
Valledupar	4
Florencia	3
Buenaventura	2
Corozal	2
DORADO	2
Ipiales	2
Mitu	2
SIA-AIM	2
Carepa	1
Equipos Sta. Sofia	1
Guapi	1
Linea 3000	1
San Jose del Guaviare	1
Tolu	1
Total	3.962

Top 10 de las principales amenazas detectadas durante el mes de noviembre.

En la siguiente tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de noviembre, donde se evidencia que la mayoría de las amenazas presentadas (***Autorun.inf y Core Protection - Sanitize McAfee processes***) se dieron principalmente por el intento ejecución del aplicativo **Autorun.inf** en los equipos **BO0991CEA** y **RG0963STE** y la ejecución del aplicativo **Trusteer Rapport** y **Bonjour** en los equipos **BO004SAR** y **PT9440INF**.

ENS: Las 10 principales amenazas detectadas mes de Noviembre - 2022

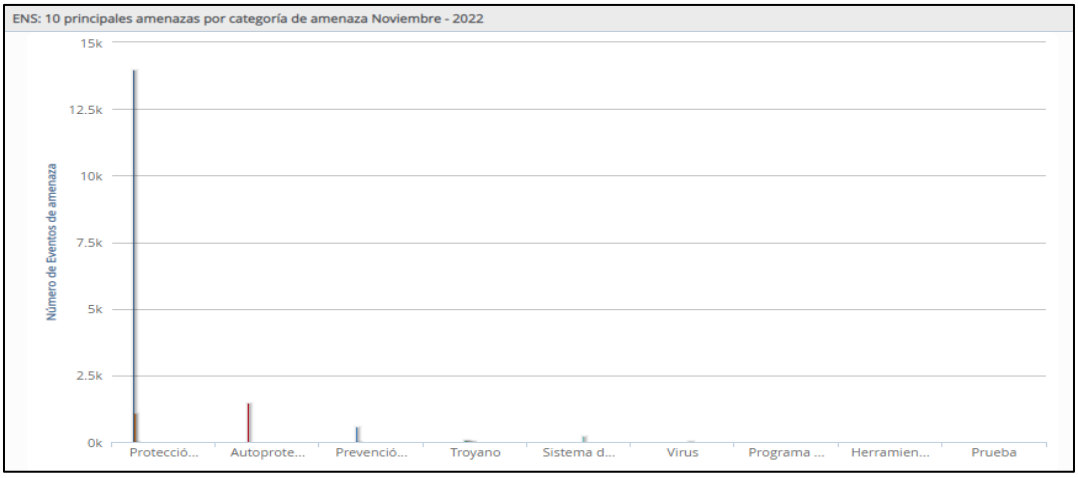
Nombre de amenaza	Número de Eventos de amenaza
autorun.inf	14.002
Core Protection - Sanitize McAfee processes	1.491
Prueba malware	1.093
Suspicious Double File Extension Execution	594
ExP:NIPS Violation	234
ATP/Suspect!cb377e2ba78e	73
ATP/Suspect!f1efb0fddc15	67
ATP/Suspect!50ef7c645fd5	51
ATP/Suspect!8d7c2fd35436	40
Malware Behavior: Windows EFS abuse	33
Total	17.678

Por otro lado, la tercera amenaza para este mes se relaciona con **Prueba Malware**, para esta ocasión con la ejecución del aplicativo **USB.Ink** en el equipo **BO7463ATS** desde un dispositivo externo **Pendrive**. El equipo fue notificado a **L3000** para la eliminación del archivo. Se gestionó una reunión con el usuario final y la agente de soporte en sitio Leidy Quiñones para entrar a detallar esta situación.

ENS: 10 principales amenazas por categoría de amenaza noviembre 2022.

Amenazas por categoría

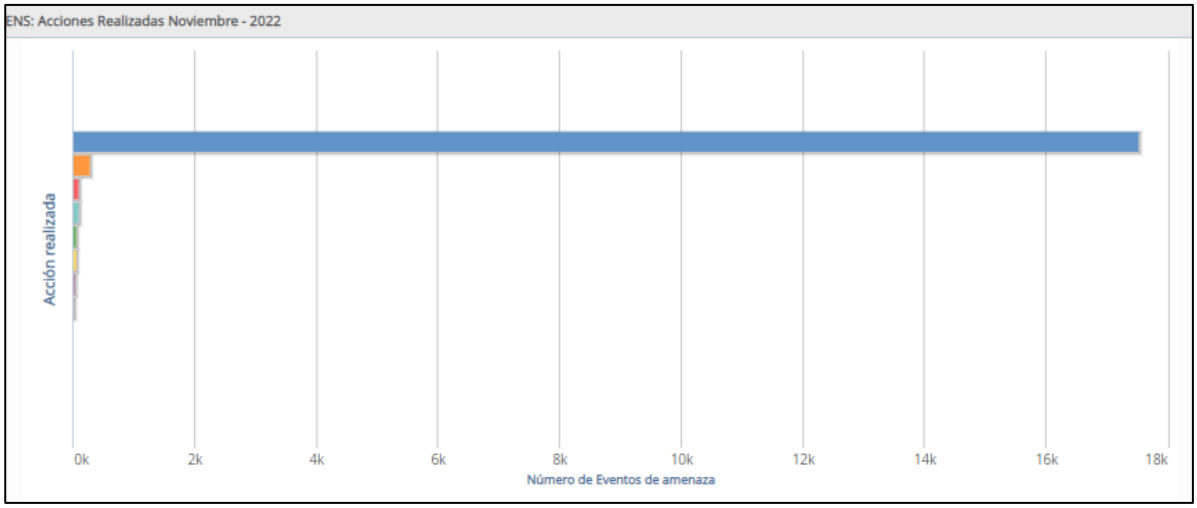
En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de noviembre, donde se puede observar que la categoría **Protección de acceso** representa un **85 %** de las amenazas detectadas en la organización. Mientras que la categoría **Autoprotección** representa un **9 %** de las amenazas detectadas en el mes. Las dos categorías principales para este mes representan el **94 %** del total de amenazas detectadas en la entidad.



Tipo de amenaza->Nombre de amenaza	Número de Eventos de amenaza
Protección de acceso	**15.129**
autorun.inf	14.002
Prueba malware	1.093
Rule 10	23
Prevent Office Malware	4
Ejecucion Exe	3
Rule 9	3
Rule 11	1
Autoprotección	**1.499**
Core Protection - Sanitize McAfee processes	1.491
Core Protection - Protect core McAfee files and folders	7
Autoprotección: Protección de los procesos de McAfee	1
Prevención de exploits	**630**
Suspicious Double File Extension Execution	594
Malware Behavior: Windows EFS abuse	33
Sticky Keys File Replacement Backdoor	3
Troyano	**330**
ATP/Suspecticb377e2ba78e	73
ATP/Suspectif1efb0fddc15	67
ATP/Suspecti50ef7c645fd5	51
ATP/Suspecti8d7c2fd35436	40
GenericRXTV-DWI9066DFF68C1D	25
ATP/Suspectid05defe2c8ef	22
Generic trojan.f	14
ATP/Suspectid4ac232d5077	13
ATP/Suspectidd399ae46303	13
ATP/Suspecti0da6c3774ef5	12
Sistema de prevención de intrusiones en la red	**234**
ExP:NIPS Violation	234
Virus	**76**
VBS/Autorun.worm.aajk	30
W32/Autorun.worm.aajv	21
W32/Autorun-FSVI4E964814FB35	17
Autorun.gallnkl74FF01575081	7
W32/Chir.gen@MMiremanants	1
Programa potencialmente no deseado	**15**
PUP-XAO-AZ	4
Crack-KMS	2
PUP-XTV-FN	2
ArtemisIA590A3B8EB80	1
Generic HTool.l	1
Generic KeyGen	1
Generic PUP.gx	1
HackTool-AutoKMS.a	1
HTool-AutoKMS	1
HTool-Keygen.d	1
Herramienta de administración remota	**1**
RemAdm-RemoteAdmin.h	1
Prueba	**1**
EICAR test file	1
Total	17.915

Acciones realizadas

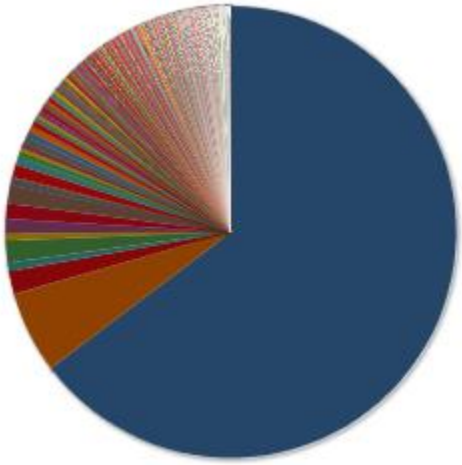
En el siguiente gráfico se muestra las acciones realizadas por el antivirus Trellix frente a las amenazas detectadas durante el mes de noviembre, el **0,8 %** de estas amenazas fueron eliminadas y el **96 %** corresponde a unidades que fueron bloqueadas durante el análisis.



Acción realizada	Número de Eventos de amenaza
Bloqueado	17.531
Protección adaptable frente a amenazas bloquearía	287
Eliminación pendiente	104
Eliminar	98
Protección adaptable frente a amenazas limpiaría	65
Permitir	64
Protección adaptable frente a amenazas contendría	36
Ninguna	18
Advertido	9
Bloquearía	3
Total	18.215

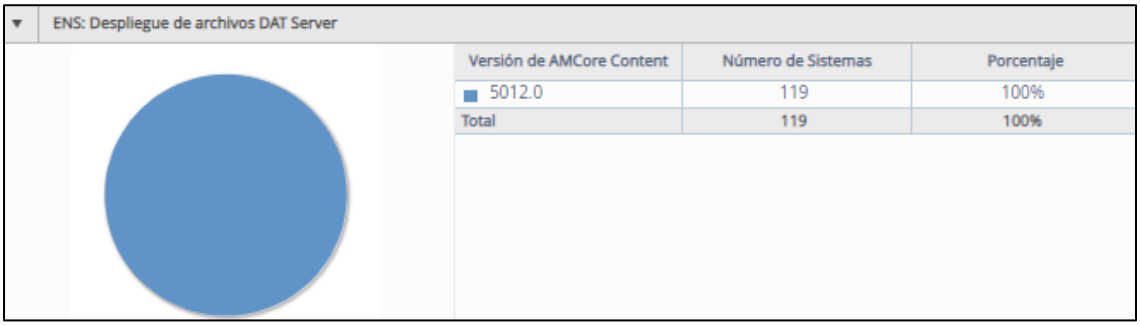
INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



Versión de AMCore Content	Número de Sistemas	Porcentaje
5012.0	1.777	65%
5011.0	161	6%
5010.0	45	2%
5009.0	17	1%
5008.0	43	2%
5007.0	15	1%
5006.0	27	1%
5005.0	30	1%
5004.0	37	1%
5003.0	7	0%
5002.0	5	0%
5001.0	4	0%
5000.0	24	1%
4999.0	16	1%
4998.0	11	0%
4660.0	1	0%
4290.0	1	0%
0.5	3	0%
	2	0%
Total	2.746	100%

En los últimos **15 días** se han estado actualizando **2219** máquinas con una versión de firma .DAT igual o superior a la **4998**. Teniendo presente que la actualización de estas se realiza de manera diaria.



En el gráfico se muestran las versiones del archivo DAT y la cantidad de equipos con **Endpoint Security** que tiene cada versión durante el mes de noviembre, igualmente se evidencia que para el caso de las Workstation el **81 %** de los equipos están actualizados con las **últimas 15 firmas**. Para el caso de los servers, al terminar la jornada estos se actualizan automáticamente a la última versión de la firma que esté disponible, para el caso actual con la versión **5012**.

Observaciones:

- En la **ePO On-premise** aún quedan equipos que no fue posible migrar a consola **ePO MVISION** debido a que no tenían comunicación reciente o tienen algún inconveniente con los productos, se ha estado enviando un listado semanal a los coordinadores de L3000 para que visualicen la cantidad de equipos que quedan en la consola antigua y realicen plan de acción para subirlos a la nube.

- Para este mes se tuvo un avance significativo en la reducción de los equipos que se encontraban sin comunicación entre **enero** y **septiembre** ya que se designó al soporte Leidy Quiñones para estar al tanto de los requerimientos, lo que generó una depuración satisfactoria de equipos semanalmente.

- Por correo electrónico se ha dado respuesta a los técnicos en sitio, indicando si los equipos han reportado correctamente en consola **ePO MVISION** o si por el contrario falta por actualizar alguno de los módulos de ENS, firma o agente. No obstante, se ha venido presentando una variante en las notificaciones para revisión de equipos por correo electrónico este mes, debido a que la mayoría de los técnicos que presentaban falencias al momento de realizar una instalación o actualización del agente y módulos ya cuentan con los conocimientos necesarios. Este mes se validaron 19 equipos.

- Se realiza a solicitud del ingeniero Jorge Torres y Coordinadores de L3000 la capacitación para los técnicos en sitio, con esta capacitación se explicó el funcionamiento y administración general de la consola **ePO MVISION** y, además, la manera correcta de instalar el agente y los módulos de ENS en un equipo haciendo uso de los recursos compartidos en **BOG7**. Dicha capacitación se realizó el día **18 de noviembre** y tuvo una duración no mayor a **2 horas**.

- Se realiza un caso a fabricante **4-23106901641** a solicitud del ingeniero Ruben Montealegre para validar directamente si desde consola **ePO MVISION** y de acuerdo con información compartida por la empresa **SafeBreach,** si el antivirus está cubierto para prevenir las vulnerabilidades detectadas de tipo **Puerta trasera – PowerShell**. Este caso se validó satisfactoriamente con fabricante donde se indica que los IoC han sido cubiertos por la DB global de Trellix para su detección en los equipos de la entidad.

- Se realiza la creación de un caso a fabricante **4-23396966681** a solicitud del ingeniero Ruben Montealegre para validar si los IoC publicados por la Agencia de Seguridad de Infraestructura y Ciberseguridad (**CISA**) y relacionados al **ransomware Hive**, se encuentran cubiertos por la DB global de **firmas .DAT** del antivirus. Los IoC compartidos en su mayoría son de tipo **URL y dominios** que como recomendación del fabricante se generó el bloqueo de estos desde el Firewall de la entidad.

- Se realiza la presentación del **informe de evaluación del antivirus Trellix** a las directivas de la entidad, en esta presentación se destacaron aspectos como: el tipo de licencia que tiene actualmente la entidad, la administración de los endpoints desde la consola **ePO MVISION**, el consumo de recursos que utiliza el antivirus con sus diferentes servicios, los tipos de tareas cliente y servidor configurados desde la consola, los registros de auditoria guardados desde consola y los procesos de actualización y alarma de amenazas que ofrece el antivirus. Dicha presentación tuvo lugar el día **30 de noviembre** con una duración no mayor a una **1 hora.**

- Se realiza la depuración de **80 equipos** de un total de **144 equipos** compartidos inicialmente por L3000. Estos equipos presentan duplicidad a nivel de serial y modelo. Los 80 registros eliminados se han validado previamente con una prueba ping para corroborar si estos aún respondían al dominio de la entidad.

Elaborado por:

Jorge Enrique Torres Beltran

Firmado digitalmente por Jorge Enrique Torres Beltran
Nombre de reconocimiento (DN): cn=Jorge Enrique Torres Beltran, o, ou, email=jorge.torres@Aerocivil.gov.co, c=<n
Fecha: 2022.12.14 11:58:38 -05'00'

Christian Ricardo Almanza Castañeda
Administrador consola ePO

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3