INFORME DE GESTION DE LA PLATAFORMA DE SEGURIDAD TRELLIX EPO

Preparado para:

AERONÁUTICA CIVIL
Unidad Administrativa Especial

BOGOTÁ
2023

CONTENIDO

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

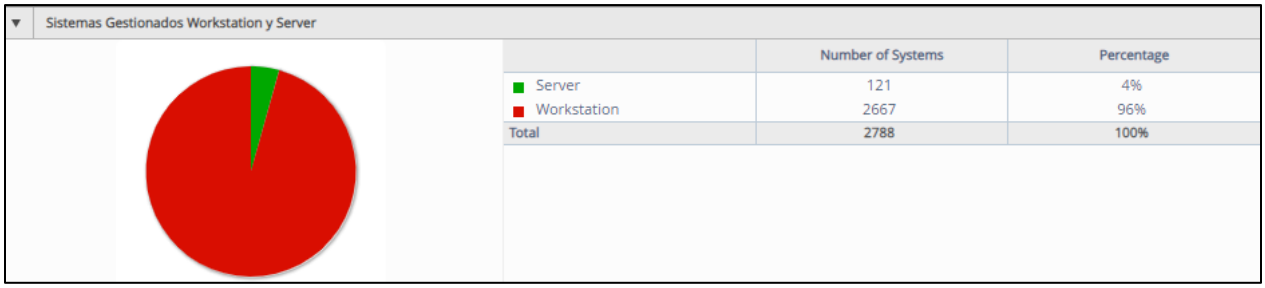
INTRODUCCIÓN

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 diciembre de 2022 y parte del mes de enero de 2023.

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 diciembre de 2022.

ITEM	Noviembre – 2022		Diciembre – 2022	
	No Sistemas Gestionados	Porcentaje	No Sistemas Gestionados	Porcentaje
Workstation	2761	96%	2667	96%
Servidores	120	4%	121	4%
Total	2881	100%	2788	100%



En el mes de diciembre y parte del mes de enero 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 47, 48 y 49. Es de aclarar, que aún siguen apareciendo nuevos equipos en consola local. A la fecha queda un reporte de **1 equipo** 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 los últimos informes de **L3000** que han notificado la eliminación de equipos al encontrase como **No operativos** o con **hostname duplicado**.

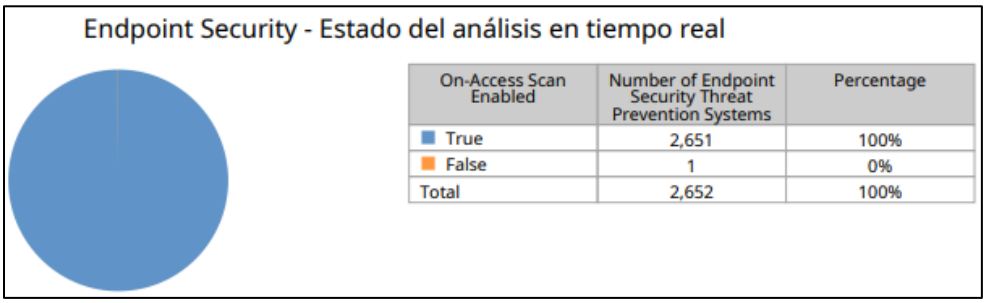
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS DICIEMBRE 2022.

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.

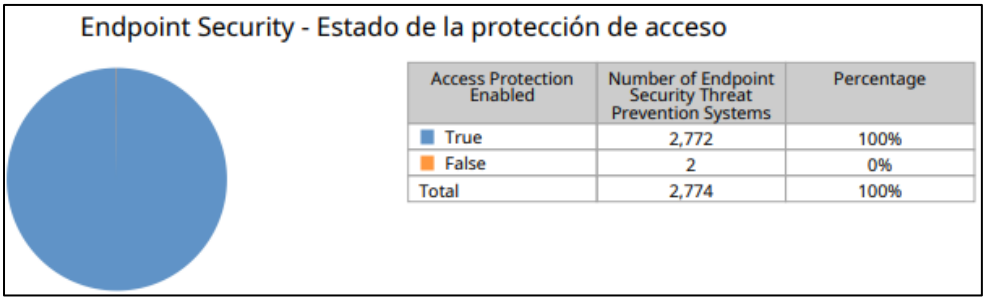
Este análisis es correspondiente al módulo de **Adaptive Threat Prevention** como detección temprana de amenazas que se puedan catalogar como amenaza en el sistema.



On-Access Scan Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,651	100%
False	1	0%
Total	2,652	100%

Estado de la Protección de Acceso.

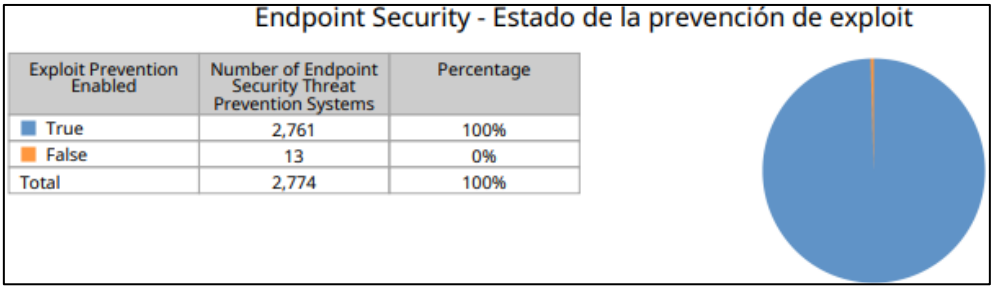
Estos eventos corresponden al módulo de **Threat Prevention** en el momento de ejecución de aplicaciones que no están permitidas.



Access Protection Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,772	100%
False	2	0%
Total	2,774	100%

Estado de la Prevención de Exploit.

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

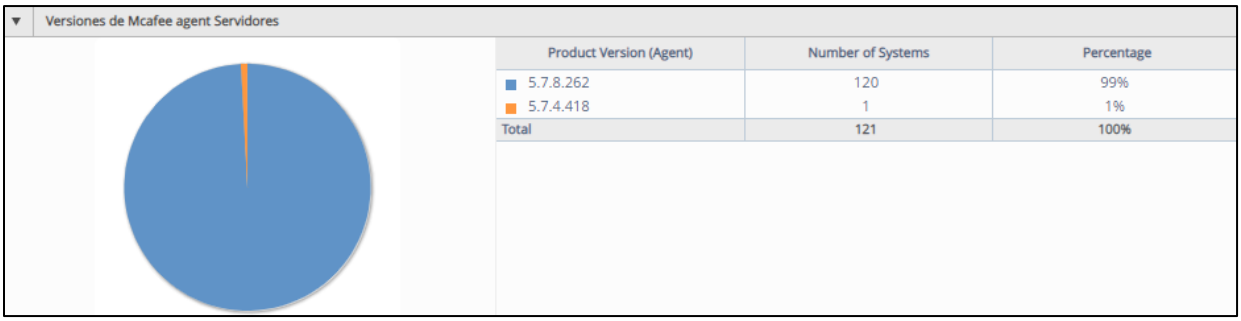


Exploit Prevention Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,761	100%
False	13	0%
Total	2,774	100%

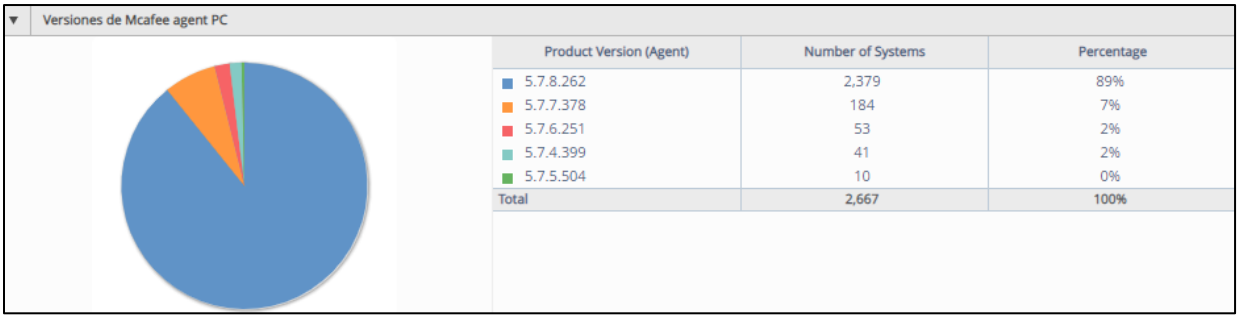
VERSIONES DE PRODUCTOS TRELLIX DEL MES DE DICIEMBRE

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.



Product Version (Agent)	Number of Systems	Percentage
5.7.8.262	120	99%
5.7.4.418	1	1%
Total	121	100%

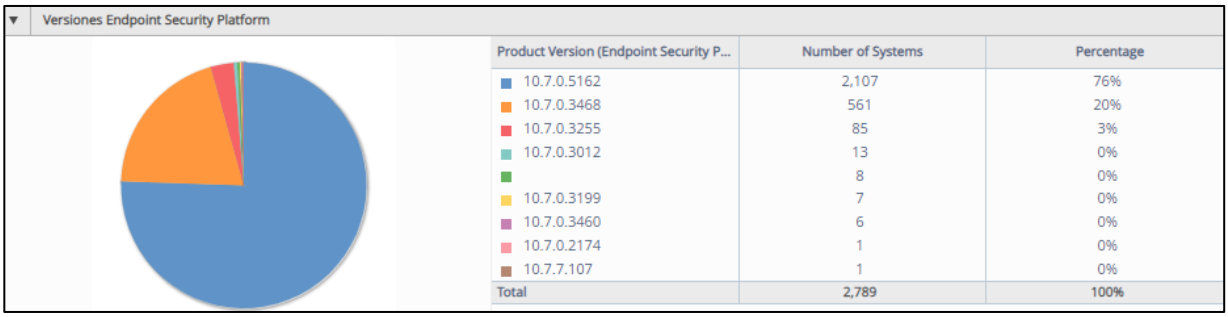


Product Version (Agent)	Number of Systems	Percentage
5.7.8.262	2,379	89%
5.7.7.378	184	7%
5.7.6.251	53	2%
5.7.4.399	41	2%
5.7.5.504	10	0%
Total	2,667	100%

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.

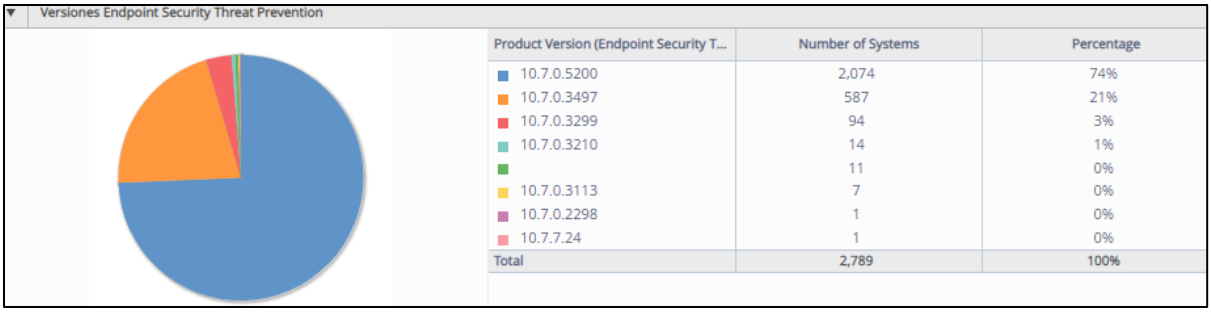


Versiones Endpoint Security Platform

Product Version (Endpoint Security P...	Number of Systems	Percentage
10.7.0.5162	2,107	76%
10.7.0.3468	561	20%
10.7.0.3255	85	3%
10.7.0.3012	13	0%
	8	0%
10.7.0.3199	7	0%
10.7.0.3460	6	0%
10.7.0.2174	1	0%
10.7.7.107	1	0%
Total	2,789	100%

Endpoint Security Threat Prevention

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

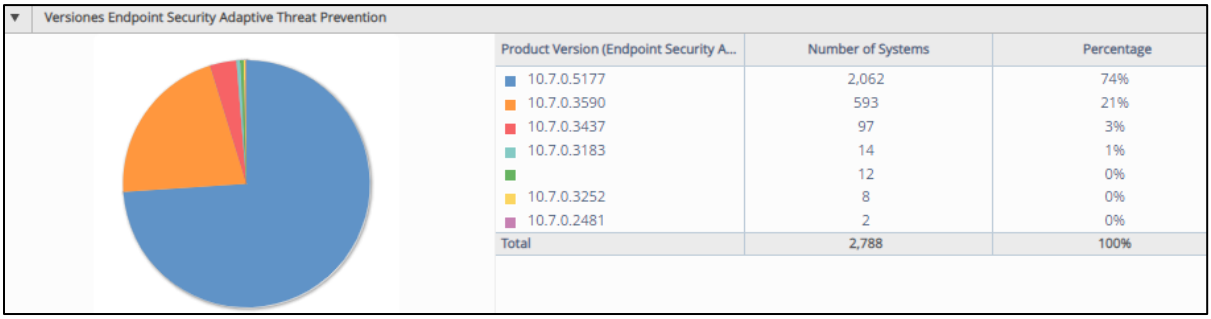


Versiones Endpoint Security Threat Prevention

Product Version (Endpoint Security T...	Number of Systems	Percentage
10.7.0.5200	2,074	74%
10.7.0.3497	587	21%
10.7.0.3299	94	3%
10.7.0.3210	14	1%
	11	0%
10.7.0.3113	7	0%
10.7.0.2298	1	0%
10.7.7.24	1	0%
Total	2,789	100%

Endpoint Security Adaptive Threat Prevention

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

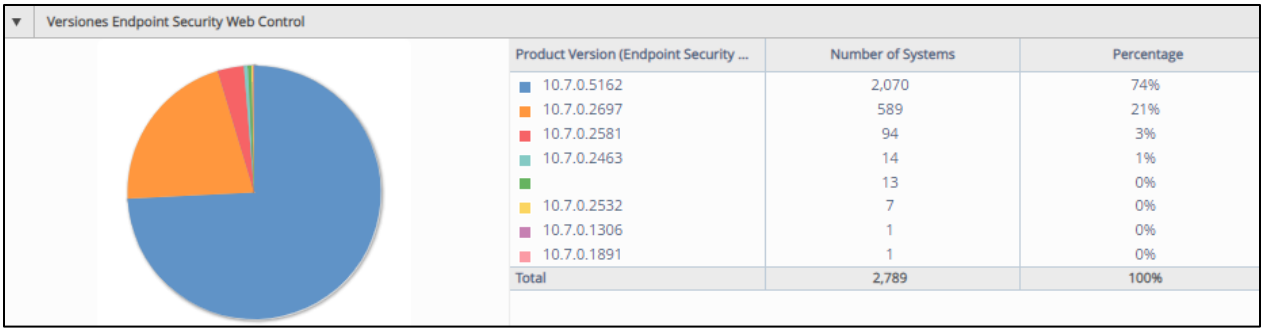


Versiones Endpoint Security Adaptive Threat Prevention

Product Version (Endpoint Security A...	Number of Systems	Percentage
10.7.0.5177	2,062	74%
10.7.0.3590	593	21%
10.7.0.3437	97	3%
10.7.0.3183	14	1%
	12	0%
10.7.0.3252	8	0%
10.7.0.2481	2	0%
Total	2,788	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 **95,2 %** 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	*10.7.0.5162*
Módulo Prevención de amenazas	*10.7.0.5200*
Módulo Protección adaptable frente amenazas	*10.7.0.5177*
Módulo Control Web	*10.7.0.5162*

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 diciembre.

En la tabla se muestra el top 10 de las máquinas que tuvieron más detecciones de amenazas durante el mes de diciembre, en total se detectaron **7.823** amenazas.

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

System Name	Number of Threat Events
BO0991CEA	3,927
BO7463ATS	1,305
BO004SAR	671
BOG120	628
BO8245PLA	397
BO0162CEA	195
BQ0162ADM	193
CL7105STE	174
VV6242AIS	172
BO7360ATS	161
Total	7,823

Se evidencia que las dos principales amenazas detectadas son de tipo **Protección de acceso**, estas se presentan debido a que el equipo **BO0991CEA** tenía el intento de creación de un archivo **Autorun.inf** en proceso, el cual se estaba ejecutando cada cinco minutos, de allí el resultado de una suma considerable de eventos. Para el caso del equipo **BO7463ATS** el requerimiento fue solucionado al aplicarse una exclusión desde la directiva Protección de acceso, desde la ruta **D:** y corroborarse que las funciones eran necesarias en las labores del usuario final. Por otro lado, el equipo **BO004SAR** presenta eventos de amenaza tipo **Autoprotección,** se realizó una solicitud a L3000 para la eliminación del aplicativo **Trusteer Rapport** la cual se llevó a buen término el día 28 de diciembre.

ENS: Detecciones de malware por Grupo Aerocivil.

Group Name	Number of Threat Events
Piso-4	887
CEA	495
CNA	454
Portatiles	452
Piso-1 y Sotano	381
Leticia	292
Cali	258
Piso-2	255
Medellin	235
CGAC	195
Piso-3	142
Pereira	121
Barranquilla	109
Cartagena	78
Villavicencio	58
Bucaramanga	56
Rionegro	50
Cucuta	48
Piso-5	46
Santa Marta	43
Arauca	41
Tame	34
Yopal	32
Guaymaral	29
ARANDA	26
Pto Asis	24
Ibague	23
Popayan	23
Armenia	17
San Andres	15
Barrancabermeja	14
BOGOTA	14
Quibdo	14
Pasto	12
Monteria	11
ALMACEN	8
DORADO	7
DE ARCHIVOS	6
Mariquita	6
Neiva	6
Girardot	5
Otros Aeropuertos	5
Florencia	4
Valledupar	4
Equipos Sta. Sofia	3
Ipiales	3
Buenaventura	2
Corozal	2
Mitu	2
Carepa	1
Guapi	1
San Jose del Guaviare	1
Tolu	1
Total	5,051

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

En la siguiente tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de diciembre, donde se evidencia que la mayoría de las amenazas presentadas (***Prueba Malware y Aturorun.inf***) se dieron principalmente por el intento ejecución del archivo **USB.lnk** desde la partición **D:** del equipo **BO7463ATS**. De igual forma, el intento de ejecución del archivo **Autorun.inf** desde el equipo **BO0162CEA** por medio del aplicativo OneDrive.

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

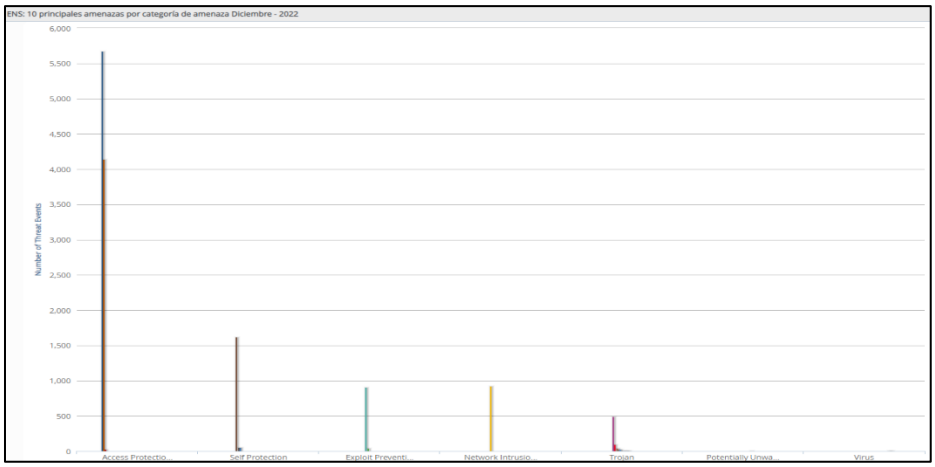
Threat Name	Number of Threat Events
Prueba malware	5,671
autorun.inf	4,140
Core Protection - Sanitize McAfee processes	1,622
ExP:NIPS Violation	924
Suspicious Double File Extension Execution	904
ATP/Suspect!f1efb0fddc15	489
ATP/Suspect!50ef7c645fd5	96
Core Protection - Protect core McAfee files and folders	57
Core Protection - Sanitize Trellix processes	52
ATP/Suspect!cb377e2ba78e	43
Total	13,998

Por otro lado, la tercera amenaza para este mes se relaciona con ***Core Protectión – Sanitize McAfee Processes***, para esta ocasión con la ejecución del aplicativo **Trusteer Rapport** en el equipo **BO004SAR.** El equipo fue notificado a **L3000** para la eliminación del archivo, el cual se desinstaló oportunamente.

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

Amenazas por categoría

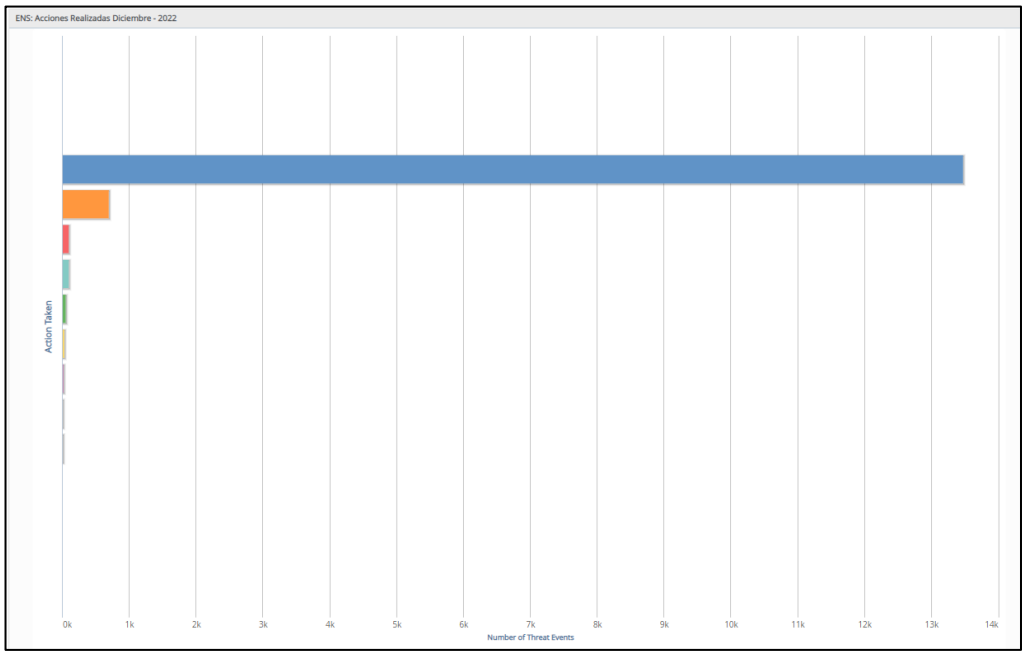
En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de diciembre, donde se puede observar que la categoría **Protección de acceso** representa un **69,5 %** de las amenazas detectadas en la organización. Mientras que la categoría **Autoprotección** representa un **12,5 %** de las amenazas detectadas en el mes. Las dos categorías principales para este mes representan el **82 %** del total de amenazas detectadas en la entidad.



Threat Type->Threat Name	Number of Threat Events
Access Protection	**9,853**
Prueba malware	5,671
autorun.inf	4,140
SkypeSetup.exe	28
CHARTER REQUEST 011608201782781929.zip	4
Prevent Office Malware	4
Rule 10	4
Rule 9	1
WinAcelerator.exe	1
Self Protection	**1,735**
Core Protection - Sanitize McAfee processes	1,622
Core Protection - Protect core McAfee files and folders	57
Core Protection - Sanitize Trellix processes	52
Autoprotección: Protección de los procesos de McAfee	3
Autoprotección: proteger los procesos de Trellix	1
Exploit Prevention	**945**
Suspicious Double File Extension Execution	904
Malware Behavior: Windows EFS abuse	41
Network Intrusion Prevention System	**924**
ExP:NIPS Violation	924
Trojan	**733**
ATP/Suspect!f1efb0fddc15	489
ATP/Suspect!50ef7c645fd5	96
ATP/Suspect!cb377e2ba78e	43
ATP/Suspect!d05defe2c8ef	27
ATP/Suspect!8d7c2fd35436	24
JTI/Suspect.393221	12
JTI/Suspect.393221!c817d9e0d995	12
JTI/Suspect.393221!6ca3343b3820	11
ATP/Suspect!4f4970c35459	10
ATP/Suspect!3bd85cf59f73	9
Potentially Unwanted Program	**23**
Crack-KMS	11
FilePatcher	3
Artemis!ACD1EBBE5662	2
Artemis!1FACB238F144	1
Artemis!3976BD5FCBB7	1
Artemis!54CF125653D0	1
Artemis!8F55A0DA8560	1
FusionCore	1
Herm-Wiper	1
HTool-KMS-IGO	1
Virus	**17**
W32/Rontokbro.a.gen@MM	6
W32/Autorun-FSV!4E964814FB35	5
W32/Gnamer	2
Artemis!14638217EF40	1
V2P6.z	1
W32/Conficker.worm.gen.a	1
W32/Sality.dr	1
Total	14,230

Acciones realizadas

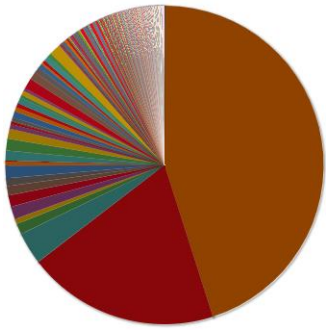
En el siguiente gráfico se muestra las acciones realizadas por el antivirus Trellix frente a las amenazas detectadas durante el mes de diciembre, el **0,5 %** de estas amenazas fueron eliminadas y el **92 %** corresponde a unidades que fueron bloqueadas durante el análisis.



Action Taken	Number of Threat Events
Blocked	13,478
Adaptive Threat Protection Would Block	698
Adaptive Threat Protection Would Clean	105
Allow	99
Delete	54
Delete pending	30
Warned	23
Adaptive Threat Protection Would Contain	14
Deny access	6
None	4
Total	14,511

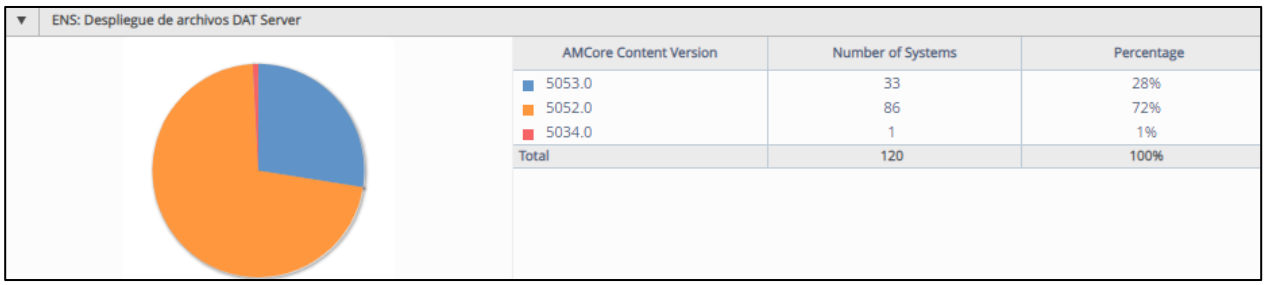
INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



AMCore Content Version	Number of Systems	Percentage
N/A	2	0%
5053.0	1,196	45%
5052.0	519	20%
5051.0	87	3%
5050.0	29	1%
5049.0	14	1%
5048.0	34	1%
5047.0	31	1%
5046.0	25	1%
5045.0	21	1%
5044.0	34	1%
5043.0	11	0%
5042.0	2	0%
5041.0	27	1%
5040.0	32	1%
5039.0	27	1%
4680.0	1	0%
4670.0	2	0%
4666.0	1	0%
4660.0	1	0%
0.5	4	0%
	3	0%
Total	2,658	100%

En los últimos **15 días** se han estado actualizando **2089** máquinas con una versión de firma .DAT igual o superior a la **5039**. Teniendo presente que la actualización se realiza de manera diaria. Cabe resaltar que se encuentran alrededor de **9 equipos** sin una versión de firma definida.



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 diciembre, igualmente se evidencia que para el caso de las Workstation el **78 %** 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 **5053**.

Observaciones:

- Actualmente ya no quedan equipos pendientes por migrar de manera forzada desde consola On-Premise. El último equipo listado pertenecía a la ciudad de Bucaramanga donde se esclareció que el equipo no pertenece a la red de la entidad, por ende, se solicito la desinstalación de la solución.

- Para el mes de diciembre se tuvo un avance significativo en la reducción de los equipos que se encontraban sin comunicación entre **enero** y **octubre** 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 26 equipos notificados en su mayoría por Leidy Quiñones, Mario Diaz y Emerson Barrera.

- Se realiza en los meses de diciembre y enero una depuración considerable de máquinas, ya que estas se encontraron en un estado no operativo o con hostname duplicado en consola. Lo anterior ha permitido una depuración de registros satisfactoria y una oportuna liberación de licencias de antivirus.

- Se presenta para el mes de diciembre, el informe final de especificaciones técnicas junto con el formato 8 de especificaciones técnicas de la entidad debidamente diligenciado. Lo anterior, fue solicitado por el supervisor de contrato para dar por terminada la etapa oficial del contrato y dar inicio al periodo de calidad ofrecido por el contratista.

- Se notifica por parte del administrador de directorio activo el ingreso del server **BOG148** al cual se le instala la solución de ENS y su agente. Este equipo comienza a estar en monitoreo desde el día 19 de diciembre.

- Se realiza un análisis detallado de vulnerabilidades en el equipo del ing. Jose Ignacio Restrepo ya que presentaba inconvenientes en el almacenamiento de información desde un

dispositivo Pendrive. Se esclarece que el dispositivo se compró fuera de un almacén de cadena, es por ello por lo que se procede a realizar un caso a fabricante **4-23462905841** donde se expone la situación y desde allí logran diagnosticar que se trata de un daño en la lectura y escritura del dispositivo.

- Se realiza la creación de un caso a fabricante **4-23519423521** a solicitud del ingeniero Ruben Montealegre para validar si el antivirus se encuentra o no cubierto con la nueva variante del **ransomware RansomExx**. Por parte de fabricante se realiza una validación y gestiona posteriormente una reunión donde se esclarece que efectivamente a nivel de firmware estamos cubiertos en sistemas operativos Windows y Linux.

Elaborado por:



Jorge Enrique Torres Beltran

Firmado digitalmente por Jorge Enrique Torres Beltran
Nombre de reconocimiento (DN): cn=Jorge Enrique Torres Beltran, o=Aerocivil, ou=Grupo Operacion Servicios Tecnologicos, email=jorge.torres@aerocivil.gov.co, c=CO
Fecha: 2023.02.06 15:49:16 -05'00'

Christian Ricardo Almanza Castañeda
Administrador consola ePO

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3