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 OCTUBRE 2022. 4
MCAFEE ENDPOINT SECURITY 5
VERSIONES DE PRODUCTOS MCAFEE DEL MES DE OCTUBRE 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 octubre. 9
Top 10 de las principales amenazas detectadas durante el mes de octubre. 11
ENS: 10 principales amenazas por categoría de amenaza octubre 2022. 11
Amenazas por categoría 11
Acciones realizadas 12
INFORMACION DE ACTUALIZACIONES 14
ENS: Top 10 de las actualizaciones DAT 14
Observaciones 14

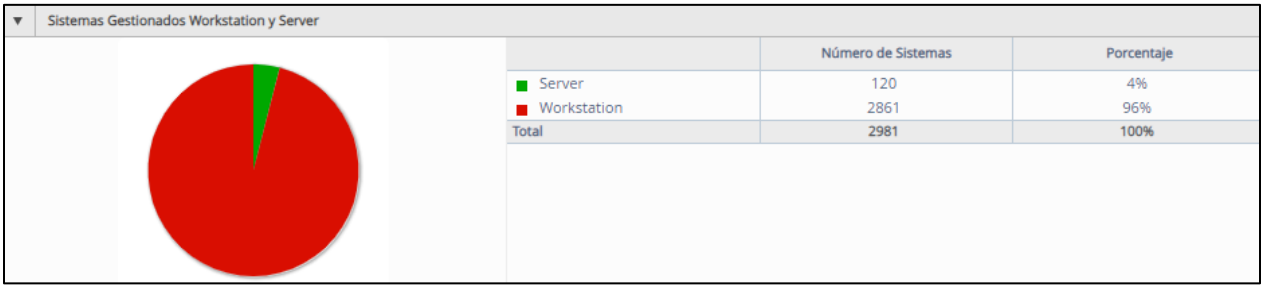
INTRODUCCIÓN

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 octubre 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	Septiembre - 2022		Octubre - 2022	
	No Sistemas Gestionados	Porcentaje	No Sistemas Gestionados	Porcentaje
Workstation	2814	96%	2853	96%
Servidores	120	4%	119	4%
Total	2934	100%	2972	100



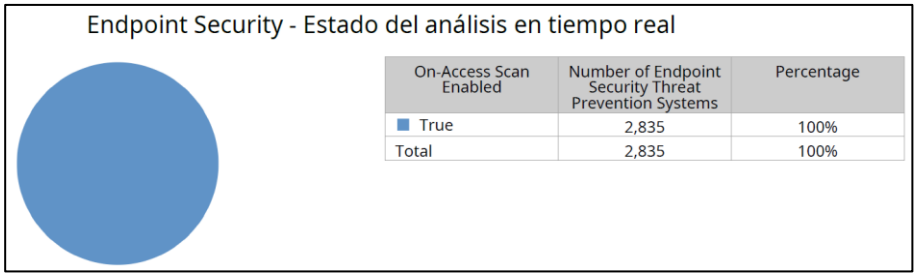
En el mes de octubre se continuó con migración de equipos a consola en la nube. Se realizo depuración con base en la revisión de equipos que presentaban una versión de firma desactualizada, más concretamente equipos con versión 48. Es de aclarar, que aún siguen apareciendo nuevos equipos en consola local. A la fecha queda un reporte de 10 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. El aumento de equipos gestionados en el mes de octubre ha sido de 38 frente al mes anterior.

ESTADO ACTUAL PROTECCIÓN ANTIVIRUS OCTUBRE 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

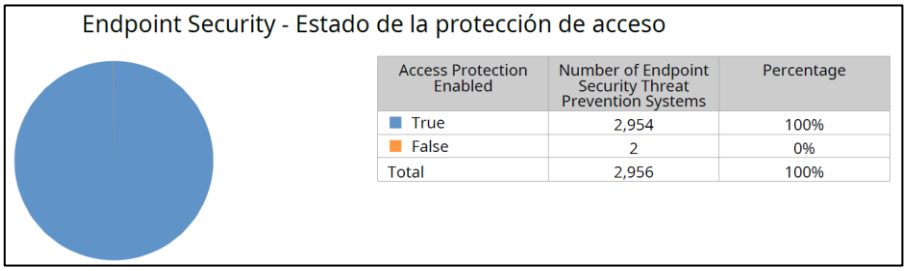
Estado del análisis en tiempo real.



On-Access Scan Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,835	100%
Total	2,835	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.

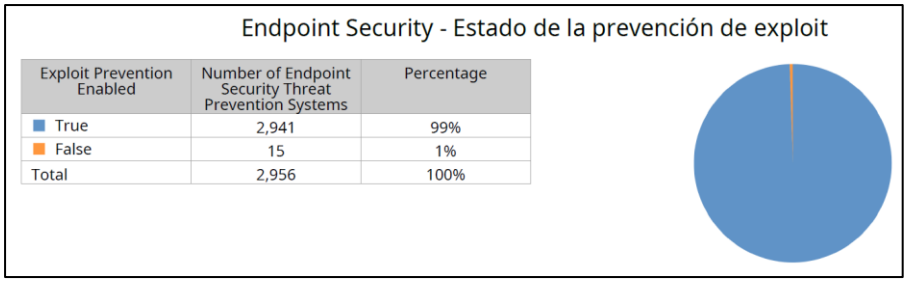
Estado de la Protección de Acceso.



Access Protection Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,954	100%
False	2	0%
Total	2,956	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.



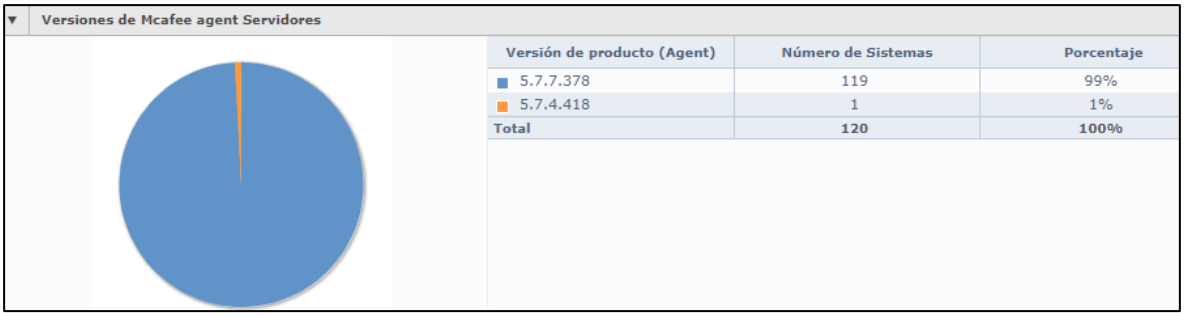
Exploit Prevention Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,941	99%
False	15	1%
Total	2,956	100%

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

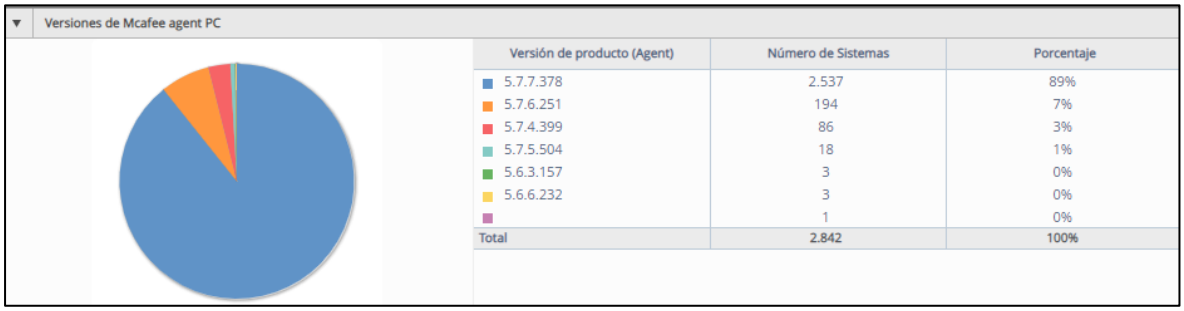
VERSIONES DE PRODUCTOS TRELLIX DEL MES DE OCTUBRE

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 (Agent)	Número de Sistemas	Porcentaje
5.7.7.378	119	99%
5.7.4.418	1	1%
Total	120	100%

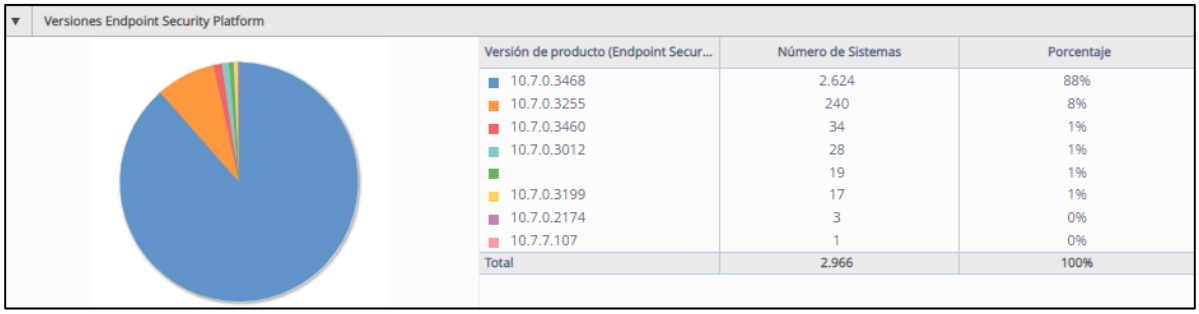


Versión de producto (Agent)	Número de Sistemas	Porcentaje
5.7.7.378	2.537	89%
5.7.6.251	194	7%
5.7.4.399	86	3%
5.7.5.504	18	1%
5.6.3.157	3	0%
5.6.6.232	3	0%
	1	0%
Total	2.842	100%

Desde el mes de Julio, se generó una nueva versión del agente **5.7.7.378**, 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 **5.7.7.378.** 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

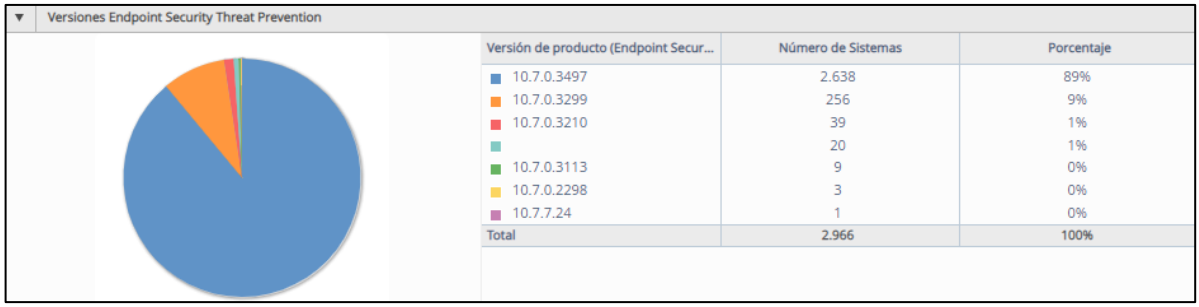
ENS Platform es la interfaz gráfica donde van integrados todos los módulos de ENS.



Versión de producto (Endpoint Secur...	Número de Sistemas	Porcentaje
10.7.0.3468	2.624	88%
10.7.0.3255	240	8%
10.7.0.3460	34	1%
10.7.0.3012	28	1%
	19	1%
10.7.0.3199	17	1%
10.7.0.2174	3	0%
10.7.7.107	1	0%
Total	2.966	100%

Endpoint Security Threat Prevention

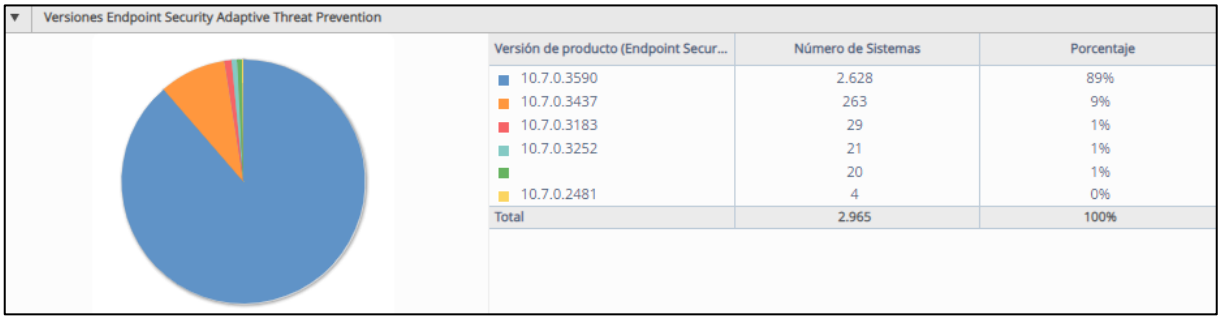
ENS Threat Prevention es el módulo protección y el antivirus del sistema.



Versión de producto (Endpoint Secur...	Número de Sistemas	Porcentaje
10.7.0.3497	2.638	89%
10.7.0.3299	256	9%
10.7.0.3210	39	1%
	20	1%
10.7.0.3113	9	0%
10.7.0.2298	3	0%
10.7.7.24	1	0%
Total	2.966	100%

Endpoint Security Adaptive Threat Prevention

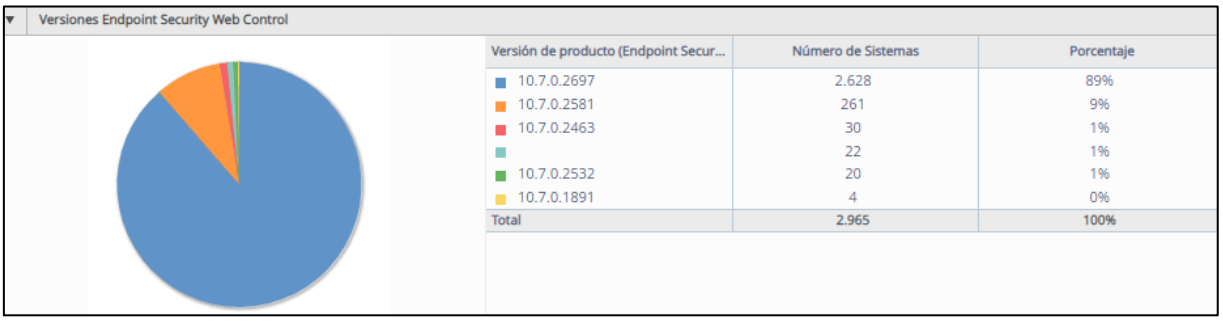
ENS ATP es el módulo de protección en tiempo real y detección temprana.



Versión de producto (Endpoint Secur...	Número de Sistemas	Porcentaje
10.7.0.3590	2.628	89%
10.7.0.3437	263	9%
10.7.0.3183	29	1%
10.7.0.3252	21	1%
	20	1%
10.7.0.2481	4	0%
Total	2.965	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.



Versión de producto (Endpoint Secur...	Número de Sistemas	Porcentaje
10.7.0.2697	2.628	89%
10.7.0.2581	261	9%
10.7.0.2463	30	1%
	22	1%
10.7.0.2532	20	1%
10.7.0.1891	4	0%
Total	2.965	100%

Se evidencia que aproximadamente el **97,5%** 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 realizaron una serie de correos para la apertura de casos a la **linea3000** 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	*5.7.7.378*
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 octubre.

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 **15.896** amenazas.

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

Nombre de sistema	Número de Eventos de amenaza
BO0991CEA	8.325
RG0963STE	2.823
BO7463ATS	1.041
BO004SAR	938
BOG120	791
BOG130	778
PP6170ADM	441
BOG182	262
LT0771SEI	260
BO0162CEA	237
Total	15.896

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. La ruta en la que se presenta este tipo de novedad en ambos equipos apunta al aplicativo **OneDrive**. 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** pero este no fue eliminado para la respectiva solución.

ENS: Detecciones de malware por Grupo Aerocivil.

Nombre de grupo	Número de Eventos de amenaza
Portatiles	422
Piso-1 y Sotano	369
CEA	364
CNA	284
Leticia	258
Piso-4	234
Cali	216
Medellin	206
Piso-2	191
CGAC	171
Piso-3	122
Rionegro	96
Barranquilla	90
Villavicencio	57
Cartagena	43
Pereira	41
Piso-5	38
Santa Marta	37
Cucuta	34
Tame	27
ARANDA	20
Bucaramanga	18
Popayan	18
Pto Asis	18
Yopal	18
Ibague	17
Guaymaral	16
Barrancabermeja	10
Arauca	9
San Andres	9
Armenia	8
Monteria	8
Quibdo	7
ALMACEN	6
BOGOTA	6
Pasto	6
Neiva	5
DE ARCHIVOS	4
Girardot	4
Florencia	3
Mariquita	3
Valledupar	3
Buenaventura	2
Corozal	2
DORADO	2
Mitu	2
Otros Aeropuertos	2
Carepa	1
Equipos Sta. Sofia	1
Guapi	1
Ipiales	1
Linea 3000	1
San Jose del Guaviare	1
Tolu	1
Total	3.533

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

En la siguiente tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de octubre, donde se evidencia que la mayoría de las amenazas presentadas (***Autorun.inf y ExP:NIPS Violation***) se dieron principalmente por el intento ejecución del aplicativo **Autorun.inf** en los equipos **BO0991CEA** y **RG0963STE** y el bloqueo recurrente de varias direcciones IP de origen malicioso que intentaron hacer comunicación con el DNS externo secundario configurado en el server **BOG120**. De igual forma, el número elevado de eventos se debe a unas pruebas de intrusión llevadas a cabo en varios equipos de la entidad desde la dirección IP **172.16.51.164**.

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

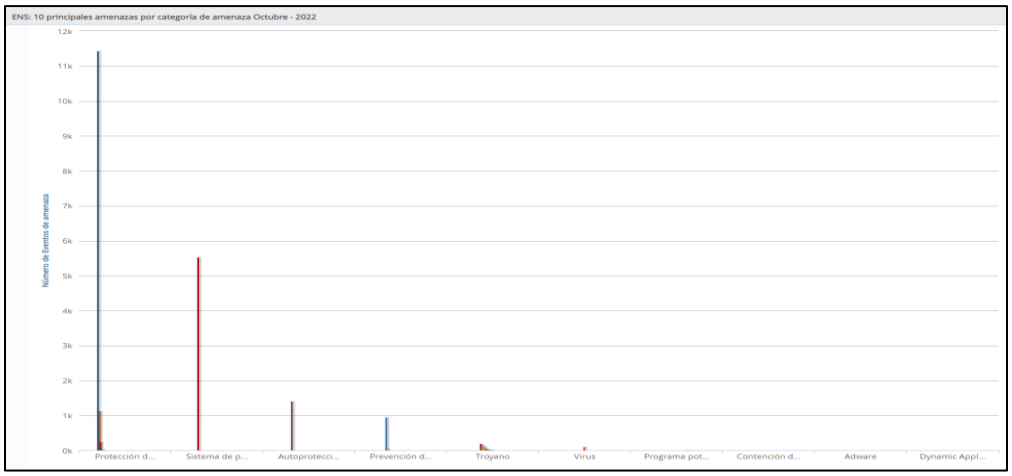
Nombre de amenaza	Número de Eventos de amenaza
autorun.inf	11.429
ExP:NIPS Violation	5.540
Core Protection - Sanitize McAfee processes	1.410
Prueba malware	1.123
Suspicious Double File Extension Execution	950
Block Cifrado	251
ATP/Suspect!f1efb0fddc15	189
ATP/Suspect!50ef7c645fd5	165
W32/Autorun-FSV!4E964814FB35	113
ATP/Suspect!8d7c2fd35436	105
Total	21.275

Por otro lado, la tercera amenaza para este mes se relaciona con **Core Protection - Sanitize McAfee processes**, para esta ocasión con la ejecución del aplicativo **Bonjour** y ***Trusteer Rapport***. Los equipos en los que se generaron mas eventos han sido **PP6170ADM** y **BO004SAR.** Ambos equipos de igual forma fueron notificados a **L3000** para la eliminación de los aplicativos.

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

Amenazas por categoría

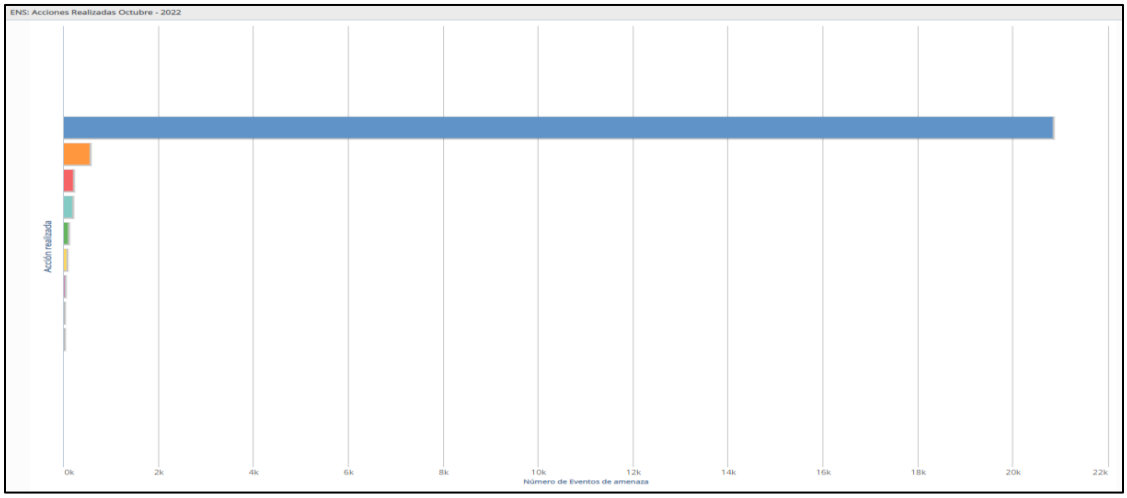
En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de octubre, donde se puede observar que la categoría **Protección de acceso** representa un **59.2 %** de las amenazas detectadas en la organización. Mientras que la categoría **Sistema de prevención de intrusiones en la red** representa un **25.5 %** de las amenazas detectadas en el mes. Las dos categorías principales para este mes representan el **84.7 %** del total de amenazas detectadas en la entidad.



Tipo de amenaza->Nombre de amenaza	Número de Eventos de amenaza
Protección de acceso	**12.848**
autorun.inf	11.429
Prueba malware	1.123
Block Cifrado	251
Rule 10	36
SkypeSetup.exe	5
Prevent Office Malware	3
Rule 9	1
Sistema de prevención de intrusiones en la red	**5.540**
ExP:NIPS Violation	5.540
Autoprotección	**1.416**
Core Protection - Sanitize McAfee processes	1.410
Core Protection - Protect core McAfee files and folders	6
Prevención de exploits	**1.006**
Suspicious Double File Extension Execution	950
Malware Behavior: Windows EFS abuse	56
Troyano	**726**
ATP/Suspect!f1efb0fddc15	189
ATP/Suspect!50ef7c645fd5	165
ATP/Suspect!8d7c2fd35436	105
Artemis!040CD888E971	104
ATP/Suspect!d05defe2c8ef	53
JS/Autorun.a!lnk	44
ATP/Suspect!eee8b2573f71	20
LNK/Trojan-FQBL!6D73DF36EC18	18
ATP/Suspect!cb377e2ba78e	14
GenericRXNJ-VD!E2840606372A	14
Virus	**122**
W32/Autorun-FSV!4E964814FB35	113
W32/Rontokbro.a.gen@MM	2
Artemis!14638217EF40	1
Artemis!91599413DA44	1
VBS/Autorun.worm.aajk	1
W32/Autorun.worm.dp	1
W32/Gamarue.d!lnk	1
W32/Rimecud.gen.bv	1
W32/Swisyn.ag	1
Programa potencialmente no deseado	**28**
Crack-KMS	9
Unknown	6
HTool-AutoKMS	3
Tool-RenewPass	3
HTool-Keygen.c	2
Artemis!311D64E4892F	1
Artemis!88E22021CB8B	1
Artemis!8FB45F99C486	1
Artemis!B68BB641AC93	1
Artemis!DD588A065B7D	1
Contención de aplicación dinámica	**3**
DAC:Contained	1
DAC:Released	1
T1543.003 - Modifying the Services registry location	1
Adware	**1**
Adware-OpenCandy	1
Dynamic Application Containment	**1**
ATP/Suspect!b3728ad271b3	1
Total	21.691

Acciones realizadas

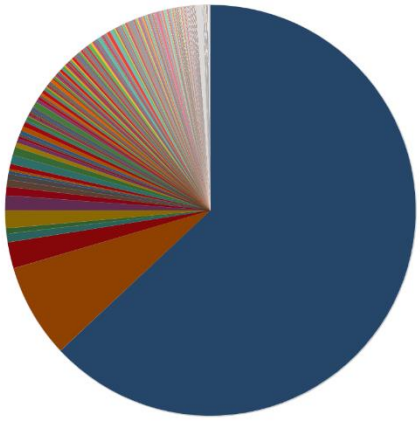
En el siguiente gráfico se muestra las acciones realizadas por el antivirus McAfee frente a las amenazas detectadas durante el mes de octubre, el **0.85 %** de estas amenazas fueron eliminadas y el **94.4 %** corresponde a unidades que serían bloqueadas durante el análisis.



Acción realizada	Número de Eventos de amenaza
Bloqueado	20.856
Protección adaptable frente a amenazas bloquearía	567
Eliminación pendiente	216
Eliminar	188
Permitir	112
Protección adaptable frente a amenazas limpiaría	64
Ninguna	32
Protección adaptable frente a amenazas contendría	25
Advertido	23
Continuar con el análisis	5
Total	22.088

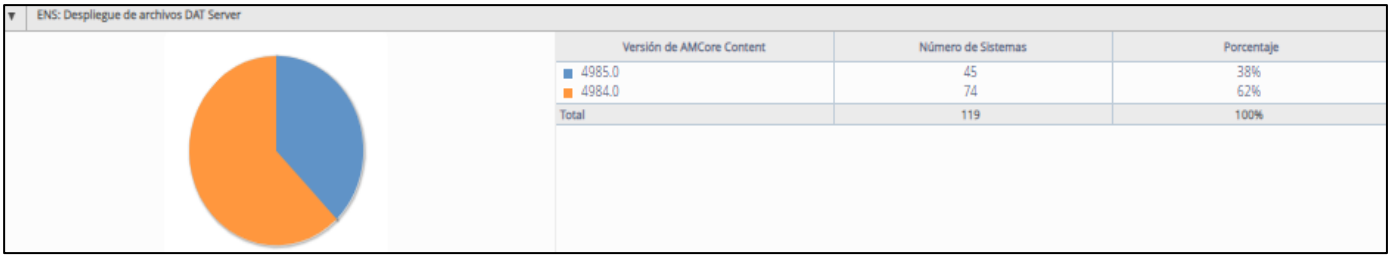
INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



Versión de AMCore Content	Número de Sistemas	Porcentaje
4985.0	1.770	63%
4984.0	208	7%
4983.0	58	2%
4982.0	19	1%
4981.0	12	0%
4980.0	39	1%
4979.0	33	1%
4978.0	19	1%
4977.0	15	1%
4976.0	13	0%
4975.0	6	0%
4974.0	5	0%
4973.0	11	0%
4972.0	20	1%
4971.0	18	1%
4970.0	11	0%
4290.0	1	0%
0.5	4	0%
	2	0%
Total	2.808	100%

En los últimos **15 días** se han estado actualizando **2257** máquinas con una versión de firma .DAT igual o superior a la **4970**. 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 octubre, igualmente se evidencia que para el caso de las Workstation el **79.7 %** 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.

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 enviado 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 no se tuvo un avance significativo en la reducción de los equipos que se encontraban sin comunicación entre **enero** y **agosto** a pesar de que se estuvieron enviando los informes.

- Por correo electrónico se ha dado respuesta a los técnicos en sitio, indicándo 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 un decremento en las notificaciones para revisión de equipos por correo electrónico este mes, debido a que la mayoría de los técnicos presentan falencias al momento de realizar una instalación o actualización del agente y módulos.

- Se han estado configurando una serie de tareas cliente con el fin de poder desinstalar en 27 equipos el módulo FW. Estos despliegues están configurados para actualizar el versionamiento del módulo y luego proceder a desinstalarlo apenas se efectúe una comunicación con el agente. A la fecha queda un total de **11 equipos** pendientes por desinstalar el módulo.

- Se realiza un caso a fabricante **4-23256588711** a solicitud del ingeniero Ruben Montealegre para validar directamente si el antivirus se encuentra o no cubierto para prevenir las vulnerabilidades 0day en Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082). Se informe por parte de fabricante que apenas se tenga la POC por parte de Microsoft, esta será agregada y cubierta por el antivirus.

- Se realiza un caso a fabricante **4-23282225381** a solicitud del ingeniero Ruben Montealegre para validar directamente si desde consola **ePO MVISION** existe la posibilidad de agregar un hash de tipo **SHA-256** para lo cual el fabricante comparte instrucciones, donde se agregan y aplican los IoC´s por medio de una regla experta en las directivas correspondientes. Este caso estuvo relacionado con el ransomware Prestige.

- 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 encuentra pendiente para validar por fabricante.

- Se realiza un caso a fabricante **4-23243508121** a solicitud del ingeniero Ruben Montealegre para constatar si desde consola **ePO MVISION** se puede realizar la eliminación del virus **Autorun.inf**, aplicando esta configuración a los equipos de la entidad. El fabricante valida esta información e informa que no es posible, debido a que este no se considera por el antivirus una amenaza global que pueda afectar el funcionamiento de un equipo ya que hay aplicativos que utilizan este tipo de archivo para su correcta ejecución.

- Se realiza la validación de los equipos que estarán siendo atendidos por los ingenieros de la FAC para la instalación del agente de Tenable. Se esperaron instrucciones para validar que tipo de exclusiones aplicar desde consola ePO MVISION.

Elaborado por:

Christian Ricardo Almanza Castañeda
Administrador consola ePO

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: 2022.11.28 09:39:00 -05'00'

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3