CII
CYBERPEACE

INFORME MENSUAL

DEACERO

www.cyberpeace.tech

SGSI-DOC-SOC-06 DEACERO-INFORME MENSUAL								
Elaborado por:	Josué Nahum Cruz Domínguez							
Aprobado por:	Iván Hernández							
Fecha:	30/06/23							
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

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 **DEACERO** 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.

Introducción

El presente informe se encarga de documentar y reportar la actividad sospechosa o potencialmente critica que se registró mediante el monitoreo del SIEM.

Al final de este reporte se anexan recomendaciones por parte de Cyberpeace que se espera sean atendidas para poder robustecer la infraestructura de **DEACERO** 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 **DEACERO**.

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.

Alertamientos y/o notificaciones enviadas por el SOC

A continuación, en la siguiente tabla se muestran los tickets enviados por el equipo del SOC hacia DEACERO como alertamientos y actividades realizadas.

Tabla 1. Alertamientos y/o Notificaciones

Numero de ticket	Asunto	Fecha	Estado
4667/4674	Análisis de amenazas| aplicaciones validas	01/06/23	Cerrado
4682	Alertamiento temprano DeAcero	02/06/23	Cerrado
4708	Alertamiento temprano DeAcero ZGrab.Scanner	03/06/23	Cerrado
4710	Alertamiento dispositivo DA-EMC-CLAROTY no alcanzable	03/06/23	Cerrado
4717	Alertamiento DeAcero VMware.vCenter.CVE-2021-21985.Remote.Code.Execution	04/06/23	Cerrado
4746	Alertamiento dispositivo SRVEEAMQRO Servidor RPC no disponible	06/06/23	Cerrado
4749	Alertamiento temprano DeAcero	06/06/23	Cerrado
4787	Alertamiento por posible secuestro de cuentas Office365	07/06/23	Cerrado
4799	Alertamiento DeAcero VMware.vCenter.CVE-2021-21985.Remote.Code.Execution	08/06/23	Cerrado

Numero de ticket	Asunto	Fecha	Estado
4832	Alertamiento EventLog - Dispositivos inaccesibles.	09/06/23	Cerrado
4834	Informe mensual - Mayo	09/06/23	Pendiente
4837	Alertamiento EventLog - Conexiones Anomalas	09/06/23	Cerrado
4863	Alertamiento EventLog - CVE-2021-21985	11/06/23	Cerrado
4949	Alertamiento dispositivos sin alcance	15/06/23	Cerrado
4957	Alertamiento EventLog - Eventos DarkTrace	16/06/23	Cerrado
4964	Alertamiento dispositivo ACDC01 y ACDC02	16/06/23	Cerrado
4980	Alertamiento EventLog - Dispositivo Inaccesible	17/06/23	Cerrado
4986	Alertamiento EventLog - Base de Datos Llena	17/06/23	Cerrado
5006	Alertamiento temprano DeAcero	19/06/23	Cerrado
5025	Alertamiento DeAcero ALFA.TEaM.Web.Shell	19/06/23	Cerrado
5031	Alertamiento EventLog - Dispositivo Inaccesible	20/06/23	Cerrado

Numero de ticket	Asunto	Fecha	Estado
5035	Alertamiento EventLog - Dispositivo AMPDES02 Agente Caído	20/06/23	Cerrado
5061	Alertamiento EventLog - Dispositivo Caído	21/06/23	Cerrado
5078	Validación de remediación de hallazgo	22/06/23	Cerrado
5130	Alertamiento EventLog - Dispositivos Inaccesibles	25/06/2023	Cerrado
5143	Alertamiento DEACERO Quarant Files In A Detect SumEvent	26/06/2023	Cerrado
5156	Alertamiento CrowdStrike archivo ejecutable malicioso GoTo Webinar Opener.exe	27/06/2023	Cerrado
5176	Alertamiento EventLog - Ejecución de proceso sospechoso.	28/06/2023	Cerrado
5184	Alertamiento CrowdStrike archivo ejecutable malicioso EasyPDFCombineTooltab	28/06/2023	Cerrado
5221	Alertamiento EventLog - Dispositivos Inaccesibles	30/06/2023	Cerrado

Actividad en los Firewalls

Durante el periodo que va del día 1ro de junio al día 30 de junio de 2023, en los equipos de Fortinet se observa la siguiente tendencia de comportamiento durante el mes.

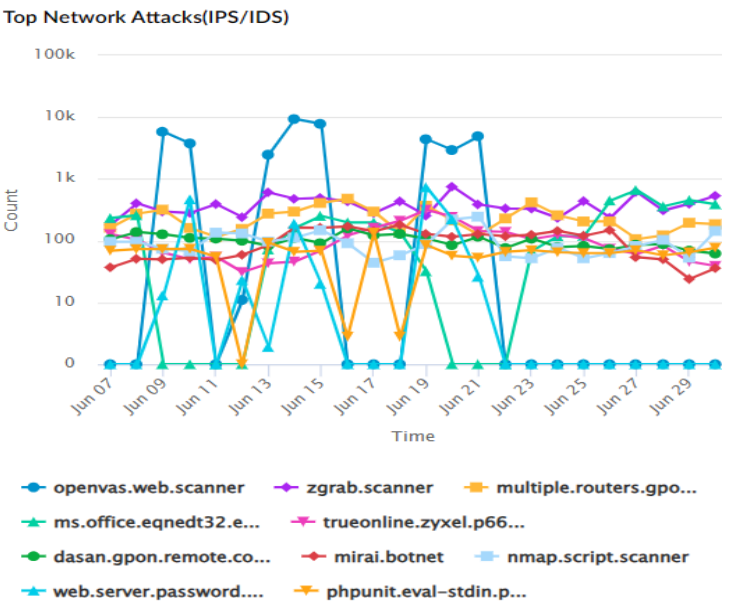
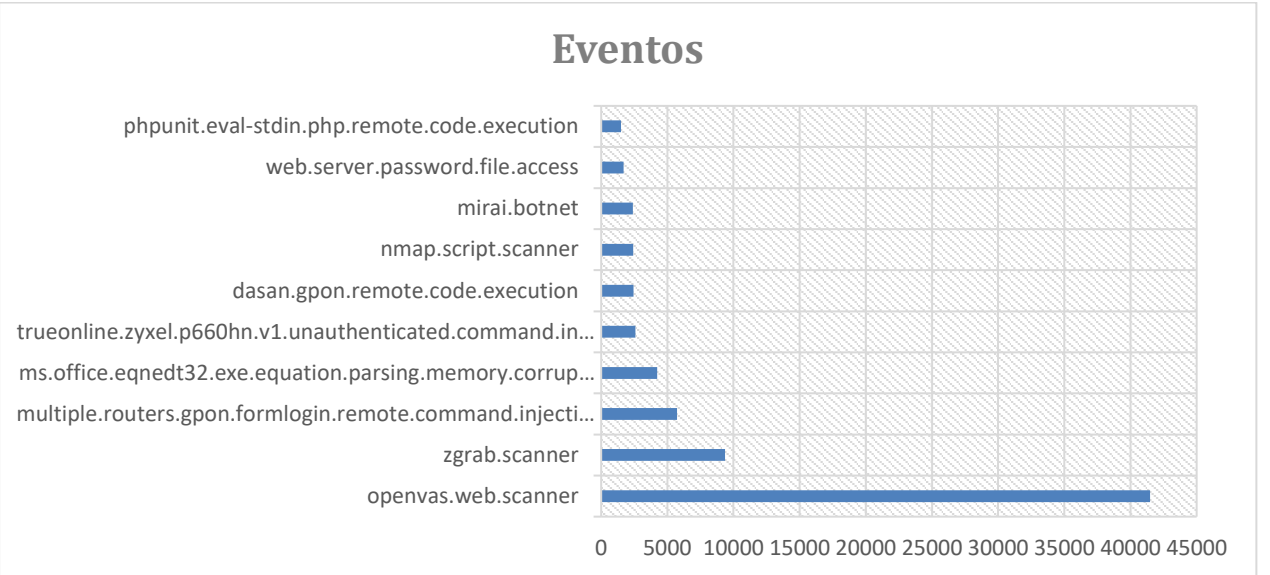
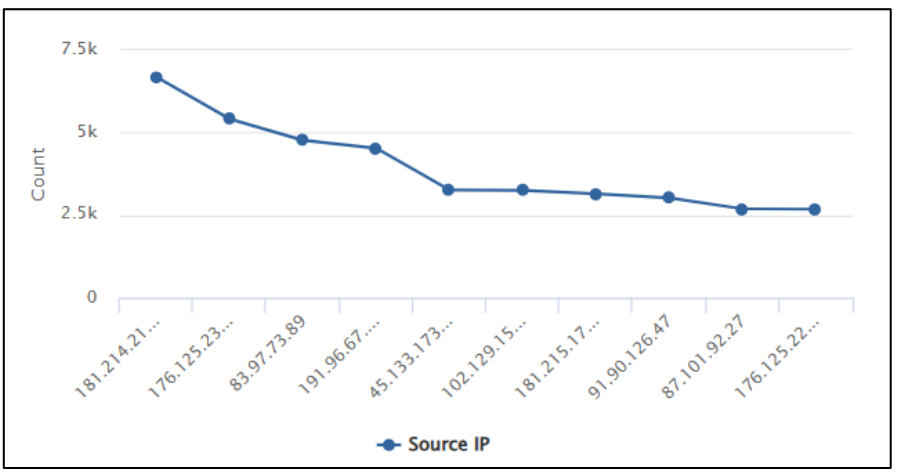


Imagen 1. Tendencia de actividad maliciosa en los firewalls

En la tendencia de intentos de escaneos de red, de análisis de vulnerabilidades, intentos de inyección de código SQL, así como otras amenazas provenientes desde el exterior hacia la red interna de DEACERO. Dicha actividad maliciosa fue bloqueada y/o contenida por los equipos de seguridad perimetral, cabe mencionar que son eventos de internet hacía DeAcero.



Gráfica 1. Eventos detectados por el IPS



Gráfica 2. IP con mayor actividad

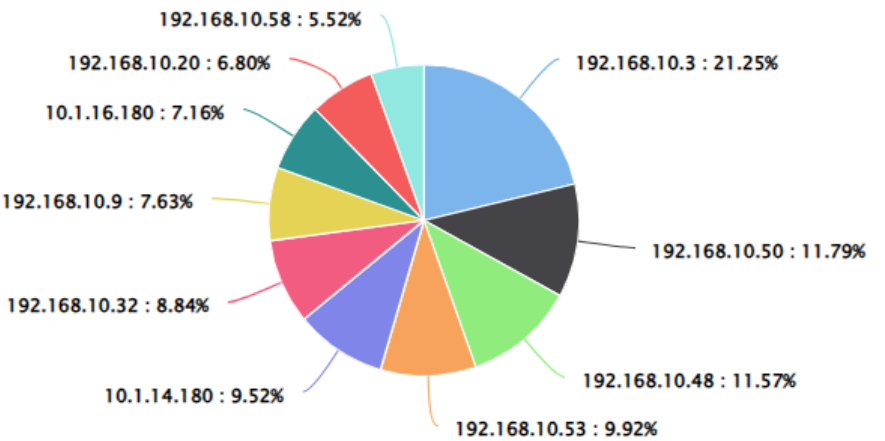
Tabla 2. IP Origen maliciosas

IP Origen externas maliciosas			
181.214.218.46	176.125.230.19	83.97.73.89	181.215.176.16
191.96.67.169	45.133.173.109	87.101.92.27	

Tabla 3. IP Origen no maliciosas

IP Origen externas no maliciosas	
102.129.152.55	91.90.126.47

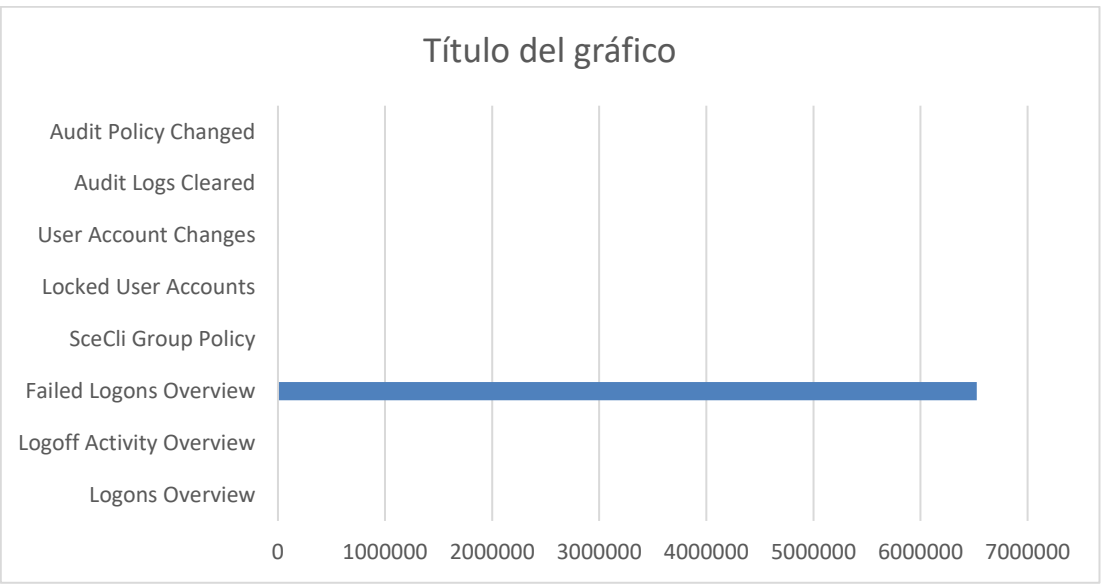
En la siguiente gráfica podemos obervar las direcciones IP de internas con mayores detecciones de direcciones IP externas.



Gráfica 3. IP Origen con mayor actividad en el periodo.

Actividad en dispositivos Windows

Durante el periodo de monitoreo realizado, fueron capturados múltiples eventos de Windows donde se engloban eventos como inicios de sesión tanto exitosos como fallidos los cuales se presentan los más relevantes en la gráfica siguiente.

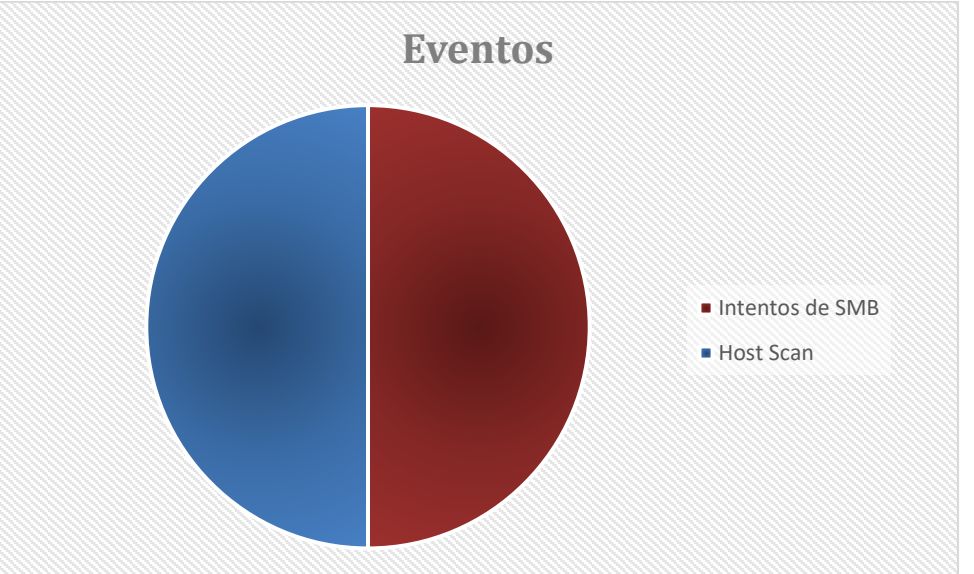


Gráfica 4. Eventos de Windows relevantes

En la gráfica previa mostrada se observa que el evento “Failed Logons Overview” cuenta con 22 registros. El evento de "Logon Overview" es útil para los administradores de sistemas que necesitan monitorear y auditar los inicios de sesión de los usuarios en el sistema. También puede ayudar a identificar problemas de inicio de sesión y detectar intentos de inicio de sesión no autorizados o inusuales.

Actividad en CLAROTY

Durante el periodo de monitoreo realizado este mes, fueron capturados múltiples eventos en relación con la tecnología CLAROTY, la cual capturó eventos relacionados a alertas de intentos fallidos de transferencia de datos mediante uso de SMB y actividades de reconocimiento.



Gráfica 5. Resumen de eventos CLORATY

En relación con los intentos de inicio de sesión mediante el protocolo SMB se enlistan las direcciones IP de origen y de destino correspondientes.

Tabla 4. Actividad SMB

SMB ATTEMPS	
Origen	**Destino**
141.1.9.4	141.1.42.15
141.1.77.152	141.1.47.141
141.1.77.192	141.1.77.148
141.1.9.4	141.1.77.191
141.1.92.22	
141.1.77.148	
141.1.77.191	
142.1.21.246	
141.1.62.23	

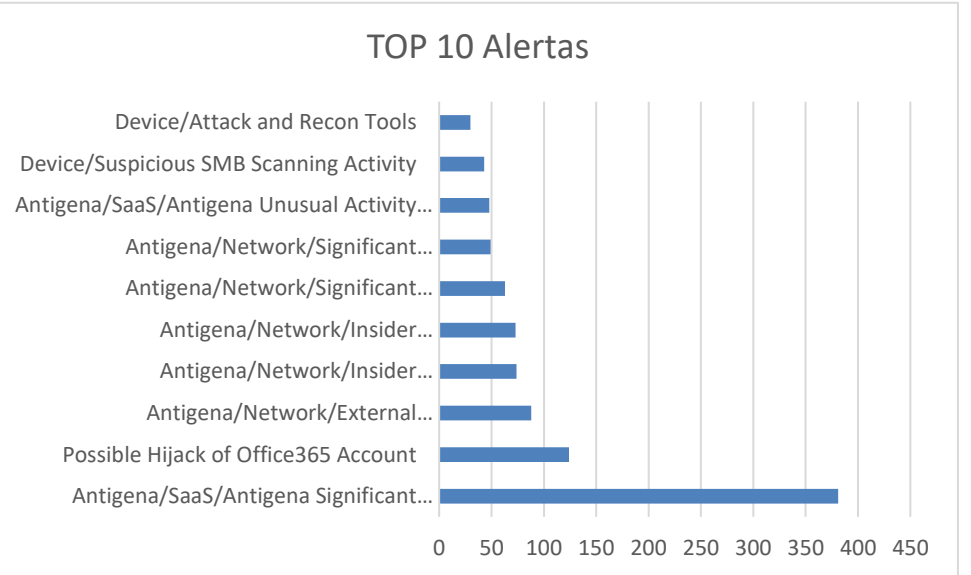
En este apartado son alertas de comportamiento originario desde las IP origen, a lo que el log no muestra el destino, a que es a múltiples host.

Tabla 5. HOST SCAN

HOST SCAN	
Origen	**Destino**
142.1.21.246	Múltiples host

Actividad en dispositivos Darktrace

En cuanto a los eventos capturados mediante la inteligencia Darktrace, fueron capturados 1067 eventos durante el periodo reportado. Entre las categorías capturadas, se muestra un top 10 de amenazas capturadas, teniendo como primer lugar el evento "Antigena Significant Compliance Activity Block" con 381 eventos previos capturados. Como segundo lugar tenemos el "Possible Hijack of Office365 Account" con 124 eventos capturados. Por último, también fueron capturados eventos con relación a "Antigena File then New Outbound Block" con 88 detecciones durante el mes de abril.



Gráfica 6. Top 10 amenazas Darktrace

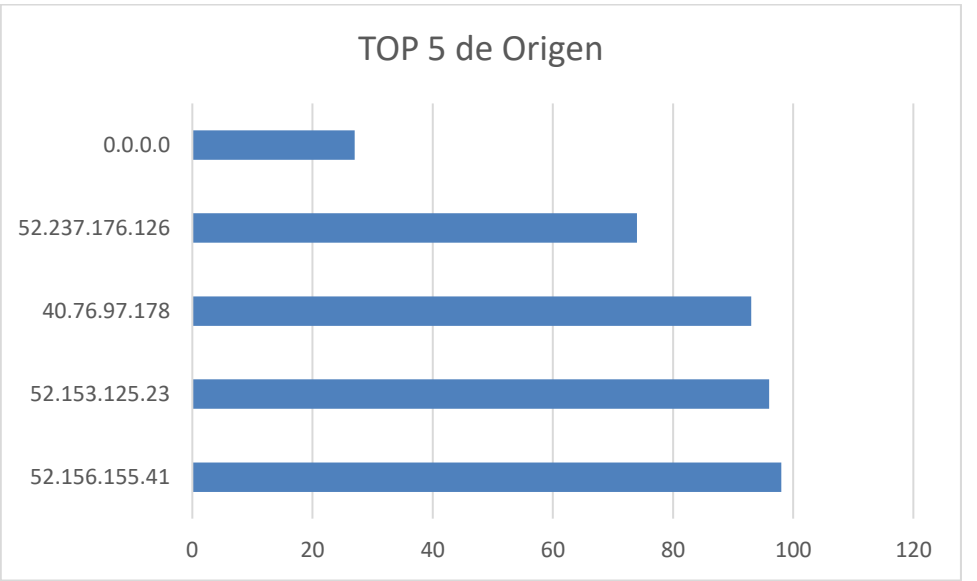
Sin embargo, a fin de brindar un desglose en cuanto a los eventos de Darktrace es anexada la siguiente tabla.

Tabla 6. Eventos Darktrace

Clasificación	Eventos
Antigena/SaaS/Antigena Significant Compliance Activity Block	381
Possible Hijack of Office365 Account	124
Antigena/Network/External Threat/Antigena File then New Outbound Block	88
Antigena/Network/Insider Threat/Antigena Network Scan Block_DeAcero	74
Antigena/Network/Insider Threat/Antigena Unusual Privileged User Activities Block	73
Antigena/Network/Significant Anomaly/Antigena Breaches Over Time Block	63
Antigena/Network/Significant Anomaly/Antigena Controlled and Model Breach	49
Antigena/SaaS/Antigena Unusual Activity Block	48

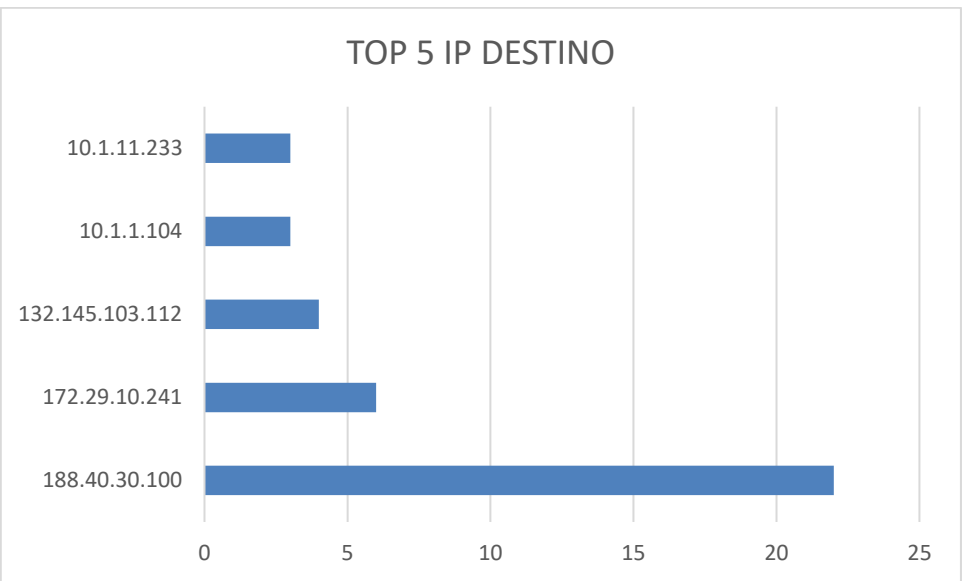
Device/Suspicious SMB Scanning Activity	43
Device/Attack and Recon Tools	30
Antigena/Network/Insider Threat/Antigena Large Data Volume Outbound Block	18
Anomalous File/Anomalous Octet Stream (No User Agent)	15
Antigena/Network/External Threat/Antigena Suspicious Activity Block	8
Antigena/Network/Significant Anomaly/Antigena Enhanced Monitoring from Client Block	4
Possible HTTP Command and Control to Multiple Endpoints	4
Compromise/Large DNS Volume for Suspicious Domain	4
Device/Anomalous Github Download	2
Compromise/Suspicious Spam Activity	2
Device/SMB Lateral Movement	3
Device/Network Scan	3
Antigena/SaaS/Antigena Unusual Access Block	2
SaaS/Compromise/Unusual Login and Account Update	2
Antigena/SaaS/Antigena Suspicious SaaS Activity Block	2
Inoculation/HTTP to Suspicious Subdomain	2
Unusual Activity/Sustained Unusual Activity from New Device	2
Compromise/High Volume Domain Fluxing	2
Device/Multiple Lateral Movement Model Breaches	2
SaaS/Unusual Activity/Multiple Unusual External Sources For SaaS Credential	2
SaaS/Admin/Mail Forwarding Enabled	2
Anomalous File/Numeric File Download	0
Anomalous Connection/Suspicious Read Write Ratio and Unusual SMB	1
Antigena/Network/External Threat/SMB Ratio Antigena Block	1
Compromise/Connections with Suspicious DNS	1
Possible HTTP Command and Control	1
ICS/Anomaly Then New ICS Commands	1
Compromise/DGA Beacon	1
Compromise/Suspicious File and C2	1
Anomalous File/Suspicious HTTP Redirect	1

En alcance a los eventos alertados se muestra el TOP 5 de direcciones IP de origen en relación con los eventos de Darktrace capturados en donde es posible observar a la dirección IP 52.156.155[.]41 en primer lugar con 98 detecciones, seguido de la dirección IP 52.153.125[.]23 con 96 detecciones y en tercer lugar se encuentra la dirección IP 40.76.97[.]178 con 93 detecciones capturadas las cuales hacen uso de servicios tales como Microsoft representando un bajo riesgo en cuanto a alcance de seguridad.



Gráfica 7. TOP 5 IP ORIGEN.

Asimismo, a su vez, fue realizado el recuento de eventos alertados en donde se muestra el TOP 5 de direcciones IP de destino en relación con los eventos de Darktrace capturados en donde es posible observar a la dirección IP 188.40.30[.]100 en primer lugar con 22 detecciones, seguido de la dirección IP 172.29.10[.]241 con 6 detecciones y en tercer lugar se encuentra la dirección IP 132.145.103[.]112 con 4 detecciones capturadas.



Gráfica 8. TOP 5 IP DESTINO.

Tras realizarse el análisis correspondiente se anexan las cuentas de correo involucradas en las alertas de Darktrace, los cuales incluyen eventos de SaaS.

Tabla 7. Tabla de usuarios con alertamientos.

Dirección de correo electrónico		
josmon@deacero.com	iramos@deacero.com	anagarza@deacero.com
jpantoja@deacero.com	irrodriguez@deacero.com	angomez@deacero.com
jpola@deacero.com	ivillalvazo@deacero.com	aquintanillaf@deacero.com
jprosa@deacero.com	jaleal@deacero.com	arielr@deacero.com
jquintanilla@deacero.com	jalopezch@deacero.com	arodriguezl@deacero.com
jrgomez@ingetek.com.mx	jasantoyo@deacero.com	aruizr@deacero.com
jrmoreno@deacero.com	javiergcia@deacero.com	asalazarr@deacero.com
jrodriguezm@deacero.com	javmar@deacero.com	avillarreal@deacero.com
jrojo@deacero.com	jbarajas@deacero.com	axelguerra@deacero.com
jrubio@deacero.com	jbravo@deacero.com	azael.perez@bigwavedata.mx
jsancheze@deacero.com	jcalvin@mcswusa.com	bamedrano@deacero.com
jsbarranco@deacero.com	jccordova@deacero.com	basculamex@deacero.com
jtamez@deacero.com	jclopez@deacero.com	bdiaz@deacero.com
jtorresu@deacero.com	jclopezr@ingetek.com.mx	belizondo@deacero.com
jtrejo@deacero.com	jcmoralesv@deacero.com	bescudero@deacero.com
jtzontecomani@ingetek.com.mx	jcmtzr@deacero.com	bgamez@deacero.com
judithlozano@deacero.com	jcmunguia@deacero.com	bmedina@deacero.com
juribe@deacero.com	jcruz@deacero.com	bmigliori@deacero.com
jvaleriano@deacero.com	jcruzs@deacero.com	bnfhermosillo@deacero.com
jvgomez@deacero.com	jcvilla@deacero.com	bperez@deacero.com
jvillalpando@deacero.com	jdelacruzg@deacero.com	brcantu@deacero.com
jzapata-ext@deacero.com	jdeleonp@deacero.com	bverdin@deacero.com
karla@compusolucionescsp.onmicrosoft.com	jennifer.gonzalez@mcswusa.com	caaguinaga@deacero.com
kfernandez@deacero.com	jesriv@deacero.com	calidadptagarcia@ingetek.com.mx
kortega@deacero.com	jfarias@deacero.com	carari@ingetek.com.mx
ktamayo@deacero.com	jfcastro@deacero.com	carmed@deacero.com
laluna@deacero.com	jfernandez@deacero.com	ccaballero@deacero.com
lerodriguez@deacero.com	jfigueroa@deacero.com	ccano@deacero.com
lfloresg@deacero.com	jgarciah@ingetek.com.mx	ccastro@deacero.com
lhinojosa@deacero.com	jguajardo@deacero.com	cchavezr@deacero.com

lizavega@deacero.com	jherrerap@mcswusa.com	cdelgado@deacero.com
lmalacara@deacero.com	jhgonzalez@deacero.com	cdmedina@deacero.com
lmartinez@deacero.com	jjalvarez@deacero.com	cdreyes@deacero.com
lmendez@deacero.com	jlcantu@ingetek.com.mx	ceguach@deacero.com
lrdz@deacero.com	jlmontero@deacero.com	cescamilla@deacero.com
ltrevino@deacero.com	jlopezp@deacero.com	cfernandez@ingetek.com.mx
luvillasenor@deacero.com	jlugo@deacero.com	cgodinez@deacero.com
lvillalobos@deacero.com	jmatamoros@deacero.com	cgomezv@deacero.com
lzazueta@deacero.com	jmguajardo@deacero.com	cguerra@deacero.com
mahdz@deacero.com	jmonroy@deacero.com	clasificadorespmxl@deacero.com
maquezada@deacero.com	jmunozv@deacero.com	cleyva@ingetek.com.mx
marceloalv@deacero.com	jogarcia@deacero.com	cmancera@deacero.com
masolis@deacero.com	jojeda@deacero.com	cocegueda@deacero.com
matjoq@deacero.com	jolvera@deacero.com	cpatsannico@deacero.com
mavina@deacero.com	jonasp@deacero.com	cpratt@mcswusa.com
mayrodri@deacero.com	jorrod@deacero.com	cramireza@deacero.com
mbeltran@deacero.com	josalv@deacero.com	crobledo@deacero.com
mcabello@deacero.com	eligut@deacero.com	crodriguezp@deacero.com
mcasa@deacero.com	erendon@deacero.com	ctrlacc2@deacero.com
mcastruita@deacero.com	etadeo@deacero.com	ctrocoli@deacero.com
mcduran@deacero.com	ezreyes@deacero.com	cvallei@deacero.com
mchavez@deacero.com	facevedo@deacero.com	cygarza@deacero.com
mchen@deacero.com	fburnes@ingetek.com.mx	easanchez@deacero.com
mcromo@deacero.com	fcastaneda@deacero.com	ecasbern@deacero.com
mdelrio@deacero.com	furselay@deacero.com	echavez@mcswusa.com
mfarias@deacero.com	gegarza@deacero.com	ecorrea@deacero.com
mfserrano@deacero.com	gesteodacecel2@deacero.com	eduarte@deacero.com
mgalben@deacero.com	gherjim@deacero.com	eescobedo@deacero.com
mgaona@deacero.com	glomeli@deacero.com	efgzz@deacero.com
mgasca@ingetek.com.mx	guiarv@deacero.com	eguerrero@deacero.com
mjsepulveda@deacero.com	hdflores@deacero.com	egutierrez@deacero.com
mlmartinezc@deacero.com	hviveros@deacero.com	ehdzb@deacero.com
mmoran@deacero.com	ijgarza@deacero.com	emorenor@deacero.com
mmorenor@deacero.com	itrujillo@deacero.com	ericer@deacero.com
mperea@deacero.com	jccazarez@deacero.com	eucastillo@deacero.com
mponce@deacero.com	jcortez@deacero.com	eugalv@ingetek.com.mx
mramirezq@deacero.com	jcreyes@deacero.com	eusanchez@deacero.com

mrbueno@deacero.com	jcruzch@deacero.com	facosta@deacero.com
mserranop@deacero.com	jcvaldez@deacero.com	fgonzalezr@deacero.com
msledezma@deacero.com	jdeleon@deacero.com	fgutierrez@deacero.com
mtorresg@deacero.com	jecruz@ingetek.com.mx	fjalvarez@deacero.com
mvcaballero@deacero.com	jedavila@deacero.com	fjrodriguezc@deacero.com
mzamarron@deacero.com	jerivera@deacero.com	frdzestrada@deacero.com
naguirre@deacero.com	jesteban@deacero.com	fsamaniego@deacero.com
ndehoyos@deacero.com	jfcardenas@deacero.com	gabgon@deacero.com
nlucio@deacero.com	jgpuente@deacero.com	gcanales@deacero.com
nrrojas@deacero.com	jhernand@deacero.com	geotam@mcswusa.com
nsanagu@deacero.com	jhidalgo@deacero.com	ggtzn@deacero.com
oamartinezj@deacero.com	jmadrid@deacero.com	gjaguilarm@ingetek.com.mx
obaez@deacero.com	jmayoral@deacero.com	gmezac@deacero.com
ogdelacruz@deacero.com	jmchavezs@deacero.com	gnrodriguez@deacero.com
omart@deacero.com	jmendieta@deacero.com	gpenaflor@deacero.com
osbadi@deacero.com	jmmayorga@deacero.com	halvarezg@deacero.com
oslopez@deacero.com	joscas@deacero.com	harmenta@deacero.com
paldape@deacero.com	jvenancio@deacero.com	hdelapena@deacero.com
pmoreno@deacero.com	lamancilla@deacero.com	hhuerta@deacero.com
psantoyo@deacero.com	lavargas@deacero.com	hreyes@deacero.com
qperez@deacero.com	lgalicia@deacero.com	hvazquez@deacero.com
raguilara@deacero.com	lggarcia@deacero.com	iaguirre@ingetek.com.mx
ralanis@deacero.com	libarra@deacero.com	iavidaurri@deacero.com
rcastilloa@deacero.com	lolvera@deacero.com	ifloresr@deacero.com
rchavez@ingetek.com.mx	lperezv@deacero.com	igbarrios@deacero.com
rcorrea@ingetek.com.mx	lrmadrigal@deacero.com	iguerrero@deacero.com
rdonez@deacero.com	mgonzalez@deacero.com	ihinojosa@deacero.com
rguerrau@deacero.com	mmercado@deacero.com	abtorres@deacero.com
rigonzalezs@deacero.com	mmherrera@ingetek.com.mx	acabriales@deacero.com
rimendez@ingetek.com.mx	msaldanar@deacero.com	acavazos@deacero.com
rlarrea@deacero.com	abtorres@deacero.com	afjuarez@deacero.com
rmuzquiz@deacero.com	acabriales@deacero.com	agarciahdz@ingetek.com.mx
rpardo@deacero.com	acavazos@deacero.com	aggonzalez@deacero.com
rperez-ext@deacero.com	afjuarez@deacero.com	agsiller@deacero.com
rroldan@deacero.com	agarciahdz@ingetek.com.mx	aloredo@ingetek.com.mx
rvelav@deacero.com	aggonzalez@deacero.com	alrodriguezr@deacero.com
rzambrano@deacero.com	agsiller@deacero.com	amora@deacero.com

rzarate@deacero.com	aloredo@ingetek.com.mx	amsanchez@deacero.com
s1crobledo@deacero.com	alrodriguezr@deacero.com	amunizr@deacero.com
s1kuribe@deacero.com	amora@deacero.com	andloz@deacero.com
s1victormtz@deacero.com	amsanchez@deacero.com	aramon@deacero.com
samartinez@deacero.com	amunizr@deacero.com	ardz@deacero.com
sarellano@deacero.com	andloz@deacero.com	ardzv@deacero.com
sayala@deacero.com	aramon@deacero.com	averduzco@deacero.com
seguros_ingetek@ingetek.com.mx	ardz@deacero.com	bjpadilla@deacero.com
sjrdz@deacero.com	ardzv@deacero.com	bparas@deacero.com
snavarro@deacero.com	averduzco@deacero.com	cbancer@ingetek.com.mx
sprieto@deacero.com	bjpadilla@deacero.com	ccastilla@deacero.com
svillasenor@deacero.com	bparas@deacero.com	cglz@deacero.com
syarza@deacero.com	cbancer@ingetek.com.mx	cparris@mcswusa.com
tdeluna@deacero.com	ccastilla@deacero.com	cponce@deacero.com
tfavela@deacero.com	cglz@deacero.com	crlopez@deacero.com
tom_utz@deacero.com	cparris@mcswusa.com	csalas@deacero.com
tvidaurri@deacero.com	cponce@deacero.com	csanchezl@deacero.com
vdelgado@deacero.com	crlopez@deacero.com	ctellez@deacero.com
vhzamora@deacero.com	csalas@deacero.com	czavalam@deacero.com
vmartinezz@deacero.com	csanchezl@deacero.com	czenteno@deacero.com
vmosqueda@deacero.com	ctellez@deacero.com	daortizb@deacero.com
vrodriguez@deacero.com	czavalam@deacero.com	davmun@deacero.com
vtapia@deacero.com	czenteno@deacero.com	dcardoso@deacero.com
ymateu@deacero.com	daortizb@deacero.com	despinoza@deacero.com
ysalinase@deacero.com	davmun@deacero.com	destrada@deacero.com
amzucker@deacero.com	dcardoso@deacero.com	dmendez@deacero.com
efrodriguezf@deacero.com	despinoza@deacero.com	dmramos@deacero.com
egastelum@deacero.com	destrada@deacero.com	dnocker@deacero.com
egonzalez@deacero.com	dmendez@deacero.com	drmarcial@ingetek.com.mx
amejiav@deacero.com	dmramos@deacero.com	ebarranco@ingetek.com.mx
eblanco@deacero.com	dnocker@deacero.com	eblanco@deacero.com
	drmarcial@ingetek.com.mx	efrodriguezf@deacero.com
	ebarranco@ingetek.com.mx	egastelum@deacero.com

Recomendaciones

- En base a los hallazgos reportados en el periodo se recomienda mantener los sistemas actualizados con el fin de mitigar y/o reducir la superficie de ataque en la infraestructura tanto de TI como OT.

- Realizar campañas de concientización internas sobre las mejores prácticas de uso de contraseñas robustas y evitar compartir información de la empresa por canales no oficiales.

- Fortalecer las listas negras agregando los IOC que el SOC notifique a DeAcero en sus diferentes herramientas de seguridad para evitar y/o prevenir actividades provenientes de estas.

CII