International Interdisciplinary Congress on Renewable Energies, Industrial Maintenance, Mechatronics and Informatics

Booklets

RENIECYT 1702902 CONACYT

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Cybersecurity Dashboard

Authors: LEDESMA-URIBE, Norma Alejandra, JUÁREZ-SANTIAGO, Brenda, MENDOZA-HERNÁNDEZ, Guillermo and ALVARADO-MALDONADO, Ricardo

Editorial label ECORFAN: 607-8695
BCIERMMI Control Number: 2021-01
BCIERMMI Classification (2021): 271021-0001

Pages: 10
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

Introduction

Methodology

Results

Annexes

Conclusions

References

Introduction

Se requiere visualizar información sobre ciberseguridad de todas las unidades en un solo lugar de manera especifica.

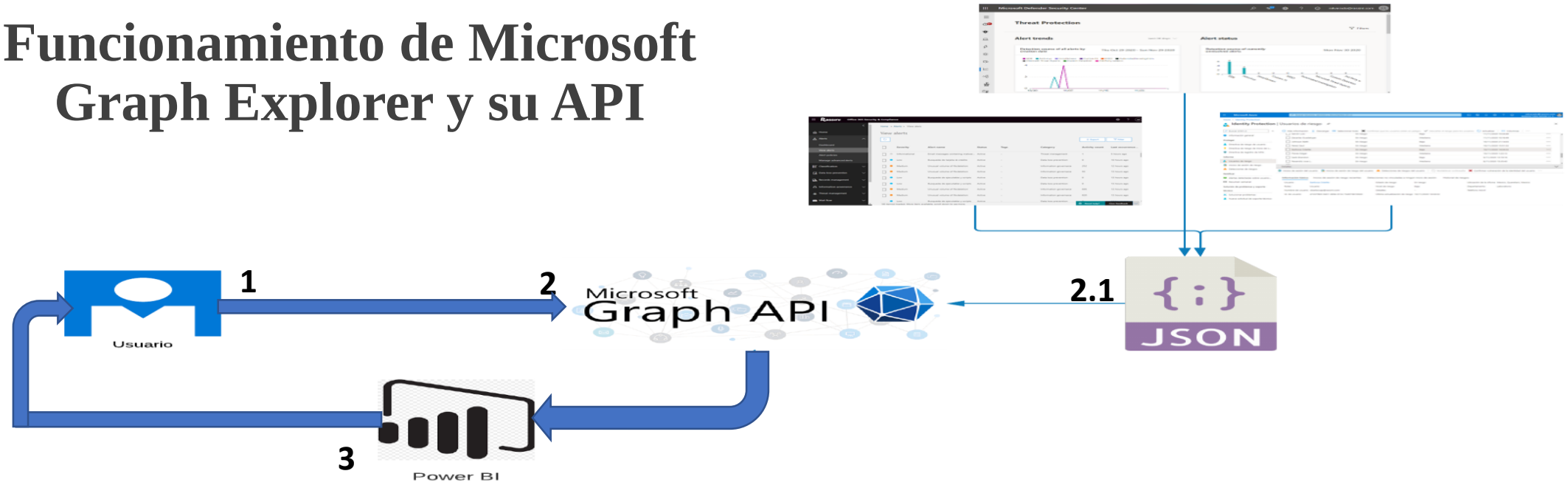
La información de ciberseguridad se encuentra descentralizada

Entrelazar información de los portales de ciberseguridad

Visualizar información importante y concreta en un solo lugar

Methodology

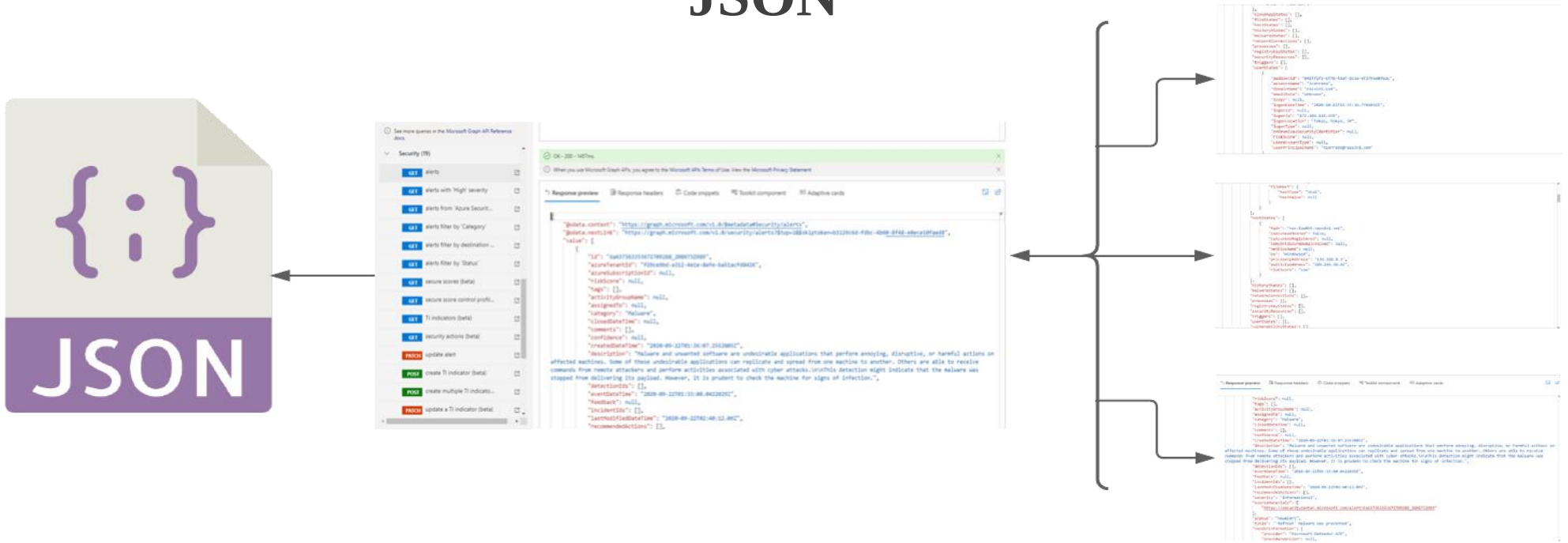
Funcionamiento de Microsoft Graph Explorer y su API



Se desarrolló a partir de una API ya construida llamada Microsoft Graph, donde los datos se encontraban sin transformar en un formato de texto llamado JSON donde después los visualizaremos en Power BI

Methodology

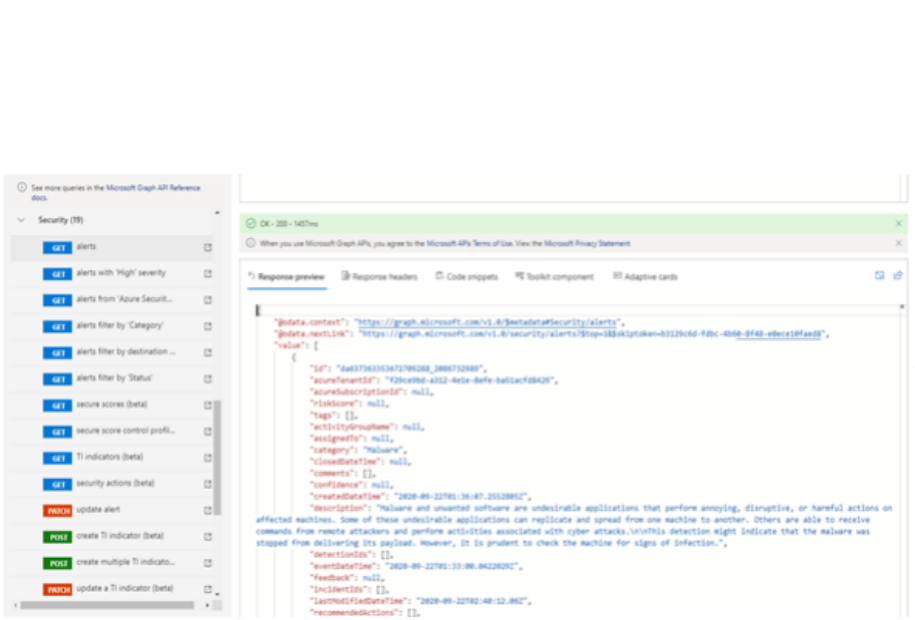
Estructura de los datos en formato JSON

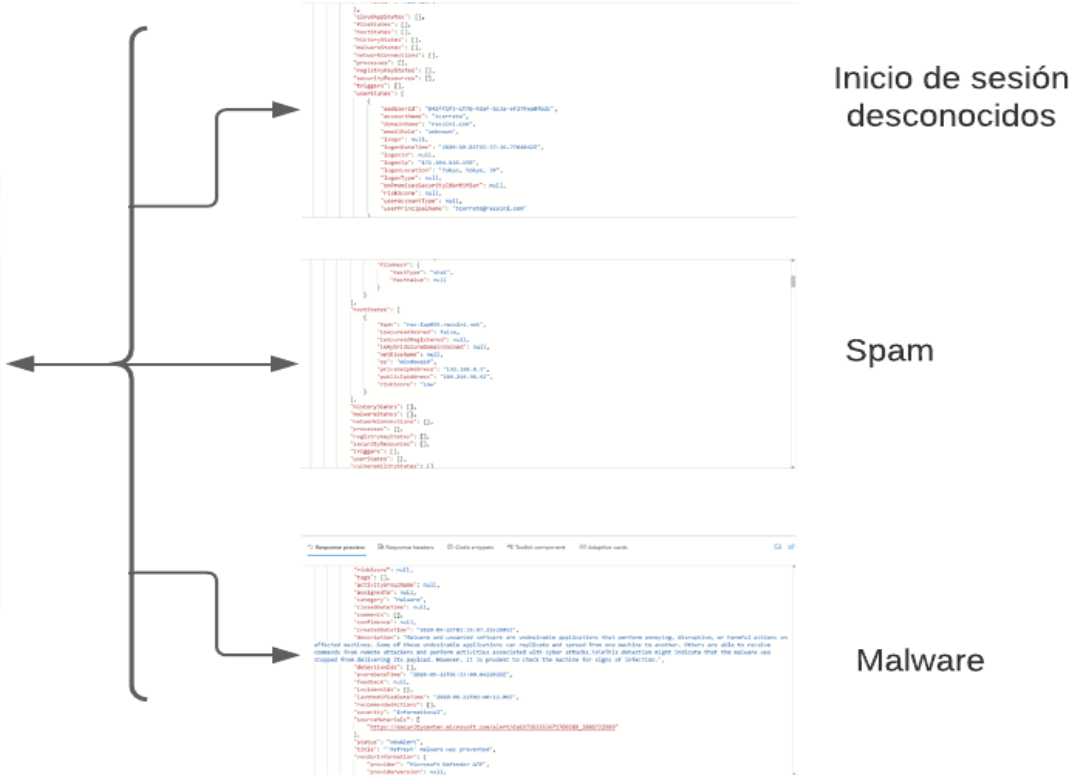


Los metadatos se encuentran en el JSON de forma desordenada donde nosotros los ordenamos de manera que tengan un sentido al lector

Methodology

Ejemplo de como se ven algunas situaciones sobre ciberseguridad





Inicio de sesión desconocidos

Spam

Malware

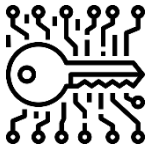
Methodology

Ejemplo de categorías de ciberseguridad

Ataques a maquinas virtuales

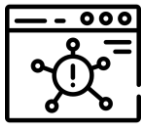
Manejo de amenazas

Búsqueda de ejecutables y scripts



Descargas de archivos sospechosos

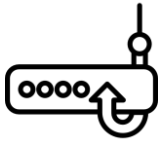
Creación de reglas de trafico en la red



eDiscovery

IP Maliciosas

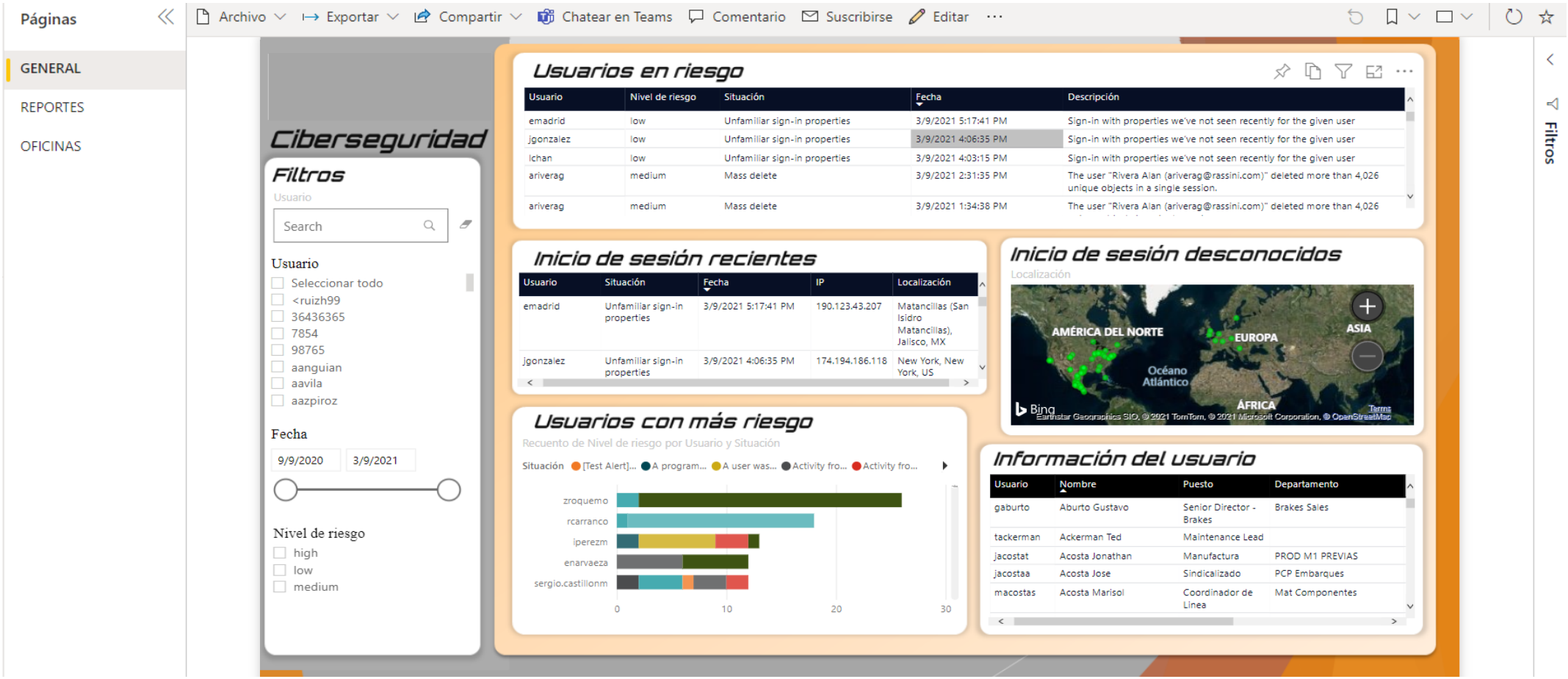
Gobierno de datos



Búsqueda de tarjetas de crédito

Eliminación/Descarga de archivos masivamente

Results


Páginas
GENERAL
REPORTES
OFICINAS
Archivo
Exportar
Compartir
Chatear en Teams
Comentario
Suscribirse
Editar
Ciberseguridad
Filtros
Usuario
Search
Usuario
Seleccionar todo
<ruizh99
36436365
7854
98765
aanguian
aavila
aazpiroz
Fecha
9/9/2020
3/9/2021
Nivel de riesgo
high
low
medium
Usuarios en riesgo
Usuario | Nivel de riesgo | Situación | Fecha | Descripción
emadrid | low | Unfamiliar sign-in properties | 3/9/2021 5:17:41 PM | Sign-in with properties we've not seen recently for the given user
jgonzalez | low | Unfamiliar sign-in properties | 3/9/2021 4:06:35 PM | Sign-in with properties we've not seen recently for the given user
lchan | low | Unfamiliar sign-in properties | 3/9/2021 4:03:15 PM | Sign-in with properties we've not seen recently for the given user
ariverag | medium | Mass delete | 3/9/2021 2:31:35 PM | The user "Rivera Alan (ariverag@rassini.com)" deleted more than 4,026 unique objects in a single session.
ariverag | medium | Mass delete | 3/9/2021 1:34:38 PM | The user "Rivera Alan (ariverag@rassini.com)" deleted more than 4,026
Inicio de sesión recientes
Usuario | Situación | Fecha | IP | Localización
emadrid | Unfamiliar sign-in properties | 3/9/2021 5:17:41 PM | 190.123.43.207 | Matancillas (San Isidro Matancillas), Jalisco, MX
jgonzalez | Unfamiliar sign-in properties | 3/9/2021 4:06:35 PM | 174.194.186.118 | New York, New York, US
Inicio de sesión desconocidos
Localización
AMÉRICA DEL NORTE
EUROPA
ASIA
Océano Atlántico
ÁFRICA
Bing
Usuarios con más riesgo
Recuento de Nivel de riesgo por Usuario y Situación
Situación [Test Alert]... A program... A user was... Activity fro... Activity fro...
zroquemo
rcarranco
iperezm
enarvaeza
sergio.castillonm
0
10
20
30
Información del usuario
Usuario | Nombre | Puesto | Departamento
gaburto | Aburto Gustavo | Senior Director - Brakes | Brakes Sales
tackerman | Ackerman Ted | Maintenance Lead |
jacostat | Acosta Jonathan | Manufactura | PROD M1 PREVIAS
jacostaa | Acosta Jose | Sindicalizado | PCP Embarques
macostas | Acosta Marisol | Coordinador de Linea | Mat Componentes
Filtros

Results

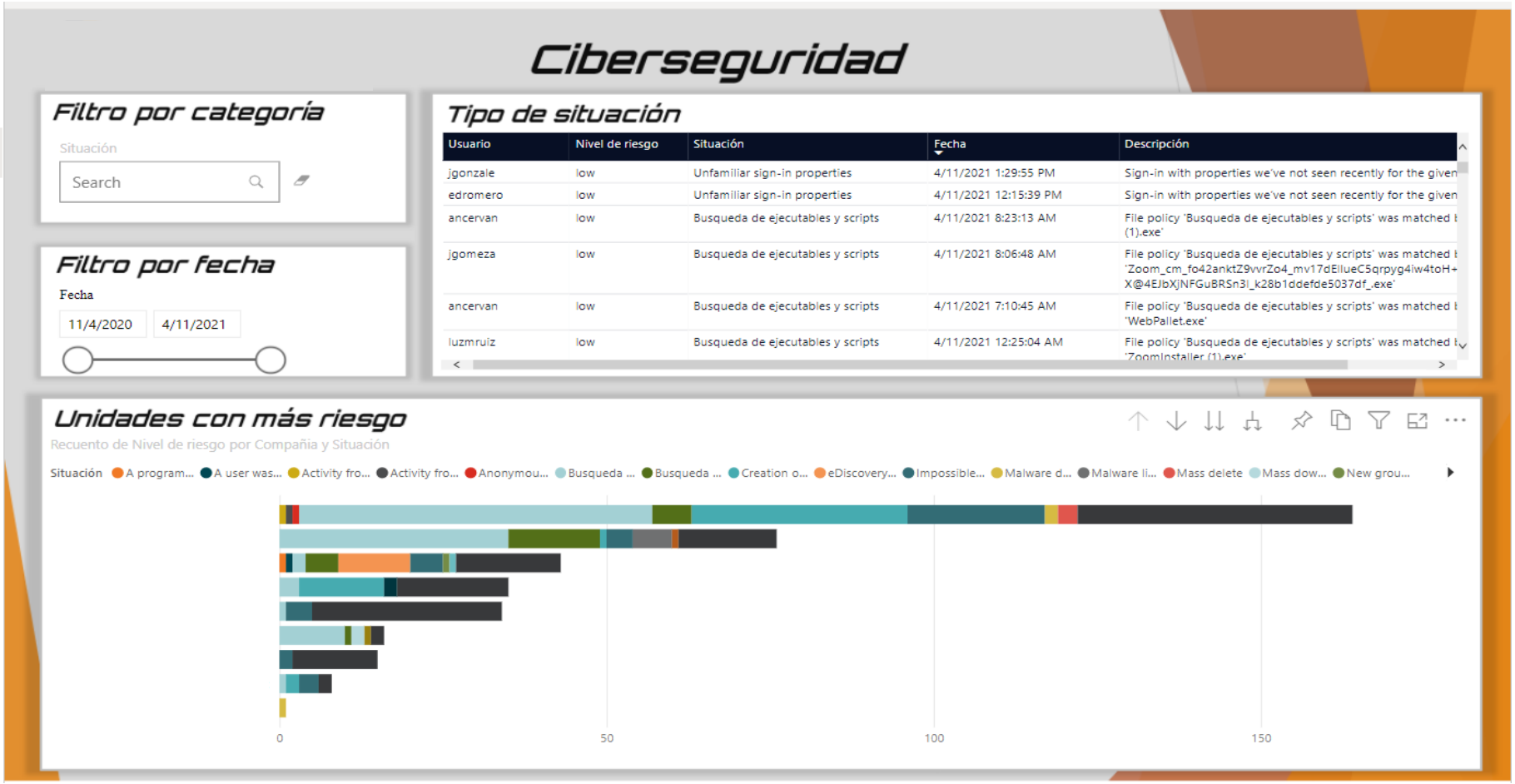

GENERAL
REPORTES
OFICINAS
Ciberseguridad
Filtro por categoría
Situación
Search
Filtro por fecha
Fecha
11/4/2020
4/11/2021
Situaciones mas concurridas
Recuento por Situación y Nivel de riesgo
Nivel de riesgo high low medium
100
0
Reporte de tráfico de email
Recuento de tráfico de emaill por Recuento de tr...
Email messages co...
Email report...
Traffic detected...
Reporte de detecciones de Malware
Recuento de Situación y Primera fecha: Situación p...
5
4
3
2
mar 15
abr 07
Porcentaje de equipos con Cryhod por unidad
Cryhod desplegado
Seleccionar todo
Baja
Desplegado no configurado
NO
NO - Equipo donado
NO - Equipo pruebas
Pendiente de validación
SI
Unidad
Seleccionar todo
RBY
ROC
Recuento y Recuento
0
128
128
Unidad
Usuario responsable
Equipo Asociado
Cryhod desplegado
RBY acaballero RBY-LAP020 SI
RBY atovar RBY-LAP065 SI
RBY axochimitl RBY-LAP057 SI
RBY bpotrero RBY-LAP046 SI
Reporte de detecciones de Spam
Recuento de Spam por Fecha
3 mil
2 mil
1 mil
0 mil
mar 15
abr 09

Results

GENERAL

REPORTES

OFICINAS



Conclusions

Se dispone de un dashboard interactivo donde tenemos información, graficas y reportes a nuestras necesidades.

No hay necesidad de buscar de un portal a otro la información de los usuarios en riesgo.

Interfaz y filtros amigables con el usuario

ECORFAN®