Cybersecurity dashboard

Cuadro de mando de ciberseguridad

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

Universidad Tecnológica de San Juan del Río, Mexico

ID 1st Autor: *Norma Alejandra, Ledesma-Uribe* / **ORC ID:** 0000-0001-8422-2046, **CVU CONACYT ID:** 673202

ID 1st Co-author: *Brenda, Juárez-Santiago* / **ORC ID:** 0000-0001-9071-9243, **CVU CONACYT ID:** 511613

ID 2nd Co-author: *Guillermo, Mendoza-Hermández* / **ORC ID:** 0000-0001-9117-7255, **CVU CONACYT ID:** 1132974

ID 3rd Co-author: *Ricardo, Alvarado-Maldonado* / **ORC ID:** 0000-0003-3004-4306, **CVU CONACYT ID:** 1115883

DOI: 10.35429/JTI.2021.22.8.20.28 Received January 15, 2021; Accepted June 30, 2021

Abstract

The main objective of the present article is to report results gathered from an interactive dashboard application, which main objective is to apply new software and IT technologies to collect information by using several APIS in order to get information and centralize it, then it can be visualized in an interactive dashboard. The methodology used in this project was based mainly by using an specialized software for data analysis which offers an structured an ordered information of data, besides this software also displays alarms that are found in the organization's web pages that are located in cloud services and integrated through Microsoft Azure. In order to weave the different possible attacks which each individual platform could detect such as: malware, authentication bypass, phishing on e-mails, targeted attacks to the companie's virtual machines, malicious ip, etc. The contribution of this project is the integration of several local platforms or those ones located in cloud services serving to SME (Small and medium enterprises) and which are distributed in several branches, either domestic or abroad, then after the interactive dashboard would show live alerts in order to make the correct decisions concerned to cybersecurity issues.

Interactive dashboard, Cybersecurity, Azure

Resumen

El presente trabajo presenta los resultados obtenidos de la aplicación del dashboard interactivo. El cual tiene como objetivo aplicar un nuevo software y tecnologías para la recolección de la información a través de varias API para centralizar la información y poder visualizarla en un tablero interactivo. La metodología de desarrollo se basó principalmente con un software especializado para el análisis de datos, que ofrece una visualización ordenada y estructurada de los datos y alertas encontradas en varios portales de la organización localizados en la nube e integrados a través de Microsoft Azure, para entrelazar los diversos posibles ataques que cada plataforma de manera individual pueda detectar como malware detectado, inicio de sesión desconocidos por parte de los usuarios, phishing en los correos, ataques a máquinas virtuales de la compañía, IP maliciosas, etc. La contribución de este proyecto es la integración de diversas plataformas locales o en la nube que se tienen en muchas pymes, distribuidas en varias sucursales, ya sea en el país o en el extranjero y se puede tener la información y las alertas de manera inmediata para la toma de decisiones relacionadas con la ciberseguridad.

Pizarrón interactivo, Ciberseguridad, Azure

Citation: LEDESMA-URIBE, Norma Alejandra, JUÁREZ-SANTIAGO, Brenda, MENDOZA-HERNÁNDEZ, Guillermo and ALVARADO-MALDONADO, Ricardo. Cybersecurity dashboard. Journal of Technology and Innovation. 2021. 8-22:20-28.

* Correspondence of the Author (Email: nledesma@utsjr.edu.mx)
† Researcher contributing as first author.

Introduction

One of the purpose of new technologies is to give several benefits to society and to final users; it has been accomplished to some extent. New technologies have also created new attractive markets with great growing capabilities. However those capabilities come together with risks almost inherently, therefore not only do we get opportunities but also new threats. (KIPPEO, 2020).

Nowadays many companies undergo cyberattacks and these attacks remain growing, this according to the opinion of more than 750 experts and worldwide decision makers. The 76.1% of these experts indicate that from 2020 on cyberattacks will grow and will be focused to infrastructure, 75 % of these experts also indicate that cyberattacks specialized in getting money and valuable information assets will increase.

According to a report, cyberattacks are in 7th position of a lists of main risks that we will face worldwide in 2020 these risks are also in the 8th position in the level of impact (Blog Smartekh, 2018).

Cybersecurity is the area of informatics that protects IT infrastructure as well as, stored or moving information. In order to protect information cybersecurity uses standards, rules, protocols, methodologies, tools and laws to minimize risks related to infrastructure or information.

According to Kaspersky Lab y B2B International (See Figure1), the average cost of a cybersecurity incident in Latin America continues rising , it is interesting to mention that not only does the average cost increase within companies but also by third parties. Therefore, companies must apply cibersecurity measures to their infrastructures and companies must know how partners deal with cibersecurity issues.

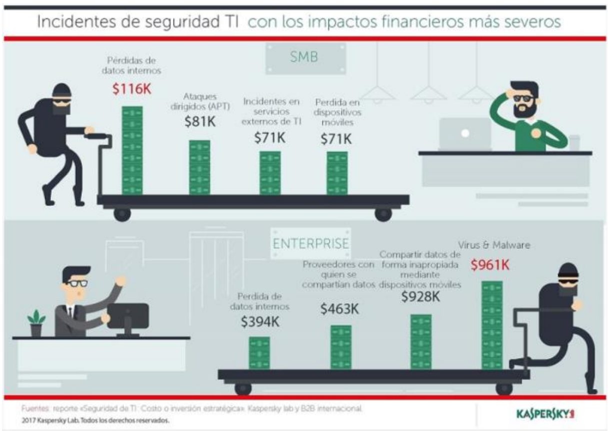


Figure 1 Cibersecurity incidents in 2017
Source: Kaspersky

Nowadays Information is considered as one of the most important assets in an organization and information security as well, informatics security must protect the integrity, confidentiality and availability of information.

Being successful when protecting the 3 basic principles of information, security allows companies to ensure business continuity.

However, the most important asset is corporate reputation. Companies that do not know how manage a cybersecurity incident specially costumers communications and shareholders will undergo a damage in their reputation which is extremely difficult to deal with and recover. A Forbes Insight report indicates that 46% of organizations had already suffered a damage in their reputation and in the value of their brands as a result of an attack. (Sofistic Cybersecurity, 2019).

Informatics security encompasses software (databases, metadata, files), hardware and everything that organizations values and represents risks, if third parties get confidential information then it becomes a privileged information then it could be used against organizations, therefore informatics security is a very important area that must be taken into account by organization to keep safe critical information.

Another topic to consider is data analysis to improve important data visualization for companies; data visualization examines a set of data to make conclusions so that companies can make the best decisions or just to get more information about several topics.

With the development of internet and use of mobile devices in productivity today there is a term used mainly by youngsters called BYOD (Bring your own device) with BYOD young people in an organization prefer to use mobile devices for productivity at work. There are several companies such as Blackberry, Miradore etc, that have already created services and dashboards in order to manage enterprise management mobility (EMM) and BYOD management, EMM services manage applications, data , real time monitoring of users sessions, resources, network monitoring, geolocating, remote destruction of mobile devices, security incidents monitoring, geolocation of stolen equipment, users blocking, users location etc.

EMM services are and excellent tool to protect integrity, confidentiality and availability in information in organizations.

Problem

In most of the SME (Small and medium enterprises) information related to cybersecurity obtained from different sources within the companies is decentralized, that information does not have a proper format, design, or a correct interaction for users, hence it is not possible display information of all areas or branches when a cyberattack occurs.

Justification

By having an interactive cybersecurity dashboard for real time cybersecurity incidents it concentrates information with tailored filters and requested reports for each IT department in every branch, it is also very possible to reduce or eliminate with high precision cyberattacks performed within the organization.

Methodology

Stage methodology proposal with 5 stages:

Stage 1, Licensed Software analysis owned by the company which is: Power BI,Tableau and QlickView

Stage 2, tools comparison and learning curve. It was found that either Tableau or Power BI allows to perform several advanced visualizations which let take the best of data.

It was also found that Tableau is oriented to make tailored analysis performing into a deeper level, whereas Power BI generates powerful dashboards from an executive insight this is due to its great level of integration and compatibility.

A Power BI great feature is that that allows import visualizations that are generated from other users who use the platform. That visualization may be re-used or be adapted into a new report that is being generated.

Stage 3, Using Azure API to chart

Stage 4, Selecting a tool to import data in order to integrate all the dashboard tools, for this case JSON was selected due to its ease of functionality and security.

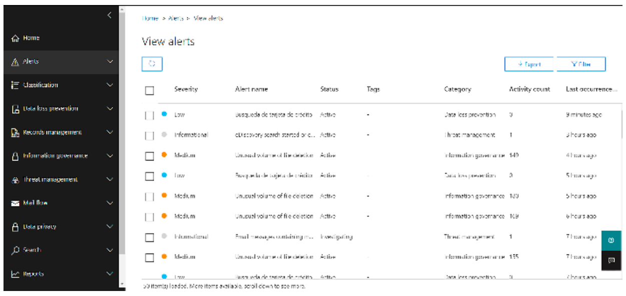
Stage 5, Connecting API with data and JSON integration tools

Development

In order to develop the present project the corresponding cybersecurity topics were applied, to create a specialized dashboard.

Very specific technologies were also used to centralize the information related to cybersecurity, there were also used analysis tools to solve cyberattacks situations that occur within the company and then to come up with immediate solutions to security incidents

In figure 2 we can see the integration of risk events.



	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
□	Low	Busqueda de tarjeta de crédito	Active	-	Data loss prevention	0	9 minutes ago
□	Informational	eDiscovery search started or c...	Active	-	Threat management	1	3 hours ago
□	Medium	Unusual volume of file deletion	Active		Information governance	149	4 hours ago
□	Low	Busqueda de tarjeta de crédito	Active		Data loss prevention	0	5 hours ago
□	Medium	Unusual volume of file deletion	Active	-	Information governance	180	5 hours ago
□	Medium	Unusual volume of file deletion	Active	-	Information governance	169	6 hours ago
□	Informational	Email messages containing m...	Investigating		Threat management	1	7 hours ago
□	Medium	Unusual volume of file deletion	Active		Information governance	155	7 hours ago
	Low	Busqueda de tarjeta de crédito	Active	-	Data loss prevention	0	7 hours ago

50 item(s) loaded. More items available, scroll down to see more.

Figure 2 Visualization of alerts in the application Microsoft Azure Identity Protection web page
Source: own elaboration

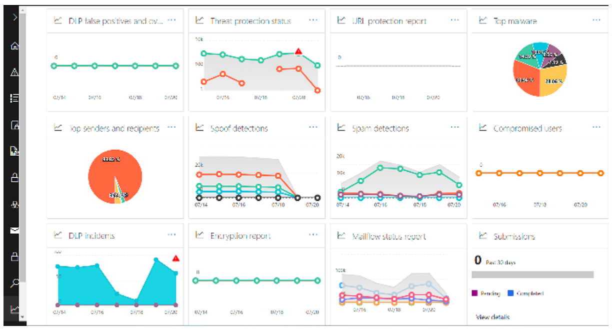
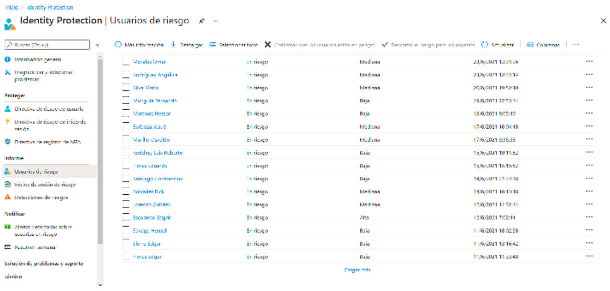


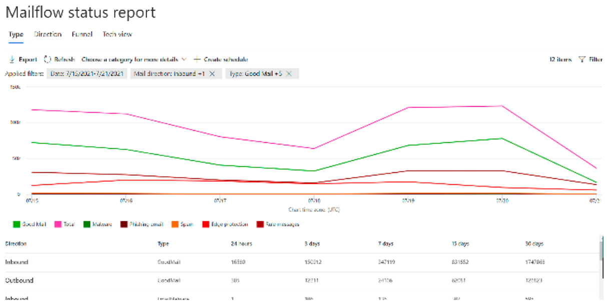
Figure 3 Screen shot from the Application showing charts Microsoft Azure Identity Protection web page
Source: own elaboration

The figure 3, shows the most common cyberattacks with vulnerability rates in real time, where as figure 4 shows a report about users at risk, figure 4 also shows location in facilities and departments, figure 5 shows a report of types of attacks with date and time.


Inicio > Identity Protection
Identity Protection | Usuarios de riesgo
Buscar (Ctrl+/)
Más información
Descargar
Seleccionar todo
Confirmar que los usuarios están en peligro
Descartar el riesgo para los usuarios
Actualizar
Columnas
Información general
Diagnosticar y solucionar problemas
Proteger
Directiva de riesgo de usuario
Directiva de riesgo de inicio de sesión
Directiva de registro de MFA
Informe
Usuarios de riesgo
Inicios de sesión de riesgo
Detecciones de riesgos
Notificar
Alertas detectadas sobre usuarios en riesgo
Resumen semanal
Solución de problemas y soporte técnico
Cargar más

Morales Omar	En riesgo	Mediana	21/6/2021 13:31:26
Rodriguez Angélica	En riesgo	Mediana	21/6/2021 12:11:14
Silva Mario	En riesgo	Mediana	20/6/2021 19:52:10
Murguía Fernando	En riesgo	Baja	19/6/2021 22:53:14
Martinez Nestor	En riesgo	Baja	18/6/2021 8:03:10
Barbosa Josué	En riesgo	Mediana	17/6/2021 10:04:18
Murillo Osvaldo	En riesgo	Mediana	17/6/2021 8:36:58
Redding Luis Roberto	En riesgo	Baja	15/6/2021 19:11:52
Flores Eduardo	En riesgo	Baja	15/6/2021 15:15:52
Santiago Constantino	En riesgo	Baja	14/6/2021 21:27:10
Alexander Rick	En riesgo	Mediana	14/6/2021 16:13:10
Lorenzo Gabriel	En riesgo	Mediana	12/6/2021 11:32:14
Escobedo Edgardo	En riesgo	Alta	12/6/2021 7:02:11
Savage Hanadi	En riesgo	Baja	11/6/2021 18:02:38
Sierra Edgar	En riesgo	Baja	11/6/2021 13:16:42
Flores Edgar	En riesgo	Baja	11/6/2021 11:33:48

Figure 4 Screen shot from the application showing a risk users report from Microsoft Azure Identity Protection web pages
Source: Own elaboration



Direction	Type	24 hours	3 days	7 days	15 days	30 days
Inbound	GoodMail	16550	150312	347119	831552	1747863
Outbound	GoodMail	305	12211	24106	62051	121823
Inbound	[illegible]	1	[illegible]	[illegible]	[illegible]	[illegible]

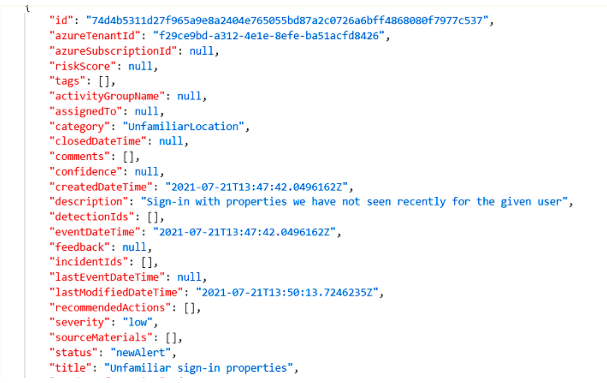
Figure 5 Screen shot from the application showing types of attacks. Microsoft Azure Identity Protection web pages
Source: own elaboration

The company in which this study was applied counts with 4 industrial plants, 200 employees each one, distributed in the Mexican area called the Bajio, 100 employees have access to Microsoft Azure platform, within the same platform there can be found several sections that gather different types of information.

Therefore in the moment in which the person in charge of cybersecurity requires to check any issue related to cybersecurity events has to deal with the problem of accessing an specific section of the platform to get any specific information and then again to visit another section to get that specific information about the same problem once again. A tool was integrated in Azure to make the charts, in the charts it can be displayed data and information obtained from cyberattacks in real time.

With that API it is possible to visualize the information mentioned before in any web browser.

In order to achieve the visualization in any browser the methods HTTP, GET, POST, PUT, DELETE were used. The output format that is obtained only JSON hence, manipulation, storing and processing of information does not require previous treatment for its analysis. See Figure 6 to check the code that was used.



```
{
    "id": "74d4b5311d27f965a9e8a2404e765055bd87a2c0726a6bff4868080f7977c537",
    "azureTenantId": "f29ce9bd-a312-4e1e-8efe-ba51acfd8426",
    "azureSubscriptionId": null,
    "riskScore": null,
    "tags": [],
    "activityGroupName": null,
    "assignedTo": null,
    "category": "UnfamiliarLocation",
    "closedDateTime": null,
    "comments": [],
    "confidence": null,
    "createdDateTime": "2021-07-21T13:47:42.0496162Z",
    "description": "Sign-in with properties we have not seen recently for the given user",
    "detectionIds": [],
    "eventDateTime": "2021-07-21T13:47:42.0496162Z",
    "feedback": null,
    "incidentIds": [],
    "lastEventDateTime": null,
    "lastModifiedDateTime": "2021-07-21T13:50:13.7246235Z",
    "recommendedActions": [],
    "severity": "low",
    "sourceMaterials": [],
    "status": "newAlert",
    "title": "Unfamiliar sign-in properties",
```

Figure 6 reference code to an structured JSON o in Microsoft Graph Explorer
Source: own creation

The methods that were mentioned before make a search of metadata to get an update of the electronic dashboard by using recent data.

In order to review every classified vulnerability it is necessary to make an effective risk analysis, the first step is to identify all the assets within the organization. Those assets include every resource that is used to manage and exchange information within the organization, such as software, hardware, communication devices, digital and analog documents, even human resources must be considered.

Risk analysis requires creating detailed reports about cybersecurity and the several measures applied in the organization. Those reports let us measure the level of success that the organization is undergoing when preventing and mitigating cybersecurity incidents, reports also let us detect weakness or errors that require applying corrective measures.

Talking about these measures, we can stand out the next ones.

- Security software and firewalls installation.

- Automated security systems in the cloud and disaster recovery plans implementation.

- Implementation of security protocols to reinforce security in passwords.

- Implementation and review users roles and policies for minimum privilege.

- Implementation of mirror servers to ensure high availability in the systems, use of alternative systems.

In this study case the electronic dashboard was developed considering the ISO 27001:2015 norm: Information Security Management Systems (ISMS) it is an international norm that allows ensure confidentiality, integrity and availability in data and in information and also in systems that process confidential or sensitive information. Any organization in the world owns sensitive or confidential information that must be protected against cyberattacks that represent a risk or a threat. The information is the most important asset in an organization, one of the main objectives of the norm ISO 27001 is to helps us protect our information assets.

As a solution for the proposal a security dashboard was developed, in the section Security it can filter information related to security incidents as it can be seen in figures 2,3,4 and 5, there it can be shown filtered information in different categories, risk level, status, information destination, security actions and indicators.

For this study case we focused in categories, status and risk level in which cyberattacks can be identified by their filters and policies that are used to classify a type of attack occurring, which office is being affected, users involved or affected in the attack and additional information that is integrated within the cybersecurity dashboard.

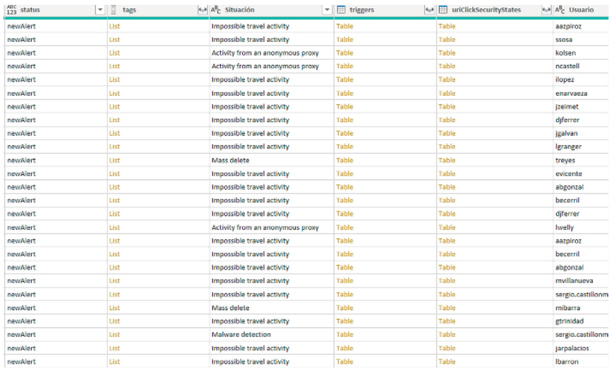
In order to visualize information or online reports on the security dashboard 3 compatibles solutions were analyzed, respecting the main objective of the application: Power BI, Tableau and QlikView. It was found that either Tableau or Power BI allows different advanced visualizations and take the best of data and information.

It was also identified that Tableau is oriented for tailored and deeper data analysis, in the other hand with Power BI it is possible to generate or create more powerful dashboards for executive use it is due to its great integration level and compatibility.

One advantage when using Power BI is that one that allows importing visualizations from other users in the platform, and they (visualizations) can be reused or be adapted in a new report that is being generated.

Once a tool was defined the connection was made by using the exclusively developed API to work with Microsoft Graph Security.

The APPI mentioned before collects information from different platforms and from user’s services such as e-mails, anti-viruses, policies for malware detection. The APPI gives the opportunity to the developers to create their own queries and also to generate reports from scratch, it also allows to know much deeper how the organization’s infrastructure works, this information can be seen in figure 7.



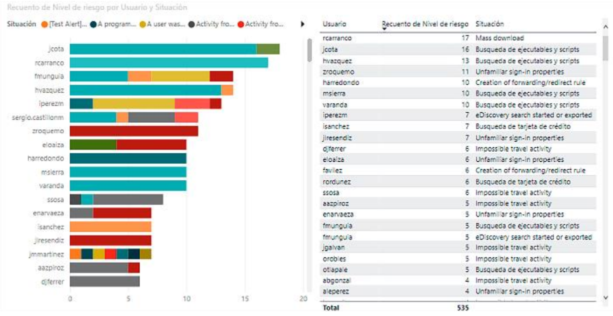
status	tags	Situación	triggers	uriClickSecurityStates	Usuario
newAlert	List	Impossible travel activity	Table	Table	aazpiroz
newAlert	List	Impossible travel activity	Table	Table	ssosa
newAlert	List	Activity from an anonymous proxy	Table	Table	kolsen
newAlert	List	Activity from an anonymous proxy	Table	Table	ncastell
newAlert	List	Impossible travel activity	Table	Table	ilopez
newAlert	List	Impossible travel activity	Table	Table	enarvaeza
newAlert	List	Impossible travel activity	Table	Table	jzeimet
newAlert	List	Impossible travel activity	Table	Table	djferrer
newAlert	List	Impossible travel activity	Table	Table	jgalvan
newAlert	List	Impossible travel activity	Table	Table	lgranger
newAlert	List	Mass delete	Table	Table	treyes
newAlert	List	Impossible travel activity	Table	Table	evicente
newAlert	List	Impossible travel activity	Table	Table	abgonzal
newAlert	List	Impossible travel activity	Table	Table	becerril
newAlert	List	Impossible travel activity	Table	Table	djferrer
newAlert	List	Activity from an anonymous proxy	Table	Table	lwelly
newAlert	List	Impossible travel activity	Table	Table	aazpiroz
newAlert	List	Impossible travel activity	Table	Table	becerril
newAlert	List	Impossible travel activity	Table	Table	abgonzal
newAlert	List	Impossible travel activity	Table	Table	mvillanueva
newAlert	List	Impossible travel activity	Table	Table	sergio.castillonm
newAlert	List	Mass delete	Table	Table	mibarra
newAlert	List	Impossible travel activity	Table	Table	gtrinidad
newAlert	List	Malware detection	Table	Table	sergio.castillonm
newAlert	List	Impossible travel activity	Table	Table	jarpalacios
newAlert	List	Impossible travel activity	Table	Table	lbarron

Figure 7 Screen shot that shows the process for information and data transformation by using Power BI
Source: Power BI application

Power BI offers several types of connections that allow us to make designs, connections and reports for the electronic cybersecurity dashboard where, according to the assigned permissions users can access to the different levels of information.

Once that required information in the dashboard was identified, different charts were chosen, also reports and filters, this according to information requirements, and validations from users in the dashboard for each possible cybersecurity issue.

The figure 5 shows the highest level with 22 recurrences and value of 5 as a minimum vulnerable value.



Usuario	Recuento de Nivel de riesgo	Situación
rcarranco	17	Mass download
jcota	16	Busqueda de ejecutables y scripts
hvazquez	13	Busqueda de ejecutables y scripts
zroquemo	11	Unfamiliar sign-in properties
harredondo	10	Creation of forwarding/redirect rule
msierra	10	Busqueda de ejecutables y scripts
varanda	10	Busqueda de ejecutables y scripts
iperezm	7	eDiscovery search started or exported
isanchez	7	Busqueda de tarjeta de crédito
jiresendiz	7	Unfamiliar sign-in properties
djferrer	6	Impossible travel activity
eloaiza	6	Unfamiliar sign-in properties
favilez	6	Creation of forwarding/redirect rule
rordunez	6	Busqueda de tarjeta de crédito
ssosa	6	Impossible travel activity
aazpiroz	5	Impossible travel activity
enarvaeza	5	Unfamiliar sign-in properties
fmunguia	5	Busqueda de ejecutables y scripts
fmunguia	5	eDiscovery search started or exported
jgalvan	5	Impossible travel activity
orobles	5	Impossible travel activity
otlapale	5	Busqueda de ejecutables y scripts
abgonzal	4	Impossible travel activity
aleperez	4	Unfamiliar sign-in properties
Total	535	

Figure 8 Screen shot of data transformation to charts by using Power BI
Source: Own elaboration

Results

Within the tests and results, it was concluded that the electronic dashboard includes new functions, charts, reports and information that was not found in the other sites. It gives an interactions to what we read, besides it also adds prioritization in an interactive way which allows personal in charge of cybersecurity to locate areas that must be attended and reinforce cybersecurity and mitigate or eliminate attacks that the organization is undergoing.

Besides some other benefits are included:

- Own interactive platform creation.
- Information and data centralization for better cybersecurity management.

- The use of new technologies to display critical information and to be able to interact with data and information that was not possible to visualize in the platforms that were mentioned before.

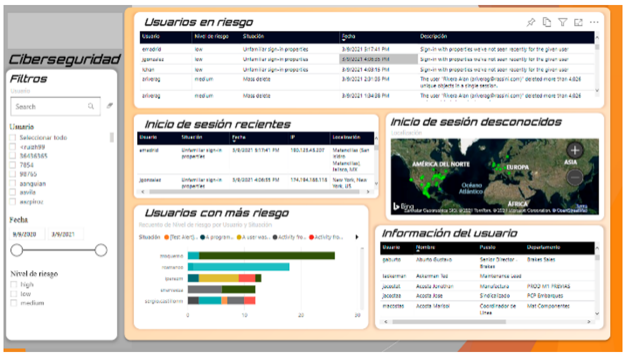
- In the dashboard more precise data is presented that can be used in future audits.

- The electronic dashboard also comes with options that let add more information origin points; it also lets to create an extra relation with information and data that can be used by the company and the people in charge of cybersecurity.

- Analysis and data management is more precise when using tools like the present dashboard.

Figure 9 shows the main screen with the different states of security levels in the organization, in which we can review users at risk separated by date, users, risk level and a description of the current situation. Here we can also check recent and unknown sessions, it helps us locate in which part of the world an unknown session was established.

The dashboard also shows in a chart the exact time the unknown session occurred so that we can see users at higher risk levels in the organization.



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 4:08:55 PM	Sign-in with properties we've not seen recently for the given user
lchan	low	Unfamiliar sign-in properties	3/9/2021 4:08:15 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

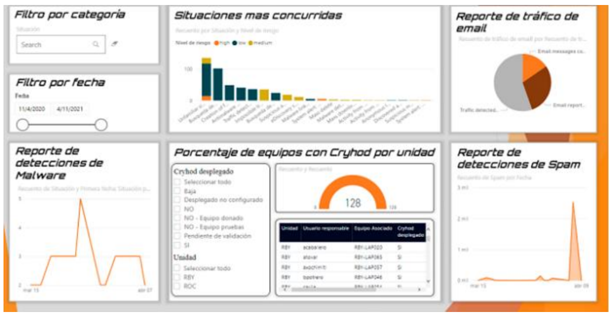
Usuario	Situación	Fecha	IP	Localización
emadrid	Unfamiliar sign-in properties	3/9/2021 5:17:41 PM	[illegible]	Matamoros (San Isidro Matamoros), Jalisco, MX
jgonzalez	Unfamiliar sign-in properties	3/9/2021 4:08:55 PM	174.194.188.118	New York, New York, US

Información del usuario

Usuario	Nombre	Puesto	Departamento
gaburto	Aburto Gustavo	Senior Director - Brakes	Brakes Sales
lackerman	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

Figure 9 Dashboard screen shot at its final state
Source: own elaboration.

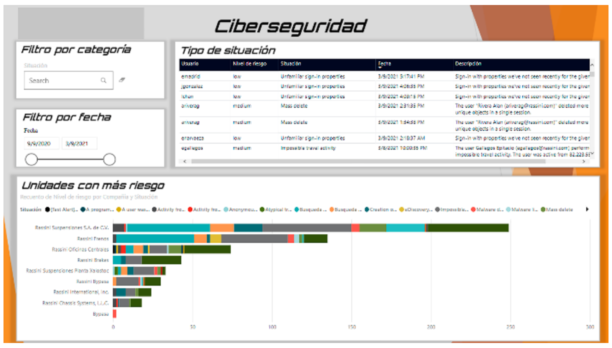
In figure 10 we can see the charts created due to the organizations' need in order to verify weekly and monthly information about cyberattacks that were detected in users, virtual machines, cloud storage, data bases and e-mail service and also being able to review in numbers each one of the situations at risk.


Filtro por categoria
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 email 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
128
Reporte de detecciones de Spam
Recuento de Spam por Fecha
3 mil
2 mil
1 mil
0 mil
mar 15
abr 08

Unidad	Usuario responsable	Equipo Asociado	Cryhod desplegado
RBY	acabiliero	RBY-LAP020	Si
RBY	alovar	RBY-LAP065	Si
RBY	axochimilt	RBY-LAP057	Si
RBY	bpothero	RBY-LAP046	Si

Figure 10 Dashboard screen shot at its final state
Source: Own elaboration

In figure 11 we can see detailed reports for the different offices in the organization, these reports are used to carry out a correct cybersecurity incident management, according to the work areas, in order to get a feedback to each office depending on the risk level exposure.


Ciberseguridad
Filtro por categoria
Situación
Search
Filtro por fecha
Fecha
9/9/2020
3/9/2021
Tipo de situación
Unidades con más riesgo
Recuento de Nivel de riesgo por Compañía y Situación
Situación ● [Test Alert]... ● A program... ● A user was... ● Activity fro... ● Activity fro... ● Anonymou... ● Atypical tr... ● Busqueda ... ● Busqueda ... ● Creation o... ● eDiscovery... ● Impossible... ● Malware d... ● Malware i... ● Mass delete
Rassini Suspensiones S.A. de C.V.
Rassini Frenos
Rassini Oficinas Centrales
Rassini Brakes
Rassini Suspensiones Planta Xalostoc
Rassini Bypasa
Rassini International, Inc.
Rassini Chassis Systems, LLC.
Bypasa
0
50
100
150
200
250
300

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 giver
jgonzalez	low	Unfamiliar sign-in properties	3/9/2021 4:06:35 PM	Sign-in with properties we've not seen recently for the giver
lchan	low	Unfamiliar sign-in properties	3/9/2021 4:03:15 PM	Sign-in with properties we've not seen recently for the giver
ariverag	medium	Mass delete	3/9/2021 2:31:35 PM	The user "Rivera Alan (ariverag@rassini.com)" deleted more unique objects in a single session.
ariverag	medium	Mass delete	3/9/2021 1:54:35 PM	The user "Rivera Alan (ariverag@rassini.com)" deleted more unique objects in a single session.
enarvaeza	low	Unfamiliar sign-in properties	3/9/2021 2:18:37 AM	Sign-in with properties we've not seen recently for the giver
egallegos	medium	Impossible travel activity	3/8/2021 10:00:55 PM	The user Gallegos Epitacio (egallegos@rassini.com) perform impossible travel activity. The user was active from 82.223.5

Figure 11 Screen shot with information per office
Source: own elaboration

Conclusions

At the end of the development of the present project we conclude, that it contributed with new opportunities to create reports and also using the information and data that was never used for cybersecurity main objectives within the organization.

By having an electronic dashboard, the organization has total control over the different risks and cyber threats that occur day by day. The dashboard also lets us make a more detailed analysis of how cyberattacks occur and how to avoid them.

The electronic dashboard creates a new way to depict data through Power BI software. Data analysis is a very powerful tool that is currently being developed all together with new IT technologies.

Data analysis also helps the organization to better organize data and information in order to make better decisions. Converting data from the application into visual.

Turning data from the application into visual representations helps employees to describe concepts, discover areas of opportunity, explore options and to make the best decisions everything carried out in a persuasive way.

Virtual supports are necessary to help people make the best decisions.

Cybersecurity is a topic affects everybody in the same way either by having just an e-mail or by managing an entire web site with sensitive information.

It just a failure in the chain that can compromise our security systems, therefore organizations should always attend security information recommendations to avoid major problems.

References

Avansis. (November 11th 2019) . *avansis.es*. Obtained from What is cibersecurity?: https://www.avansis.es/ciberseguridad/que-es-ciberseguridad/

Barrera, A. (February 19th , 2018). *next_u*. Obtained from What is json?: https://www.nextu.com/blog/que-es-json/

BBVA. (August 2016). *BBVA API_Market*. Obtained from Radiography of an API Hows does an APPI really work?: https://www.bbvaapimarket.com/es/mundo-api/radiografia-de-una-api-como-funciona-realmente/

Blog Smartekh. (October 1st., 2020). *Marketing*. Obtained from an effective cibersecurity strategy : https://blog.smartekh.com/-pasos-para-una-estrategia-de-ciberseguridad

Camprovin, C. (June 27th., 2019). *Ibermatica365.com*. Obtained from Power B everything you need to know about microsoft power bi: https://www.ibermatica365.com/todo-lo-que-siempre-quisiste-saber-sobre-microsoft-power-bi/

Cisco. (January 27th 2019). *Security* Obtained from What is ciber security? https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Del Medico, F. (March 2nd. 2020). *Maplink*. Obtained from how to use APIS: https://maplink.global/es/blog/como-usar-apis/#:~:text=API%20es%20el%20acr%C3%B3nimo%20utilizado,a%20sitios%20web%20y%20aplicaciones.

Empey, C. (February 28th., 2018). *Avast blog*. Obtained from a basic guide of ranssomware and how to get protected: https://blog.avast.com/es/guia-basica-sobre-el-ransomware-y-como-protegerse

Grupo Bit Analytics. (February 16th., 2019). *bussiness-intelligence.grupobit.net*. Obtained from data analysis : https://business-intelligence.grupobit.net/blog/que-es-el-analisis-de-datos-y-como-funciona

Hewlett Packard Enterprise. June 7th., 2018). *HPE.COM*. Obtained from What is cloud infraestructure ?: https://www.hpe.com/mx/es/what-is/cloud-infrastructure.html#:~:text=%C2%BFQu%C3%A9%20es%20la%20infraestructura%20de%20la%20nube%20como%20servicio%3F,que%20se%20pueden%20escalar%20f%C3%A1cilmente.

infosecurity. (April 4th., 2017 . *Cibersecurity obtained from cibersecurity history* : https://www.infosecuritymexico.com/es/ciberseguridad.html

kaspersky. (July 14th., 2019). *Definitions*. Obtained from What is cibersecurity ?: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KIPPEO. (May 28th 2020). *Cibersecurity*. Obtained from ¿Do you know the consequences of data theft?: https://kippeo.com/conoces-las-consecuencias-del-robo-de-datos-2/

Lanz, L. (May 22nd., 2018). *openwebinars.net*. Obtained from What is cibersecurity?: https://openwebinars.net/blog/que-es-la-ciberseguridad/

Martínez, J. M. (April 11th., 2012). *clavei*. Obtained from analitics in business: https://www.clavei.es/blog/que-es-qlikview-hablando-de-business-intelligence/

Microsoft. (July 12th. ,2016). *powerbi.microsoft.com*. Obtained from What is Power BI ?: https://powerbi.microsoft.com/es-es/what-is-power-bi/

Microsoft. (July 5th. ,2020). *Microsoft Docs*. Obtained from What is Azure Active Directory?: https://docs.microsoft.com/es-mx/azure/active-directory/fundamentals/active-directory-whatis

Microsoft. (September 29th. , 2020). *Microsoft Graph*. Obtained from general information, Microsoft Graph: https://docs.microsoft.com/es-es/graph/overview

pandasecurity. (February 21st. ,2016). *pandasecurity.com*. Obtained from 10 advices to avoid phishing attacks : https://www.pandasecurity.com/es/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

Pastorino, C. December 6th. , 2017). *welivesecurity.com*. Obtained from Budapest agreementg : benefits and implications for informatics security : https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

PowerData. (March 19th. ,2016 obtained from Que son los metadatoswhat is metadata? https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/que-son-los-metadatos-y-cual-es-su-utilidad

Qlik. (April 21st. , 2020). *Qlikview*. Obtained form What is QlikView?: https://help.qlik.com/es-ES/qlikview/April2020/Content/QV_HelpSites/what-is.htm

QuestionPro. (January 13th. ,2018). *questionpro.com*. Obtained from data analysis: https://www.questionpro.com/es/analisis-de-datos.html

Red Hat. (March 24th. ,2020). *CLOUD COMPUTING*. Obtained from What is cloud infraestructure ?: https://www.redhat.com/es/topics/cloud-computing/what-is-cloud-infrastructure

Red Hat. (June 17th. 2020). *Red HAT*. Obtained from What are application programming interfaces: https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Rodríguez, A. (October 10th. , 2020). *aprendeaprogramar.com*. Obtained from What is JSON and how does it work for ?: https://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=956:ique-es-y-para-que-sirve-json-especificacion-oficial-javascript-object-notation-diferencia-de-xml-cu01213f&catid=83&Itemid=212

SOFISTIC CYBERSECURITY. (November 30th., 2019 obtained from a brief history of cibersecurity : https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

Tecon. (June 18th., 2019). *informatics solutions* . Obtained from What is Microsoft Azure? How does it work ?: https://www.tecon.es/que-es-microsoft-azure-como-funciona/

Tecon. (December 13th., 2019). *informatics solutions Tecon I* Obtained from types of cloud infraestructure : laaS, PaaS and Saas: https://www.tecon.es/infraestructura-cloud-iaas-paas-y-saas/

Westreicer, G. (August 14th., 2020). *Economipedia.com*. Obtained from data analysis : https://economipedia.com/definiciones/analisis-de-datos.html