

---

# **Creando una Trayectoria Profesional en Seguridad Digital**

## *Laboratorio 3: Gestión de incidentes*

Agosto, 2021

## Índice

<b>1. Laboratorio 3</b>	<b>3</b>
1.1. Laboratorio 3A . . . . .	3
1.2. Laboratorio 3B . . . . .	11

## 1. Laboratorio 3

### Acerca del Laboratorio 3

**Objetivos:** *Reporte y cadena de incidentes.*

**Requerimientos:**

- Utilice la máquina virtual en la nube establecidas para el curso con la plataforma [MISP](#)
- Utilice la cuenta generada en la herramienta de análisis de amenazas en tráfico de red [CloudShark](#).

Credenciales de acceso para la GUI de MISP:

- Email: admin@admin.test
- Password: Password1234

### 1.1. Laboratorio 3A

1. Inicie sesión en la herramienta de análisis amenazas en tráfico de red [CloudShark](#)
2. Añada la captura de paquetes de red `oea-labs.pcap` contenida en la carpeta de la nube [Laboratorio 3](#). Después arrastre la captura en la opción *Drag & Drop Files*

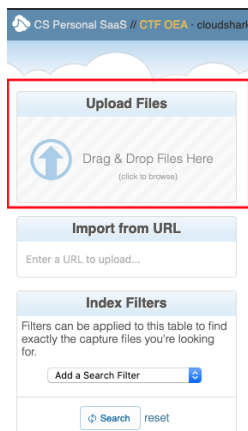


Figura 1:

3. Compruebe que las capturas se hayan añadido correctamente en la herramienta

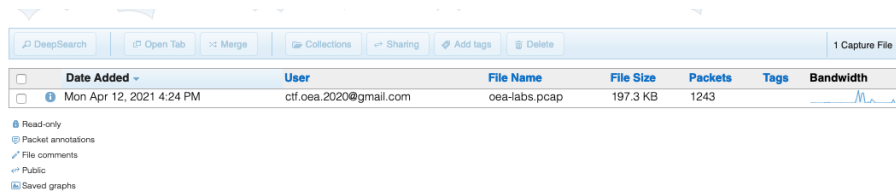


Figura 2:

4. Filtre las conversaciones mediante el protocolo HTTP e identifique los puntos de acceso de la conversación de red: *Analysis Tools/ Network Endpoints*.

Viewing 5 **ipv4** Endpoints for oea-labs.pcap

Address	Packets	Bytes	Tx Packets	Rx Packets	Tx Bytes	Rx Bytes	Country	City	AS Number	AS Organization	Latitude	Longitude
172.31.38.46	1239	181941	575	664	107709	74232	Mexico	Mexico City	17072	TOTAL PLAY TELECOMUNICACIONES SA DE CV	19.4358	-99.1441
187.189.215.229	1216	179019	653	563	72857	106162						
172.31.0.2	4	397	2	2	249	148						
3.142.167.4	17	1593	8	9	536	1057	United States	Columbus	16509	AMAZON-02	39.9625	-83.0061
172.31.32.1	2	932	1	1	590	342						

[GeoIP Map](#)
[Open in new window](#)
[Done](#)

Figura 3:

**¿Qué observa en relación de los paquetes transmitidos (Tx) y recibidos (Rx)**

**¿Se muestran proveedores de servicios de Internet?**

**¿Se muestran locaciones geográficas de las comunicaciones?**

5. Filtre el mapa geográfico de los paquetes enviados *Analysis Tools/ GeoIP World Map*. Después, filtre *Map Data/Total Packets*

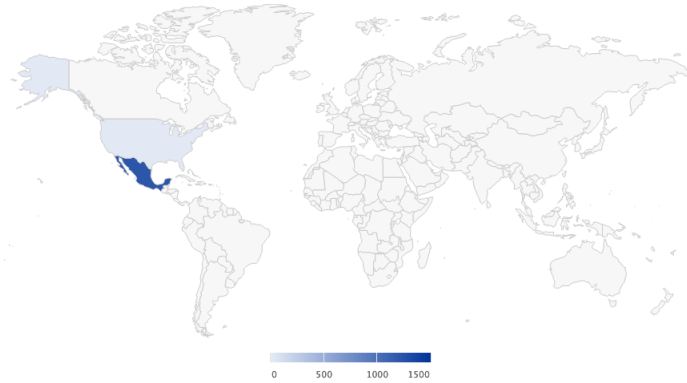
GeoIP World Map for [oea-labs.pcap](#)Map Data: Total Packets 

Figura 4:

**¿Se muestra el envío de más paquetes de una sola locación?****¿Será un comportamiento anormal?**

6. Observe la longitud de los paquetes

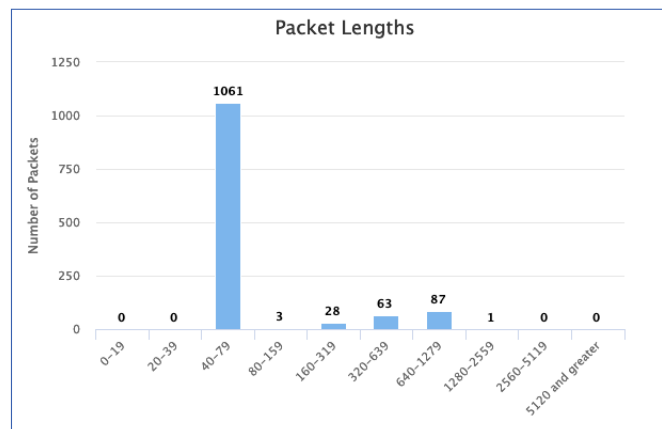


Figura 5:

**¿Los paquetes de longitud mayor a un tráfico regular indican un posible ataque?**7. Realice un gráfico (*Graphs/Current Display Filter*) con el filtro `http` para visualizar el comportamiento del tráfico

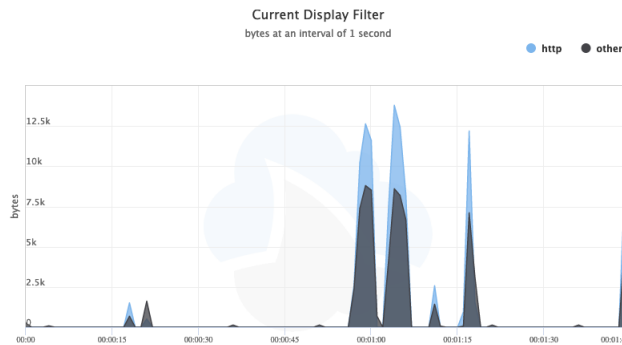


Figura 6:

**¿Qué observa en relación a los picos (en cantidad de bytes) de mensajes por el protocolo HTTP? ¿Será esto un indicador de inyección SQL?**

8. En la pestaña *Analysis Tools/ Threat Assessment*, despliegue la evaluación del riesgo como se muestra en la siguiente Figura

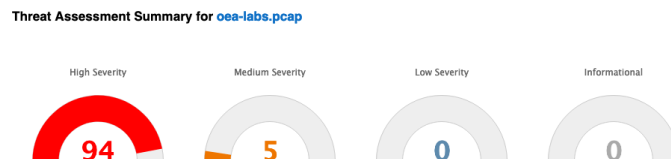


Figura 7:

9. En la pestaña del resumen *Threat Assessment Summary* despliegue el análisis avanzado (*Open Advanced Analysis*).

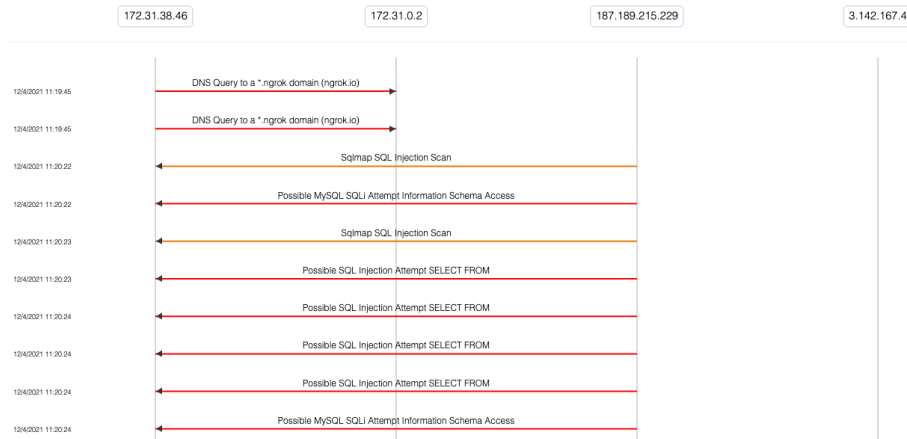


Figura 8:

### ¿Qué tipo de amenazas fueron detectadas?

- En el panel superior derecho, despliegue las estadísticas de las amenazas detectadas y observe las categorías y firmas de comportamiento detectadas



Figura 9:



Figura 10:

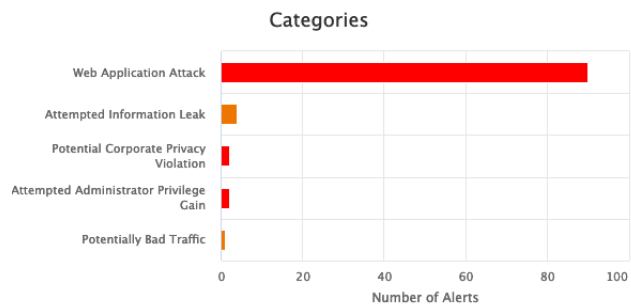


Figura 11:



Figura 12:

11. En la pestaña *Table view* liste la tabla de alertas detectadas y observe las categorías, conjunto de reglas, firmas y severidad del paquete



## 1.1 Laboratorio 3A

Relative Time	Packet	Source	Source Port	Destination	Dest Port	Category	Rule Set	Signature	Severity
21.0	22	172.31.38.46	49068	172.31.0.2	53	Potential Corporate Privacy Violation	ET POLICY	DNS Query to a *.ngrok domain (ngrok.io)	1
21.0	23	172.31.38.46	49068	172.31.0.2	53	Potential Corporate Privacy Violation	ET POLICY	DNS Query to a *.ngrok domain (ngrok.io)	1
58.0	100	187.189.215.229	20721	172.31.38.46	80	Attempted Information Leak	ET SCAN	Sqlmap SQL Injection Scan	2
58.0	59	187.189.215.229	20718	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt SELECT FROM	1
58.0	59	187.189.215.229	20718	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt UNION SELECT	1
58.0	59	187.189.215.229	20718	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Script tag in URI Possible Cross Site Scripting Attempt	1
58.0	59	187.189.215.229	20718	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Attempt To Access MSSQL xp_cmdshell Stored Procedure Via URI	1
58.0	59	187.189.215.229	20718	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible MySQL SQLi Attempt Information Schema Access	1
59.0	130	187.189.215.229	20723	172.31.38.46	80	Attempted Information Leak	ET SCAN	Sqlmap SQL Injection Scan	2
59.0	220	187.189.215.229	20729	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt SELECT FROM	1
60.0	287	187.189.215.229	20734	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt SELECT FROM	1
60.0	298	187.189.215.229	20736	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt SELECT FROM	1
60.0	329	187.189.215.229	20737	172.31.38.46	80	Web Application Attack	ET WEB_SERVER	Possible SQL Injection Attempt SELECT FROM	1

Figura 13:

12. Siga uno de los paquetes dando click al número del mismo. En la ventana de de-codificación del protocolo ingrese a la pestaña *Follow TCP/Follow UDP* dependiendo el caso



Figura 14:

Observe el payload de inyección de SQL enviado al servidor



## 1.2. Laboratorio 3B

### ¿Qué es MISP?

Malware Information Sharing Platform (MISP) es una plataforma de código abierto que permite almacenar, guardar y correlacionar indicadores de compromiso de ciber-ataques, inteligencia e amenazas, información de fraude e taxonomías de vulnerabilidades. Gran parte de sus bases de datos tienen como fundamento las categorías propuestas por el marco de trabajo [MITRE ATT&CK](#). Una vez identificada una amenaza, será necesario modelarla y publicarla de manera colaborativa para que otros centros de respuesta a incidentes puedan observar el comportamiento y tomar decisiones oportunas.

[Hoja de códigos de la herramienta.](#)

1. Acceder al siguiente reporte de Actividad Maliciosa, en relación al ransomware `ryuk.exe` para el sistema operativo Windows: [Ryuk | Malware Trends Tracker](#). Puede de manera adicional observar el diagrama de [procesos interactivos](#)

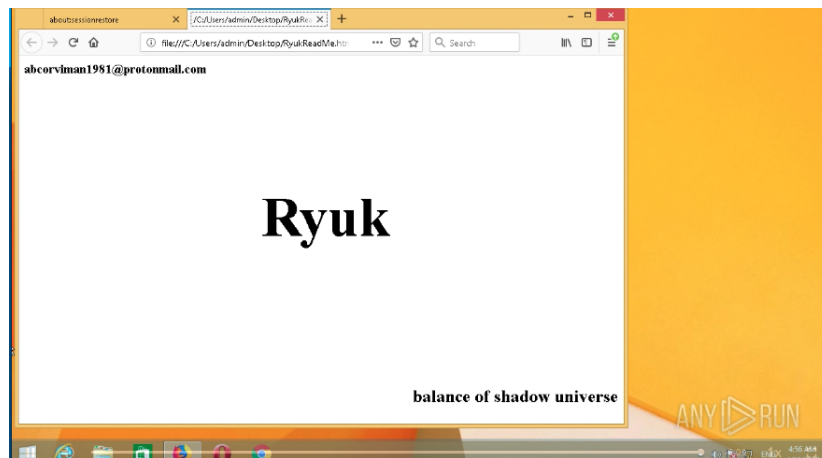


Figura 17:

2. Inicie sesión en la interfaz gráfica en la herramienta de Inteligencia de Amenazas MISP
3. Añada un evento con el reporte de actividad maliciosa.

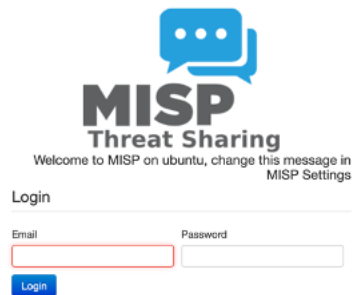


Figura 18:

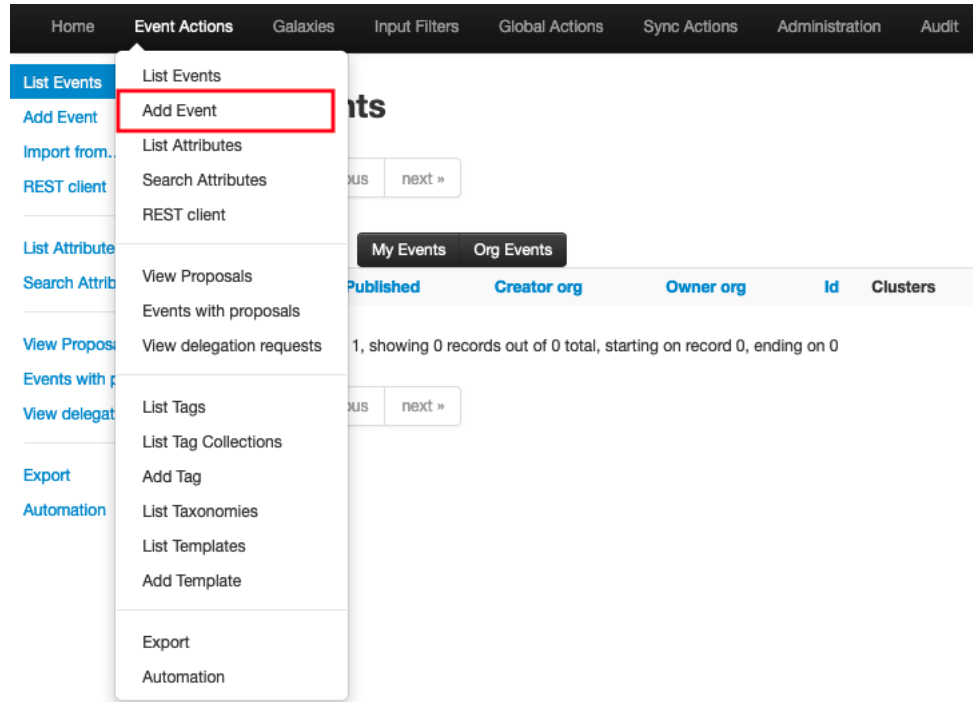


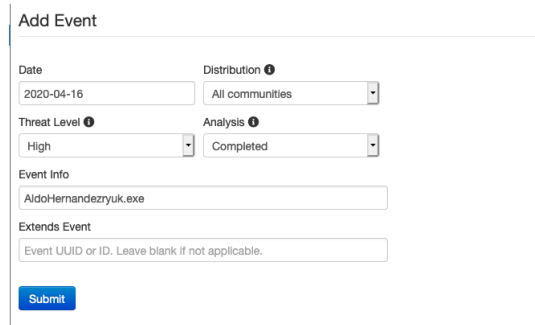
Figura 19:

4. Observe el reporte y añada los datos obtenidos del mismo:

- **Date:** 4/16/2020, 11:51:00 ¿Cuándo se creó?
- **Distribution:** All Comunités ¿Qué comunidades del MISP po-

drán recibir el reporte?

- **Threat Level:** Alto ¿Qué nivel de riesgo tiene? [Ver nivel de riesgo de Microsoft](#)
- **Event Info:** NombreApellidosryuk.exe ¿Qué nombre tiene el reporte?



Add Event

Date: 2020-04-16 Distribution: All communities

Threat Level: High Analysis: Completed

Event Info: AldoHernandezryuk.exe

Extends Event: Event UUID or ID. Leave blank if not applicable.

Submit

Figura 20:

## 5. Comprobar el estado del evento

### AldoHernandezryuk.exe







Event ID	2
UUID	b4be5e1a-396a-4f1c-9f6f-2dbac8d265aa +
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Tags	 +  +
Date	2020-04-16
Threat Level	High
Analysis	Completed
Distribution	All communities  
Info	AldoHernandezryuk.exe
Published	No
#Attributes	0 (0 Object)
First recorded change	
Last change	2021-04-17 21:00:30
Modification map	
Sightings	0 (0) - restricted to own organisation only. 

Figura 21:

Observe que el evento se ha añadido pero no está publicado. Ingrese a la pestaña *Event Actions* y compruebe que el evento ya se encuentre listado

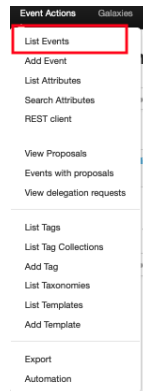


Figura 22:

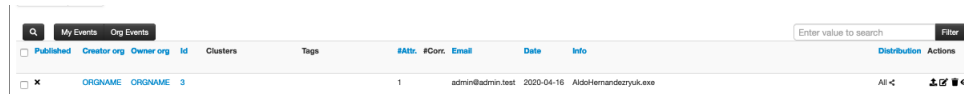


Figura 23:

6. Ingrese al evento y dirjase a la pestaña de acciones, seleccione la pestaña *Galaxy*. Una *Galaxy* es un método para expresar un objeto que puede ser añadido a los eventos de MISP, estos están basados en vocabularios de estándares como [STIX \(Structured Threat Information Expression\)](#), [VERIS](#) y como se ha mencionado anteriormente del [MITRE ATT&CK](#)

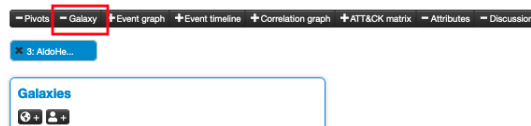


Figura 24:

Ingrese al icono *Add a tag* y seleccione *Attack Pattern*. Visualice las opciones correspondientes y seleccione aquellas que respondan:



ejecutables, solicitudes de DNS, comunicación a Centro de Control y Comando (C & C) etc. Ingrese otra vez al evento creado, en panel izquierdo seleccione *Add Attribute*

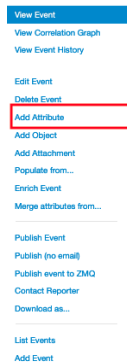


Figura 28:

Del reporte generado por `any .run` desplácese hasta la sección *Dropped Files*. Observe los procesos con PIDs 3344 y 73212. **¿Un ransomware necesitará la descarga de más archivos en el host infectado?**

## Dropped files

PID	Process	Filename	Type
3344	ryuk.exe	C:\Users\admin\AppData\Local\Temp\NpdOrMrlHlan.exe	executable
		MD5: 6BFDA9EF91AF32C3D47C521C5AAEA618 SHA256: D6E66598876136C507AADF10929E663F3CE109D1B	
3344	ryuk.exe	C:\Users\admin\AppData\Local\Temp\zCbTzvOfElan.exe	executable
		MD5: 6BFDA9EF91AF32C3D47C521C5AAEA618 SHA256: D6E66598876136C507AADF10929E663F3CE109D1B	
73212	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\virk3p2gvi.default\prefs.js	text
		MD5: 7C2BC558DDC9168B36653CF321DA10D1 SHA256: C1D95D903A3C7CD081B7AA0A3613D9A696852975E	

Figura 29:

Seleccione alguno de los tres atributos y complete la información solicitada:

- **Category** es la categoría del objeto detectado: *Artifacts dropped* ya que se descargan más archivos maliciosos
- **Type** es la firma *hash* descrita por el reporte. Como no puede existir más de una firma igual seleccione *other* y añada la firma *hash* correspondiente en el campo *Value*, agregando sus iniciales al final de la cadena. Por ejemplo:  
6bfd9ef91af32c3d47c521c5aaea618AHS.



## 1.2 Laboratorio 3B

Después agregue el nombre del artefacto malicioso en el campo *Contextual Comment*, por ejemplo:

C: \Users\admin\AppData\Local\Temp\NpdQrMr1Hlan.exe

- **For intrusion Detection System:** permitirá que la información puede ser utilizada como firma por un dispositivo perimetral de defensa como IPS (Intrusion Prevention System) o IDS (Intrusion Detection System)
- **Batch import:** si existen muchos atributos parecidos, cada uno será procesado de forma *batch*
- **Disable correlation:** en caso de que el atributo tenga diferentes correlaciones con otros, se hará más eficiente la importación en caso de que existan muchos

Figura 30:

Confirme si el atributo se añadió correctamente

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2021-04-16		Artifacts dropped	other	d6e6598876136c507aadf10929e663f3ce109d1bc2ef88e3b02cc939458c450AHS			C:\Users\admin\AppData\Local\Temp\NpdQrMr1Hlan.exe								

Figura 31:

- El reporte está listo para ser publicado y diseminado como un nuevo *feed* de alerta de incidentes. De nuevo dirijase al panel izquier-

do del evento. Seleccione *Publish (no-email)* y observe el nuevo estado del evento.

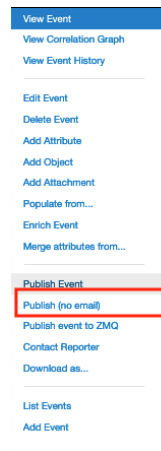


Figura 32:









AldoHernandezryuk.exe	
Event ID	3
UUID	718c743e-724c-4509-add0-234533cbb2ad 
Creator org	<a href="#">ORGNNAME</a>
Owner org	<a href="#">ORGNNAME</a>
Creator user	admin@admin.test
Tags	  
Date	2020-04-16
Threat Level	High
Analysis	Completed
Distribution	All communities  
Info	AldoHernandezryuk.exe
Published	Yes (2021-04-18 18:41:47)
#Attributes	1 (0 Object)
First recorded change	2021-04-18 18:41:24
Last change	2021-04-18 18:41:24
Modification map	
Sightings	0 (0) - restricted to own organisation only. 

Figura 33: