LAC4

Latin America and Caribbean Cyber Competence Centre

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

QUIÉN SOY

NOMBRE DE USUARIO:
OSCAR ENCARNACIÓN LIZ

A QUÉ ME DEDICO:
INGENIER(O) EN CIBERSEGURIDAD

QUÉ ME APASIONA:
BLUE TEAM & SEGURIDAD DE LA INFORMACIÓN

EN QUÉ ME ESPECIALIZO:
GENERACIÓN DE INTELIGENCIA OBTENIDA A TRAVÉS DE PROCESOS DE CRAWLING, ANÁLISIS Y CORRELACIÓN DE DATOS MASIVOS SOBRE AMENAZAS.

EN QUÉ ME ESPECIALIZO:
PERFIL MULTIDISCIPLINAR CON CONOCIMIENTOS SOBRE ADMINISTRACIÓN DE SISTEMAS, REDES Y LENGUAJES DE PROGRAMACIÓN Y CIBER INTELIGENCIA.

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

PROYECTO

EU CYBERNET

EU CYBERNET SE PUSO EN MARCHA EN

SEPTIEMBRE DE 2019

CON EL OBJETIVO DE FORTALECER LA EJECUCIÓN, LA COORDINACIÓN Y LA COHERENCIA GLOBAL DE LOS PROYECTOS EXTERNOS DE CREACIÓN DE CAPACIDAD CIBERNÉTICA DE LA UE Y REFORZAR LA PROPIA CAPACIDAD DE LA UE PARA PROPORCIONAR ASISTENCIA TÉCNICA A TERCEROS PAÍSES EN EL ÁMBITO DE LA CIBERSEGURIDAD Y LA CIBERDELINCUENCIA.

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

EN DICIEMBRE DE 2020

LA COMISIÓN EUROPEA ENCARGÓ A EU CYBERNET PARA QUE LIDERE LA CREACIÓN DE UN CENTRO REGIONAL DE CIBERCAPACIDADES EN LA REPÚBLICA DOMINICANA PARA PERMITIR UNA CREACIÓN DE CAPACIDAD MÁS ESPECÍFICA Y SISTEMÁTICA EN LA REGIÓN DE AMÉRICA LATINA Y EL CARIBE.

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

METODOLOGÍA OPERATIVA DE UNA CIBER INVESTIGACIÓN

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

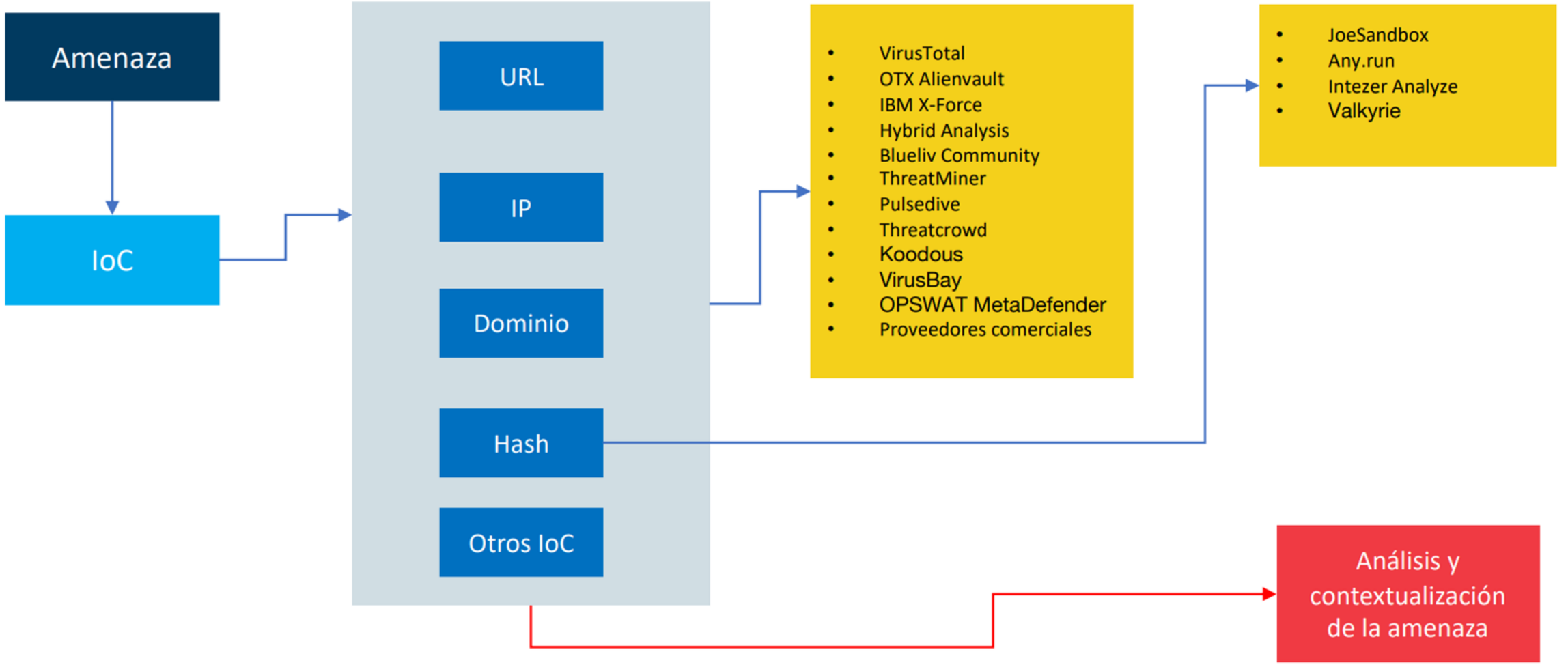
LAC4
Latin America and Caribbean Cyber Competence Centre

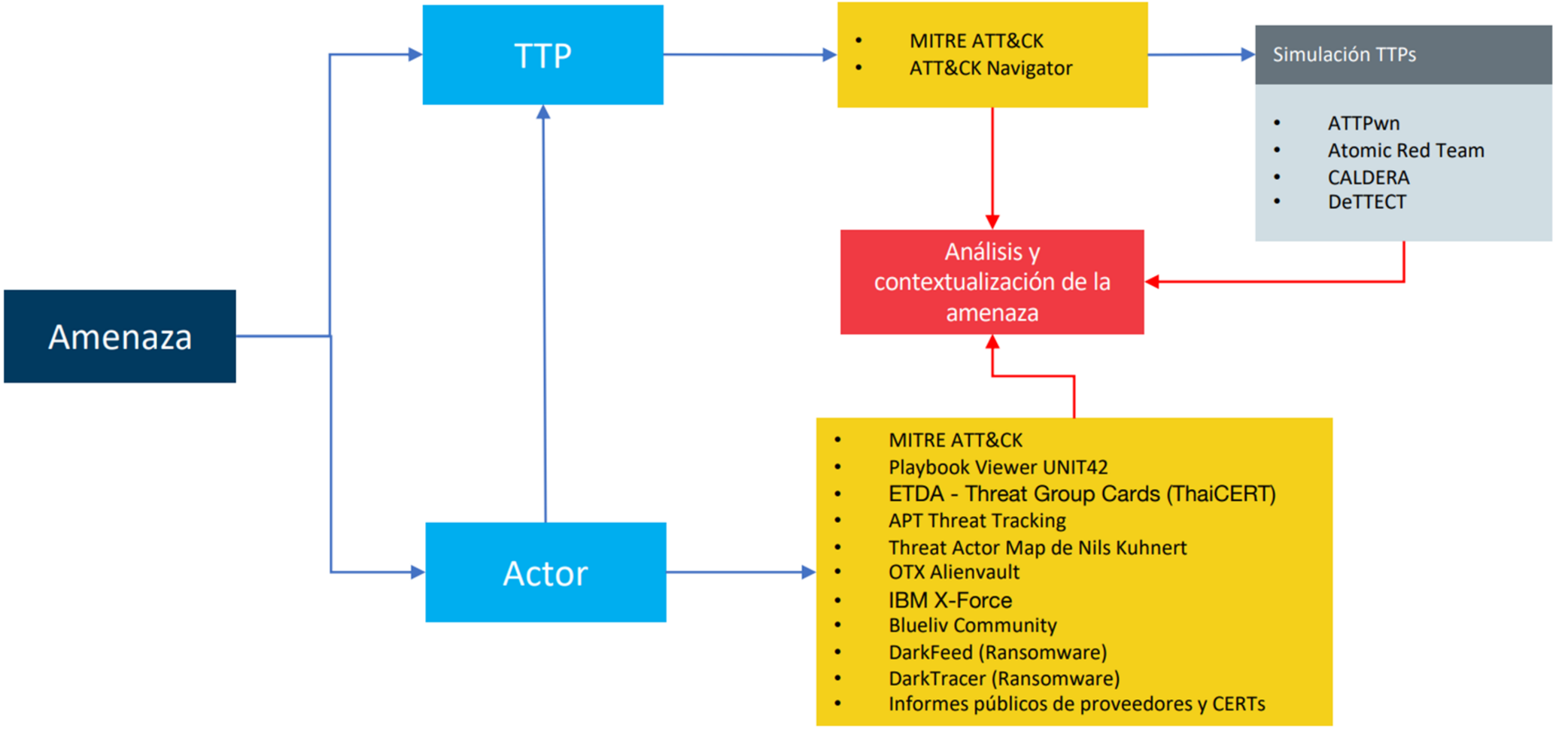
CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

METODO Y CONTEXTO DE LA AMENAZA

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**


Amenaza
IoC
URL
IP
Dominio
Hash
Otros IoC
VirusTotal
OTX Alienvault
IBM X-Force
Hybrid Analysis
Blueliv Community
ThreatMiner
Pulsedive
Threatcrowd
Koodous
VirusBay
OPSWAT MetaDefender
Proveedores comerciales
JoeSandbox
Any.run
Intezer Analyze
Valkyrie
Análisis y contextualización de la amenaza


TTP
MITRE ATT&CK
ATT&CK Navigator
Simulación TTPs
ATTPwn
Atomic Red Team
CALDERA
DeTTECT
Análisis y contextualización de la amenaza
Amenaza
Actor
MITRE ATT&CK
Playbook Viewer UNIT42
ETDA - Threat Group Cards (ThaiCERT)
APT Threat Tracking
Threat Actor Map de Nils Kuhnert
OTX Alienvault
IBM X-Force
Blueliv Community
DarkFeed (Ransomware)
DarkTracer (Ransomware)
Informes públicos de proveedores y CERTs

MODELADO DE AMENAZAS

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

Los feeds

MITRE ATT&CK · ALIEN VAULT · DarkFeed · Google Custom Search Engine · CISA · CCN-CERT centro criptológico nacional · ANSSI · CROWDSTRIKE · FireEye · VIRUSTOTAL · DarkTracer · malpedia · TREND MICRO · paloalto NETWORKS · FORTINET · redcanary · SOPHOS

1

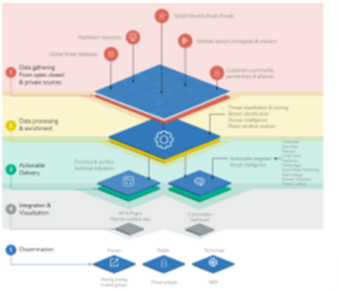
Obtención / Colección de los datos sobre amenazas consultando:

- API feed
- RSS feed
- Blog feed

Procesamiento de datos XML,JSON, TXT, PDF ..

2

PDF Threat reports



blueliv.com

Información

Analizar / Normalizar la información en un formato adecuado para el análisis:

- Estándar
- Trazabilidad
- La autoría
- Traffic Light Protocol (TLP)
- Intercambio y correlación
- Visualización

STIX™

¿Contexto?

¿Accionable?

Analista

3

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

LAC4 Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA

CSIRT-RD Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

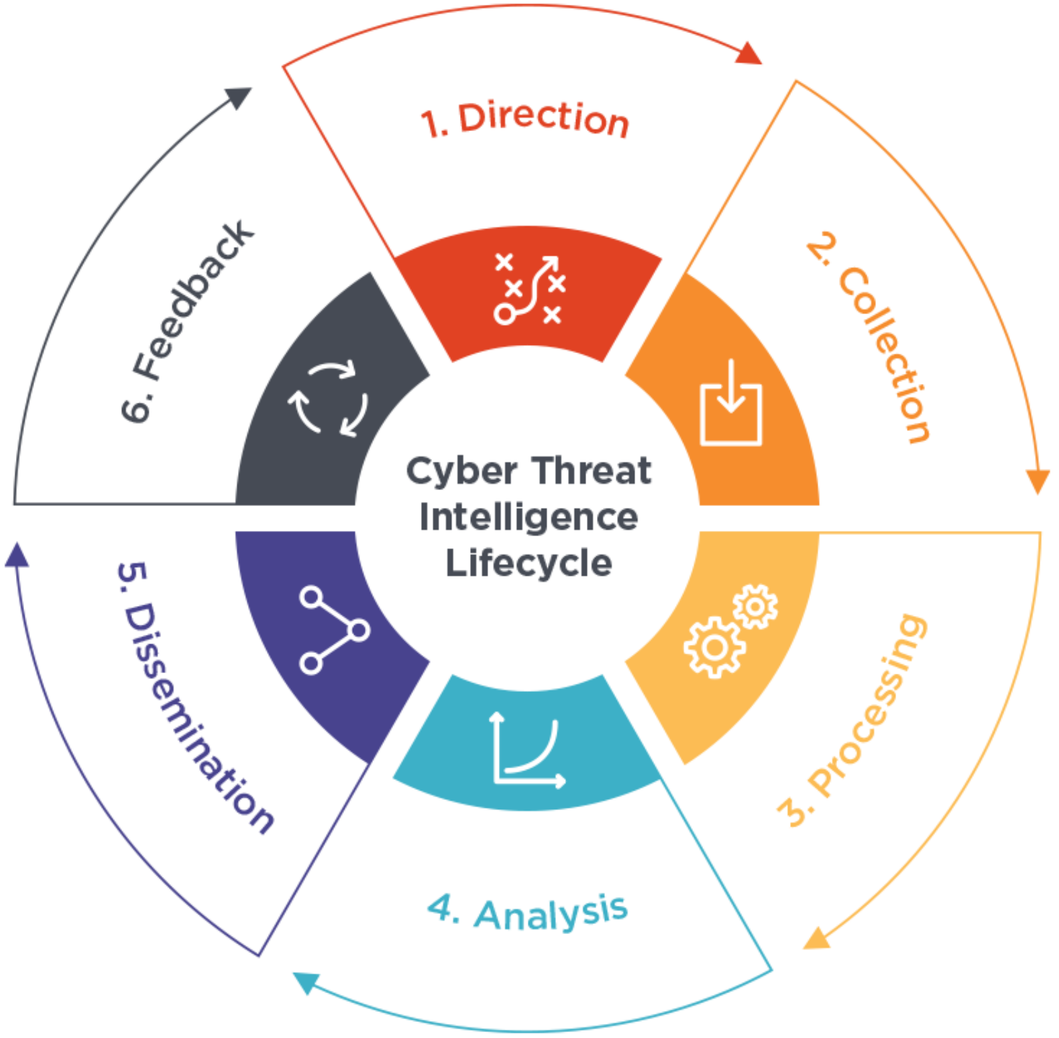
ENRRIQUECIMIENTO BASADO EN WORKFLOWS

OSCAR ENCARNACIÓN LIZ – CSIRT-RD

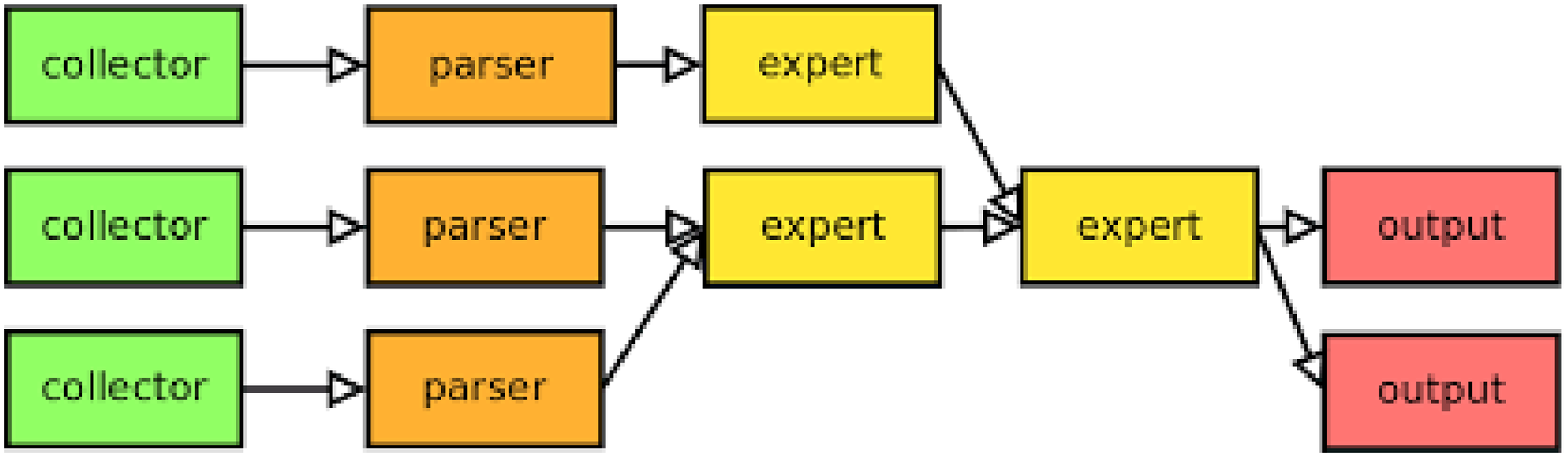
LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

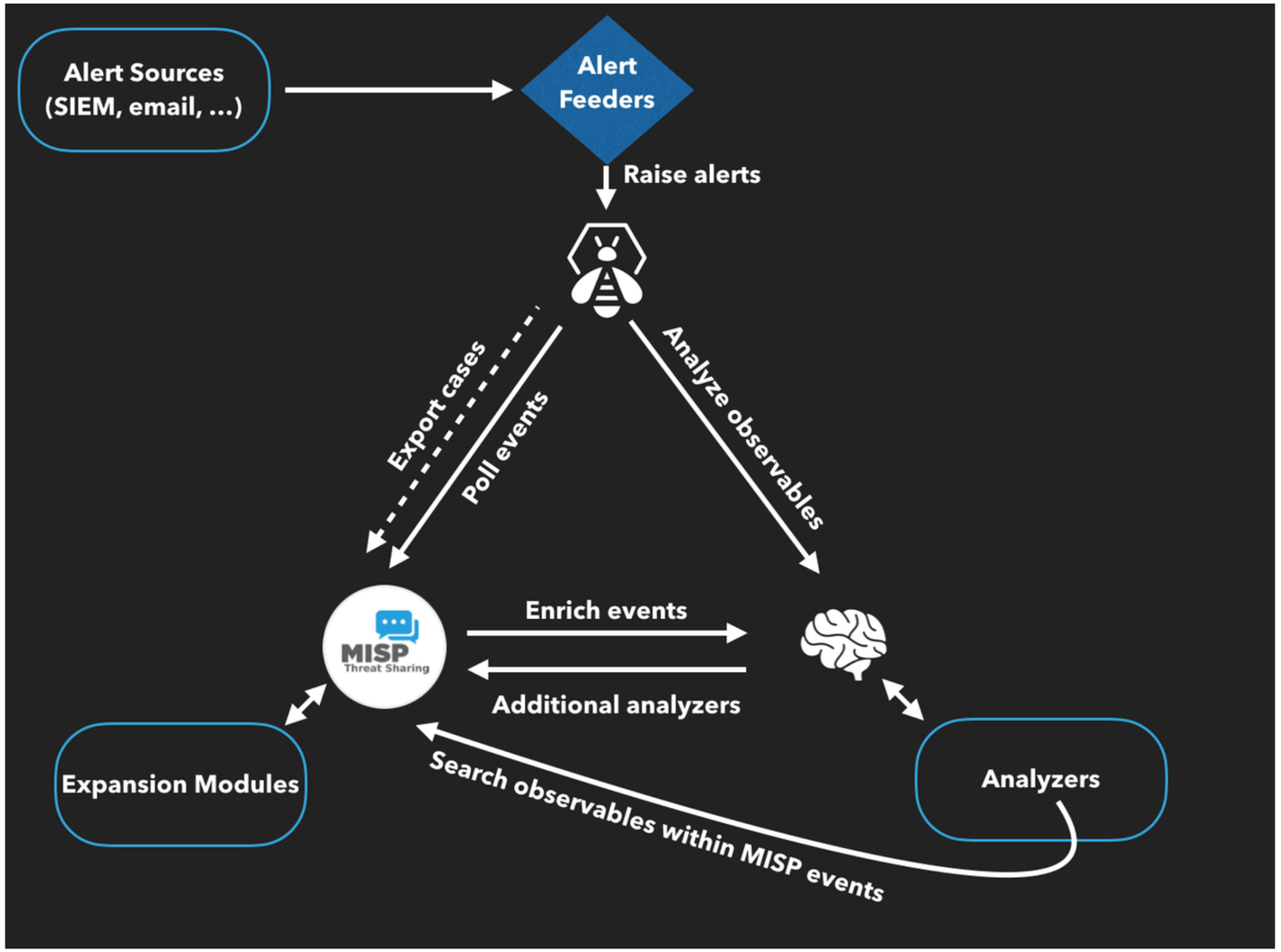
CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

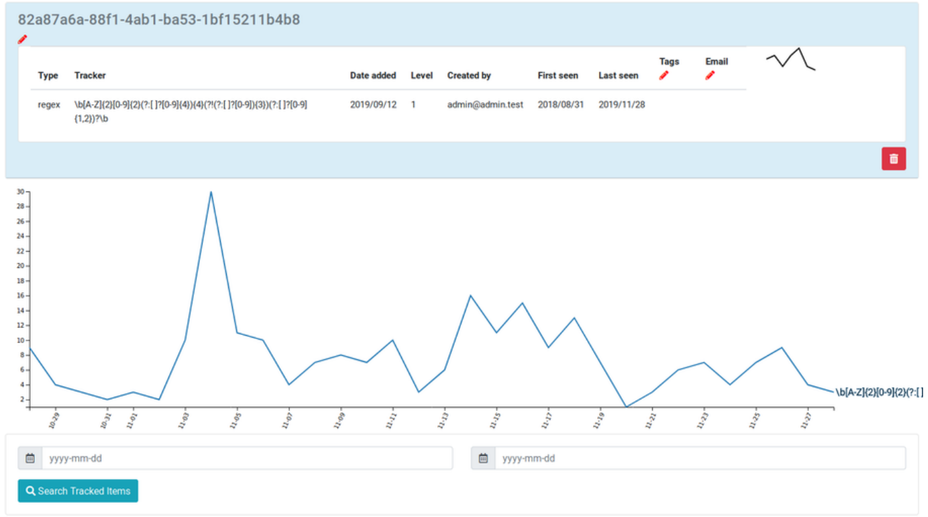

1. Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback
Cyber Threat Intelligence Lifecycle

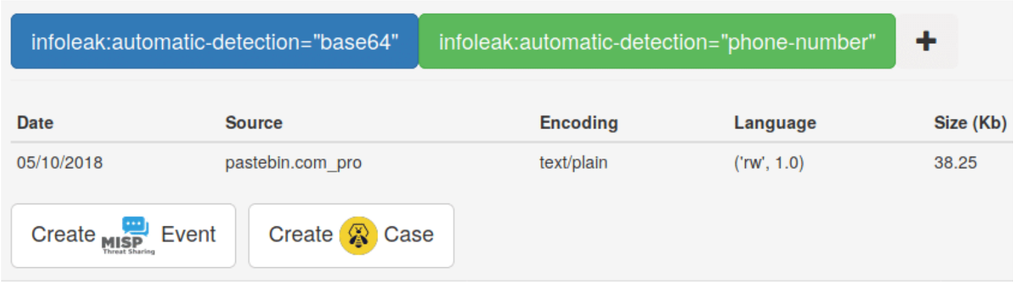
INTELMQ



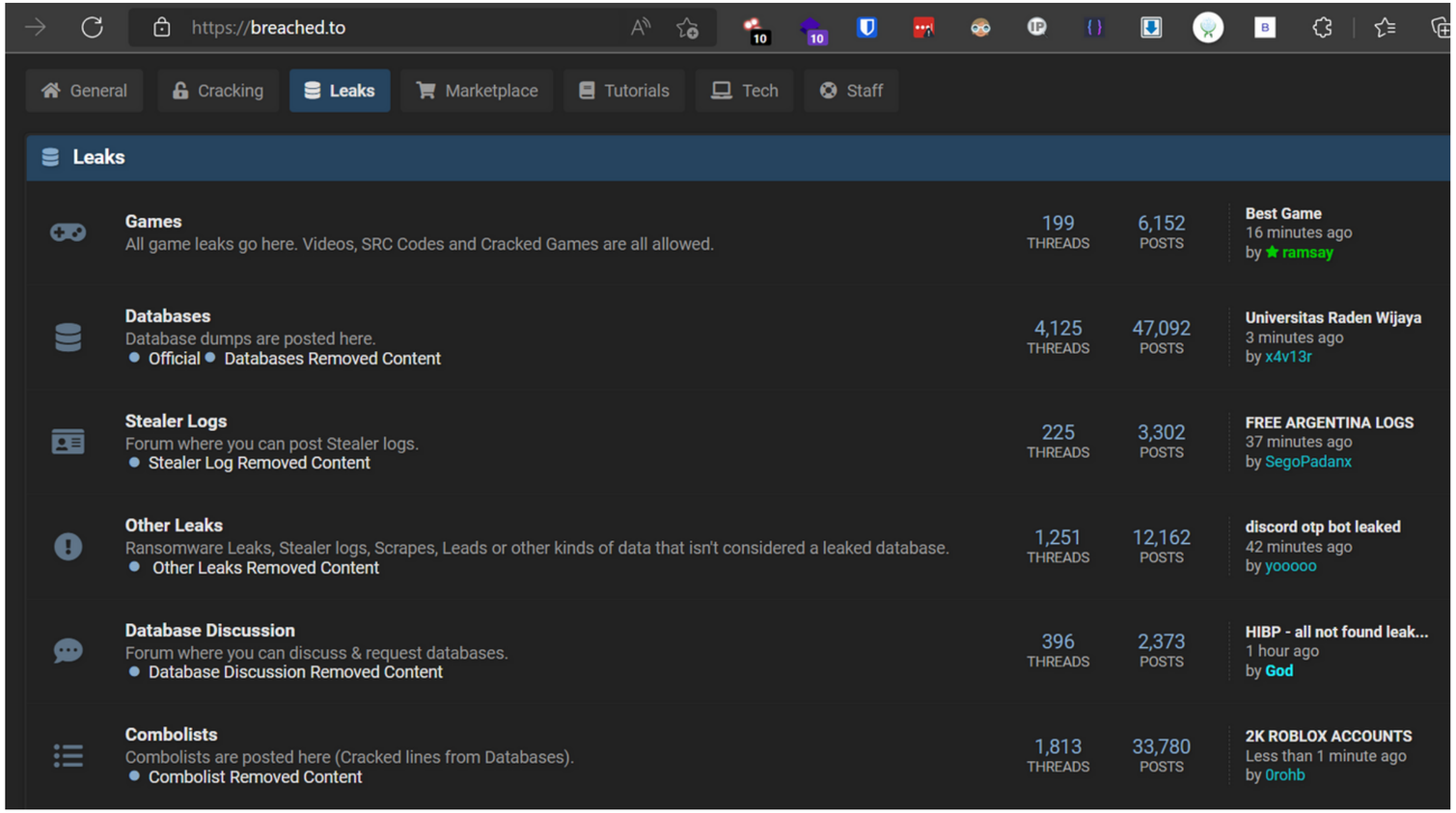
OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

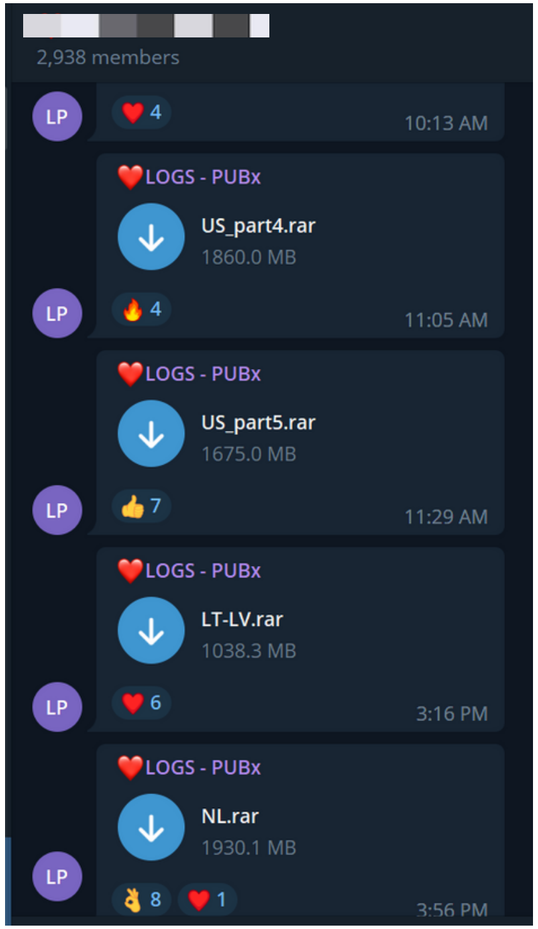

Alert Sources
(SIEM, email, ...)
Alert
Feeders
Raise alerts
Export cases
Poll events
Analyze observables
MISP
Threat Sharing
Enrich events
Additional analyzers
Expansion Modules
Analyzers
Search observables within MISP events


82a87a6a-88f1-4ab1-ba53-1bf15211b4b8
Type
Tracker
Date added
Level
Created by
First seen
Last seen
Tags
Email
regex
2019/09/12
1
admin@admin.test
2018/08/31
2019/11/28
yyyy-mm-dd
yyyy-mm-dd
Search Tracked Items


infoleak:automatic-detection="base64"
infoleak:automatic-detection="phone-number"
Date
Source
Encoding
Language
Size (Kb)
05/10/2018
pastebin.com_pro
text/plain
('rw', 1.0)
38.25
Create MISP Event
Create Case

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**


https://breached.to
General
Cracking
Leaks
Marketplace
Tutorials
Tech
Staff
Leaks
Games
All game leaks go here. Videos, SRC Codes and Cracked Games are all allowed.
199 THREADS
6,152 POSTS
Best Game
16 minutes ago
by ramsay
Databases
Database dumps are posted here.
Official Databases Removed Content
4,125 THREADS
47,092 POSTS
Universitas Raden Wijaya
3 minutes ago
by x4v13r
Stealer Logs
Forum where you can post Stealer logs.
Stealer Log Removed Content
225 THREADS
3,302 POSTS
FREE ARGENTINA LOGS
37 minutes ago
by SegoPadanx
Other Leaks
Ransomware Leaks, Stealer logs, Scrapes, Leads or other kinds of data that isn't considered a leaked database.
Other Leaks Removed Content
1,251 THREADS
12,162 POSTS
discord otp bot leaked
42 minutes ago
by yooooo
Database Discussion
Forum where you can discuss & request databases.
Database Discussion Removed Content
396 THREADS
2,373 POSTS
HIBP - all not found leak...
1 hour ago
by God
Combolists
Combolists are posted here (Cracked lines from Databases).
Combolist Removed Content
1,813 THREADS
33,780 POSTS
2K ROBLOX ACCOUNTS
Less than 1 minute ago
by 0rohb


2,938 members
LP
4
10:13 AM
LOGS - PUBx
US_part4.rar
1860.0 MB
4
11:05 AM
LOGS - PUBx
US_part5.rar
1675.0 MB
7
11:29 AM
LOGS - PUBx
LT-LV.rar
1038.3 MB
6
3:16 PM
LOGS - PUBx
NL.rar
1930.1 MB
8
1
3:56 PM

grep -A3 -B1 -RnE '((URL |Username):.*)(gob.bo|gov\.bo)|edu\.bo|com\.bo|org\.bo)' > leaks.txt

BO[0B90EB87EBB4FD1D424F62501C047E1A] [2...	10/4/2022 9:48 PM	File folder
BO[0B321C885245AA2D16FA02837B305EBD] [...	10/4/2022 9:48 PM	File folder
BO[0BFD0D0BC8E6CAEC5599971529C996B1] [...	10/4/2022 9:48 PM	File folder
BO[0D05485EA6F3B345F379534373D4B3BB] [...	10/4/2022 9:48 PM	File folder
BO[0DAAA8060554D6ABA70BE5E9B4BF4F2B] [...	10/4/2022 9:48 PM	File folder
BO[0EFEC0F16C598A35DBF8D45F02A767C4] [...	10/4/2022 9:48 PM	File folder
BO[0F41F520A9431654FBC8323264C7B10C] [2...	10/4/2022 9:48 PM	File folder
BO[0FA63EAE376C04FDF415C69BC8BB8E38] [2...	10/4/2022 9:48 PM	File folder
BO[0FCEA570D87B6C6E5C4665752CA4AF23] [...	10/4/2022 9:48 PM	File folder
BO[1A9E29E4C75BBCB163572A92F603BC03] [2...	10/4/2022 9:48 PM	File folder
BO[1B69FDB82DFB555495E07614BE2CFC8D] [...	10/4/2022 9:48 PM	File folder
BO[1B70E59B2447929AC91EBB35DFBBAAB5] [...	10/4/2022 9:48 PM	File folder
BO[1B133899D533EC5FC84A1A69EAEE0CE3] [...	5/3/2022 6:50 AM	File folder
BO[1BED3F67A5714825AC5C7FC74B2C11F0] [...	10/4/2022 9:48 PM	File folder
BO[1BFDA60F357AA1ED142AD79F0D143190] ...	10/4/2022 9:48 PM	File folder

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

```
sswords.txt-71-===============
sswords.txt:72:URL: https://salvatuagenda.tigo.com.bo/otp_login.jsf
sswords.txt-73-Username: 69208579
sswords.txt-74-Password: [redacted]
sswords.txt-75-Application: Google_[Chrome]_Profile 16

sswords.txt-101-===============
sswords.txt:102:URL: https://www.bnb.com.bo/BNBNet/IniciarSesion/IniciarIdentificador
sswords.txt-103-Username: nsawg
sswords.txt-104-Password: [redacted]
sswords.txt-105-Application: Google_[Chrome]_Profile 16

sswords.txt-111-===============
sswords.txt:112:URL: https://www.bnb.com.bo/BNBNet/IniciarSesion/IniciarIdentificador
sswords.txt-113-Username: loflxf
sswords.txt-114-Password: [redacted]
sswords.txt-115-Application: Google_[Chrome]_Profile 16
```

```
ternational Sort)/Passwords.txt-607-===============
ternational Sort)/Passwords.txt:608:URL: http://www.plataforma.amerinst.edu.bo/
ternational Sort)/Passwords.txt-609-Username: riveroespinozaangela.ia
ternational Sort)/Passwords.txt-610-Password: [redacted]
ternational Sort)/Passwords.txt-611-Application: Google_[Chrome]_Profile 1

ternational Sort)/Passwords.txt-617-===============
ternational Sort)/Passwords.txt:618:URL: http://www.plataforma.amerinst.edu.bo/
ternational Sort)/Passwords.txt-619-Username: riveroespinozajosue.ia
ternational Sort)/Passwords.txt-620-Password: [redacted]
ternational Sort)/Passwords.txt-621-Application: Google_[Chrome]_Profile 1

ternational Sort)/Passwords.txt-880-===============
ternational Sort)/Passwords.txt:881:URL: http://www.plataforma.amerinst.edu.bo/
ternational Sort)/Passwords.txt-882-Username: riveroespinozajosue.ia
ternational Sort)/Passwords.txt-883-Password: [redacted]
ternational Sort)/Passwords.txt-884-Application: Google_[Chrome]_Profile 7

ternational Sort)/Passwords.txt-945-===============
ternational Sort)/Passwords.txt:946:URL: http://www.plataforma.amerinst.edu.bo/
ternational Sort)/Passwords.txt-947-Username: riveroezpinozaangela.ia
ternational Sort)/Passwords.txt-948-Password: [redacted]
ternational Sort)/Passwords.txt-949-Application: Google_[Chrome]_Profile 7
```

```
"
# Dateadded (UTC),URL,URL_status,Threat,Host,IPaddress,ASnumber,Country
"2022-10-04 00:03:08","http://200.58.91.248:44866/Mozi.m","online","malware_download","200.58.91.248","200.58.91.248","27839","BO"
"2022-10-03 12:03:06","http://200.110.48.161:56620/Mozi.m","online","malware_download","200.110.48.161","200.110.48.161","27839","BO"
"2022-10-03 03:04:06","http://201.150.183.241:45315/Mozi.m","online","malware_download","201.150.183.241","201.150.183.241","27839","BO"
"2022-10-01 06:04:06","http://200.90.145.12:54722/Mozi.m","offline","malware_download","200.90.145.12","200.90.145.12","27839","BO"
"2022-09-29 03:04:06","http://200.110.49.254:56850/Mozi.m","offline","malware_download","200.110.49.254","200.110.49.254","27839","BO"
"2022-09-27 03:04:05","http://201.150.176.149:54951/Mozi.m","offline","malware_download","201.150.176.149","201.150.176.149","27839","BO"
"2022-09-27 00:04:06","http://200.90.147.243:58912/Mozi.m","offline","malware_download","200.90.147.243","200.90.147.243","27839","BO"
"2022-09-26 16:32:05","http://200.90.145.246:44457/i","offline","malware_download","200.90.145.246","200.90.145.246","27839","BO"
"2022-09-25 00:18:06","http://200.110.49.218:48675/i","offline","malware_download","200.110.49.218","200.110.49.218","27839","BO"
"2022-09-25 00:04:07","http://200.110.57.53:52405/Mozi.m","online","malware_download","200.110.57.53","200.110.57.53","27839","BO"
"2022-09-24 19:08:06","http://201.150.183.160:36459/i","online","malware_download","201.150.183.160","201.150.183.160","27839","BO"
"2022-09-24 15:09:06","http://200.90.149.216:54681/i","offline","malware_download","200.90.149.216","200.90.149.216","27839","BO"
"2022-09-24 00:04:07","http://201.150.178.226:41671/Mozi.m","online","malware_download","201.150.178.226","201.150.178.226","27839","BO"
"2022-09-23 21:03:07","http://200.58.89.251:45414/Mozi.m","offline","malware_download","200.58.89.251","200.58.89.251","27839","BO"
"2022-09-23 15:04:06","http://201.150.179.207:60788/Mozi.m","offline","malware_download","201.150.179.207","201.150.179.207","27839","BO"
"2022-09-23 01:52:07","http://201.150.174.204:60824/mozi.m","offline","malware_download","201.150.174.204","201.150.174.204","27839","BO"
"2022-09-22 18:04:06","http://201.150.182.56:50546/Mozi.m","offline","malware_download","201.150.182.56","201.150.182.56","27839","BO"
"2022-09-22 09:04:06","http://201.150.175.47:39015/Mozi.m","offline","malware_download","201.150.175.47","201.150.175.47","27839","BO"
"2022-09-21 15:37:06","http://200.90.145.241:49105/i","offline","malware_download","200.90.145.241","200.90.145.241","27839","BO"
"2022-09-21 12:16:05","http://200.110.56.164:55685/mozi.m","offline","malware_download","200.110.56.164","200.110.56.164","27839","BO"
"2022-09-21 07:16:05","http://200.58.88.165:47084/i","online","malware_download","200.58.88.165","200.58.88.165","27839","BO"
"2022-09-20 03:04:07","http://201.150.177.22:38474/Mozi.m","offline","malware_download","201.150.177.22","201.150.177.22","27839","BO"
"2022-09-19 22:44:05","http://201.150.185.24:54931/i","offline","malware_download","201.150.185.24","201.150.185.24","27839","BO"
"2022-09-19 17:13:11","http://201.150.179.207:60788/i","offline","malware_download","201.150.179.207","201.150.179.207","27839","BO"
"2022-09-19 14:20:06","http://200.110.49.253:39796/i","offline","malware_download","200.110.49.253","200.110.49.253","27839","BO"
"2022-09-19 06:04:06","http://201.150.188.71:48604/Mozi.m","offline","malware_download","201.150.188.71","201.150.188.71","27839","BO"
"2022-09-18 19:12:05","http://201.150.186.166:47622/i","online","malware_download","201.150.186.166","201.150.186.166","27839","BO"
```

4,364
Count

1
Count

Request Map

Requests by country

Export

Country	Count
Bolivia	4,364

Top IPs

Export

IP	Country	Count
177.222.9...	Bolivia	121
181.115.1...	Bolivia	110
181.115.1...	Bolivia	92
177.222.5...	Bolivia	73
181.115.1...	Bolivia	66
2803:940...	Bolivia	66
181.115.1...	Bolivia	61
2800:cd0:...	Bolivia	53

1 2 3 4 5

Top requests by host

Export

Host	Requests
optic.gob.do	1,450

Top requests by URL

Export

Full URL.keyword: Descending	Count
https://optic.gob.do/nortic/images/sello...	295

```
Date,Group,Country,Domain,
2022/09/04,djebbaranon,Bolivia,sinacom.gob.bo/pwn.html
2022/08/02,djebbaranon,Bolivia,censosbolivia.ine.gob.bo
```

Defacement

Cuida tu web,
que no le cambien la cara

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

DETECCION DE INTRUSOS CON THREAT INTEL

OSCAR ENCARNACIÓN LIZ – **CSIRT-RD**

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

Threat Intel Indicator Match

Oct 4, 2022 @ 08:32:33.000

Overview | Threat Intel 1 | Table | JSON

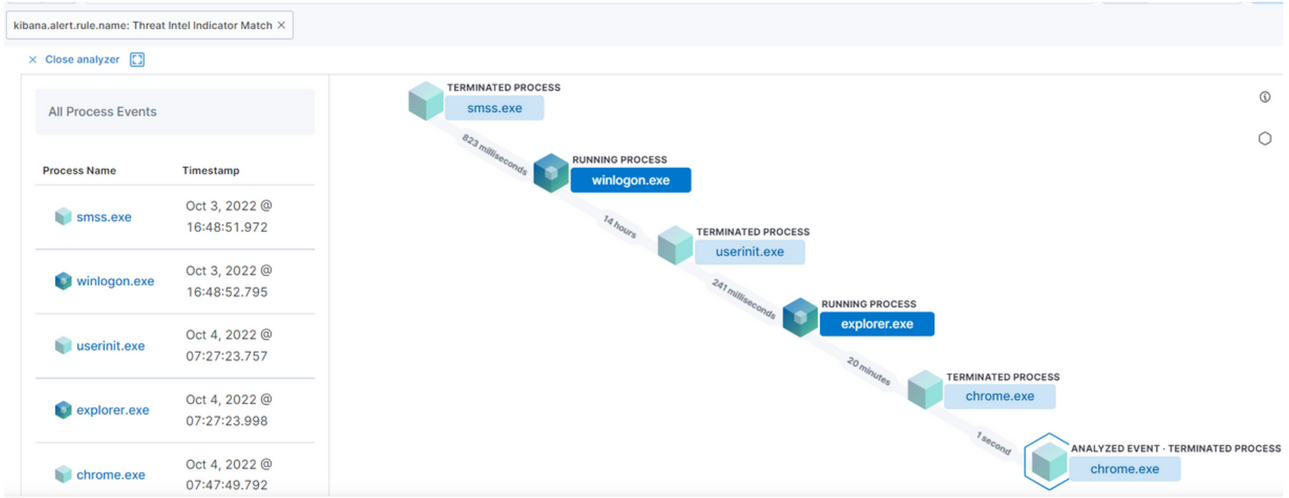
Status	Severity	Risk Score	Rule
Open	Critical	99	Threat Intel Indicator Match

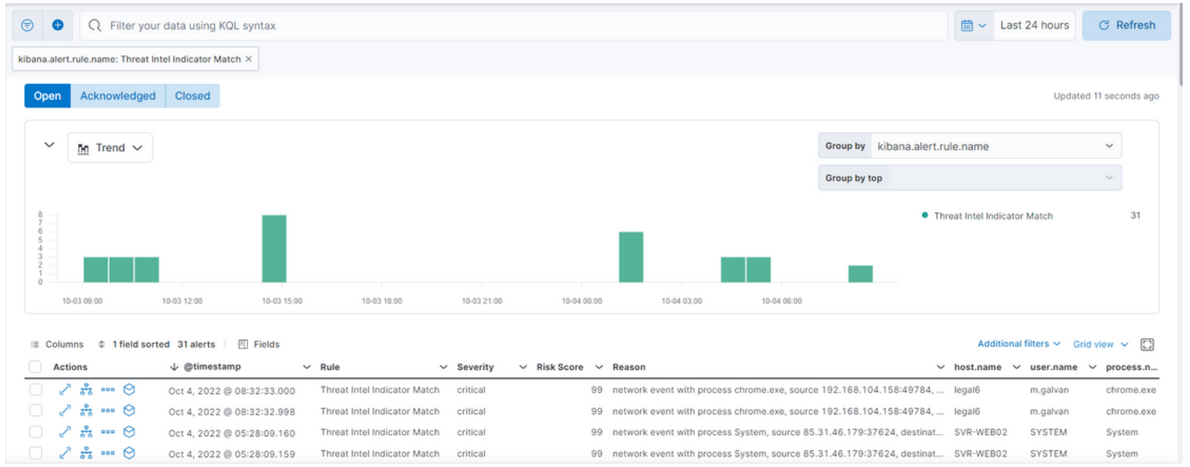
network event with process chrome.exe, source 192.168.104.158:49784, destination 151.139.128.11:443, by m.galvan on legal6 created critical alert Threat Intel Indicator Match.

Highlighted fields — View all fields in table

Field	Value	Alert prevalence
host.name	legal6	7
Agent status	Unhealthy	—
user.name	m.galvan	7
Rule type	threat_match	31
destination.address	151.139.128.11	4
destination.port	443	4

Take action





OSCAR ENCARNACIÓN LIZ – CSIRT-RD

Investigación – IoC

- VirusTotal - https://www.virustotal.com/gui/home/search
- OTX Alienvault - https://otx.alienvault.com
- IBM X-Force - https://exchange.xforce.ibmcloud.com
- Hybrid Analysis - https://www.hybrid-analysis.com
- Blueliv Community - https://community.blueliv.com
- ThreatMiner - https://www.threatminer.org
- PhishTank - https://phishtank.org
- Pulsedive - https://pulsedive.com
- Threatcrowd - https://www.threatcrowd.org
- JoeSandbox - https://www.joesandbox.com
- Any.run - https://app.any.run
- Koodous - https://koodous.com
- VirusBay - https://beta.virusbay.io
- OPSWAT MetaDefender - https://metadefender.opswat.com

STIX

- STIX - https://oasis-open.github.io/cti-documentation/stix/intro.html
- CTI STIX Validator - https://github.com/oasis-open/cti-stix-validator
- CTI STIX Visualization - https://github.com/oasis-open/cti-stix-visualization
- STIX Modeler - https://github.com/STIX-Modeler/UI
- Visual Studio Code - https://code.visualstudio.com/download
- STIX View - https://github.com/traut/stixview
- Jupyter STIX View - https://github.com/traut/jupyter-widget-stixview

Investigación – TTPs

- MITRE ATT&CK - https://attack.mitre.org
- ATT&CK Navigator - https://mitre-attack.github.io/attack-navigator

Investigación – Simulación TTPs

- ATTPwn - https://github.com/Telefonica/ATTPwn
- Atomic Red Team - https://github.com/redcanaryco/atomic-red-team
- CALDERA - https://github.com/mitre/caldera
- DeTTECT - https://github.com/rabobank-cdc/DeTTECT

Tools

- OpenCTI - https://www.opencti.io

CONTACTO

OSCARLIZZ

OSCAR-ENCARNACION-LIZ

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

PREGUNTAS

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

MUCHAS GRACIAS

CONTACT US:
EUCYBERNET@RIA.EE
HTTPS://WWW.LAC4.EU/

Funded by
the European Union

LAC4
Latin America and Caribbean Cyber Competence Centre

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS