Ministerio del Interior y Seguridad Pública

SEGURIDAD DIGITAL PARA PYMES

CENTRO DE MONITOREO DE BAJO COSTO

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Contenido

Autor: Carlos Montoya.
Director: Carlos Landeros C.
Edición: Katherina Canales M. y Sergio Rosales G.
Diseño: Jaime Millán G.
Corrección: Patricio Quezada A. y Carolina Covarrubias E.
Correo: comunicaciones@interior.gob.cl
Santiago de Chile, 08 de octubre de 2020

1. Presentación del artículo

El presente artículo de la colección de investigaciones sobre Análisis de Amenazas Cibernéticas, tiene como objetivo invitar al lector, especialmente a quienes administren plataformas digitales y virtuales expuestas a internet en sus pequeños y medianos negocios, para que pueden proteger la confidencialidad, integridad y disponibilidad de sus activos informáticos.

Con ese propósito, Carlos Montoya, autor invitado en esta oportunidad, comparte con nosotros la base de técnica para la implementación de un sistema de "ciberdefensa para las PYMES" basado en herramientas *open source*, el que debe sostenerse necesariamente en un estrategia general de protección.

Este artículo tiene como finalidad servir de guía para el uso integrado de siete herramientas, partiendo de la base de mínima para implementar esta arquitectura.

El trabajo también comparte una reflexión del autor en su breve estudio introductorio en torno a los desafíos de la industria 4.0., el que apunta a lograr una madurez organizacional basada en las personas, los procesos y las tecnologías.

2. Introducción: Industria 4.0, la seguridad digital y la ciberdefensa

En la actualidad, en la era de la transformación digital, amplios sectores han tenido que enfrentar los desafíos digitales que la industria 4.0 (Deloitte, 2017) trae consigo. Desde luego todas las transacciones financieras se deben generar en un ambiente digital cada vez más ágil para el cliente, quien a través de un dispositivo móvil pueda manejar todos los productos que, por ejemplo, una entidad bancaria ofrece abiertamente. Esto hace que las empresas sean conscientes de que su negocio depende cada vez más de los datos (Oracle, 2020).

Todo lo anterior hace que la ciberseguridad o seguridad digital, participe como condición *sine qua non* en los directorios de la industria financiera, donde el cumplimiento de normativas nacionales e internacionales, sumado a la de buenas prácticas y uso de estándares, hacen que la ciberseguridad sea también una cuestión importante. La exposición que genera la industria 4.0 hace que la superficie de las empresas aumente, ampliando las posibilidades de ciberataques por parte de los ciberdelincuentes (mincotur, 2017).

En este contexto, se hace de suma importancia mantener las capacidades de ciberdefensa en la industria financiera, para así, enfrentar los ciberataques a la infraestructura tecnológica y mantener la continuidad operativa del negocio. Para ello, es necesario enfocarse en una estrategia de ciberdefensa más robusta (Blueliv, 2019), otorgándole capacidades de inteligencia de amenazas y análisis de malware, así como un *team* de respuesta ante incidentes computacionales entre otros.

Después de observar que para la industria financiera 4.0 el ciberespacio extendió el territorio de ataque, y que por este motivo se hace necesario para las empresas del sector contar con capacidades de ciberdefensa, adquiere gran relevancia poseer una estrategia de ciberseguridad que tenga como objetivos proteger los activos críticos de las empresas, y a su vez, entregarle continuidad operativa al negocio entendiendo que cada segundo es una pérdida financiera para la compañía.

Finalmente, esta estrategia debe contemplar la visión de lograr una madurez dentro de la organización aplicada en tres dimensiones, las personas, en la continua educación y concientización sobre las materias de seguridad digital, los procesos, donde el ejercicio diario se retro alimente con los conceptos de la estrategia de ciberseguridad de la compañía y su cumplimiento, y finalmente la tecnología que es inherente a la evaluación natural de la seguridad digital.

3. Ciberdefensa en las Pymes

En la actualidad, la pequeña y mediana empresa, se encuentra en una economía impulsada por la industria 4.0 (chile, 2019), donde la necesidad de emplear las mejores prácticas en el ámbito de la seguridad digital puede ser muchas veces clave o crucial en la convivencia del ecosistema que la rodea. También podemos identificar la relevancia que trae consigo el cuidado que estas empresas deben tener con los datos o información de todos sus clientes, donde deben velar y custodiar la información que en sus sistemas circulan o reposan.

Es en este escenario donde es importante la defensa —concepto derivado de la teoría de la guerra, en este caso aplicada el ciberespacio—, en tanto práctica necesaria y permanente frente a ataques informáticos, y donde la pequeña y mediana empresa debe estar preparada para que los productos no sufran menoscabo.

Asimismo, podemos señalar que un estudio denominado "*Cost of a Data Breach Report 2019*" realizado por IBM Security en Estados Unidos, determinó que la pérdida de información relevante para una Pyme, puede significar su cierre en 6 meses. (revistaemprende.cl, 2019). En un solo ataque se han visto solicitudes de rescate de datos provocadas por ransomware en pymes de 3.000, 10.000 y hasta de 12.000 euros (país, 2020), donde muchas veces esos valores son el conjunto de la facturación de una pyme en un mes.

Es en el contexto anterior, donde es necesario que cada pequeña o mediana empresa posea un mínimo de seguridad digital (entendida esta como la capacidad de defensa frente a ciberdelincuentes), y a su vez, que las comunidades de la defensa digital, como es el CSIRT de Gobierno, Whilolab, el centro de investigación de ciberseguridad de la Universidad Mayor y Sochisi, apoyen el desarrollo de capacidades de ciberdefensa a este sector muchas veces olvidado.

Finalmente, se puede señalar que las pymes se encuentran en una gran desventaja frente a los ciberdelincuentes, si no se preocupan de la seguridad digital en la industria 4.0, ya que la diversidad de los ataques que se presentan en el día a día, donde grupos organizados de ciberdelincuentes en pro de mantener sus organizaciones, no evaluaran el tamaño de la empresa para lograr su objetivo, generando ataques importantes a todo tipo de sector económico.

4. Implementación de un sistema de ciberdefensa para redes básico para pymes.

Para la implementación de un sistema de ciberdefensa, es necesario contar con una arquitectura adecuada para registrar los eventos que generen los dispositivos conectados en la red, como puede ser un firewall, un switch, un router o un computador. Es por ello, que en este artículo se propone una arquitectura de ciberdefensa en la red compuesta por lo siguiente:

- 1 (un) TRUSTTECH Network Security Firewall es un firewall perimetral diseñado para administrar, proteger y brindar acceso seguro la red Corporativa de pequeñas y medianas Empresas (trusttech, 2020).

- 2 (dos) detectores de incidentes de seguridad (o IDS por sus siglas en inglés —Intrusion Detection System). El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.

- 1 (un) SIEM o correlacionador de eventos, que centraliza el almacenamiento, la interpretación de los registros y permite un análisis en tiempo real que permite al personal de seguridad tomar medidas defensivas más rápidas frente a un incidente digital.

- 1 (un) sistema de registro de incidente, que en esta oportunidad es instalará thehive, una plataforma de respuesta a incidentes de seguridad gratuita, de código abierto y escalable, estrechamente integrada con MISP (plataforma de intercambio de información de malware), diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de seguridad de la información que se ocupe de incidentes de seguridad que deban investigarse rápidamente (thehive, 2020).

- 1 (un) registro de indicadores de compromiso, como lo es MISP, Una plataforma de inteligencia de amenazas para recopilar, compartir, almacenar y correlacionar indicadores de compromiso de ataques dirigidos, inteligencia de amenazas, información de fraude financiero, información de vulnerabilidad o incluso información de lucha contra el terrorismo. (MISP, 2020).

Esta arquitectura ayudará a proteger una red mediante el firewall e ids, a detectar tráfico malicioso con el correlacionador, y a responder el incidente mediante las plataformas de thehive y misp, 3 de los 5 pilares del nist. (NIST, 2018).

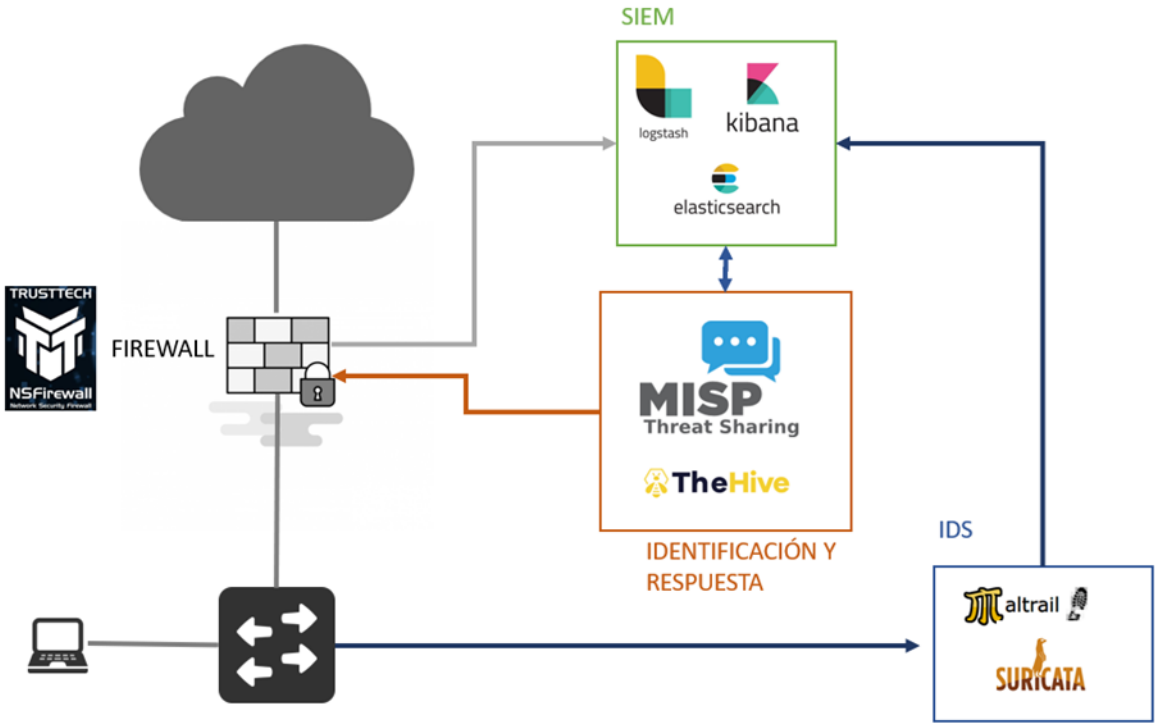

Ilustración 1: Arquitectura de ciberdefensa básica

5. Implementación de la arquitectura de ciberdefensa para una red de pyme.

Para la implementación de este sistema de ciberdefensa en la red se ocuparán dos servidores virtualizados, más un firewall propiedad de trusttech.

5.1. Requisitos de los servidores virtuales

5.1.1. Servidor para la instalación de ELK y IDS

a. 8 GB de RAM
b. 4 CPU
c. 100 GB disco
d. S.O. Debian 10

5.1.2. Servidor para la instalación de MISP y thehive

a. 8 GB de RAM
b. 4 CPU
c. 100 GB disco
d. S.O. Debian 10

5.2. Implementación IDS (Detectar de intrusos)

a. MATRAIL

Maltrail es un sistema de detección de tráfico malicioso, que utiliza listas públicas (negras) que contienen rastros maliciosos y / o generalmente sospechosos, junto con rastros estáticos compilados a partir de varios informes de AV y listas personalizadas definidas por el usuario, donde el rastro puede ser cualquier cosa del nombre del dominio.

Implementación de maltrail:

Para la implementación de maltrail instalamos la librería Python-pcapy necesaria para la operatividad del software. La instalación de esta librería se realiza con el siguiente comando:
apt-get install git 8ython-pcapy

Una vez instalada la librería, descargamos el software con el siguiente comando;
git clone https://github.com/stamparm/maltrail.git

Entramos a la carpeta de maltrail

```
root@localhost:~/maltrail# ls
core    html     maltrail.conf  plugins    requirements.txt  server.py   trails
docker  LICENSE  misc           README.md  sensor.py         thirdparty
```

Ilustración 2: carpeta maltrail

Una vez, dentro de la carpeta maltrail, ejecutamos el comando para iniciar el sensor de maltrail que comienza a recolectar indicadores desde las fuentes que el sensor tiene, y comienza a analizar el tráfico y a verificar coincidencias.

```
stamparm@beast:~/maltrail$ sudo python sensor.py
Maltrail (sensor) #v0.9.104

[i] using configuration file '/home/stamparm/maltrail/maltrail.conf'
[i] using '/var/log/maltrail' for log storage
[?] at least 384MB of free memory required
[i] updating trails (this might take a while)...
 [o] 'https://reputation.alienvault.com/reputation.generic'
 [o] 'https://www.autoshun.org/files/shunlist.csv'
 [o] 'https://www.badips.com/get/list/any/2?age=7d'
 [o] 'http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.txt'
 [o] 'http://osint.bambenekconsulting.com/feeds/dga-feed.txt'
 [o] 'http://www.binarydefense.com/banlist.txt'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/bitcoin_nodes_1d.ipset'
 [o] 'http://lists.blocklist.de/lists/all.txt'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/botscout_1d.ipset'
 [o] 'http://danger.rulez.sk/projects/bruteforceblocker/blist.php'
 [o] 'http://cinsscore.com/list/ci-badguys.txt'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/cruzit_web_attacks.ipset'
 [o] 'http://cybercrime-tracker.net/all.php'
 [o] 'https://intel.deepviz.com/recap_network.php?tw=7d&active=network_domains'
 [o] 'http://www.dshield.org/feeds/suspiciousdomains_High.txt'
 [o] 'http://feeds.dshield.org/top10-2.txt'
 [o] 'http://rules.emergingthreats.net/open/suricata/rules/botcc.rules'
 [o] 'http://rules.emergingthreats.net/open/suricata/rules/compromised-ips.txt'
 [o] 'https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules'
 [o] 'https://feodotracker.abuse.ch/blocklist/?download=domainblocklist'
 [o] 'https://feodotracker.abuse.ch/blocklist/?download=ipblocklist'
 [o] 'http://blocklist.greensnow.co/greensnow.txt'
 [o] 'https://raw.githubusercontent.com/Neo23x0/Loki/master/iocs/otx-c2-iocs.txt'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/malc0de.ipset'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/malwaredomainlist.ipset'
 [o] 'http://malwaredomains.lehigh.edu/files/domains.txt'
 [o] 'https://lists.malwarepatrol.net/cgi/getfile?receipt=f1417692233&product=8&list=dansguardian'
 [o] 'https://www.maxmind.com/en/proxy-detection-sample-list'
 [o] 'https://myip.ms/files/blacklist/htaccess/latest_blacklist.txt'
 [o] 'http://www.nothink.org/blacklist/blacklist_malware_irc.txt'
 [o] 'http://www.openbl.org/lists/base.txt'
 [o] 'https://openphish.com/feed.txt'
 [o] 'https://palevotracker.abuse.ch/blocklists.php?download=combinedblocklist'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxylists_1d.ipset'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxyrss_1d.ipset'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/proxyspy_1d.ipset'
 [o] 'https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/ri_web_proxies_30d.ipset'
```

Ilustración 3: actualización de indicadores de instrucción

Terminado el proceso de inicio del sensor, iniciamos la aplicación server.py con el siguiente comando para levantar la interfaz web a monitorear.

```
root@localhost:~/maltrail# python server.py
Maltrail (server) #v0.22.9

[i] using configuration file '/root/maltrail/maltrail.conf'
[i] starting HTTP server at http://0.0.0.0:8338/
[o] running...
```

Ilustración 4: ejecución de servidor

Una vez levantado, podemos ir al sitio web como señala la configuración y acceder a las detecciones que ha generado el sensor.

Ilustración 5 web mailtrail

Una vez dentro del software, podemos identificar el tipo de conexión y los patrones maliciosos que ejecutan las visitas.

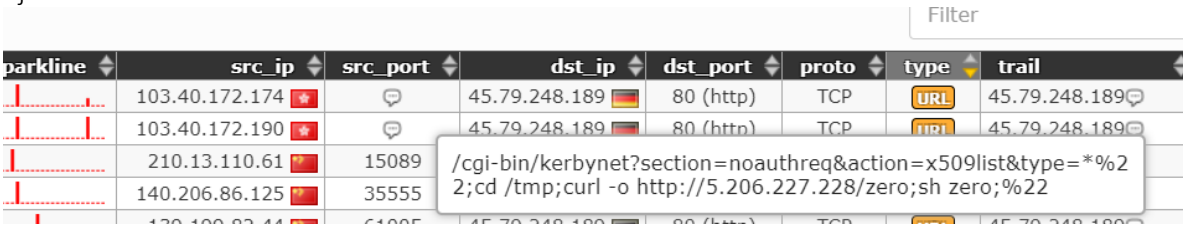

Ilustración 6 detalle de evento en mailtrail

b. SURICATA

Suricata es un motor de detección de amenazas de red gratuito, de código abierto, maduro, rápido y robusto.

El motor Suricata es capaz de detección de intrusión en tiempo real (IDS), prevención de intrusión en línea (IPS), monitoreo de seguridad de red (NSM) y procesamiento de pcap fuera de línea.

Implementación de Suricata:

Para la instalación de suricata se aplican los siguientes filtros:

apt-get install suricata

Una vez instalado suricata, bajamos las reglas para comenzar a operar el detector; ingresamos al archivo oinkmaster.conf
nano /etc/oinkmaster.conf
y agregamos la url para bajar las reglas.
url = http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz

Una vez, cargada las reglas, configuramos el aplicativo suricata, ingresamos a suricata.yaml
nano /etc/suricata/suricata.yaml
y editamos los siguientes componentes del archivo:

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[10.0.0.0]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
```

Ilustración 7 configuración suricara 1

```
# a line based log of HTTP requests (no alerts)
- http-log:
    enabled: yes
    filename: http.log
    append: yes
    #extended: yes     # enable this for extended logging information
    #custom: yes       # enabled the custom logging format (defined by customformat)
    #customformat: "%{%D-%H:%M:%S}t.%z %{X-Forwarded-For}i %H %m %h %u %s %B %a:%p -> %A:
    #filetype: regular # 'regular', 'unix_stream' or 'unix_dgram'
```

Ilustración 8 configuración suricata 2

Una vez configurados los elementos señalados, se ejecuta la aplicación

```
root@localhost:/etc/suricata# suricata -c /etc/suricata/suricata.yaml -i etho
6/10/2020 -- 22:39:30 - <Notice> - This is Suricata version 4.1.2 RELEASE
```

Ilustración 9 ejecución de suricata

Podemos identificar la ejecución de la aplicación verificando los log de la aplicación con el siguiente comando, el cual indicará el tráfico detectado.

```
root@localhost:/etc/suricata# tail -f /var/log/suricata/eve.json
```

Ilustración 10 verificación de suricata en ejecución


```
{"timestamp":"2020-10-06T22:41:10.287037+0000","event_type":"stats","stats":{"uptime":6551739,"capture":{"
kernel_packets":12604143,"kernel_drops":1,"errors":0},"decoder":{"pkts":12604142,"bytes":2336871640,"inval
id":94413,"ipv4":11990292,"ipv6":613900,"ethernet":12604143,"raw":0,"null":0,"sll":0,"tcp":12050300,"udp":
157575,"sctp":1,"icmpv4":46230,"icmpv6":255636,"ppp":0,"pppoe":0,"gre":50,"vlan":0,"vlan_qinq":0,"ieee8021
ah":0,"teredo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":185,"max_pkt_size":1518,"erspan
":0,"ipraw":{"invalid_ip_version":0},"ltnull":{"pkt_too_small":0,"unsupported_type":0},"dce":{"pkt_too_sma
ll":0}},"flow":{"memcap":0,"tcp":878657,"udp":42581,"icmpv4":9843,"icmpv6":26636,"spare":10000,"emerg_mode
_entered":0,"emerg_mode_over":0,"tcp_reuse":6277,"memuse":7236432},"defrag":{"ipv4":{"fragments":0,"reasse
mbled":0,"timeouts":0},"ipv6":{"fragments":0,"reassembled":0,"timeouts":0},"max_frag_hits":0},"tcp":{"sess
ions":872375,"ssn_memcap_drop":0,"pseudo":0,"pseudo_failed":0,"invalid_checksum":1568,"no_flow":0,"syn":10
58889,"synack":566606,"rst":946480,"midstream_pickups":0,"pkt_on_wrong_thread":937,"segment_memcap_drop":0
,"stream_depth_reached":124,"reassembly_gap":18531,"overlap":2231109,"overlap_diff_data":0,"insert_data_no
rmal_fail":0,"insert_data_overlap_fail":0,"insert_list_fail":0,"memuse":2293760,"reassembly_memuse":393216
},"detect":{"engines":[{"id":0,"last_reload":"2020-07-23T02:46:03.819665+0000","rules_loaded":39294,"rules
_failed":5}],"alert":105962},"app_layer":{"flow":{"http":13346,"ftp":1,"smtp":0,"tls":5680,"ssh":295654,"i
map":0,"msn":0,"smb":4,"dcerpc_tcp":0,"dns_tcp":0,"nfs_tcp":0,"ntp":2021,"ftp-data":0,"tftp":105,"ikev2":1
,"krb5_tcp":0,"dhcp":0,"failed_tcp":23,"dcerpc_udp":0,"dns_udp":24818,"nfs_udp":0,"krb5_udp":8,"failed_udp
":15628},"tx":{"http":238348,"ftp":0,"smtp":0,"tls":0,"ssh":0,"smb":6,"dcerpc_tcp":0,"dns_tcp":0,"nfs_tcp"
:0,"ftp-data":0,"krb5_tcp":0,"dcerpc_udp":0,"dns_udp":55491,"nfs_udp":0,"ntp":2021,"tftp":100,"ikev2":1,"k
rb5_udp":0,"dhcp":0},"expectations":0},"flow_mgr":{"closed_pruned":835483,"new_pruned":71117,"est_pruned":
51111,"bypassed_pruned":0,"flows_checked":0,"flows_notimeout":0,"flows_timeout":0,"flows_timeout_inuse":0,
"flows_removed":0,"rows_checked":65536,"rows_skipped":65536,"rows_empty":0,"rows_busy":0,"rows_maxlen":0},
"dns":{"memuse":0,"memcap_state":0,"memcap_global":0},"http":{"memuse":0,"memcap":0},"ftp":{"memuse":0,"me
mcap":0}}}
```


Ilustración 11 log de suricata en ejecución

5.3. Implementación SIEM (correlacionador de eventos)

a. ELASTICSEARCH

Elasticsearch es un servidor de búsqueda basado en Lucene. Provee un motor de búsqueda de texto completo, distribuido y con capacidad de multi-tenencia con una interfaz web RESTful y con documentos JSON. Elasticsearch está desarrollado en Java y está publicado como código abierto bajo las condiciones de la licencia Apache.

Implementación de elasticsearch:

Para la implementación de elasticsearch generaremos los siguientes comandos:
Descargamos los certificados desde elastic
wget –qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -

Agregamos la librería de descarga de los paquetes de elastic a nuestro sistema operativo.
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | tee -a /etc/apt/sources.list.d/elastic-7.x.list

Actulizamos.

apt-get update
e instalamos elasticsearch
apt-get install elasticsearch

Una vez instalado, modificamos su archivo de configuración para poder levantar los servicios adecuados y conectarnos al servicio.

```
bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowe
network.host: 10.0.0.0
#
# Set a custom port for HTTP:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["10.0.0.0"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
cluster.initial_master_nodes: ["10.0.0.0"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# ---------------------------------- Gateway -----------------------------------
```

Ilustración 12 archivo de configuración de elastisearch

Estando las configuraciones adecuadas, se procede a reiniciar los servicios;
systemctl restart elasticsearch
y comprobamos que elasticsearch esté en ejecución.
curl -X GET http://IPSERVER:9200

Si las configuraciones se encuentran correctas, nos debería enviar una respuesta de "you know, for Search"

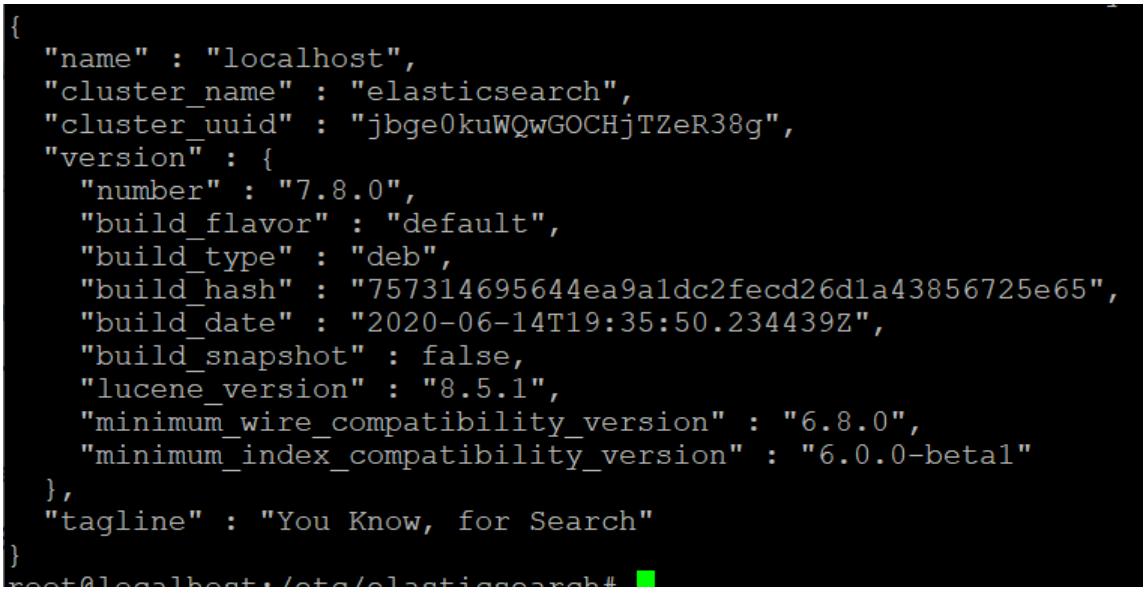

Ilustración 13 verificación de elasticsearch en ejecución

b. LOGTASH

Logstash es una herramienta para la administración de logs. Esta herramienta se puede utilizar para recolectar, parsear y guardar los logs para futuras búsquedas. La aplicación se encuentra basada en jRuby y requiere de Java Virtual Machine para correr. Como corre en JVM puede ser ejecutada en cualquier Sistema Operativo que corra JVM (Linux, Mac OS X, Windows).

Implementación de logstash:

Esta vez, instalaremos logstash y recolectaremos la información de suricata para poder modelarla finalmente con kibana.

Para iniciar con la instalación de logstash ejecutamos el siguiente comando,

```
root@localhost:~# apt-get install logstash
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/168 MB of archives.
After this operation, 296 MB of additional disk space will be used.
Selecting previously unselected package logstash.
(Reading database ... 229374 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.8.0-1_all.deb ...
Unpacking logstash (1:7.8.0-1) ...
Setting up logstash (1:7.8.0-1) ...
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely
be removed in a future release.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by com.headius.backport9.modules.Modules to method sun.nio.ch.NativeThr
ead.signal(long)
WARNING: Please consider reporting this to the maintainers of com.headius.backport9.modules.Modules
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.31/lib/pleaserun/platform/base.rb:112: wa
rning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
[master c3b7e93] committing changes in /etc made by "apt-get install logstash"
 9 files changed, 32 insertions(+), 1 deletion(-)
 create mode 100644 systemd/system/logstash.service
```

Ilustración 14 instalación de logstash

Una vez instalado, creamos el archivo suricata_eve.conf con el siguiente comando,
nano /etc/logstash/conf.d/suricata_eve.conf
y dentro del archivo copiamos lo siguiente:

```
================= código archivo ===============
input {
  file {
    path => ["/var/log/suricata/eve.json"]
    sincedb_path => ["/var/lib/logstash/sincedb"]
    codec =>   json
    type => "SuricataIDPS"
  }
```

```
}

filter {
 if [type] == "SuricataIDPS" {
  date {
   match => [ "timestamp", "ISO8601" ]
  }
 ruby {
  code => "
   if event.get('[event_type]') == 'fileinfo'
     event.set('[fileinfo][type]', event.get('[fileinfo][magic]').to_s.split(',')[0])
   end
   "
 }
 if [src_ip]  {
  geoip {
   source => "src_ip"
   target => "geoip"
   #database => "/usr/share/GeoIP/GeoIP.dat"
   add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
   add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}"  ]
  }
  mutate {
   convert => [ "[geoip][coordinates]", "float" ]
  }
  if ![geoip.ip] {
   if [dest_ip]  {
    geoip {
     source => "dest_ip"
     target => "geoip"
     #database => "/usr/share/GeoIP/GeoIP.dat"
     add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
     add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}"  ]
    }
    mutate {
     convert => [ "[geoip][coordinates]", "float" ]
    }
   }
  }
 }
}
}

output {
 elasticsearch {
  hosts => "localhost"
```

```
  }
}
=================================================================
```

Estando el archivo creado iniciamos logsatsh,
systemctl start logstash.service

Estando iniciado podemos verificar de su ejecución de la siguiente forma:

tail -f /var/log/logstash/logstash-plain.log
donde el mensaje sería
INFO][logstash.agent] Successfully started Logstash API endpoint {:port=>9600}

c. KIBANA

Kibana es un complemento de visualización de datos de código abierto para Elasticsearch. Proporciona capacidades de visualización sobre el contenido indexado en un clúster de Elasticsearch. Los usuarios pueden crear diagramas de barras, líneas y dispersión, o gráficos circulares y mapas sobre grandes volúmenes de datos.

Implementación de kibana:

Para la implementación de kibana ejecutaremos el siguiente comando.
apt-get install kibana
editamos el archivo de configuración
nano /etc/kibana/kibana.yml
y agregamos los datos de nuestro elastic

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "10.0.0.0"
```

Ilustración 15 archivo de configuración de kibana

Reiniciamos kibana

systemctl restart kibana
e ingresamos mediante navegador a kibana para revisar los datos ingresados.

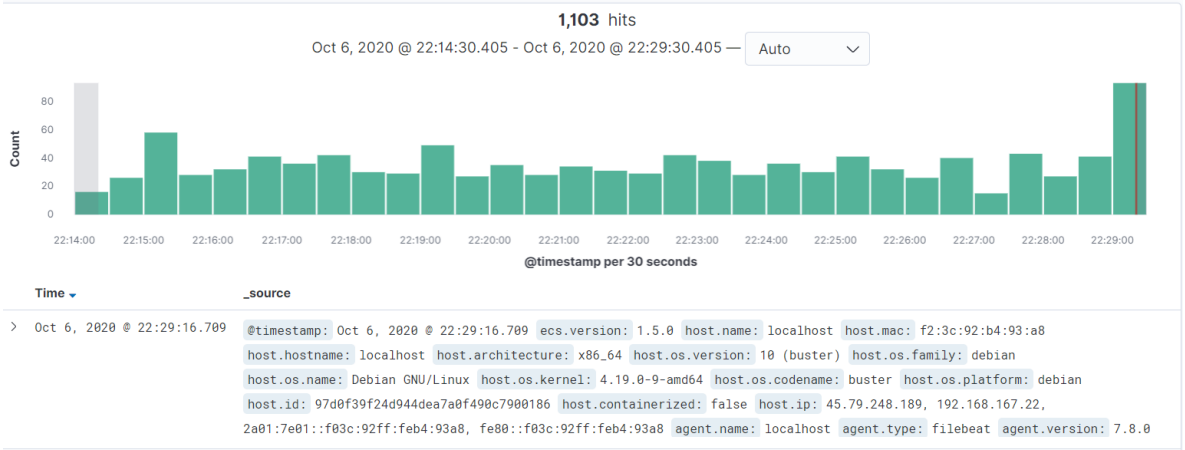

Ilustración 16 grafico de kibana

Ya teniendo datos en kibana podemos genera varios gráficos para nuestro sistema de monitoreo.

Ilustración 17 grafico de georreferencia de ataques

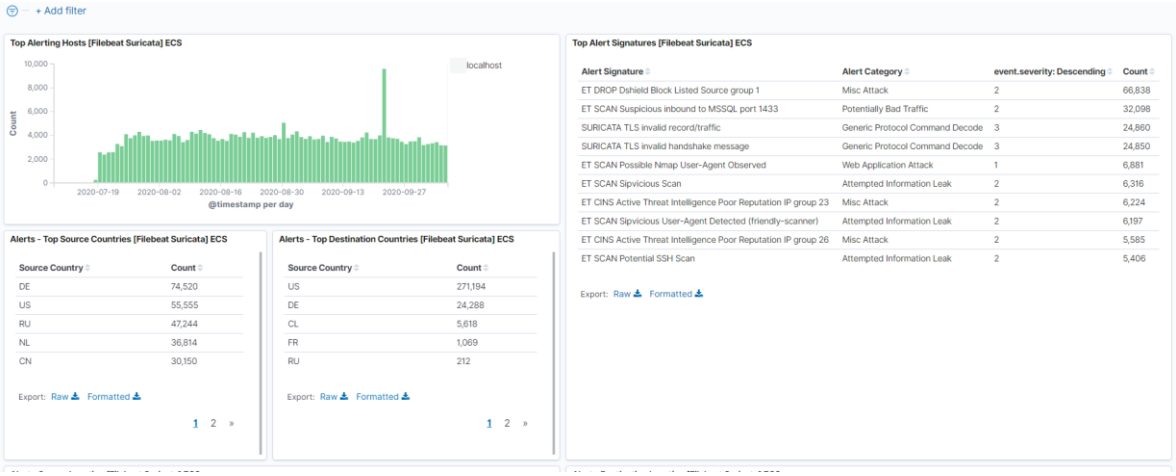

Ilustración 18 gráficos de kibana 2

d. THEHIVE

Lo primero para instalar thehive es instalar Elasticsearch como lo señalamos anteriormente,
Y después de eso aplicar lo siguiente:

```
  23  echo 'deb https://dl.bintray.com/thehive-project/debian-stable any main'
| sudo tee -a /etc/apt/sources.list.d/thehive-project.list
  24  apt-get update
  25  sudo apt-key adv --keyserver hkp://pgp.mit.edu --recv-key 562CBC1C
  26  apt-get update
  27  sudo apt-get install thehive
  28  cd /etc/thehive/
  29  ls
  30  nano application.conf
```

Ilustración 19 instalación thehive

```
# Secret Key
# The secret key is used to secure cryptographic functions.
# WARNING: If you deploy your application on several servers, make sure to use the same key.
play.http.secret.key="***hackspace***"

# Elasticsearch
search {
  ## Basic configuration
  # Index name.
  index = the_hive
  # ElasticSearch instance address.
  uri = "http://10.0.0.0:9200/"
```

Ilustración 20 archivo de configuración thehive

Modificando el archivo de configuración, podemos verificar la implementación.

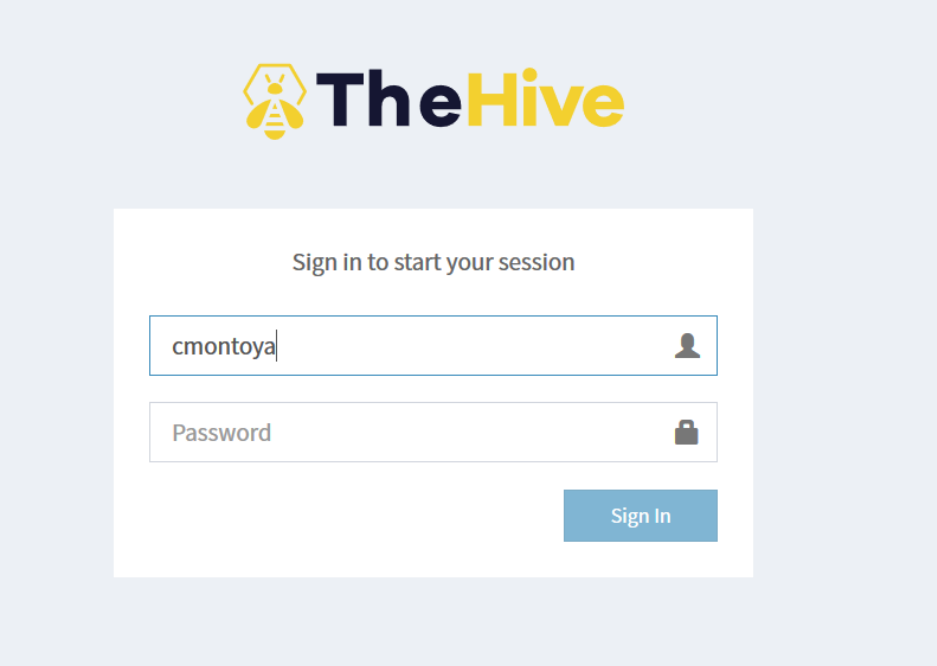

Ilustración 21 login thehive

Una vez dentro podemos ingresar eventos generados por las plataformas de ids

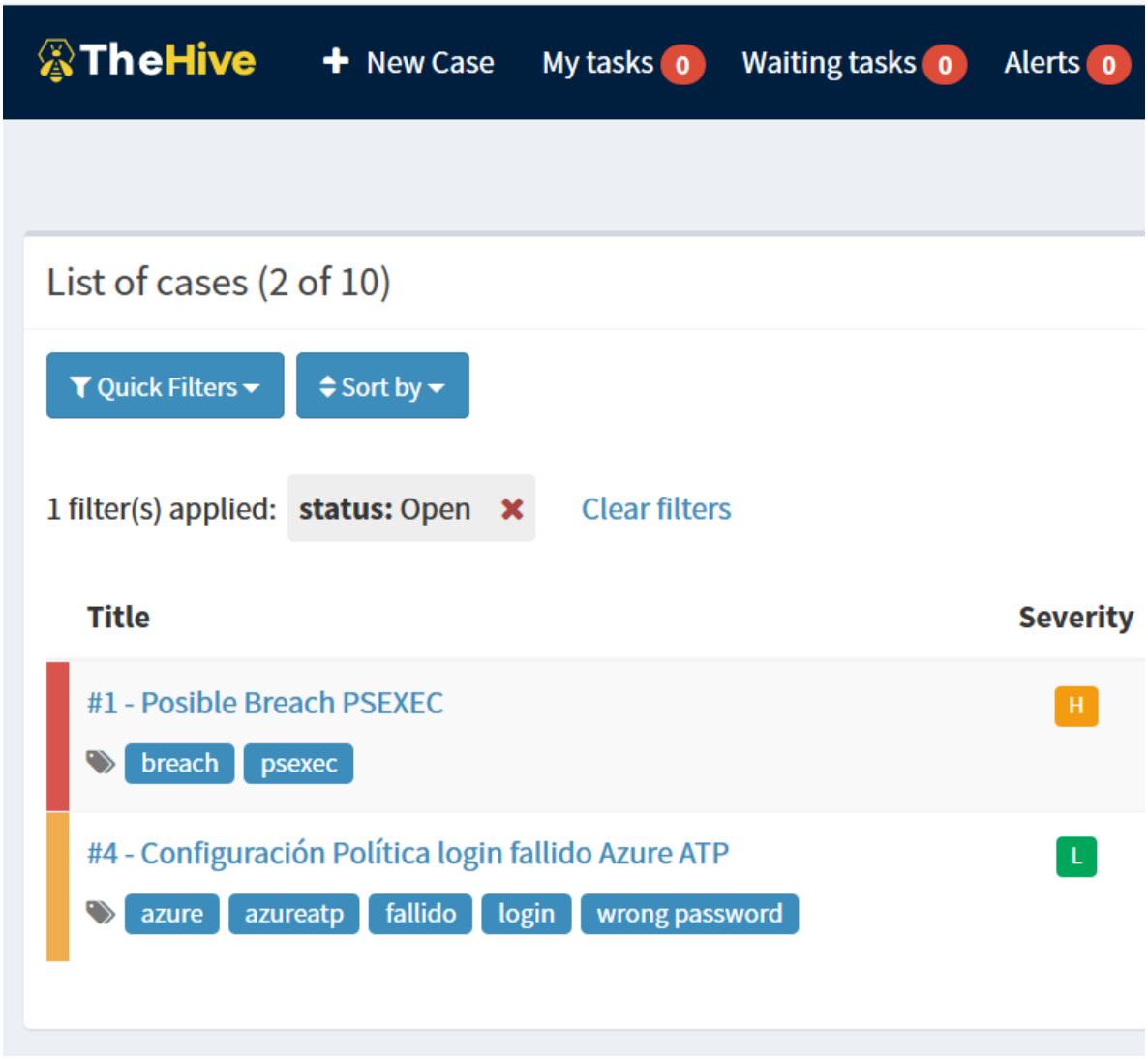

Ilustración 22 detalle de thehive

e. MISP

Para la implementación del misp nos basta con ingresar lo siguiente:

```
    8  wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP
/MISP/2.4/INSTALL/INSTALL.sh ; bash /tmp/INSTALL.sh -c
```

Ilustración 23 Comandos de instalación misp

Ingresamos al misp

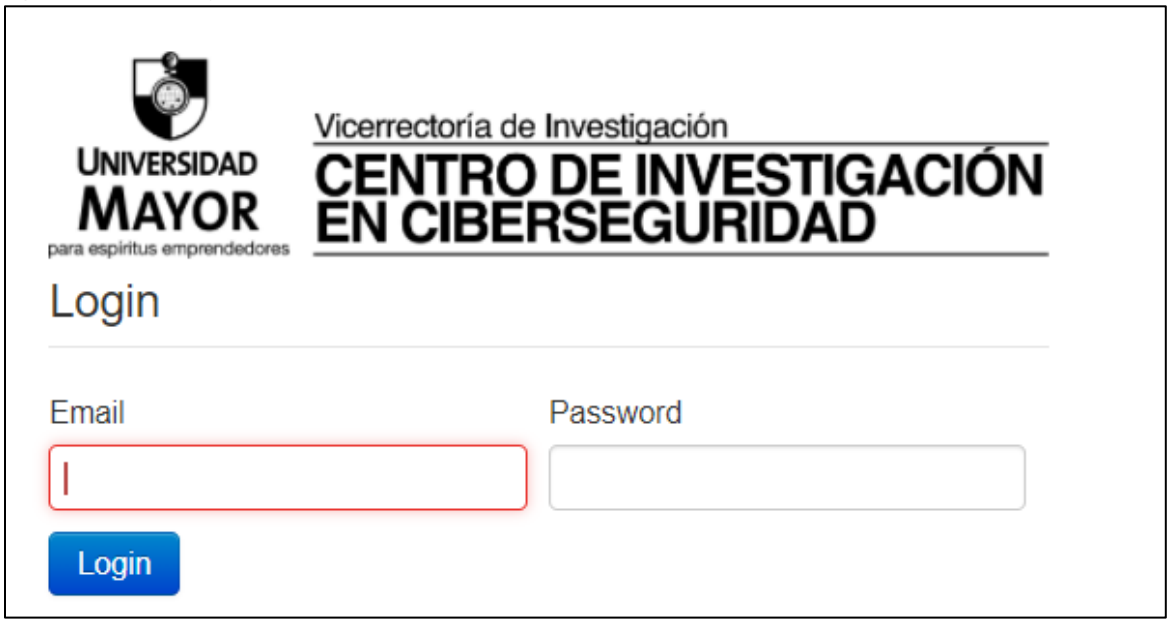

Ilustración 24 login misp

Una vez dentro podemos ingresar los indicadores que detectamos en el centro de monitoreo y desplegarlos a nuestros sistemas de seguridad como es el firewall que declaramos en un inicio.

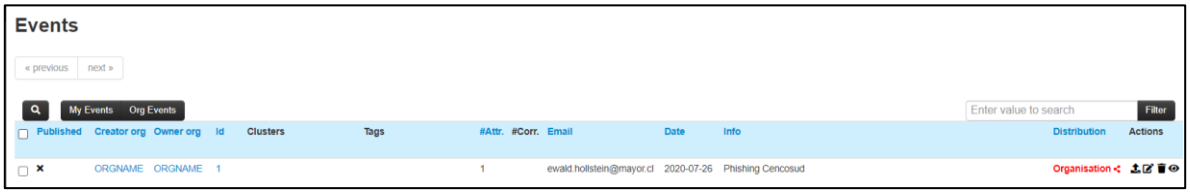

Ilustración 25 detalle de vistas misp

6. Conclusiones

Las herramientas que compartimos en este artículo pueden servir para generar una ciberdefensa en diferentes partes o elementos dentro del ecosistema de la seguridad digital.

En su conjunto, estas herramientas *open source* pueden suministrar seguridad a los activos de la información en una organización. No solamente obtenemos seguridad perimetral a través del Firewall, también se proporciona la capacidad de detectar amenazas con las herramientas de **elastic** como es **Elasticsearch**, **Logstash** y **Kibana,** las que nos permiten acceder a información visual y modelable que facilita la visualización de las amenazas presentes en la red, mientras que **thehive** y **misp** nos ayudan a reaccionar frente a las detecciones que nos muestran los sistemas tanto perimetrales (como el firewall), como de seguridad analítica (como los ids).

Un objetivo central de este artículo es fomentar la seguridad digital a todas las organizaciones que la pueden requerir. En ese sentido, y como miembro del centro de investigación de ciberseguridad de la Universidad Mayor, como presidente de Whilolab, y vicepresidente de Sochisi, quisiera expresar que la ciberseguridad necesita contar con mecanismos que nos permitan reaccionar de mejor forma a los ciberataques de los ciberdelincuentes nacionales como internacionales. Este trabajo quiere aportar en ese sentido, asumiendo que la seguridad digital es una necesidad y tarea de todos, y no solo de algunos.

7. Referencias

Blueliv. (12 de 2019). *Blueliv.* Obtenido de Blueliv: https://www.blueliv.com/resources/white-papers/Finance_whitepaper_ENG.pdf

chile, u. d. (Julio de 2019). *¿ESTÁN PREPARADAS LAS PYMES EN CHILE PARA LA INDUSTRIA 4.0?* Obtenido de ¿ESTÁN PREPARADAS LAS PYMES EN CHILE PARA LA INDUSTRIA 4.0?: https://unegocios.uchile.cl/eventos/estan-preparadas-las-pymes-en-chile-para-la-industria-4-0/

Deloitte. (14 de 12 de 2017). *deloitte.com*. Obtenido de deloitte.com: https://www2.deloitte.com/es/es/pages/manufacturing/articles/que-es-la-industria-4.0.html

Elastic. (2020). *instalaciónde elasticsearch.* Obtenido de https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html

elastic. (2020). *kibana.* Obtenido de https://www.elastic.co/guide/en/kibana/current/deb.html

elastic. (2020). *logstash.* Obtenido de https://www.elastic.co/guide/en/logstash/current/installing-logstash.html

ids, s. (2020). Obtenido de https://suricata-ids.org/

maltrail. (2020). Obtenido de https://github.com/stamparm/maltrail

mincotur. (2017). *.mincotur.gob.es.* Obtenido de .mincotur.gob.es: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ANA%20I%20AYERBE.pdf;

MISP. (2020). *misp-project.* Obtenido de misp-project: https://www.misp-project.org/

NIST. (2018). *NIST.* Obtenido de https://www.nist.gov/cyberframework/online-learning/five-functions

Oracle. (09 de 03 de 2020). *Oracle*. Obtenido de Oracle: https://www.oracle.com/es/applications/enterprise-resource-planning/roles/chief-financial-officer/features/finance-digital-transformation/

pais, D. e. (16 de 02 de 2020). *Ciberataques que matan a las empresas.* Obtenido de Ciberataques que matan a las empresas: https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html

revistaemprende.cl. (30 de 12 de 2019). *revistaemprende.cl.* Obtenido de Seguridad informática en empresas “La pérdida de información de una pyme puede significar su cierre en 6 meses”: https://revistaemprende.cl/seguridad-informatica-en-empresas-la-perdida-de-informacion-de-una-pyme-puede-significar-su-cierre-en-6-meses/

thehive. (2020). *thehive.* Obtenido de the hive: https://thehive-project.org/

trusttech. (2020). *https://www.nsfirewall.cl/.* Obtenido de https://www.nsfirewall.cl/: https://www.nsfirewall.cl/

8. Ilustraciones

9. Reconocimiento

CSIRT agradece la colaboración de Carlos Montoya para participar en la presenta edición de Análisis de Amenazas Cibernéticas dedicada a la seguridad digital para PYMES.

Carlos Montoya fue jefe de informática y oficial de seguridad de la información en la Subsecretaria de Defensa, desempeñando labores por 10 años en esa repartición pública. Además fue jefe de informática de SENDA. Hoy trabaja tanto de forma independiente como en el sector financiero, es Presidente de la Fundación Whilolab, y forma parte de diversas organizaciones, como SC2, TrustTech Felipe Hott y la Universidad Mayor.