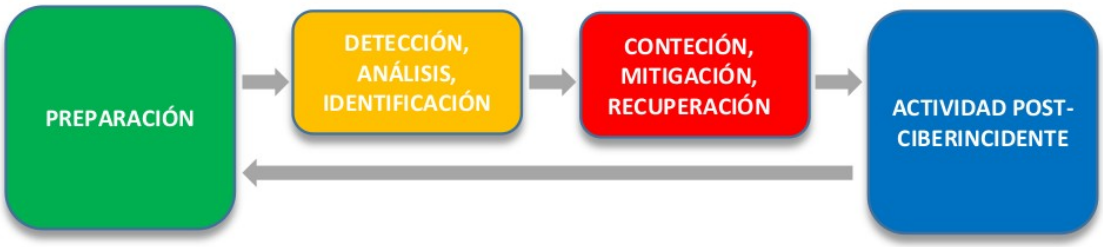
Gestión de los ciberincidentes

En la actualidad la gestión de ciberincidentes se ve como un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.



- **Preparación**: se desplieguen herramientas, se elabora una estrategia y normativa de seguridad en cuanto a la gestión de incidentes, y se desarrollan procesos a seguir por la organización.
- **Detección**: se deben de detectar a través de los canales establecidos en la primera etapa, aquellas brechas de seguridad de los sistemas de información. Para que este etapa suceda, los distintos usuarios que actúan en los sistemas de información han tenido que disponer de formación y casos prácticos, para que puedan detectar de las brechas. Así mismo, existen sistemas automatizados de seguridad que realizan las detecciones.
- **Análisis/Identificación**: hay que investigar el incidente, determinar su alcance y los sistemas afectados. Para ello es necesario recurrir a la información recogida en los logs, sistemas de alertas, ... La fase de preparación es fundamental para poder tener datos sobre los que trabajar para analizar el incidente.
- **Contención**: si un atacante ha logrado comprometer un dispositivo, se debe evitar que pueda comprometer un segundo; si ha logrado extraer un documento del servidor de archivos, la labor del equipo de respuesta, en este momento, es evitar que salga más información al exterior.
- **Mitigación**: la medida de mitigación más adecuada suele empezar por realizar un borrado seguro de los medios de almacenamiento comprometidos y una reinstalación del sistema pero desgraciadamente no siempre posible; en algunos casos porque no existe una copia de seguridad reciente de la información y en otros casos porque volver a poner un sistema en producción sin conocer las causas del ciberincidente puede acarrear un nuevo e idéntico problema.

  Las medidas de mitigación dependerán del tipo de ciberincidente, así, en casos de denegaciones de servicio distribuidas (DDoS) puede ser necesario solicitar asistencia de entidades externas, que puedan apoyar en el análisis y definición de la estrategia de mitigación.
- **Recuperación**: se trata de de devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes.

  Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa como procesos extraños, cuentas de usuario no autorizadas, nuevas entradas en el registro, conexiones no identificadas, cualquier síntoma que pueda indicar que el problema está volviendo a ocurrir.
- **Actividad post-incidente**: cuando se ha vuelto a la normalidad es momento de analizar las causas del problema y la forma en que se ha desarrollado la actividad durante la gestión del incidente. La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir. Esto ayudará también a evaluar los procedimientos de actuación, la cadena de mando, las políticas de seguridad y entrenará a los Implicados para futuras situaciones de crisis.

Network-based evidence (NBE)

En la gran mayoría de ciberincidentes, los atacantes se aprovechan de algún modo de las redes de comunicaciones: envío de spam, descarga de adjuntos maliciosos, descarga de artefactos al equipo víctima tras la infección, comunicación con el equipo víctima mediante canales C2 (Command and Control), exfiltración de información, movimientos laterales, ...

Para poder detectar esta actividad es necesario la recolección y análisis de evidencias de red:

- Full content data
- Session data (flows)
- Alert data
- Statistical data

A mayores están los registros (logs) de dispositivos como firewalls, routers, servidores web, ..., que también pueden reflejar las actividades de los cibercriminales.

Full Content data

Se trata de capturas de los paquetes que circulan por la red y que permite a los analistas acceder a toda la información del paquete: cabeceras de los distintos protocolos y datos de usuario.

```
▾ Ethernet II, Src: Dell_c2:09:6a (a4:1f:72:c2:09:6a), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
  ▸ Destination: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
  ▸ Source: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.4.10.4, Dst: 10.4.10.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 83
    Identification: 0x095f (2399)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xc8ab [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.4.10.4
    Destination: 10.4.10.132
▾ User Datagram Protocol, Src Port: 53, Dst Port: 54662
    Source Port: 53
    Destination Port: 54662
    Length: 63
    Checksum: 0x5fd4 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▸ [Timestamps]
▾ Domain Name System (response)
    Transaction ID: 0xa002
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ proforma-invoices.com: type A, class IN
  ▾ Answers
    ▾ proforma-invoices.com: type A, class IN, addr 217.182.138.150
        Name: proforma-invoices.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 14398 (3 hours, 59 minutes, 58 seconds)
        Data length: 4
        Address: 217.182.138.150
    [Request In: 204]
    [Time: 0.786002000 seconds]
```

El cifrado de las comunicaciones hace que parte de la información que aportan los paquetes quede oculta, pero siguen siendo muy útiles gracias a todo lo que no va cifrado. Suponen un reto para las organizaciones por el espacio de almacenamiento que conllevan y también para el analista por el gran volumen de información que aportan.

Session data (*flows*)

Los *session data* proporcionan información sobre los *network Flow* (*stream*) o flujo de red, que vienen a ser un grupo de paquetes asociados junto con metadatos y normalmente correspondientes a una conversación entre dos entidades de red

A continuación se ve como una conversación entre dos equipos consistente en 1312 paquetes se transforma en un *network flow*:

```
192.168.0.110     150.214.5.135     TCP      74 57228 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=546218 TSecr=0 WS=32
150.214.5.135     192.168.0.110     TCP      74 80 → 57228 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1452 SACK_PERM=1 TSval=2596279322 TSecr=546218 WS=512
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=546236 TSecr=2596279322
192.168.0.110     150.214.5.135     HTTP   1506 GET /ubuntu/dists/lucid/Release.gpg HTTP/1.1 GET /ubuntu/dists/lucid/main/i18n/Translation-es.bz2 HTTP/1.1 GET /ubuntu/dists/luc
192.168.0.110     150.214.5.135     HTTP    934 GET /ubuntu/dists/lucid-updates/Release.gpg HTTP/1.1 GET /ubuntu/dists/lucid-updates/main/i18n/Translation-es.bz2 HTTP/1.1 GET /
150.214.5.135     192.168.0.110     TCP      66 80 → 57228 [ACK] Seq=1 Ack=1441 Win=8704 Len=0 TSval=2596279437 TSecr=546237
150.214.5.135     192.168.0.110     HTTP    231 HTTP/1.1 304 Not Modified
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2309 Ack=166 Win=6912 Len=0 TSval=546265 TSecr=2596279438
150.214.5.135     192.168.0.110     HTTP    234 HTTP/1.1 304 Not Modified
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2309 Ack=334 Win=8000 Len=0 TSval=546266 TSecr=2596279439
150.214.5.135     192.168.0.110     HTTP   1506 HTTP/1.1 304 Not Modified HTTP/1.1 304 Not Modified HTTP/1.1 304 Not Modified HTTP/1.1 200 OK  (text/plain)HTTP/1.1 404 Not Fou
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2309 Ack=1774 Win=10880 Len=0 TSval=546285 TSecr=2596279509
150.214.5.135     192.168.0.110     HTTP   1433 HTTP/1.1 404 Not Found  (text/html)HTTP/1.1 404 Not Found  (text/html)HTTP/1.1 404 Not Found  (text/html)
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2309 Ack=3141 Win=13792 Len=0 TSval=546286 TSecr=2596279509
192.168.0.110     150.214.5.135     HTTP    526 GET /ubuntu/dists/lucid/Release HTTP/1.1 GET /ubuntu/dists/lucid-updates/Release HTTP/1.1
150.214.5.135     192.168.0.110     HTTP    233 HTTP/1.1 304 Not Modified
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2769 Ack=3308 Win=16672 Len=0 TSval=546947 TSecr=2596282165
150.214.5.135     192.168.0.110     TCP    1506 80 → 57228 [ACK] Seq=3308 Ack=2769 Win=14848 Len=1440 TSval=2596282166 TSecr=546926 [TCP segment of a reassembled PDU]
192.168.0.110     150.214.5.135     TCP      66 57228 → 80 [ACK] Seq=2769 Ack=4748 Win=19552 Len=0 TSval=546949 TSecr=2596282166
150.214.5.135     192.168.0.110     TCP    1506 80 → 57228 [ACK] Seq=4748 Ack=2769 Win=14848 Len=1440 TSval=2596282166 TSecr=546926 [TCP segment of a reassembled PDU]
```

```
                                                  |       <-      | |       ->      | |     Total     |      Absolute Date    |   Duration   |
                                                  | Frames  Bytes | | Frames  Bytes | |  Frames  Bytes |          Start        |              |
192.168.0.110:57228     <->     150.214.5.135:80        761   1126387     551     46994     1312   1173381    2011-07-18 10:22:02        13,4380
```

Para un analista, los *session data* le proporcionan información suficiente para responder a las siguientes preguntas:

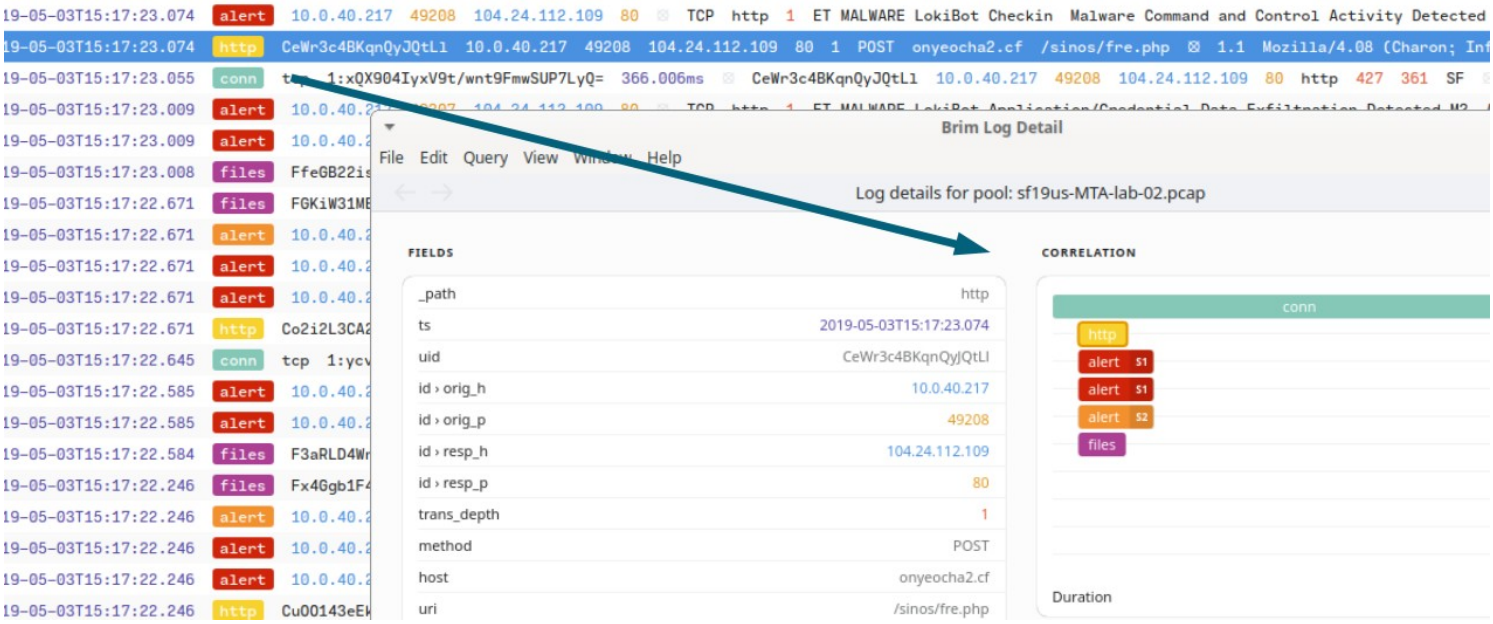
- ¿Quién habló con quien?
- ¿Cuándo?¿durante cuánto tiempo?
- ¿bytes/paquetes transmitidos y en qué sentido?

El cifrado de las comunicaciones no les afecta y no suponen el reto de espacio de almacenamiento de los *full content data*.

Al hablar de *session data* hay que hablar de *Netflow*, introducido por Cisco y cuyo definición tradicional es la de una secuencia unidireccional de paquetes que comparten los siguientes 7 valores:

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto UDP o TCP de origen.
- Puerto UDP o TCP de destino.
- Protocolo IP.
- Interfaz
- Tipo de servicio IP

Especialmente relevante es Zeek que analiza el tráfico de red y crea *transaction logs* con información detallada no sólo de los flujos de paquetes, sino también de los protocolos de nivel de aplicación. En la siguiente imagen puede verse una captura de Brim (software que proporciona una interfaz gráfica a Zeek y al IDS Suricata). Puede apreciarse como a mayores de la información de sesión (*conn*) hay información de la transacción http asociada: método http usado, cabeceras host, uri, user-agent, ...



Alert data

Las alertas se generan al detectarse un evento de interés (patrón de bytes o de actividad, ...). Típicamente las alertas las generan los NIDS (*Network Intrusion Detection Systems*) como Suricara o Snort en base a un conjunto de reglas. En las siguientes imágenes se ve la regla Emerging-malware.rules – SID: 2031241 que detecta la exfiltración de documentación por parte del malware Trickbot y un paquete http que la dispara:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Win32/Trickbot Data Exfiltration";
flow:established,to_server; http.method; content:"POST"; http.request_body; content:"name=|22|proclist|22|";
content:"svchost.exe"; content:"name=|22|sysinfo|22|"; content:"ipconfig"; content:"net view /all";
fast_pattern; content:"nltest"; distance:0; reference:md5,f99adab7b2560097119077b99aceb40d; classtype:command-
and-control; sid:2031241; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target Client_Endpoint, created_at 2020_11_27, deployment Perimeter, former_category MALWARE,
performance_impact Low, signature_severity Major, updated_at 2020_11_27;)
```

```
POST /lib496/PHANTASMEDIA-DC_W617601.160C6A2D543C55638A9E11592C15203B/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=Arasfjasu7
User-Agent: test
Host: 186.159.1.217:8082
Content-Length: 4597
Cache-Control: no-cache

--Arasfjasu7
Content-Disposition: form-data; name="proclist"

              ***PROCESS LIST***

[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
svchost.exe
```

Para que los NIDS sean útiles hay que configurar adecuadamente las reglas para evitar los falsos positivos y negativos y maximizar los positivos verdaderos:

- Falso positivo (*false positive*): se dispara una alerta para tráfico esperado, pero que el NIDS considera malicioso.
- Falso negativo (*false negative*): hay tráfico malicioso pero el NIDS no lo detecta.
- Positivo verdadero (true positive): cuando hay tráfico malicioso es detectado por el NIDS.

Statistical data

Existen diferentes tipos de datos estadísticos: jerarquía de protocolos, equipos más/menos activos, conversaciones, tamaño medio de paquetes, ratios, ...

Los datos estadísticos ofrecen al analista información sobre duración de captura, horas de inicio/fin, equipos menos activos, horas de tráfico punta, tamaño medio de paquete, ...

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	3334	100.0	2083406	153 k
Ethernet	100.0	3334	2.2	46676	3.442
Internet Protocol Version 4	99.6	3320	3.2	66400	4.897
User Datagram Protocol	4.2	141	0.1	1128	83
NetBIOS Datagram Service	0.1	2	0.0	402	29
SMB (Server Message Block Protocol)	0.1	2	0.0	238	17
SMB MailSlot Protocol	0.1	2	0.0	50	3
Microsoft Windows Browser Protocol	0.1	2	0.0	66	4
Multicast Domain Name System	0.1	3	0.0	132	9
Domain Name System	1.4	46	0.1	2990	220
Data	2.7	90	0.1	2880	212
Transmission Control Protocol	94.3	3144	94.0	1958258	144 k
Malformed Packet	0.0	1	0.0	0	0
Hypertext Transfer Protocol	9.1	305	78.4	1633697	120 k
Portable Network Graphics	0.2	6	0.6	12385	913
Media Type	0.5	16	58.7	1222598	90 k
Line-based text data	1.3	42	10.2	212565	15 k
JPEG File Interchange Format	0.2	6	0.9	19753	1.456
Compuserve GIF	0.5	16	0.2	5089	375
FTP Data	0.1	2	0.1	1602	118
Line-based text data	0.1	2	0.1	1602	118
File Transfer Protocol (FTP)	0.8	27	0.1	1711	126
Internet Control Message Protocol	1.0	35	0.1	1388	102
Address Resolution Protocol	0.4	14	0.0	554	40

Forense en red: metodología OSCAR

ENISA (*European Union Agency for Network and Information*) propone la metodología OSCAR:

- Obtener información (*Obtain information*): en la primera fase se debe recopilar información sobre el incidente en sí y el entorno:
  - Fecha y hora de la detección del incidente.
  - Personas y sistemas involucrados.
  - Qué sucedió inicialmente.
  - Qué acciones se tomaron desde la detección.
  - Quién está al cargo.
  - Entorno del incidente (personas, equipamientos, organización, ...)
- Planificación (*Strategize*): debido a la volatilidad de las evidencias de red, la investigación debe planificarse cuidadosamente. A diferencia de otras evidencias forenses, como archivos en disco duros, los paquetes de red que no se capturan no se pueden recuperar. Hay que planificar la adquisición de evidencias teniendo en cuenta:

  - La volatilidad.
  - El valor potencial para la investigación.
  - El esfuerzo/coste para obtenerlas.
  - Restricciones legales/normativas.
- Adquisición de evidencias (*Collect evidence*): ver transparencias/vídeo
- Análisis (*Analyse*): en esta fase se tratará de dar respuesta a las preguntas propias de una investigación forense:
  - ¿Qué sucedió?
  - ¿Dónde y cuándo sucedió?
  - ¿Quién está involucrado?
  - ¿Cómo y por qué?

  Típicos puntos de partida en un análisis son:
  - Alertas IDS.
  - Anomalías evidentes: actividad de virus o DoS.
  - Anomalías en los logs.
  - Desviaciones de parámetros normales de funcionamiento (*baseline*).
  - Marco temporal.

  Indicadores de compromiso (*IoC - Indicators Of Compromise*) se encuentran en:
  - Direcciones IP extranjeras (de países sin relación con la organización).
  - Logins desde múltiples IPs y/o horas inusuales.
  - Gran número de intentos fallidos de login.
  - Consultas anormales desde un equipo.
  - Dominios DNS sospechosos:
    - longitud de consulta superior a 25 caracteres (posible exfiltración a través de canales DNS).
    - más de 5 respuestas.
    - dominios TLD (*Top Level Domain*) sospechosos: .ga, .biz, .work, .click, .loan, ... (usados frecuentemente por malware).
    - creados recientemente.
    - nombres de dominio generados 'aleatoriamente' usando DGA (*Domain Generation Algorithms*) (p.e. *e2b483cf1ac9ca728aa712298d3390f2.ue*).

ts	_path	id › orig_h	id › resp_h	id › resp_p	proto	query
2021-06-09T04:28:44.825	dns	10.20.57.3	10.10.2.22	53	udp	e7f1018ea0310f25bba0610936fd1cc2af.cisco-update.com
2021-06-09T04:28:45.678	dns	10.20.57.3	10.10.2.22	53	udp	0cfe016cb105e87901f6020958d084ff84.cisco-update.com
2021-06-09T04:28:45.833	dns	10.20.57.3	10.10.2.22	53	udp	4ecd018ea07bdf2f097a3f093785aca8a5.cisco-update.com
2021-06-09T04:28:46.743	dns	10.20.57.3	10.10.2.22	53	udp	68db016cb1578377236f60095966668cb6.cisco-update.com
2021-06-09T04:28:46.898	dns	10.20.57.3	10.10.2.22	53	udp	98da018ea0b4c09d26d9f9093892846540.cisco-update.com
2021-06-09T04:28:47.753	dns	10.20.57.3	10.10.2.22	53	udp	0c5a016cb1989be2677eef095a045ee12e.cisco-update.com
2021-06-09T04:28:47.903	dns	10.20.57.3	10.10.2.22	53	udp	bb9f018ea06b115c282fa8093935ece49d.cisco-update.com
2021-06-09T04:28:48.764	dns	10.20.57.3	10.10.2.22	53	udp	d6c8016cb1fb1d5f3add05095b8474f090.cisco-update.com
2021-06-09T04:28:48.967	dns	10.20.57.3	10.10.2.22	53	udp	08cd018ea04fcf8ff1e5e1093a8a8a82b1.cisco-update.com
2021-06-09T04:28:49.825	dns	10.20.57.3	10.10.2.22	53	udp	dc85016cb1f2bf4592825b095c41d4cb5f.cisco-update.com
2021-06-09T04:28:49.980	dns	10.20.57.3	10.10.2.22	53	udp	cd79018ea0edb0256e0549093b284e5b5f.cisco-update.com
2021-06-09T04:28:50.845	dns	10.20.57.3	10.10.2.22	53	udp	2877016cb14f9f5b1aa181095d144bdc1a.cisco-update.com

  - Agentes de usuario/certificados digitales sospechosos.

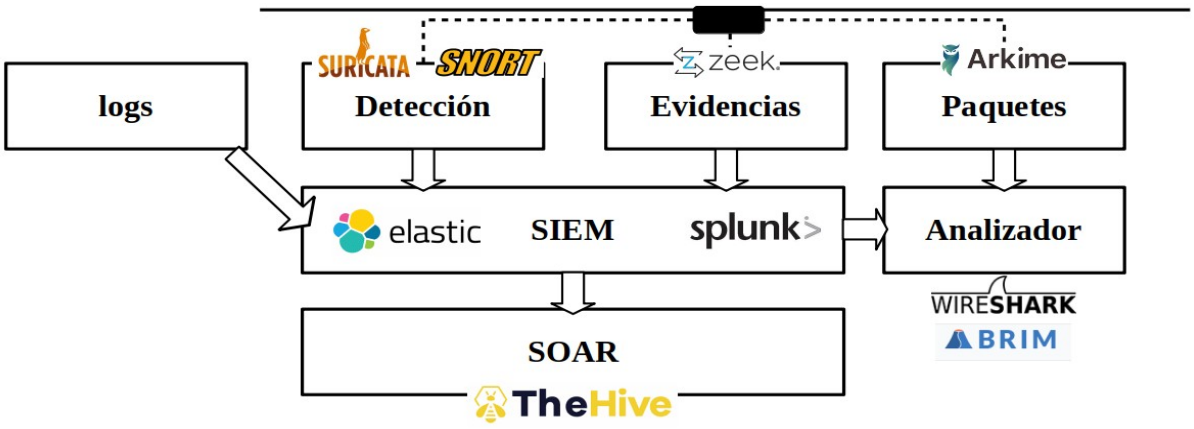
- Protocolos o tráfico a puertos inusuales (dns a tcp/80, tftp, 69/udp, RDP 3389/tcp, ...)
- Peticiones http masivas (posible canal de mando y control C2).
- Tamaño de respuestas HTML.
- Extensiones de fichero que no se corresponden con el tipo. A continuación puede verse como aparentemente se descarga una imagen .gif, cuando realmente es un ejecutable.

```
GET /counter/?
id=5552505E160B060116101724160507OF17140507014A070B095E3C5E060A1E4A070B094A091D5E17555E555050525C50505555505E55&
rnd=3090341 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: kennedy.sitoserver.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 06 Nov 2015 22:22:42 GMT
Server: Apache
Content-Disposition: attachment; filename=a340de8dc.gif
Content-Length: 323045
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/gif

MZ.....................@.....................................  .!..L.!This program cannot be run in DOS
mode.

$...........si..si..si..ld..si.Rich.si.......................PE..L.....<V.............`.................
.p....@.....................................................................c.
```

- Informe (*Report*): debe generarse un informe que detalle los resultados. Debe haber dos informes o un único informe con dos partes en caso:
  - Informe ejecutivo: destinado a ejecutivos o directores que no tienen porque tener amplios conocimiento técnicos, por lo que debe informar de los resultados para que los directivos lo entiendan pero sin entrar en detalles técnicos concretos
  - Informe técnico: destinado a personal técnico explicando con detalle lo sucedido apoyándose en las evidencias recogidas y analizadas.

Network Detection & Response

Para abordar las etapas de detección, análisis e identificación es necesario tener desplegada una infraestructura que permita recolectar datos y alimentar a un sistema que permita su análisis en el SOC (*Security Operation Center*). En la figura se muestra el esquema de un sistema de detección y respuesta de red.



- Los **NIDS** (***Network Intrusion Detection Systems***) operan supervisando el tráfico de un segmento de red concreto en busca de anomalías en el mismo, ya sea en el contenido de los paquetes, en la desviación con respecto a las especificaciones de los protocolos involucrados o en la variación con respecto a los perfiles habituales. Al detectar items de interés generan alertas que son enviadas al SIEM.
- Los **NSM** (***Network Security Monitor***) como Zeek generan logs relativos al tráfico de red que son enviados al SIEM.
- Firewalls, routers, switches, servidores web, ..., envían también sus logs al SIEM.
- En el **SIEM** (***Security Information and Event Management***) el analista tiene acceso a los datos procedentes de las distintas fuentes de información y podrá analizarlos encontrando relaciones entre ellos. Los SIEM están diseñados para recopilar eventos de seguridad a partir de una amplia variedad de fuentes dentro de una organización. Una vez que el SIEM tiene los eventos, procesa los datos para estandarizarlos, lleva a cabo el análisis de los datos "normalizados", genera alertas cuando detecta actividad anómala, y produce informes a petición de los administradores.
- Si es posible a mayores se realizan capturas de red para su revisión durante el análisis de las incidencias.
- El **SOAR** (*Security Orchestration, Automation and Response*) permite coordinar, ejecutar y automatizar tareas como respuesta a los incidentes detectados.

Todas las piezas de la infraestructura son importantes, pero especialmente relevante es el SIEM que es capaz de tomar grandes cantidades de datos y convertirlas en información, permitiendo a los analistas convertir esa información en conocimiento/inteligencia que permitirá la toma de decisiones.