

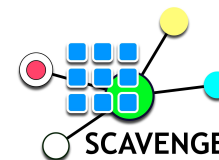


Implantación de una plataforma de monitoritzación de la seguridad informática con Security Onion

David COMPANYY ESTALL
david.company@cttc.es

¿Qué es el CTTC?

- Centre Tecnològic de Telecomunicacions de Catalunya:
Fundación sin ánimo de lucro dedicada a la investigación en tecnologías y sistemas de comunicaciones y geomática.
- 5G, Smart Grids, Optical networks, SDN, DSP, M2M, satélites, sistemas de navegación
- Infraestructuras TI
 - Varios data-centers y testbeds, repartidos en dos edificios
 - 120 usuarios
 - 40 Servidores físicos/ virtuales: email, servidores web, servidores de ficheros, simulaciones,...
 - Red ethernet y red wireless



Plataforma de monitorización de la seguridad

Funciones:

- Detección de intrusiones -> monitorización de eventos en red y equipos informáticos en busca de incidentes de seguridad
 - Capturas de paquetes
 - Datos de sesión y transacciones de datos
 - Genera alertas de seguridad de Host y de red
- Análisis de logs -> detectar ataques usando logs
 - Recepción, parseo, filtrado y agregación de eventos y logs
 - Almacenamiento: compresión, normalización, indexación



Plataforma permite gestionar

- Correlación de eventos, gestión de alertas e incidentes, generación de informes, investigación forense

Security Onion

- Distribución Linux basada en Ubuntu que contiene varias herramientas de seguridad: Snort, Suricata, Bro, OSSEC, Sguil, Squert, CapMe, NetworkMiner, WireShark, ELSA (ahora logstash + Kibana), etc.
- Todas las herramientas están integradas
 - complementadas y es sencillo pivotar de una a otra
 - sencillo de instalar y poner en marcha
- Permite la detección de intrusiones y monitorización de red y la gestión de eventos de seguridad.

<https://securityonion.net>

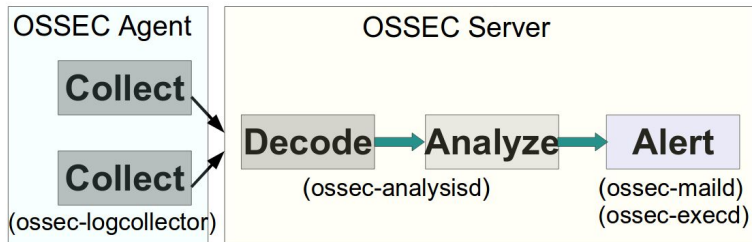


OSSEC - HIDS



Sistema de detección de intrusiones de host Open-Source

- Análisis automático de logs del host -> basado en reglas
- Verificación de la integridad de los ficheros
- Detección de rootkits
- Respuesta activa y envío de avisos en tiempo real
- Arquitectura basada en un servidor + agentes en los servidores a monitorizar



Snort - NIDS



Network IDS Open-source

- Funcionamiento
 - Sensores que capturan paquetes de red
 - Se realiza un preprocesado i normalización del tráfico
 - El resultado es comparado con patrones y reglas definidos internamente
 - Detecta amenazas o ataques y generar alertas
- Motor de detección basado en reglas se actualizan automáticamente mediante la funcionalidad pulled-pork des de repositorios gratuitos o de pago (ET)
- Se puede escoger Suricata



Bro Network Security Monitor



Framework de Monitorización de red

- Monitoriza la actividad de red y genera logs de las conexiones TCP/UDP, peticiones DNS, servicios de red y software detectados, actividad HTTP, FTP, IRC, SMTP, SSH, SSL, etc.
- Bro incluye analizadores para los protocolos más comunes
- La información se recoge en una base de datos y se puede consultar mediante ELSA o Logstash y Kibana-> complemento con información de contexto a la hora de analizar alertas.

Sguil



Consola de analista de seguridad.

- Interfaz gráfica intuitiva con la que acceder a las alertas de seguridad, los datos de sesión y las capturas de datos.
- Toda esta información se almacena en una base de datos a la que sguil accede
- Herramientas integradas CapMe, Wireshark y Network Miner
- No solo tenemos acceso a la alerta, sino también al contexto en que se ha producido

Sguil (II)

The screenshot shows the Sguil interface with the following components:

- Event History Table:**

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dat IP	DPort	Pr	Event Message
RT	3	david-virt...	3.1	2018-05-01 07:46:09	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New group added to the system
RT	3	david-virt...	3.2	2018-05-01 07:46:09	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] New user added to the system
RT	41	david-virt...	3.7	2018-05-01 07:46:38	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity checksum changed.
RT	11	david-virt...	3.12	2018-05-01 07:49:22	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Received 0 packets in designated time interval (defined in ossec.co...
RT	3	david-virt...	3.13	2018-05-01 07:50:30	0.0.0.0	0.0.0.0	0.0.0.0	0	0	[OSSEC] Integrity checksum changed again (2nd time).
RT	221	david-virt...	2.1	2018-05-01 09:37:34	10.1.1.97	49160	34.233.12.25	80	6	ET TROJAN Formbook 0.3 Checkin
RT	1	david-virt...	2.22	2018-05-01 09:55:51	10.1.1.213	55269	10.1.1.1	53	17	ET INFO DNS Query for Suspicious_gdn Domain
RT	4	david-virt...	2.22	2018-05-01 09:57:11	184.172.60.198	5938	10.1.1.213	49168	6	ET POLICY TeamViewer Keep-alive inbound
- Alert Details:** alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET TROJAN Formbook 0.3 Checkin";)
- Packet Details Table:**

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	10.1.1.97	34.233.12.25	4	5	0	1328	80	2	0	128	47892
TCP	Source Port	Dest Port	R R R	C C C	S S S	S S S	Y Y Y	I I I			
	49160	80	.	.	X
DATA	50 4F 53 54 20 2F 6F 62 2F 20 48 54 50 2F 31										

The screenshot shows a web browser window with the following content:

- File**
- Sensor Name:** david-virtualbox-eth1-1
- Timestamp:** 2018-05-01 09:37:34
- Connection ID:** david-virtualbox-eth1-1_1
- Src IP:** 10.1.1.97
- Dst IP:** 34.233.12.25
- Src Port:** 49160
- Dst Port:** 80
- OS Fingerprint:** 10.1.1.97:49160 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
- OS Fingerprint:** Signature: [8192:128:1:52:M1460,N,W8,N,S;:Windows:?]
- OS Fingerprint:** -> 34.233.12.25:80 (distance 0, link: ethernet/modem)
- SRV:** POST /ob/ HTTP/1.1
- SRV:** Host: www.jvfilmmakers.com
- SRV:** Connection: close
- SRV:** Content-Length: 455565
- SRV:** Cache-Control: no-cache
- SRV:** Origin: http://www.jvfilmmakers.com
- SRV:** User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
- SRV:** Content-Type: application/x-www-form-urlencoded
- SRV:** Accept: */*
- SRV:** Referer: http://www.jvfilmmakers.com/ob/
- SRV:** Accept-Language: en-US
- SRV:** Accept-Encoding: gzip, deflate
- SRV:** SRV:
- SRV:** dat=bWuCYce8YsQtnfnRzJAlj06p8bA6OQmTfFopKt5o2dQL2i5bV87aR9sPebqYP0AtmALeEr5EK-h5SDgG5sHlmy3yrcVl2uWvNydTWj9LQeM1sCpzdVHMUG9Zxy5OI6ZWXe9ERDZ_jkXTC5MHMqjbVUGvT056c3cly9ENAvjR3y3yeh2li7R8RvUeOzM7DB_V8d5w7StdyomFxlse960uBN0sd9x5FyPThu2DDH99X_3NbZp0ZwVdQcWbaTgoXPm6MgnOp08TRyMDD0UnYrr6EY2ArwyxOb-7LDrSL0DtbNqJQq7YrTv_WHacpHrs-6CL7PUX7z-qFzqPynDia69n503u9HHuok48Pfl2Zs3QPeg43_UnSou7yxKZ9z9HV
- Buttons:** Search, Abort, Close
- Text:** Debug Messages

- Event History
- Transcript
- Transcript (force new)
- Wireshark
- Wireshark (force new)
- NetworkMiner
- NetworkMiner (force new)
- Bro
- Bro (force new)

The screenshot shows the Wireshark interface with the following details:

- Filter:** 10.1.1.97:49160 -> 34.233.12.25:80 & fam [Wireshark 1.12.1] [Get Raw Unknown from unknown]
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.97	34.233.12.25	TCP	66	49160->80
2	0.129153	34.233.12.25	10.1.1.97	TCP	62	80->49160
- Packet Details:**
 - Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 - Ethernet II, Src: 08:02:15:04:9a:e7 (08:02:15:04:9a:e7), Dst: 08:00:0c:7c:39:da:12 (08:00:0c:7c:39:da:12)
 - Internet Protocol Version 4, Src: 10.1.1.97 (10.1.1.97), Dst: 34.233.12.25 (34.233.12.25)
 - Transmission Control Protocol, Src Port: 49160 (49160), Dst Port: 80 (80), Seq: 0, Len: 0
- Packet Bytes:**

```
0000 00 00 7c 39 da 12 00 22 15 04 9a e7 00 00 45 00 ...E...
0010 00 24 00 4e 40 00 00 00 c0 12 00 01 01 61 22 09 ...4.NQ...
0020 0c 19 c0 00 00 50 3e e5 95 k2 00 00 00 00 02 .....Pa..B.....
0030 20 00 00 0c 00 00 02 04 05 04 01 03 03 03 01 .....man..A..?..
```

Squert

the squertproject

Aplicación web de visualización de los eventos:

- Consola de analista complementaria de sguil
- Aporta información de contexto, agrupación de eventos, timeline
- Consulta la base de datos de sguil -> se basa en los mismos datos pero los muestra de manera diferente



ELSA

Plataforma de registro y visualización de logs -> Interfaz web para poder hacer búsquedas en los datos y logs recogidos en la plataforma (ahora logstash y Kibana)

The screenshot displays the ELSA web interface. On the left is a navigation menu with categories like Connections, DHCP, DNP3, DNS, Files, Firewall, FTP, Host Logs, HTTP, Intel, IRC, Kerberos, Modbus, MySQL, Notice, PE, RADIUS, RDP, RFB, and SIP. The main area shows a search query for '115.77.78.20'. Below the query bar, there are options for 'From' (2018-04-30 16:22:07) and 'To', along with buttons for 'Submit Query', 'Help', 'UTC', 'Add Term', 'Report On', 'Index', 'Reuse current tab', and 'Grid display'. A 'Field Summary' section lists various fields like host, program, class, srcip, dstip, etc. Below that, a table shows search results with columns for 'Timestamp' and 'Fields'. The results include log entries with timestamps and detailed field information.

Timestamp	Fields
Wed May 02 16:11:20	1525270279.428978 CC68C81Q04UmKEmEi 115.77.78.20 54579 10.2.1.15 80 1 GET iptechwiki.ctc.es /Main_Page http://iptechwiki.ctc.es/[1.1 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36 text/html host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=115.77.78.20 srcport=54579 dstip=10.2.1.15 dstport=80 status_code=301 content_length=351 method=GET user_agent=Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36 mime_type=text/html
Wed May 02 16:11:20	1525270279.429919 FKk05o4D78E8EMV37 10.2.1.15 115.77.78.20 CC68C81Q04UmKEmEi HTTP 0 MD5,SHA1 text/html - 0.00000 T F 351 351 0 0 F - 823ef5c2882 host=127.0.0.1 program=bro_files class=BRO_FILES seen_bytes=351 total_bytes=351 missing_bytes=0 tx_hosts=10.2.1.15 rx_hosts=115.77.78.20 source=HTTP mime_type=application/javascript sha1=9f9635141b077a792c9353ed5e4e5b739a67099
Wed May 02 16:11:22	1525270281.937817 C2wXYE23NrrOfRsp 115.77.78.20 54654 10.2.1.15 80 1 GET networks.ctc.es /mobile-networks/software-tools/lena http://iptechwiki.ctc.es/like Gecko) Chrome/39.0.2171.99 Safari/537.36 28961 200 OK -(empty) - F IE Fberoff 4IG5 -[text/html host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=115.77.78.20 srcport=54654 dstip=10.2.1.15 dstport=80 status_code=200 content_length=28961 method=GET referer=http://iptechwiki.ctc.es/Main_Page user_agent=Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36 mime_type=application/javascript sha1=633db97096d05e622149a1196cb568f568d412
Wed May 02 16:11:22	1525270282.095423 FLIEJFberoff 4IG5 10.2.1.15 115.77.78.20 C2wXYE23NrrOfRsp HTTP 0 MD5,SHA1 text/html - 0.000054 T F 28961 - 0 0 F - 4ae2a6372319e204 host=127.0.0.1 program=bro_files class=BRO_FILES seen_bytes=28961 total_bytes=0 missing_bytes=0 tx_hosts=10.2.1.15 rx_hosts=115.77.78.20 source=HTTP mime_type=application/javascript sha1=c633db97096d05e622149a1196cb568f568d412
Wed May 02 16:11:23	1525270282.600378 FwG35tcdH08xmEhf 10.2.1.15 115.77.78.20 C2wXYE23NrrOfRsp HTTP 0 MD5,SHA1 text/html - 0.00000 T F 357 357 0 0 F - d58b4aae01c28 host=127.0.0.1 program=bro_files class=BRO_FILES seen_bytes=357 total_bytes=357 missing_bytes=0 tx_hosts=10.2.1.15 rx_hosts=115.77.78.20 source=HTTP mime_type=application/javascript sha1=805ba0fed321b077a729256e37a521c4fa3bcd24
Wed May 02 16:11:23	1525270283.409136 F4iqHl2DhwbulSeNg 10.2.1.15 115.77.78.20 C2H19u2th4RofGzCh SSL 0 MD5,X509,SHA1 application/pkix-cert - 0.00000 T F 1401 - 0 0 F - 40d566660132b7f71435a096ad80d3a9 88adc2fc489a321dca955dcfc8ae533b98bde82 - host=127.0.0.1 program=bro_files class=BRO_FILES seen_bytes=1401 total_bytes=0 missing_bytes=0 tx_hosts=10.2.1.15 rx_hosts=115.77.78.20 source=SSL mime_type=application/pkix-cert sha1=88adc2fc489a321dca955dcfc8ae533b98bde82
Wed May 02 16:11:23	1525270283.409136 Fpq35C2InJr7z8Joa 10.2.1.15 115.77.78.20 C2H19u2th4RofGzCh SSL 0 MD5,X509,SHA1 application/pkix-cert - 0.00000 T F 1279 - 0 0 F - 66f73ce9813c72823a0b3c1938a7742 77b99bb2bd752e217ec099ea177516f27787cad - host=127.0.0.1 program=bro_files class=BRO_FILES seen_bytes=1279 total_bytes=0 missing_bytes=0 tx_hosts=10.2.1.15 rx_hosts=115.77.78.20 source=SSL mime_type=application/pkix-cert sha1=77b99bb2bd752e217ec099ea177516f27787cad

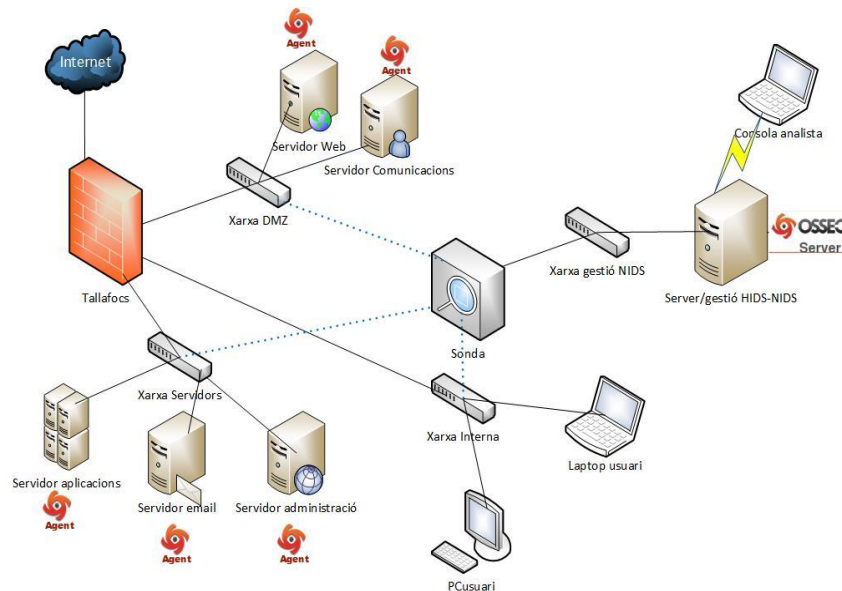
Esquema con los elementos de la plataforma

Arquitectura distribuida

- Sensores que capturan y procesan el tráfico de red
- Agentes que monitorizan la seguridad de los hosts
- Servidor que recibe las alertas generadas por los sensores y agentes
- Base de datos -> alertas, sesiones y logs normalizados
- Consola de analista

Diferentes configuraciones posibles según la distribución de la red y el tráfico

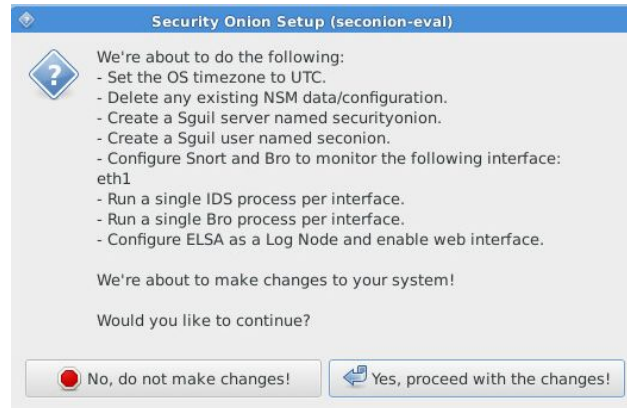
- sensor + servidor
- varios sensores + servidor
- sensor y servidor en el mismo equipo (standalone)



¿Cómo puedo probar Security Onion?

Es fácil hacer una instalación de Security Onion en modo evaluación

- Pasos:
 - Descargar la distribución de la web
 - En un equipo o VM, instalar distribución Security Onion (similar a instalar Ubuntu)
 - Ejecutar utilidad de setup para configurar interfaces de management y de captura
 - Reiniciar y ejecutar de nuevo la utilidad en modo quick-setup
-> servidor y sensor estarán en modo standalone (integrados en una misma máquina), junto con las principales utilidades de HIDS, NIDS, análisis y visualización, todo integrado y preparado para funcionar.
- Ejecutar archivo pcap y ver las alertas que se han generado



Tareas post-instalación

- Tareas post-instalación: actualizar, definir redes internas, ajustar procesos, comprobar carga de las interfaces del sensor
- Configurar consola de analista -> para acceder a las alertas
- Pruebas post-instalación: generación de alertas
- Gran número de alertas en un primer momento a ordenar en categorías
- Ajustes post-instalación para reducir el número de falsos positivos
 - Deshabilitar, modificar, crear nuevas reglas con Snort
 - Autocategorías
 - Excluir ficheros de OSSEC

¿Qué problemáticas de seguridad puede resolver?

Problemáticas de seguridad:

- detección de ataques
- detección de servidores comprometidos -> tienen actividad sospechosa
- Vulnerabilidades en servidores, servicios o equipos
- Errores de configuración
- Detectar flujos de datos sospechosos o poco habituales
- Tener evidencias en el caso de accesos no autorizados o robos de datos
- En caso de ataque con éxito, tener herramientas de análisis para determinar lo ocurrido y el alcance del problema

Valoraciones y conclusiones

- Instalación del software es rápida y sencilla (y económica)
- Gestión de actualizaciones de firmas y software bien resuelta
- Ha permitido al CTTC
 - Fortalecer la seguridad de los equipos -> detectar vulnerabilidades y errores de config.
 - Mejora de las políticas de seguridad
 - Detectar ataques e investigar las causas
 - Aumentar la visibilidad de lo que ocurre en la red
- Exige un esfuerzo continuo de ajuste del sistema
- Trabajo continuo de clasificación de alertas e investigación de incidentes