Universitat Oberta de Catalunya

uoc.edu

Implementación de las operaciones y la gestión de un SOC en una institución financiera partiendo desde cero utilizando soluciones SIEM

Grado de Tecnologías de Telecomunicación.
TFG-Administración de redes y sistemas operativos.

Daniel Rodríguez Fueyo

Índice

¿Qué es un SOC?

Definición de SOC

SOC: Security Operation Center

Forma parte del Cyber Fusion Center - **Monitorización y alerta de amenazas (SOC)**, respuesta, búsqueda de vunerabilidades, Threat intelligence

- Utiliza como herramienta base soluciones SIEM.
- Verificación y cierre/escalación de alertas.
- Información recibida: eventos creados a partir de logs en la red.

¿Qué es un SOC?

Contexto del proyecto

- ❑ El SOC es un requerimiento para instituciones financieras en Europa.
- ❑ La compañía carece de SOC implantado por el momento.

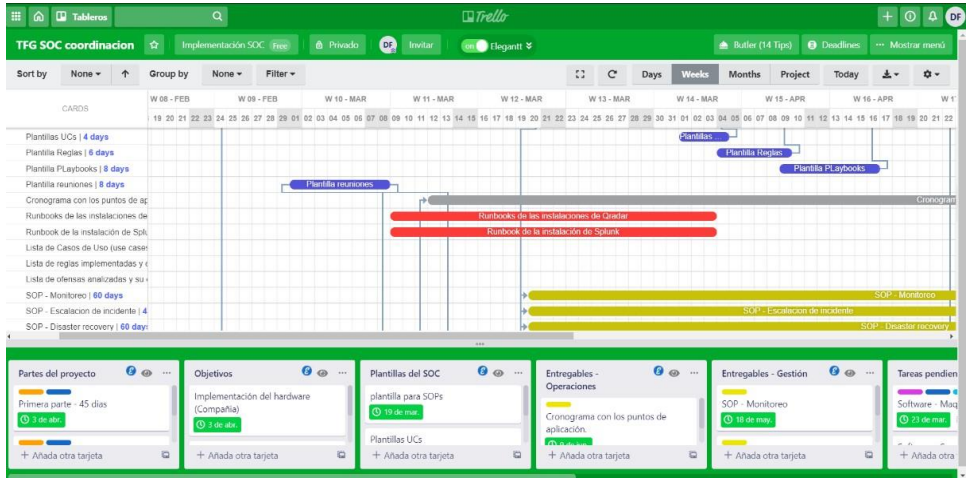
- Plazo de 6 meses para obtener aprobación de las entidades reguladoras.

- **Proyecto: 3 meses para implementación inicial de hardware, software, procedimientos y monitorización de alertas generales.**

- 3 meses restantes para verificar y mejorar el proyecto.

¿Qué es un SOC?

Objetivo



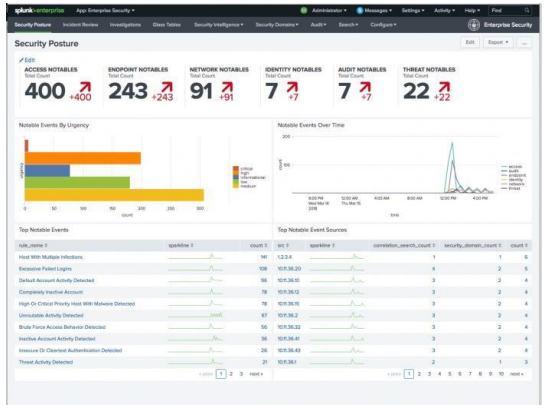
- ✓ Instalación de hardware en la red.
- ✓ Comprobación de envió de eventos a los SIEM.
- ✓ Monitorización de alertas y respuesta en tiempo y forma.
- ✓ Alta disponibilidad de los SIEM.

- ✓ Capacidad de operación independiente al finalizar
  - Creación de procedimientos
  - Generación de datos para responder ante auditores.

Herramientas SIEM

Concepto de SIEM

- Colectan todos los eventos desde otros dispositivos:
  - ❑ Servidores.
  - ❑ Routers.
  - ❑ Firewalls.
  - ❑ Endpoints (móvil, ordenador,..)
  - ❑ …
- Utilizan los eventos para relacionarlos y obtener:
  - ❑ Alertas de actividad sospechosa.
  - ❑ Reportes para otros departamentos.



SIEM → Security Information and Event Management

- Se configura la detección basándose en reglas
- Los analistas responden a estas alertas mediante Playbooks.

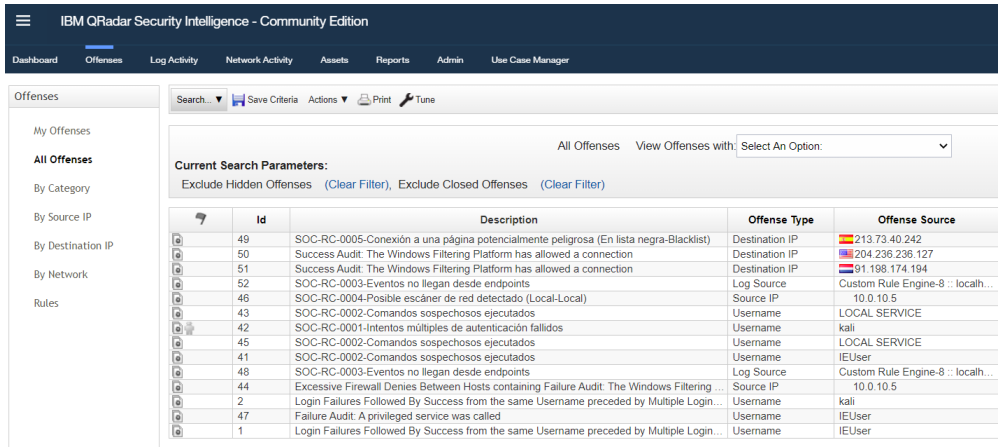
Herramientas SIEM

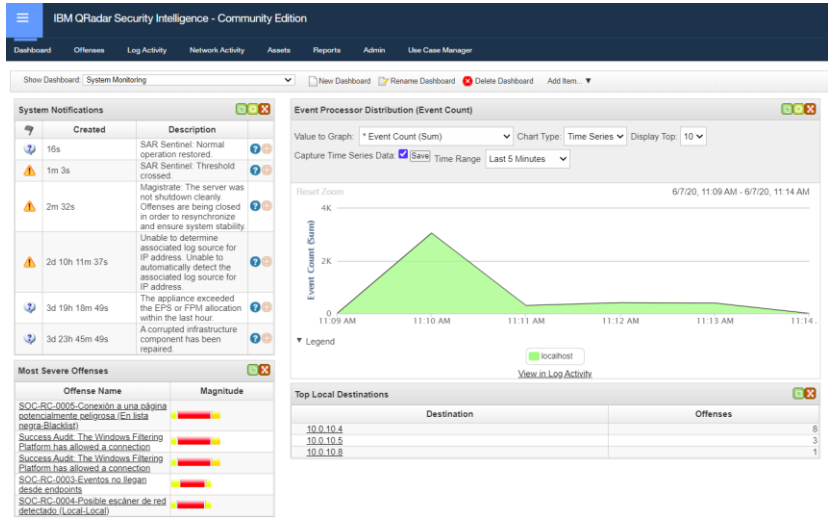
IBM Qradar

Uno de los SIEM más famosos. Disponible desde 2012.

- ⊕ Muy intuitivo y su consola es muy simple para análisis.
- ⊕ Soporte de IBM.
- ⊕ Versátil en cuanto a hardware, módulos expansibles.

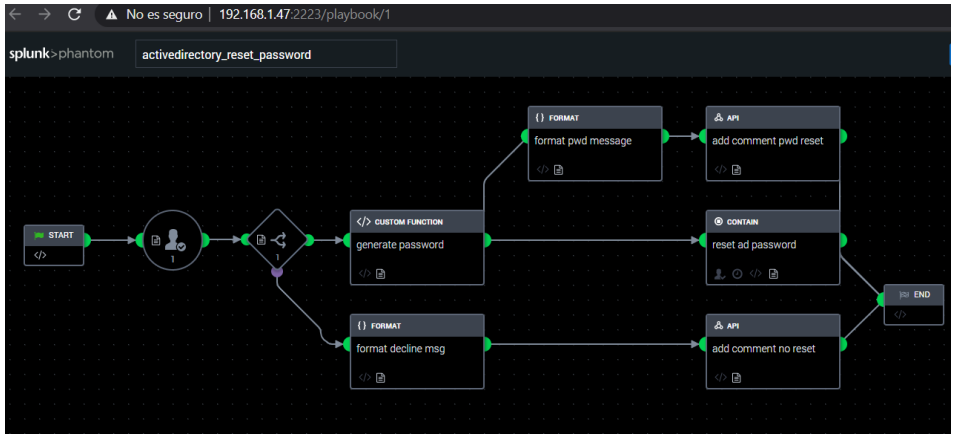
- ⊖ Licencia de pago, cara en relación con otros.
- ⊖ Programa muy pesado, requiere bastante mantenimiento.

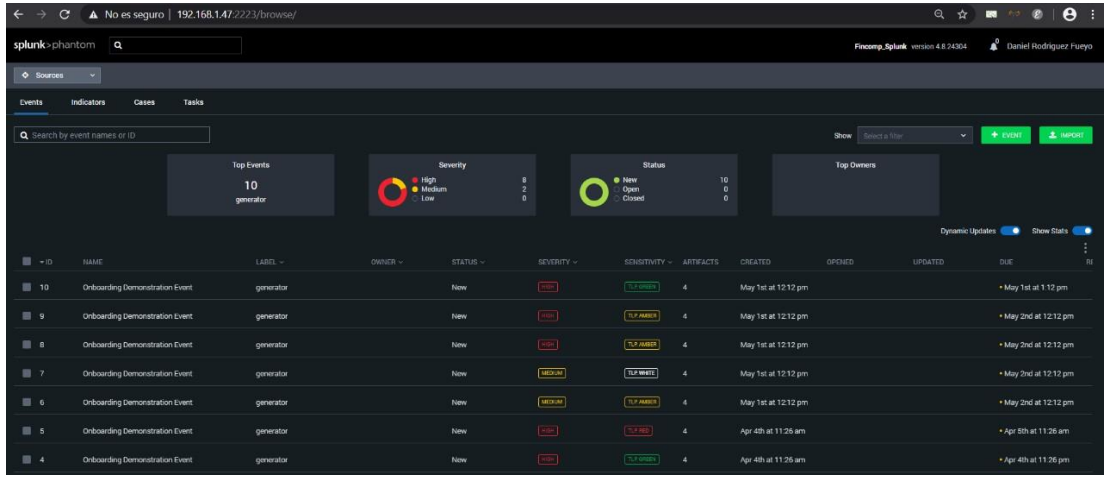




Herramientas SIEM

Splunk





Bastante reciente y optimizado. Ideal para monitorización de dispositivos de red (routing y switching)

- ✚ Alta capacidad de automatización.
- ✚ Posibilidad de uso como almacenador de logs.
- ✚ Gran comunidad detrás del producto.

- ⛔ No es tan intuitivo como otros SIEM.
- ⛔ Su coste se puede disparar, al tener licencia basada En el espacio que ocupan los logs (coste por GB/mes).

Elección de los SIEM

Cantidad:

- Al menos dos soluciones.
- Complementación entre ellos.
- Alta disponibilidad y especialización.

Calidad:

- Solución empresarial.
- Obtención de soporte adicional.
- Reputación.

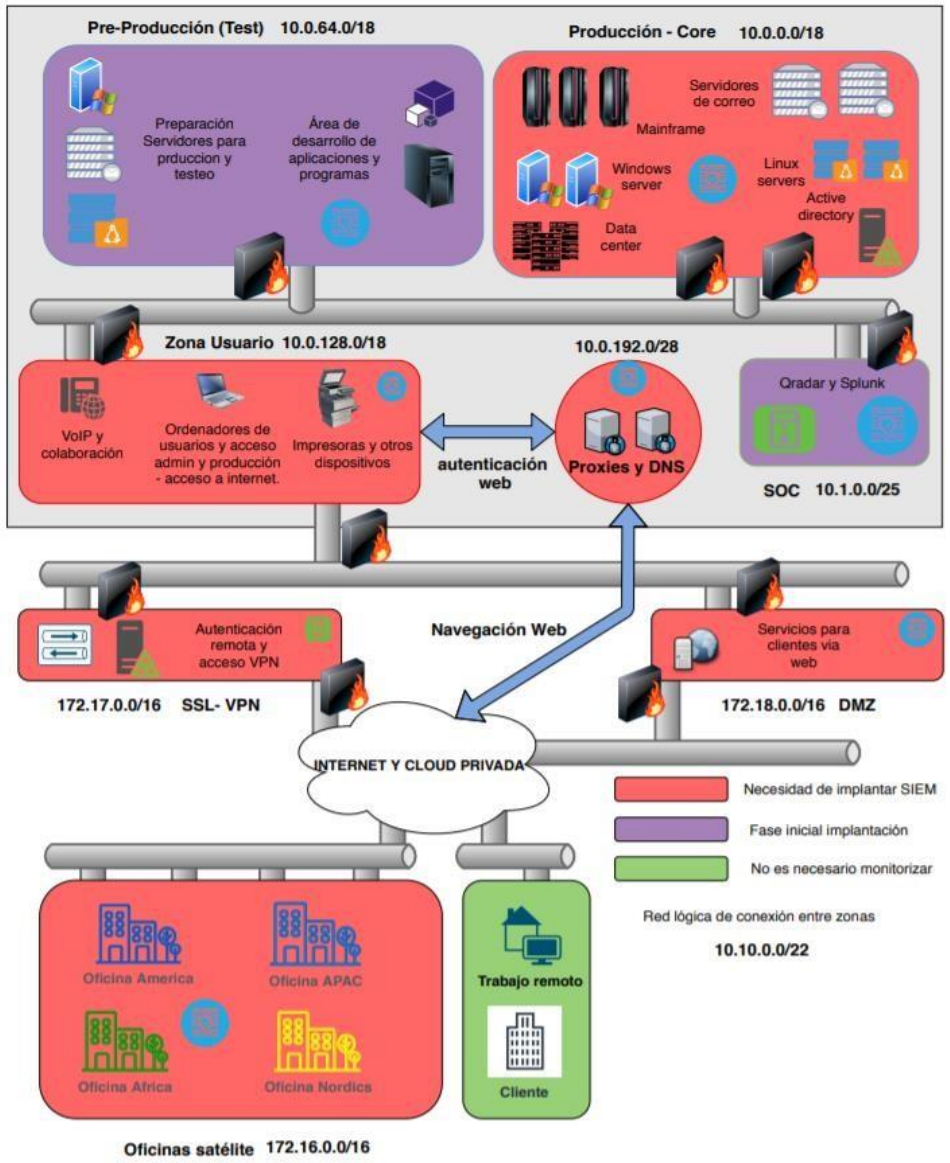
Implantación en la red empresa (1)

Mutiles redes distintas a incluir en la configuración.

- Qradar para zonas de usuario y producción, se incluye trafico web.
- Splunk para el trafico de red y la VPN.

Implantación progresiva:

Comienzo en red Test y finalización en Producción si todo funciona como se espera.



Implantación en la red empresa (2)

Distintos tipos de dispositivos de hardware necesarios:

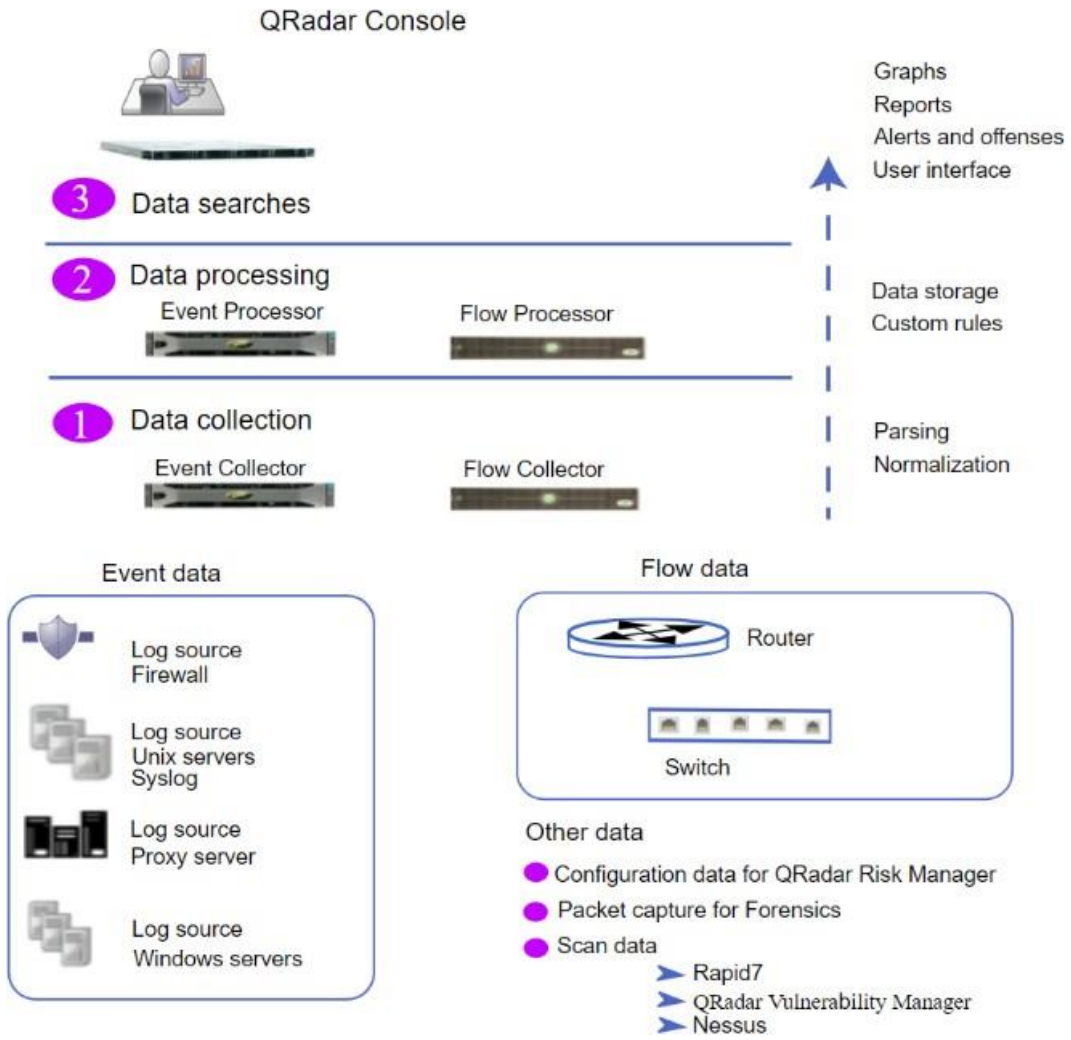
QRadar

Envío de eventos entre SIEM

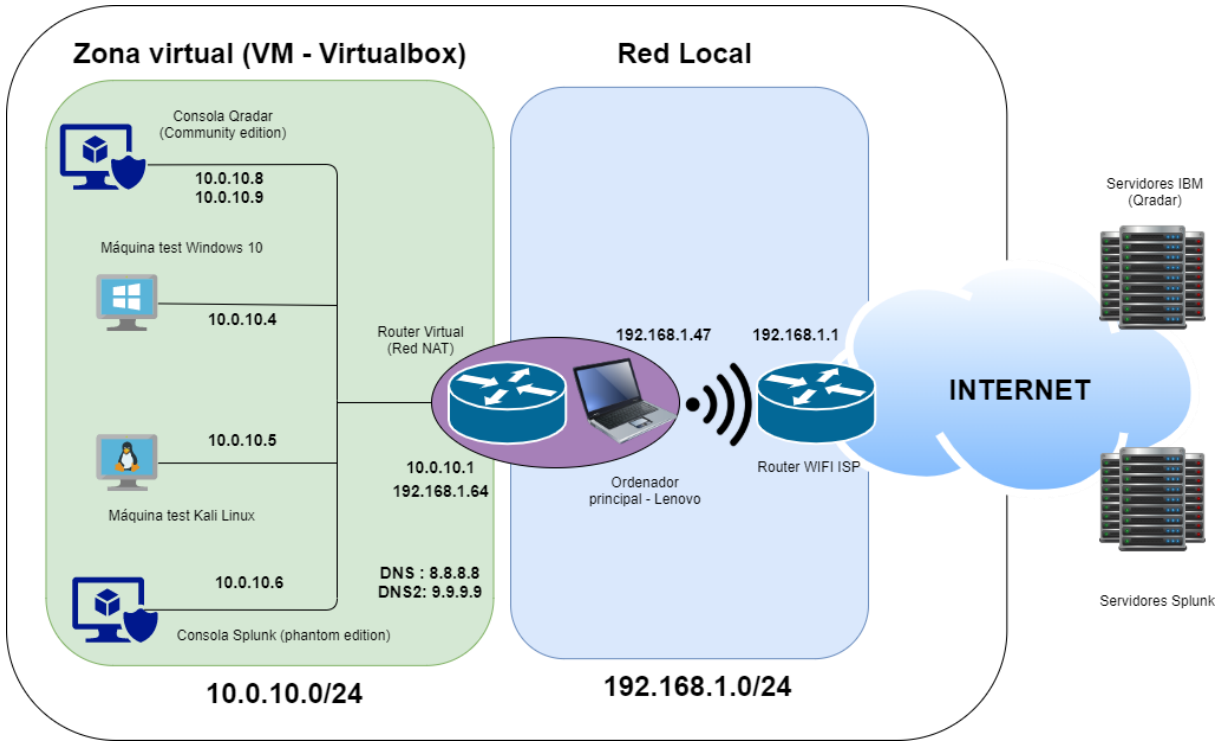
splunk>

- Event Collector
- Event Procesor
- Consola Principal

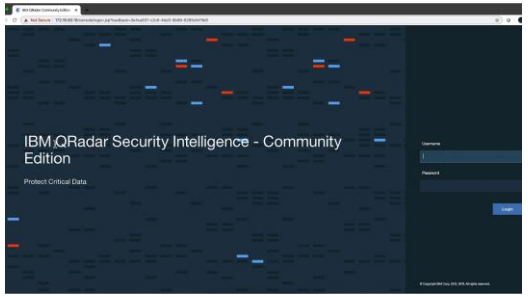
- Event Collector
- Consola



Implantación en la red de pruebas (1)



- Uso de las versiones Gratuitas de los SIEM:

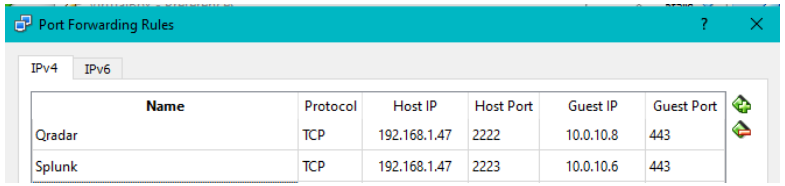


splunk> phantom

- Todo el resto de elementos virtualizados con Virtual Box:

1. Maquina Windows 10 pruebas
2. Máquina Kali Linux para ataques y alertas.

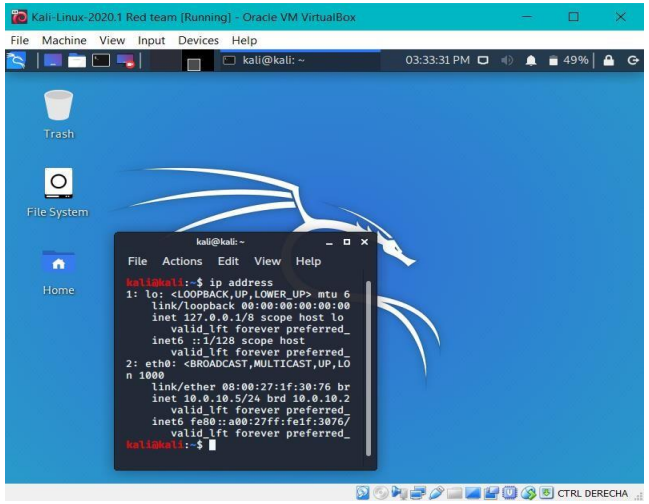
Implantación en la red de pruebas (2)



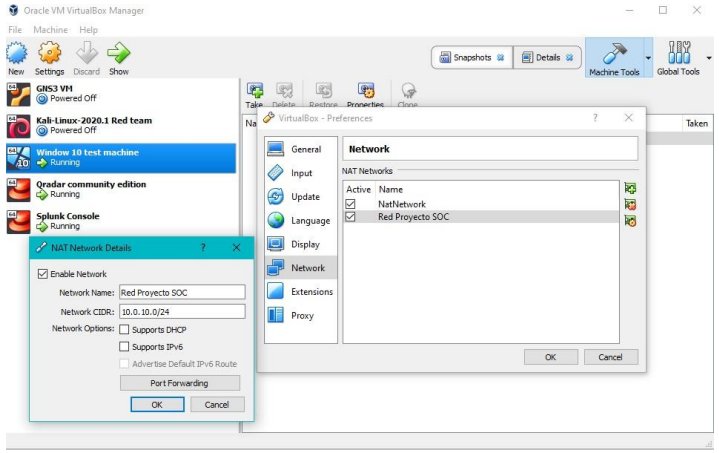
1. Configuración de acceso granular y del sistema.

2. Inserción de eventos a través de Wincollect (Windows) y Sylog (Linux)

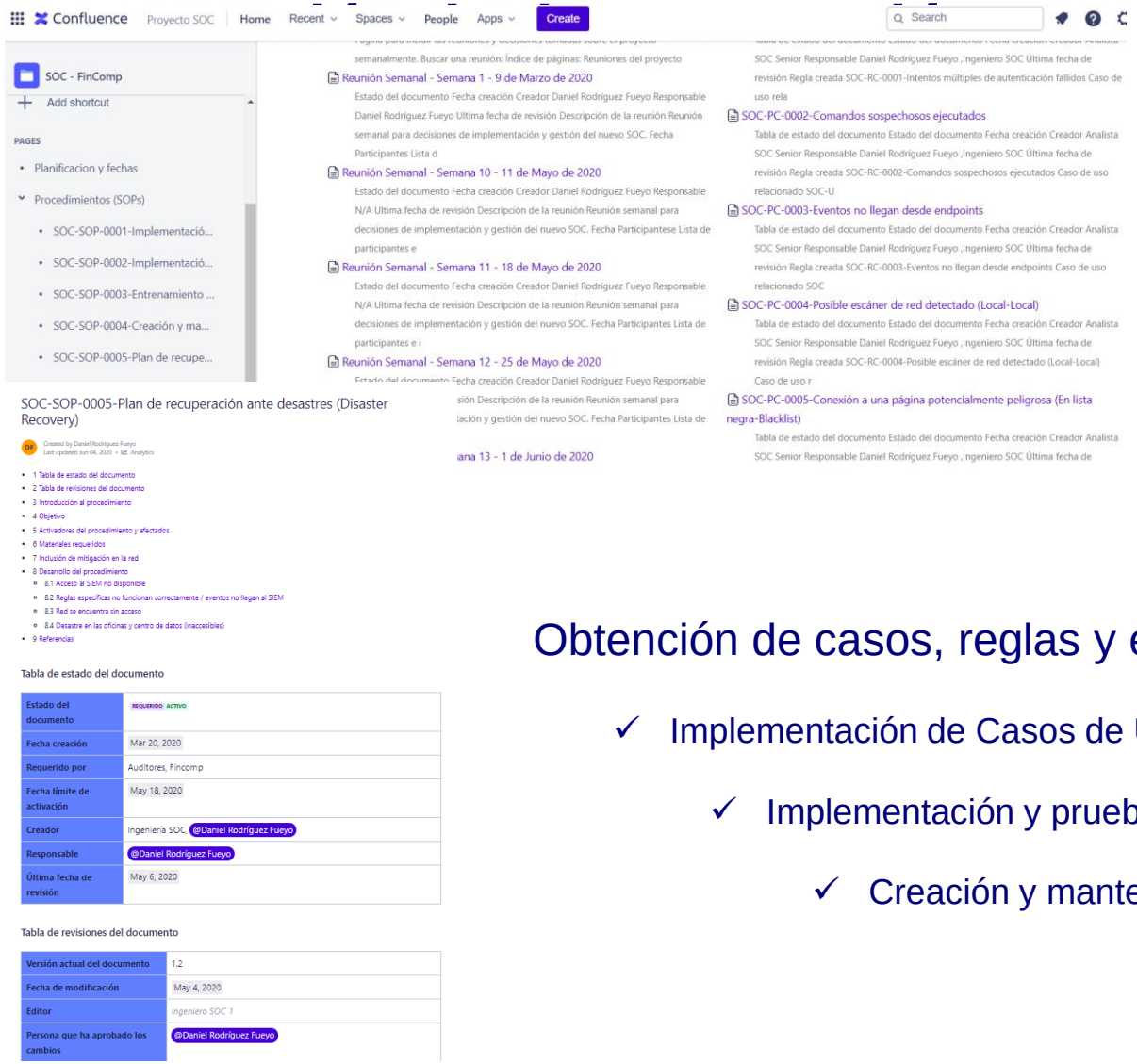
3. Creación de reglas basadas en la documentación y prueba de generación y respuesta



4. Generación de documentación para muestra de resultados.



Gestión



- Creación 5 procedimientos básicos:

✓ **Entrenamiento para analistas**
✓ **Plan de recuperación ante desastres (Disaster Recovery)**
✓ Monitorización de alertas
✓ Escalación de posibles incidentes de seguridad
✓ Modificación y mejora de reglas SIEM

Confluence

Obtención de casos, reglas y ejemplos prácticos

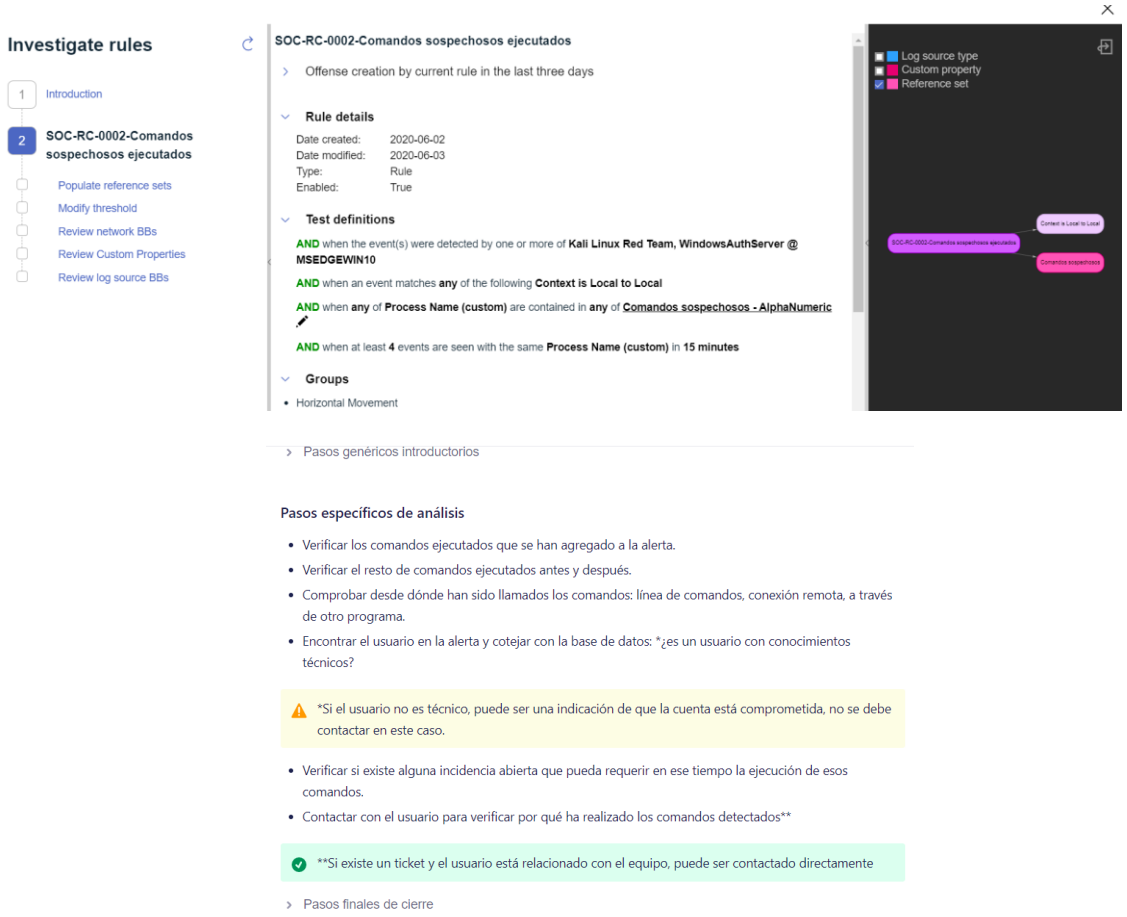
✓ Implementación de Casos de Uso .

✓ Implementación y prueba de reglas en SIEM

✓ Creación y mantenimiento de Libros de reglas (Playbooks)

Ejemplo de actuación

Monitorización y verificación de alertas (1)



1. Creación de la regla a partir del caso de uso proporcionado por la empresa:

- SOC-UC-0002-Comandos sospechosos ejecutados

- SOC-RC-0002-Comandos sospechosos ejecutados

2. Se crea el playbook de respuesta para los analistas

- SOC-PC-0002-Comandos sospechosos ejecutados

Ejemplo de actuación

Monitorización y verificación de alertas (2)

3. Se activa la alerta al coincidir con los parámetros detectados en la regla
4. El analista verifica y analiza la alerta, verificando con el Playbook si fuera necesario

All Offenses > Offense 41 (Summary)

Offense 41

Summary | Display | Events | Flows | Actions | Print | Tune

Magnitude		Status		Relevance	0	Severity	9	Credibility	3
Description	SOC-RC-0002-Comandos sospechosos ejecutados	Offense Type	Username				
		Event/Flow count	42 events and 0 flows in 5 categories				
Source IP(s)	10.0.10.4	Start	Jun 2, 2020, 5:50:17 PM				
Destination IP(s)	10.0.10.4	Duration	1h 36m 29s				
Network(s)	Net-10-172-192.Net_10_0_0_0	Assigned to	Unassigned				

Offense Source Summary

Username	IEUser		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	4	Events/Flows	74

Last 5 Notes

Notes	Username	Creation Date

Sumario de regla generada

Event Name	Success Audit: A new process has been created						
Low Level Category	Process Creation Success						
Event Description	Success Audit: A new process has been created.						
Magnitude	(5)	Relevance	9	Severity	2	Credibility	5
Username	IEUser						
Start Time	Jun 2, 2020, 7:11:31 PM	Storage Time	Jun 2, 2020, 7:11:31 PM	Log Source Time	Jun 2, 2020, 9:57:43 PM		
AccountDomain (custom)	N/A						
AccountID (custom)	N/A						
AccountName (custom)	-						
ChangedAttributes (custom)	N/A						
EventID (custom)	4688						
Logon Type (custom)	N/A						
ObjectType (custom)	N/A						
Parent Process Name (custom)	cmd.exe						
Parent Process Path (custom)	C:\Windows\System32\cmd.exe						
Process CommandLine (custom)	N/A						
Process Name (custom)	whoami.exe						
Process Path (custom)	C:\Windows\System32\whoami.exe						
Realm (custom)	N/A						
Source Workstation	N/A						

Uno de los eventos relacionados con whoami.exe

utf | hex | base64

Wrap Text

```
<13>Jun 02 21:57:45 MSEDGEWIN10 AgentDevice=WindowsLog  AgentLogFile=Security   PluginVersion=7.2.9.105
Source=Microsoft-Windows-Security-Auditing      Computer=MSEDGEWIN10    OriginatingComputer=MSEDGEWIN10 User=   Domain=
EventID=4688    EventIDCode=4688        EventType=8     EventCategory=13312     RecordNumber=129792
TimeGenerated=1591127863        TimeWritten=1591127863  Level=Log Always        Keywords=Audit Success
Task=SE_ADT_DETAILEDTRACKING_PROCESSCREATION    Opcode=Info     Message=A new process has been created.  Creator
Subject:  Security ID:  MSEDGEWIN10\IEUser  Account Name:  IEUser  Account Domain:  MSEDGEWIN10  Logon ID:  0x4B232
Target Subject:  Security ID:  NULL SID  Account Name:  -  Account Domain:  -  Logon ID:  0x0  Process Information:
New Process ID:  0x2190  New Process Name: C:\Windows\System32\whoami.exe  Token Elevation Type: %%1938  Mandatory
Label:  Mandatory Label\Medium Mandatory Level  Creator Process ID: 0x2060  Creator Process Name:
C:\Windows\System32\cmd.exe  Process Command Line:  Token Elevation Type indicates the type of token that was assigned
to the new process in accordance with User Account Control policy.  Type 1 is a full token with no privileges removed
or groups disabled.  A full token is only used if User Account Control is disabled or if the user is the built-in
Administrator account or a service account.  Type 2 is an elevated token with no privileges removed or groups disabled.
```

Payload del evento generado

Ejemplo de actuación

Monitorización y verificación de alertas (3)

Análisis de la ofensa:
El analista SOC 1 comienza a verificar la información con ayuda del libro de reglas asignado a esa regla.

- Los comandos analizados y detectados son los siguientes:
  - Cmd.exe
  - Whoami.exe
  - Svchost.exe
  - Ipconfig.exe
- Se verifican los comandos antes y después. No se aprecia mucha más actividad, pero sí que se relacionan con la alerta muchos intentos de intrusión desde otra máquina Linux en la red.
- El usuario es el mismo que el que utiliza el dispositivo de manera frecuente, por lo que, si hay actividad sospechosa, puede ser que la cuenta de usuario haya sido comprometida.
- Lo comandos han sido llamados desde línea de comandos directamente, lo que reafirma la sospecha de cuenta comprometida.
- El usuario que utiliza esta cuenta pertenece al departamento financiero, por lo que no es un usuario técnico. De nuevo más sospechas acerca de la actividad.
- Se contacta con CIRT de forma paralela para informar y preparar el envío del caso. El equipo confirma que se contacte con el usuario para comprobar si estaba utilizando el equipo en este punto. El usuario confirma que no se encontraba trabajando cuando la actividad ocurrió.
- El analista completa la información obtenida y envía el caso a l equipo de respuesta, que seguirá desde este punto.

Información encontrada por el analista:

- Numero de ofensa: 41
- Tiempo de comienzo de la actividad: Jun 2, 2020, 5:50:3617 PM
- Tiempo del comienzo del análisis: Jun 2, 2020, 6:50:00 PM
- Duración: 1:36 horas
- Asignado a: Analista SOC 3
- Dirección de origen: 10.0.10.4 (MSEDGEWIN10)
- Dirección de destino: 10.0.10.4 (MSEDGEWIN10)
- Log source: WindowsAuthServer @ MSEDGEWIN10
- Conclusión:

  La actividad parece no relacionada con el usuario, este ha confirmado que no poseía acceso al sistema en ese momento, la cuenta parece estar comprometida.

- Analista ve actividad sospechosa. Después de verificar decide escalar el incidente al equipo de respuesta

⬇

- Se ejecuta proceso de escalación creado:

SOC-SOP-0007-Escalación de posibles incidentes de seguridad

⬇

- El caso queda en manos del equipo de respuesta (CSIRT). El analista puede proceder a analizar la siguiente alerta según criterio:

SOC-SOP-0006-Monitorización de alertas

Conclusión

Proyecto finalizado:

- Inclusión de los SIEM en la infraestructura de red (fase inicial)
- Entregables proporcionados en tiempo y forma.
- Poca desviación del presupuesto inicial (2,8%↑)

- Configuración de Splunk minimizada en favor de Qradar.
- No se ha entrado en detalle en la generación de datos y estadísticas.
- No se ha entrado en detalle en las aplicaciones instaladas en los SIEM.

Conclusión

Continuación del proyecto

Mantenimiento de las operaciones en el día a día para el largo plazo

Implementación de mejoras en los SIEM

Finalización de inclusión de eventos de otras plataformas y optimización

McAfee

TRIPWIRE IP360

CYBERARK

IMPERVA SECURESPHERE

Universitat Oberta
de Catalunya

Para más información o clarificación:

Consultar la memoria del proyecto.
Enviar un correo electrónico a danielfueyo@uoc.edu

UOC.universitat
@UOCuniversidad
UOCuniversitat