

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.

- **¿Qué es un SOC?**
 - Definición de SOC
 - Contexto del proyecto
 - Objetivo
- **Herramientas SIEM**
 - Concepto de SIEM
 - IBM Qradar
 - Splunk
 - Elección de los SIEM
- **Operaciones**
 - Implantación en la red empresa
 - Implantación en la red de pruebas
- **Gestión**
 - Creación de documentación
- **Ejemplo de actuación**
 - Monitorización y verificación de alertas.
- **Conclusión**
 - Conclusión
 - Continuación del proyecto

Definición de SOC

SOC: Security Operation Center

Forma parte del Cyber Fusion Center -
Monitorización y alerta de amenazas (SOC),
respuesta, búsqueda de vulnerabilidades, 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.



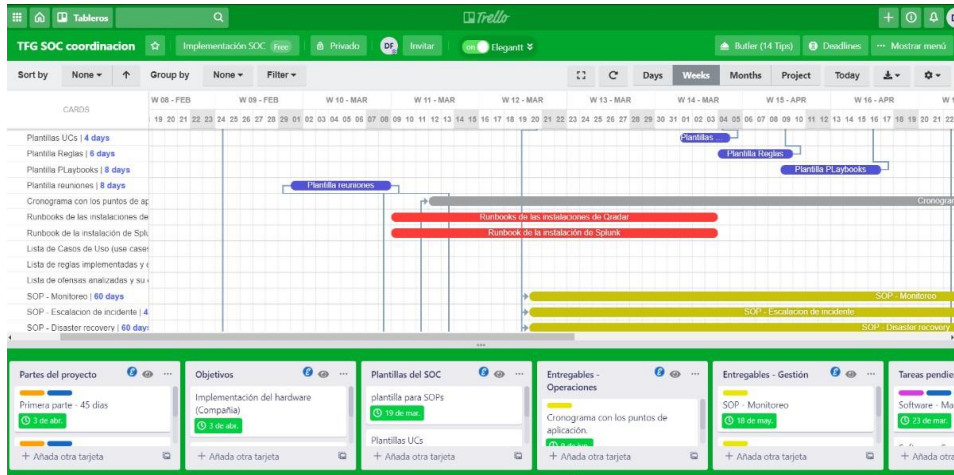
Contexto del proyecto

- ❑ 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 envío de eventos a los SIEM.
- ✓ Monitorización de alertas y respuesta en tiempo y forma.
- ✓ Alta disponibilidad de los SIEM.

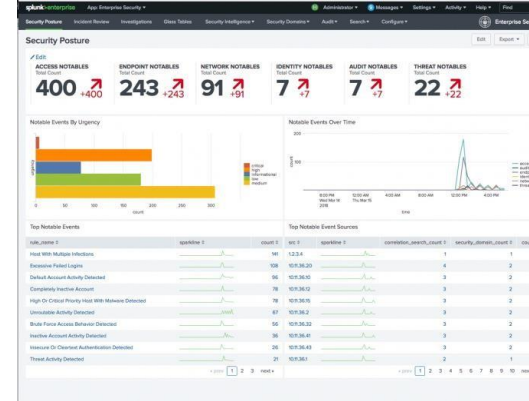


- ✓ Capacidad de operación independiente al finalizar
 - Creación de procedimientos
 - Generación de datos para responder ante auditores.

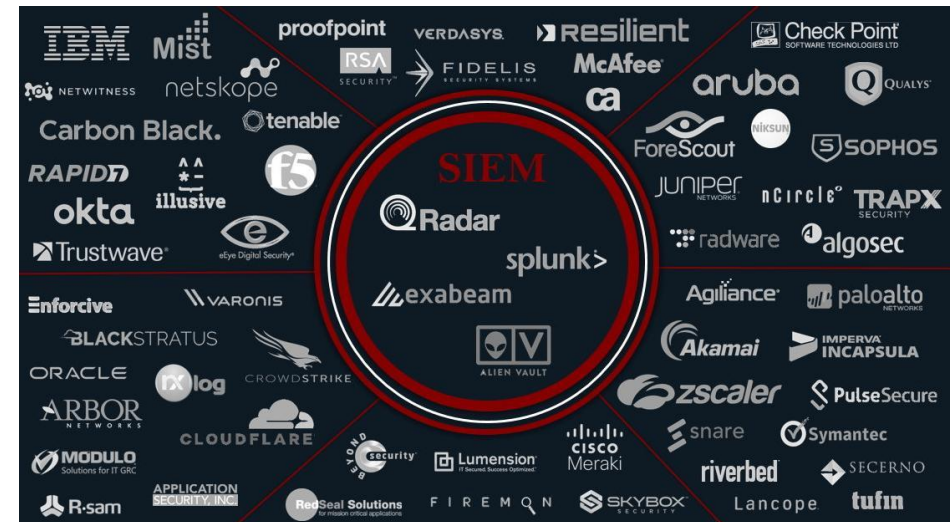
Herramientas SIEM

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



SIEM → Security Information and Event Management



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.

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Use Case Manager

Offenses

My Offenses

All Offenses

By Category

By Source IP

By Destination IP

By Network

Rules

Search... Save Criteria Actions Print Tune

All Offenses View Offenses with: Select An Option: [v]

Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source
49	SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)	Destination IP	213.73.40.242
50	Success Audit: The Windows Filtering Platform has allowed a connection	Destination IP	204.236.236.127
51	Success Audit: The Windows Filtering Platform has allowed a connection	Destination IP	91.198.174.194
52	SOC-RC-0003-Eventos no llegan desde endpoints	Log Source	Custom Rule Engine-8 :: localh...
48	SOC-RC-0004-Posible escáner de red detectado (Local-Local)	Source IP	10.0.10.5
43	SOC-RC-0002-Comandos sospechosos ejecutados	Username	LOCAL SERVICE
42	SOC-RC-0001-Intentos múltiples de autenticación fallidos	Username	kali
45	SOC-RC-0002-Comandos sospechosos ejecutados	Username	LOCAL SERVICE
41	SOC-RC-0002-Comandos sospechosos ejecutados	Username	IEUser
48	SOC-RC-0003-Eventos no llegan desde endpoints	Log Source	Custom Rule Engine-8 :: localh...
44	Excessive Firewall Denies Between Hosts containing Failure Audit: The Windows Filtering...	Source IP	10.0.10.5
2	Login Failures Followed By Success from the same Username preceded by Multiple Login...	Username	kali
47	Failure Audit: A privileged service was called	Username	IEUser
1	Login Failures Followed By Success from the same Username preceded by Multiple Login...	Username	IEUser

IBM QRadar Security Intelligence - Community Edition

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Use Case Manager

Show Dashboard: System Monitoring New Dashboard Rename Dashboard Delete Dashboard Add Item...

System Notifications

Created	Description
10s	SAR Sentinel: Normal operation restored
1m 3s	SAR Sentinel: Threshold crossed
2m 32s	Magistrate: The server was not shutdown cleanly. Offenses are being closed in order to resynchronize and ensure system stability
2d 10h 11m 37s	Unable to determine associated log source for IP address. Unable to automatically detect the associated log source for IP address
3d 19h 18m 49s	The appliance exceeded the EPS or FPL allocation within the last hour
3d 23h 45m 49s	A corrupted infrastructure component has been repaired

Most Severe Offenses

Offense Name	Magnitude
SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)	High
Success Audit: The Windows Filtering Platform has allowed a connection	Medium
Success Audit: The Windows Filtering Platform has allowed a connection	Medium
SOC-RC-0003-Eventos no llegan desde endpoints	Low
SOC-RC-0004-Posible escáner de red detectado (Local-Local)	Low

Event Processor Distribution (Event Count)

Value to Graph: Event Count (Sum) Chart Type: Time Series Display Top: 10

Capture Time Series Data [x] Save Time Range: Last 5 Minutes

Reset Zoom: 6/7/20, 11:09 AM - 6/7/20, 11:14 AM

Event Count (Sum)

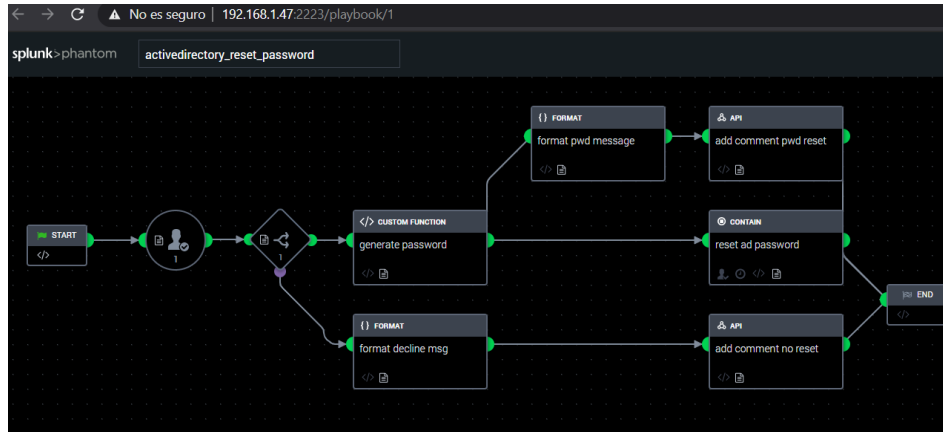
Legend: localhost

View in Log Activity

Top Local Destinations

Destination	Offenses
10.0.10.4	8
10.0.10.5	3
10.0.10.8	1

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).

The screenshot shows the Splunk Phantom interface with a table of events. The table has columns for ID, NAME, LABEL, OWNER, STATUS, SEVERITY, SENSITIVITY, ARTIFACTS, CREATED, OPENED, UPDATED, and DUE.

ID	NAME	LABEL	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED	UPDATED	DUE
10	Onboarding Demonstration Event	generator	generator	New	High	High	4	May 1st at 12:12 pm			May 1st at 12:12 pm
9	Onboarding Demonstration Event	generator	generator	New	High	High	4	May 1st at 12:12 pm			May 2nd at 12:12 pm
8	Onboarding Demonstration Event	generator	generator	New	High	High	4	May 1st at 12:12 pm			May 2nd at 12:12 pm
7	Onboarding Demonstration Event	generator	generator	New	Medium	High	4	May 1st at 12:12 pm			May 2nd at 12:12 pm
6	Onboarding Demonstration Event	generator	generator	New	Medium	High	4	May 1st at 12:12 pm			May 2nd at 12:12 pm
5	Onboarding Demonstration Event	generator	generator	New	High	High	4	Apr 4th at 11:26 am			Apr 5th at 11:26 am
4	Onboarding Demonstration Event	generator	generator	New	High	High	4	Apr 4th at 11:26 am			Apr 4th at 11:26 pm

Elección de los SIEM



Cantidad:

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

Calidad:

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

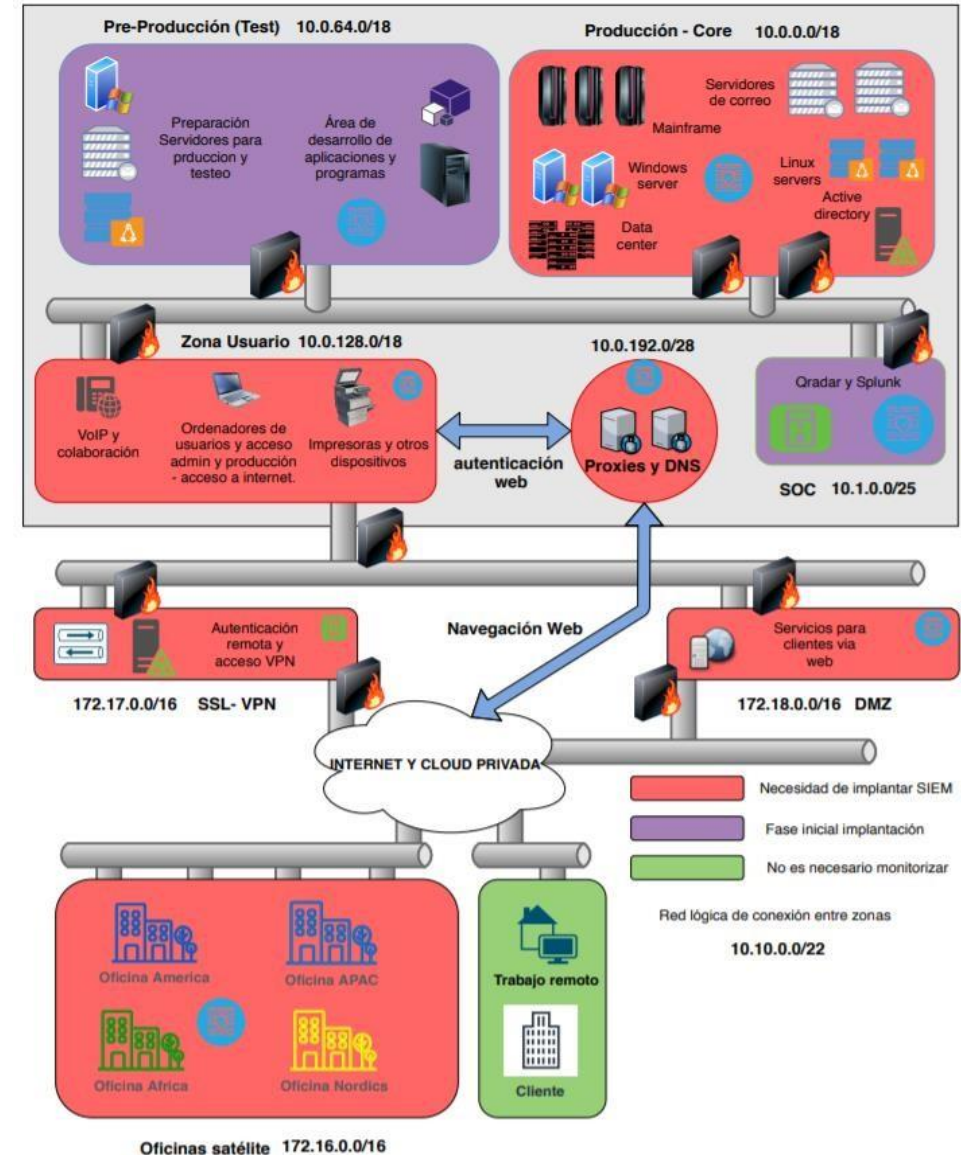
Implantación en la red empresa (1)

Múltiples redes distintas a incluir en la configuración.

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

Implantación progresiva:

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



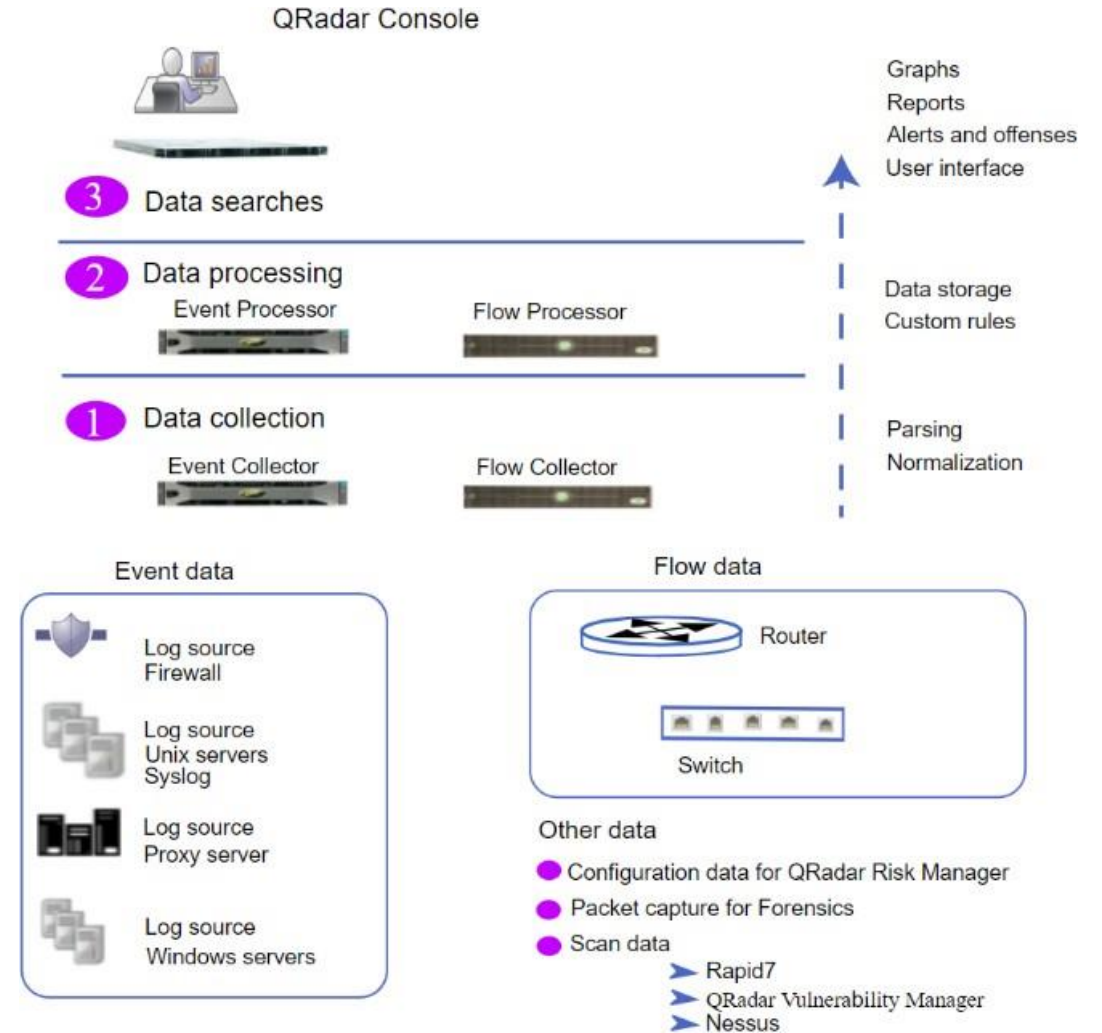
Implantación en la red empresa (2)

Distintos tipos de dispositivos de hardware necesarios:



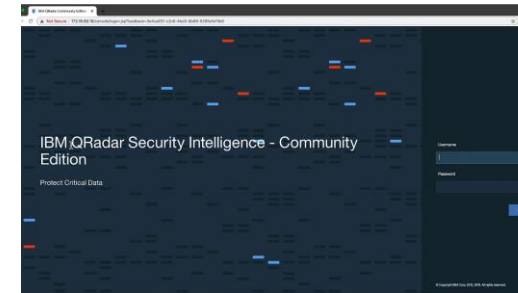
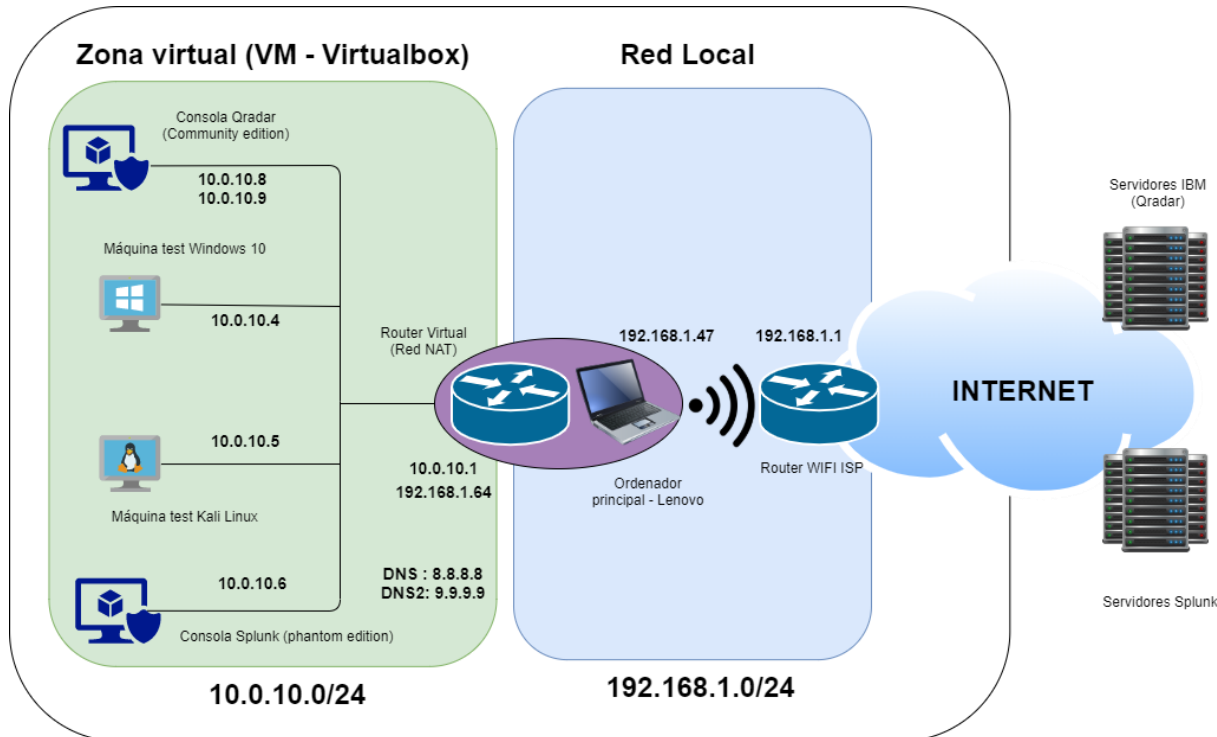
- Event Collector
- Event Procesor
- Consola Principal

- Event Collector
- Consola



Implantación en la red de pruebas (1)

- Uso de las versiones Gratuitas de los SIEM:



- Todo el resto de elementos virtualizados con Virtual Box:
 1. Máquina Windows 10 pruebas
 2. Máquina Kali Linux para ataques y alertas.

Implantación en la red de pruebas (2)

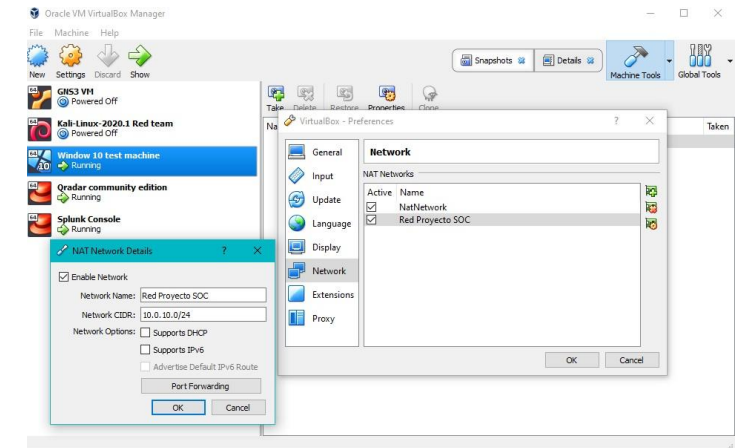
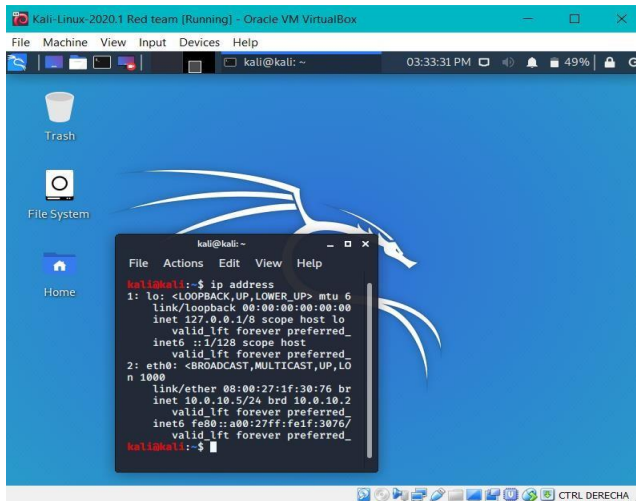
Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
Qradar	TCP	192.168.1.47	2222	10.0.10.8	443
Splunk	TCP	192.168.1.47	2223	10.0.10.6	443

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.



The screenshot shows a Confluence page titled 'SOC - FinComp'. The left sidebar contains a navigation menu with 'PAGES' and a list of documents including 'SOC-SOP-0001-Implementació...', 'SOC-SOP-0002-Implementació...', 'SOC-SOP-0003-Entrenamiento...', 'SOC-SOP-0004-Creación y ma...', and 'SOC-SOP-0005-Plan de recupe...'. The main content area displays a list of documents with titles like 'Reunión Semanal - Semana 1 - 9 de Marzo de 2020', 'Reunión Semanal - Semana 10 - 11 de Mayo de 2020', 'Reunión Semanal - Semana 11 - 18 de Mayo de 2020', 'Reunión Semanal - Semana 12 - 25 de Mayo de 2020', and 'SOC-SOP-0005-Plan de recuperación ante desastres (Disaster Recovery)'. The 'SOC-SOP-0005' document is highlighted, showing its metadata and a table of contents.

- 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



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)

Tabla de estado del documento

Estado del documento	requerido Activo
Fecha creación	Mar 20, 2020
Requerido por	Audidores, Fincomp
Fecha límite de activación	May 18, 2020
Creador	Ingeniería SOC, @Daniel Rodríguez Fueyo
Responsable	@Daniel Rodríguez Fueyo
Última fecha de revisión	May 6, 2020

Tabla de revisiones del documento

Versión actual del documento	1.2
Fecha de modificación	May 4, 2020
Editor	Ingeniero SOC 1
Persona que ha aprobado los cambios	@Daniel Rodríguez Fueyo

Monitorización y verificación de alertas (1)

Investigate rules

- 1 Introduction
- 2 SOC-RC-0002-Comandos sospechosos ejecutados**
 - Populate reference sets
 - Modify threshold
 - Review network BBs
 - Review Custom Properties
 - Review log source BBs

SOC-RC-0002-Comandos sospechosos ejecutados

- Offense creation by current rule in the last three days
- Rule details**
 - Date created: 2020-06-02
 - Date modified: 2020-06-03
 - Type: Rule
 - Enabled: True
- Test definitions**
 - AND** when the event(s) were detected by one or more of **Kali Linux Red Team, WindowsAuthServer @ MSEDGWIN10**
 - AND** when an event matches **any** of the following **Context is Local to Local**
 - AND** when **any** of **Process Name (custom)** are contained in **any** of **Comandos sospechosos -AlphaNumeric**
 - AND** when at least **4** events are seen with the same **Process Name (custom)** in **15 minutes**
- Groups**
 - Horizontal Movement

Pasos genéricos introductorios

Pasos específicos de análisis

- Verificar los comandos ejecutados que se han agregado a la alerta.
- Verificar el resto de comandos ejecutados antes y después.
- Comprobar desde dónde han sido llamados los comandos: línea de comandos, conexión remota, a través de otro programa.
- Encontrar el usuario en la alerta y cotejar con la base de datos: ¿es un usuario con conocimientos técnicos?

⚠️ *Si el usuario no es técnico, puede ser una indicación de que la cuenta está comprometida, no se debe contactar en este caso.

- Verificar si existe alguna incidencia abierta que pueda requerir en ese tiempo la ejecución de esos comandos.
- Contactar con el usuario para verificar por qué ha realizado los comandos detectados**

✅ **Si existe un ticket y el usuario está relacionado con el equipo, puede ser contactado directamente

Pasos finales de cierre

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

Monitorización y verificación de alertas (2)

- Se activa la alerta al coincidir con los parámetros detectados en la regla
- 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	<div style="width: 75%;"><div style="background-color: red; width: 75%;"></div></div>	Status	Offense Type	Relevance	Severity	Credibility		
Description	SOC-RC-0002-Comandos sospechosos ejecutados	Unassigned	Username	0	9	3		
Source IP(s)	10.0.10.4	Event/Flow count	42 events and 0 flows in 5 categories					
Destination IP(s)	10.0.10.4	Start	Jun 2, 2020, 5:50:17 PM					
Network(s)	Net:10-172-192-Net_10_0_0_0	Duration	1h 36m 29s					
Offense Source Summary		Assigned to	Unassigned					
Username	IEUser	Host Name	Unknown					
MAC Address	Unknown NIC	Last Known Machine	Unknown					
Last Known Host	Unknown	Last Known IP	Unknown					
Last Known MAC	Unknown	Last Known Group	Unknown					
Last Observed	Unknown	Events/Flows	74					
Offenses	4							
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	<div style="width: 75%;"><div style="background-color: red; width: 75%;"></div></div>	(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 MSEDGWIN10 AgentDevice-WindowsLog AgentLogFile=Security PluginVersion=7.2.9.105
Source=Microsoft-Windows-Security-Auditing Computer=MSEDGWIN10 OriginatingComputer=MSEDGWIN10 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: MSEDGWIN10\IEUser Account Name: IEUser Account Domain: MSEDGWIN10 Logon ID: 0x48232
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

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.
- Los 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 al 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 (MSEEDGEWIN10)
- Dirección de destino: 10.0.10.4 (MSEEDGEWIN10)
- Log source: [WindowsAuthServer](#) @ MSEEDGEWIN10
- 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.



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



Para más información o clarificación:

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

 UOC.universitat

 @UOCuniversidad

 UOCuniversitat
