Casos de Uso para SOC

Guía

Contenido

Tabla de contenido

CASOS DE USO PARA SOC

1. Introducción

En un entorno digital cada vez más expuesto a ciberamenazas sofisticadas y persistentes, el Security Operations Center (SOC) se posiciona como una pieza clave dentro de la estrategia de ciberseguridad de cualquier organización. Su misión principal es monitorizar, detectar, analizar y responder a incidentes de seguridad en tiempo real, minimizando el impacto de posibles ataques y garantizando la continuidad del negocio.

Este documento recoge una serie de **casos de uso prácticos** que ilustran las capacidades operativas de un SOC moderno. Cada caso de uso está diseñado para resolver un problema específico de seguridad, apoyándose en fuentes de datos, reglas de detección y análisis de contexto. La finalidad es proporcionar una visión clara y estructurada de cómo el SOC contribuye a mejorar la postura de seguridad de la organización, desde la detección temprana de amenazas hasta la respuesta y contención eficaz de incidentes.

2. Casos de Uso

2.1. Comandos PowerShell Sospechosos

- **Objetivo: Detectar ejecución de scripts maliciosos o descarga de payloads vía PowerShell.**
- **Fuente: Microsoft-Windows-PowerShell/Operational**
- **KQL:**

kql

```
Event

| where EventLog == "Microsoft-Windows-PowerShell/Operational" and EventID == 4104

| where ScriptBlockText has_any ("iex", "New-Object", "-enc", "-ep", "bypass", "download", "reg add")
```

- **Umbral de alerta: >3 eventos por host en 10 min.**

2.2. Desactivación de UAC

- **Objetivo: Detectar intentos de desactivar el control de cuentas de usuario.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where ParentImage endswith "cmd.exe" and CommandLine contains "reg.exe" and CommandLine contains "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"

- **Umbral de alerta: 1 evento.**

2.3. Eliminación de copias de sombra

- **Objetivo: Detectar intentos de borrar copias de seguridad (indicador de ransomware).**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image endswith "vssadmin.exe" and CommandLine contains "delete shadows"

- **Umbral de alerta: 1 evento por host.**

2.4. Elevación a SYSTEM

- **Objetivo: Identificar técnicas de escalada a SYSTEM.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where (ParentImage endswith "services.exe" and Image endswith "cmd.exe" and CommandLine contains "\\pipe\\")

or (Image endswith "rundll32.exe" and CommandLine contains ",a /p:")

- **Umbral de alerta: 1 evento.**

2.5. Sniffing de Red Local

- **Objetivo: Detectar herramientas de monitoreo de red no autorizadas.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image has_any ("tshark.exe", "windump.exe", "tcpdump.exe", "wprui.exe", "wpr.exe")

- **Umbral de alerta: 1 evento por host.**

2.6. Borrado de historial de PowerShell

- **Objetivo: Detectar intentos de ocultar comandos ejecutados.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where CommandLine contains_any ("HistorySavePath", "SaveNothing", "ConsoleHost_history.txt")

- **Umbral de alerta: 1 evento.**

2.7. Extracción de credenciales del registro

- **Objetivo: Identificar búsquedas de contraseñas en registro o archivos.**
- **Fuente: Sysmon, EventLog**
- **KQL:**

kql

Event

| where CommandLine contains_any ("reg query", "Get-Webconfig", "Get-CachedGPPPassword")

- **Umbral de alerta: 1 evento.**

2.8. Ejecutables con mismo hash distinto nombre

- **Objetivo: Detección de ofuscación por renombrado.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| summarize count_distinct(Image) by Hashes

| where count_distinct_Image > 1

- **Umbral de alerta: cualquier caso positivo.**

2.9. Argumentos sospechosos

- **Objetivo: Detección de herramientas renombradas por sus argumentos.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where CommandLine contains_any ("-R", "-pw", "sekurlsa", "-hp")

- **Umbral de alerta: 1 evento por usuario.**

2.10. Reconocimiento del host

- **Objetivo: Detectar comandos de descubrimiento del entorno.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image endswith_any ("hostname.exe", "ipconfig.exe", "whoami.exe", "net.exe")

- **Umbral de alerta: >5 comandos en 5 min.**

2.11. Creación remota de proceso vía WMIC

- **Objetivo: Identificar ejecución remota de procesos.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image endswith "wmic.exe" and CommandLine contains "process call create" and CommandLine contains "/node:"

- **Umbral de alerta: 1 evento.**

2.12. Bypass de UAC

- **Objetivo: Detectar técnicas conocidas de bypass UAC.**

- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where ParentImage endswith "fodhelper.exe" or Image endswith "osk.exe"

- **Umbral de alerta: 1 evento.**

2.13. Dump de credenciales con Mimikatz

- **Objetivo: Detectar acceso sospechoso a lsass.exe.**
- **Fuente: Sysmon (EventCode 10)**
- **KQL:**

kql

Sysmon

| where TargetImage endswith "lsass.exe" and GrantedAccess in ("0x1410", "0x1010", "0x143a")

- **Umbral de alerta: 1 evento.**

2.14. ProcDump sobre LSASS

- **Objetivo: Detección de uso de procdump para volcado de memoria.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image contains "procdump" and CommandLine contains "lsass"

- **Umbral de alerta: 1 evento.**

2.15. Dump de LSASS con Task Manager

- **Objetivo: Detección de volcado manual vía taskmgr.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image endswith "taskmgr.exe" and TargetFilename contains "lsass.dmp"

- **Umbral de alerta: 1 evento.**

2.16. Extracción de Active Directory con NTDSUtil

- **Objetivo: Identificar copias del archivo ntds.dit.**
- **Fuente: Sysmon**
- **KQL:**

kql

Sysmon

| where Image endswith "ntdsutil.exe" and TargetFilename contains "ntds.dit"

Umbral de alerta: 1 evento.

2.17. Certutil para descarga de archivos

- **Objetivo: Detectar uso de certutil como herramienta de exfiltración o descarga.**
- **Fuente: Endpoint Process Events**
- **KQL:**

kql

DeviceProcessEvents

| where FileName == "certutil.exe" and ProcessCommandLine contains "urlcache" and ProcessCommandLine contains "split"

- **Umbral de alerta: 1 evento por host.**

2.18. Pass the Hash

- **Objetivo: Detectar autenticaciones anómalas NTLM sin clave.**
- **Fuente: Security Event Log**
- **KQL:**

kql

SecurityEvent

| where EventID == 4624 and LogonType == 3 and LogonProcessName == "NtLmSsp" and Account == "NULL SID"

- **Umbral de alerta: >2 eventos en 5 min por IP.**

2.19. Kerberoasting

- **Objetivo: Detección de peticiones TGS con cifrado RC4.**
- **Fuente: Security Event Log**
- **KQL:**

kql

SecurityEvent

| where EventID == 4769 and TicketOptions == "0x40810000" and TicketEncryptionType == "0x17"

- **Umbral de alerta: 1 evento por usuario.**

2.20. Password Spraying

- **Objetivo: Detectar ataques de fuerza bruta distribuida (cuentas válidas o no).**
- **Fuente: Security Event Log**
- **KQL (usuarios válidos):**

kql

```
SecurityEvent
| where EventID == 4771 and FailureCode == "0x18"
| summarize count_distinct(Account) by bin(TimeGenerated, 2m), ClientIP
| where count_distinct_Account > 10
```

- **Umbral de alerta: ≥10 cuentas por IP en 2 minutos.**

2.21. Creación de Servicios Sospechosos

- **Objetivo: Detectar persistencia mediante creación de servicios nuevos.**
- **Fuente: Sysmon (Event ID 7045 o 1)**
- **KQL:**

kql

```
Event
| where EventID == 7045 and ServiceName !in ("Microsoft*", "Sysmon*")
```

- **Umbral: >1 nuevo servicio en 5 min.**

2.22. Modificación del archivo hosts

- **Objetivo: Detectar alteraciones al archivo hosts para redirecciones maliciosas.**
- **Fuente: Sysmon, File Creation**
- **KQL:**

kql

```
DeviceFileEvents

| where FileName == "hosts" and FolderPath endswith "\\drivers\\etc"
```

- **Umbral: 1 modificación fuera de horario laboral.**

2.23. Ejecución de script en unidad USB

- **Objetivo: Detectar ejecución de scripts o binarios desde dispositivos extraíbles.**
- **Fuente: Sysmon, DeviceEvents**
- **KQL:**

kql

```
DeviceProcessEvents

| where FolderPath startswith @"E:\\" or FolderPath startswith @"F:\\"
```

- **Umbral: 1 ejecución sospechosa fuera de horario.**

2.24. Conexiones a dominios recientemente registrados

- **Objetivo: Detectar beaconing o comunicación con C2s nuevos.**
- **Fuente: DNS logs + Threat Intel feed**
- **KQL:**

kql

```
DeviceNetworkEvents

| where RemoteUrl in (externalfeed_domains_last7days)
```

- **Umbral: cualquier coincidencia.**

2.25. Ejecución de binarios desde AppData o Temp

- **Objetivo: Detectar malware fuera de ubicaciones comunes.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FolderPath contains "\\AppData\\" or FolderPath contains "\\Temp\\"

- **Umbral: >2 ejecuciones por host en 5 min.**

2.26. Conexiones RDP externas

- **Objetivo: Detección de acceso remoto no autorizado.**
- **Fuente: Firewall Logs, Security Event Log**
- **KQL:**

kql

DeviceNetworkEvents

| where RemotePort == 3389 and RemoteIP !in (internal_ip_ranges)

- **Umbral: cualquier conexión externa.**

2.27. Enumeración de recursos compartidos

- **Objetivo: Identificar movimientos laterales o reconocimiento.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where ProcessCommandLine has_any ("net view", "net share", "net use")

- **Umbral: >3 comandos en 10 min.**

2.28. Ejecución de binarios maliciosos (Living off the Land)

- **Objetivo: Detección de LOLBins como mshta, regsvr32, wmic, rundll32, etc.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName in~ ("mshta.exe", "regsvr32.exe", "wmic.exe", "rundll32.exe")

- **Umbral: 1 evento si no hay justificación.**

2.29. Descarga de ejecutables sospechosos desde navegador

- **Objetivo: Detección de descarga de .exe o .dll**
- **Fuente: DeviceFileEvents**
- **KQL:**

kql

DeviceFileEvents

| where FileName endswith ".exe" or FileName endswith ".dll"

| where InitiatingProcessFileName in~ ("chrome.exe", "msedge.exe", "firefox.exe")

- **Umbral: >1 descarga por usuario/día.**

2.30. Conexiones salientes a puertos inusuales

- **Objetivo: Detectar canales de exfiltración no estándar.**
- **Fuente: Firewall Logs / Network Events**

- **KQL:**

kql

DeviceNetworkEvents

| where RemotePort notin (80, 443, 53)

- **Umbral: >3 puertos atípicos en 10 min.**

2.31. Ejecución de scripts VBS o JS

- **Objetivo: Identificar payloads en correos maliciosos.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName endswith ".vbs" or FileName endswith ".js"

- **Umbral: 1 evento por host.**

2.32. Carga de DLL sospechosa

- **Objetivo: Detectar DLL hijacking o injection.**
- **Fuente: Sysmon (Event ID 7)**
- **KQL:**

kql

DeviceImageLoadEvents

| where InitiatingProcessFileName !in~ ("explorer.exe", "svchost.exe") and

FileName endswith ".dll"

- **Umbral: 1 carga inusual.**

2.33. Persistencia en clave Run/RunOnce

- **Objetivo: Detectar persistencia mediante arranque automático.**
- **Fuente: Sysmon (Event ID 13)**
- **KQL:**

kql

DeviceRegistryEvents

| where RegistryKey has "Run" or RegistryKey has "RunOnce"

- **Umbral: cualquier escritura sospechosa.**

2.34. Uso de herramientas de pentest conocidas

- **Objetivo: Detectar herramientas como mimikatz.exe, cobaltstrike.beacon, etc.**
- **Fuente: Sysmon, AV Logs**
- **KQL:**

kql

DeviceProcessEvents

| where FileName in~ ("mimikatz.exe", "beacon.exe", "nmap.exe", "netcat.exe")

- **Umbral: cualquier ejecución.**

2.35. Ejecución de PowerShell con parámetros base64

- **Objetivo: Detección de scripts ofuscados.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName == "powershell.exe" and ProcessCommandLine contains "-enc"

- **Umbral: 1 evento.**

2.36. Ejecución remota mediante PsExec

- **Objetivo: Movimiento lateral.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName contains "psexec"

- **Umbral: cualquier ejecución.**

2.37. Creación de tareas programadas sospechosas

- **Objetivo: Persistencia mediante tareas maliciosas.**
- **Fuente: Sysmon / Windows Logs**
- **KQL:**

kql

Event

| where EventID in (4698, 106)

- **Umbral: >1 nueva tarea por host no documentada.**

2.38. Cambios en directivas de seguridad

- **Objetivo: Detectar alteraciones en políticas de auditoría o privilegios.**
- **Fuente: Security Logs (Event ID 4739, 4902)**
- **KQL:**

kql SecurityEvent

| where EventID in (4739, 4902)

- **Umbral: cualquier evento.**

2.39. Bloqueos de AV o EDR

- **Objetivo: Alertar sobre intentos de evasión.**
- **Fuente: Defender / EDR**
- **KQL:**

kql

DeviceEvents

| where ActionType in ("AntivirusDetection", "TamperProtectionBypass", "ScanAborted")

- **Umbral: >1 evento por host.**

2.40. Acceso masivo a recursos compartidos

- **Objetivo: Identificar intentos de exfiltración o ransomware.**
- **Fuente: FileAudit, Sysmon**
- **KQL:**

kql

DeviceFileEvents

| summarize count() by InitiatingProcessAccountName, bin(TimeGenerated, 5m)

| where count_ > 100

- **Umbral: >100 archivos abiertos en 5 minutos.**

2.41. Conexión a VPN fuera de horario laboral

- **Objetivo: Detectar conexiones inusuales que podrían indicar intrusión.**
- **Fuente: VPN Logs, Azure Sign-in logs**
- **KQL:**

kql

SigninLogs

| where ResourceDisplayName contains "VPN" and TimeGenerated between (datetime("19:00") .. datetime("07:00"))

- **Umbral: 1 conexión fuera de horario.**

2.42. Acceso de usuario privilegiado desde IP extranjera

- **Objetivo: Detectar posible compromiso de credenciales.**
- **Fuente: Azure AD / M365 Sign-in logs**
- **KQL:**

kql

SigninLogs

| where UserPrincipalName has "admin" and Location !in ("Spain", "Europe")

- **Umbral: cualquier coincidencia.**

2.43. Ejecución de macros en archivos Office

- **Objetivo: Detectar técnicas iniciales de infección.**
- **Fuente: Office365 logs**
- **KQL:**

kql

OfficeActivity

| where Operation == "ExecuteMacro"

- **Umbral: >1 por día por usuario.**

2.44. Ejecución de msbuild.exe desde rutas inusuales

- **Objetivo: Detección de LOLBins en rutas personalizadas.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName == "msbuild.exe" and FolderPath !startswith "C:\\Program Files\\"

- **Umbral: cualquier ejecución.**

2.45. Escaneo de puertos internos (nmap, zmap)

- **Objetivo: Identificar reconocimiento lateral.**
- **Fuente: Sysmon, EDR**
- **KQL:**

kql

DeviceProcessEvents

| where ProcessCommandLine contains "nmap" or ProcessCommandLine contains "zmap"

- **Umbral: cualquier ejecución.**

2.46. Creación de múltiples cuentas en corto periodo

- **Objetivo: Detección de automatización o abuso.**

- **Fuente: Security Event Logs (EventID 4720)**
- **KQL:**

kql

SecurityEvent

| where EventID == 4720

| summarize count() by bin(TimeGenerated, 10m)

| where count_ > 3
- **Umbral: >3 en 10 min.**

2.47. Modificación de auditoría de eventos

- **Objetivo: Intento de evasión o preparación de ataque.**
- **Fuente: Security Event Logs (EventID 4719)**
- **KQL:**

kql

SecurityEvent

| where EventID == 4719
- **Umbral: cualquier modificación.**

2.48. Múltiples inicios de sesión fallidos seguidos de éxito

- **Objetivo: Detección de bruteforce exitoso.**
- **Fuente: SecurityEvent 4625 y 4624**
- **KQL:**

kql

SecurityEvent

| where EventID == 4625 or EventID == 4624

| summarize Failed = countif(EventID == 4625), Success = countif(EventID == 4624) by Account

| where Failed > 5 and Success >= 1

- **Umbral: >5 fallos + 1 éxito.**

2.49. Cambio de contraseñas masivo

- **Objetivo: Identificar compromiso a gran escala o mal uso administrativo.**
- **Fuente: Azure AD Logs, Security Logs**
- **KQL:**

kql

AuditLogs

| where OperationName == "Change user password"

| summarize count() by bin(TimeGenerated, 10m)

| where count_ > 10

- **Umbral: >10 cambios en 10 min.**

2.50. Acceso a cuentas de servicio por usuarios

- **Objetivo: Detectar uso indebido de cuentas de servicio.**
- **Fuente: Security Logs, Azure**
- **KQL:**

kql

SigninLogs

| where UserPrincipalName endswith "@svc.domain.com"

- **Umbral: cualquier login.**

2.51. Uso de herramientas de control remoto

- **Objetivo: Detectar acceso externo no corporativo.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where FileName in~ ("TeamViewer.exe", "AnyDesk.exe", "AmmyyAdmin.exe")

- **Umbral: cualquier ejecución.**

2.52. Cambio de permisos en archivos críticos

- **Objetivo: Intento de manipulación o sabotaje.**
- **Fuente: FileAudit / Sysmon**
- **KQL:**

kql

DeviceFileEvents

| where ActionType == "FilePermissionChange" and FolderPath contains "C:\\Windows"

- **Umbral: cualquier modificación.**

2.53. Conexión persistente a dominio anómalo

- **Objetivo: Detectar beaconing o C2.**
- **Fuente: DNS logs**
- **KQL:**

kql

DeviceNetworkEvents

| summarize count() by RemoteUrl, bin(TimeGenerated, 1h)

| where count_ > 10 and RemoteUrl endswith ".xyz"

- **Umbral: >10 por hora.**

2.54. Uso de powershell con payload remoto

- **Objetivo: Descarga y ejecución en memoria.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where ProcessCommandLine contains "IEX (New-Object Net.WebClient).DownloadString"

- **Umbral: 1 evento.**

2.55. Creación de script .bat en inicio

- **Objetivo: Persistencia en usuario.**
- **Fuente: File creation logs**
- **KQL:**

kql

DeviceFileEvents

| where FolderPath contains "Startup" and FileName endswith ".bat"

- **Umbral: 1 evento.**

2.56. Elevación de privilegios mediante token theft

- **Objetivo: Privilege escalation con suplantación.**
- **Fuente: Sysmon (EventID 10)**
- **KQL:**

kql

DeviceEvents

| where InitiatingProcessCommandLine contains "DuplicateToken" or contains "ImpersonateLoggedOnUser"

- **Umbral: cualquier intento.**

2.57. Ejecución directa desde Word o Excel

- **Objetivo: Exploits a través de macros o DDE.**
- **Fuente: Sysmon**
- **KQL:**

kql

DeviceProcessEvents

| where InitiatingProcessFileName in~ ("winword.exe", "excel.exe") and

FileName !in~ ("winword.exe", "excel.exe")

- **Umbral: cualquier ejecución anómala.**

2.58. Transferencia masiva desde servidor interno

- **Objetivo: Posible exfiltración o ransomware.**
- **Fuente: Proxy / Network logs**
- **KQL:**

kql

NetworkSession

| where DestinationPort == 80 or DestinationPort == 443

| summarize TotalBytesTransferred = sum(SentBytes) by DeviceName, bin(TimeGenerated, 5m)

| where TotalBytesTransferred > 1000000000

- **Umbral: >1GB en 5 minutos.**

2.59. Cambios en configuración del EDR o AV

- **Objetivo: Intento de deshabilitar protecciones.**
- **Fuente: Defender for Endpoint**
- **KQL:**

kql

DeviceEvents

| where ActionType contains "Tamper"

- **Umbral: cualquier evento.**

2.60. Acceso a puertos de administración web (8000, 8080, 8443)

- **Objetivo: Acceso a consolas web no controladas.**
- **Fuente: Firewall / Proxy**
- **KQL:**

kql

DeviceNetworkEvents

| where RemotePort in (8000, 8080, 8443)

- **Umbral: >3 accesos por hora.**

2.61. Modificación de archivos críticos (passwd, shadow)

- **Objetivo: Detectar manipulación de archivos de cuentas de usuario.**
- **Fuente: Auditd / Syslog**
- **KQL (o equivalente en Linux):**

bash

ausearch -f /etc/passwd -i

Umbral: Cualquier modificación sin justificación.

2.62. Acceso root fuera de horario

- **Objetivo: Detectar uso del usuario root en horas inusuales.**
- **Fuente: Syslog / auth.log**
- **KQL:**

kql

inuxAuditLogs

| where User == "root" and TimeGenerated between (19:00 .. 07:00)

Umbral: 1 evento fuera de horario.

2.63. Ejecución de binarios desde /tmp o /dev/shm

- **Objetivo: Detección de ejecución desde ubicaciones temporales.**
- **Fuente: Auditd / EDR Linux**
- **KQL:**

kql

ProcessEvents

| where FolderPath startswith "/tmp" or FolderPath startswith "/dev/shm"

Umbral: 1 evento sospechoso.

2.64. Carga de módulos del kernel sospechosos

- **Objetivo: Identificar posibles rootkits o cargas maliciosas.**
- **Fuente: auditd**
- **KQL:**

bash

auditctl -l | grep init_module

Umbral: Cualquier carga no habitual.

2.65. Escalada de privilegios con sudo

- **Objetivo: Detectar abuso de sudo para escalar privilegios.**
- **Fuente: /var/log/auth.log**
- **KQL:**

kql

LinuxAuditLogs

| where CommandLine contains "sudo" and User != "root"

Umbral: >3 comandos sudo en 5 minutos.

2.66. SSH desde IPs externas inusuales

- **Objetivo: Detección de acceso remoto desde IPs no permitidas.**
- **Fuente: auth.log**
- **KQL:**

kql LinuxSSHLogs

| where RemoteIP !in (corporate_ranges)

Umbral: 1 acceso desde IP extranjera.

2.67. Ejecución de scripts con permisos suid

- **Objetivo: Detectar scripts usados para escalada de privilegios.**
- **Fuente: auditd**
- **KQL:**

bash

find / -perm -4000 -type f -exec ls -la {} \;

Umbral: cualquier script SUID nuevo.

2.68. Persistencia en crontab o systemd

- **Objetivo: Detectar mecanismos de persistencia en Linux.**
- **Fuente: auditd / journald**
- **KQL:**

bash

journalctl | grep crontab

Umbral: 1 modificación no autorizada.

2.69. Acceso a archivos de claves privadas

- **Objetivo: Detectar lectura de archivos SSH privados.**
- **Fuente: auditd**
- **KQL:**

bash

auditctl -w /home -p r -k ssh_key_access

Umbral: cualquier acceso no esperado.

2.70. Modificación de permisos binarios del sistema

- **Objetivo: Evitar que atacantes alteren binarios de sistema.**
- **Fuente: auditd**
- **KQL:**

bash

auditctl -w /bin -p wa

Umbral: cualquier cambio fuera de ventana de mantenimiento.

---

macOS

2.71. Ejecución de AppleScript sospechoso

- **Objetivo: Detectar automatización maliciosa.**
- **Fuente: Unified Logs**
- **KQL:**

kql

macOSLogs

| where ProcessName == "osascript" and CommandLine contains "do shell script"

Umbral: 1 evento.

2.72. Acceso a TCC.db sin autorización

- **Objetivo: Detectar intento de eludir controles de privacidad.**
- **Fuente: Unified Logs**
- **KQL:**

bash

log show | grep tcc

Umbral: cualquier acceso por apps no aprobadas.

2.73. Uso de herramientas como osascript o spctl

- **Objetivo: Detectar bypasses de seguridad.**
- **Fuente: macOS logs**
- **KQL:**

kql

macOSLogs

| where ProcessName in ("osascript", "spctl")

Umbral: >1 por host fuera de horario.

2.74. Desactivación de Gatekeeper

- **Objetivo: Evitar ejecución de apps no verificadas.**
- **Fuente: system.log**
- **KQL:**

bash

spctl --status

Umbral: cualquier desactivación.

2.75. Cambios en configuraciones de privacidad

- **Objetivo: Detectar acceso a cámara, micro, etc.**
- **Fuente: TCC logs**
- **KQL:**

bash

log show | grep kTCCService

Umbral: cualquier cambio no gestionado por MDM.

2.76. Conexiones salientes desde launchd

- **Objetivo: Detección de persistencia maliciosa.**
- **Fuente: Unified Logs**
- **KQL:**

kql

macOSLogs

| where ProcessName == "launchd" and RemoteIP != ""

Umbral: 1 conexión sospechosa.

2.77. Creación de servicios en ~/Library/LaunchAgents

- **Objetivo: Persistencia del usuario local.**
- **Fuente: FileAudit**
- **KQL:**

bash

ls ~/Library/LaunchAgents/

Umbral: cualquier nuevo archivo sin firma.

2.78. Acceso remoto habilitado sin consentimiento

- **Objetivo: Detección de control remoto no autorizado.**
- **Fuente: system.log**
- **KQL:**

bash

systemsetup -getremotelogin

Umbral: cualquier habilitación no autorizada.

2.79. Elevación vía sudo sin autorización

- **Objetivo: Identificar abuso de privilegios.**
- **Fuente: /var/log/system.log**
- **KQL:**

bash

grep sudo /var/log/system.log

Umbral: >3 en 5 minutos.

2.80. Carga de extensiones del sistema no firmadas

- **Objetivo: Evitar rootkits o extensiones no confiables.**
- **Fuente: kextstat**
- **KQL:**

bash

kextstat | grep -v com.apple

Umbral: cualquier kext no firmado.

2.81. Comunicaciones salientes inusuales desde dispositivos IoT

- **Objetivo: Detectar beaconing o C2.**
- **Fuente: Network Logs**
- **KQL:**

kql

NetworkTraffic

| where DeviceType == "IoT" and RemoteIP !in (trusted_ranges)

Umbral: >5 conexiones externas por hora.

2.82. Cambios en firmware no autorizados

- **Objetivo: Detección de actualización maliciosa.**
- **Fuente: Device logs**
- **KQL:**

json

{ "event": "firmware_upgrade" }

Umbral: cualquier cambio no planificado.

2.83. Uso de contraseñas por defecto detectado

- **Objetivo: Verificar configuración inicial sin cambios.**
- **Fuente: Vulnerability Scanner**
- **KQL:**

kql

VulnScanResults

| where Credential == "admin:admin"

Umbral: cualquier detección.

2.84. Acceso a puertos telnet o SSH abiertos

- **Objetivo: Reducir superficie expuesta.**
- **Fuente: Nmap / PortScan**
- **KQL:**

kql

PortScanResults

| where DeviceType == "IoT" and Port in (23, 22)

Umbral: 1 host afectado.

2.85. Ejecución remota de comandos

- **Objetivo: Detectar actividad no autorizada.**
- **Fuente: Device Logs**
- **KQL:**

json

{ "cmd_exec": true }

Umbral: 1 evento.

2.86. Conexión frecuente a IPs maliciosas

- **Objetivo: Detección de botnets.**
- **Fuente: Threat Intel + NetLogs**
- **KQL:**

kql

NetworkTraffic

| where RemoteIP in (threat_feed)

Umbral: >3 eventos en 10 min.

2.87. Presencia de malware como Mirai

- **Objetivo: Detectar comportamiento tipo botnet.**
- **Fuente: IDS/IPS**
- **KQL:**

kql

IDSAlerts

| where Signature contains "Mirai"

Umbral: cualquier alerta.

2.88. Cambios de configuración sin login registrado

- **Objetivo: Detectar abuso o backdoors.**
- **Fuente: Syslogs**
- **KQL:**

json

{ "config_changed": true, "user": "unknown" }

Umbral: cualquier evento.

2.89. Sobrecarga de red desde IoT

- **Objetivo: Posible DDoS o abuso interno.**
- **Fuente: Netflow**
- **KQL:**

kql

Netflow

| where DeviceType == "IoT"

| summarize sum(SentBytes) by DeviceName

| where SentBytes > 100000000

Umbral: >100MB en 10 min.

2.90. Acceso fuera del patrón horario normal

- **Objetivo: Acceso sospechoso.**
- **Fuente: Device auth logs**
- **KQL:**

kql

IoTAuthLogs

| where TimeGenerated between (00:00 .. 05:00)

Umbral: 1 acceso.

2.91. Inyecciones SQL detectadas en logs de WAF

- **Objetivo: Detectar intentos de manipulación de bases de datos a través de peticiones maliciosas.**
- **Fuente: WAF / Proxy / Apache / Nginx logs**
- **KQL:**

kql

WAFLogs

| where RequestURI contains_any ("UNION SELECT", "' OR 1=1", "xp_cmdshell", "--", "sleep(")

Umbral: >5 intentos por IP en 10 minutos.

2.92. Escaneo de directorios con patrones comunes

- **Objetivo: Detectar reconocimiento automatizado de rutas sensibles.**
- **Fuente: Access Logs / WAF**
- **KQL:**

kql

WebAccessLogs

| where RequestURI contains_any ("/admin", "/.git", "/phpinfo.php", "/config", "/backup")

Umbral: >10 URIs sensibles en 5 minutos por IP.

2.93. Accesos con user-agents sospechosos

- **Objetivo: Detectar herramientas automatizadas como Burp Suite, sqlmap o curl.**

- **Fuente: Web server logs**
- **KQL:**

kql

```
WebAccessLogs

| where UserAgent contains_any ("sqlmap", "curl", "nikto", "fuzzer", "scanner")
```

Umbral: 1 detección por IP.

2.94. Múltiples errores 401/403 seguidos

- **Objetivo: Detectar fuerza bruta o intentos de acceso no autorizados.**
- **Fuente: Apache/Nginx/WAF**
- **KQL:**

kql

```
WebAccessLogs

| where StatusCode in (401, 403)

| summarize count() by ClientIP, bin(TimeGenerated, 5m)

| where count_ > 10
```

Umbral: >10 errores por IP en 5 minutos.

2.95. Carga de archivos maliciosos vía POST

- **Objetivo: Identificar intentos de subir webshells u otros binarios.**
- **Fuente: WAF / Proxy / SIEM**
- **KQL:**

kql

```
WebAccessLogs

| where Method == "POST" and FileName endswith_any (".php", ".jsp", ".exe",
".aspx")
```

Umbral: cualquier evento.

2.96. Explotación de vulnerabilidades LFI/RFI

- **Objetivo: Detectar inclusión de archivos locales o remotos.**
- **Fuente: WAF / Logs de aplicación**
- **KQL:**

kql

```
WebAccessLogs

| where RequestURI contains_any ("etc/passwd", "http://", "file=", "php://input", "data://")
```

Umbral: >3 eventos por IP en 10 minutos.

2.97. Tráfico elevado a /admin o /login

- **Objetivo: Identificar escaneo o fuerza bruta a interfaces de administración.**
- **Fuente: Web logs**
- **KQL:**

kql

```
WebAccessLogs

| where RequestURI contains_any ("/admin", "/login")

| summarize count() by ClientIP, bin(TimeGenerated, 5m)

| where count_ > 15
```

Umbral: >15 accesos por IP.

2.98. Bypass de autenticación detectado

- **Objetivo: Detectar acceso a zonas protegidas sin login exitoso previo.**
- **Fuente: Logs de autenticación y acceso**
- **KQL:**

kql

```
WebAccessLogs
| where AuthStatus == "Anonymous" and RequestURI contains "/dashboard"
```

Umbral: cualquier acceso.

2.99. Uso de comandos del sistema en parámetros (RCE)

- **Objetivo: Detección de intentos de ejecución remota.**
- **Fuente: WAF / Logs aplicación**
- **KQL:**

kql

```
WebAccessLogs
| where RequestURI contains_any (";ls", ";cat", ";ping", "`id`", "|whoami")
```

Umbral: 1 intento.

2.100. Uso de técnicas de fuzzing (burpsuite, ffuf)

- **Objetivo: Detectar exploración agresiva o automatizada.**
- **Fuente: Web server logs**
- **KQL:**

kql

```
WebAccessLogs
| where UserAgent contains_any ("ffuf", "dirb", "dirbuster", "burp", "intruder")
```

Umbral: cualquier detección.

Autor de esta guía

Julián David Delgado Piraquive

Head of Offensive Security & MDR

Julián es un experto en ciberseguridad, especializado en seguridad ofensiva y respuesta ante incidentes. Lidera equipos de Red Team y MDR en Factum Information Technologies, además es docente de Máster de Ciberseguridad.

Ver más contenido de este autor

Puedes encontrar más contenido como este en www.cylum.tech

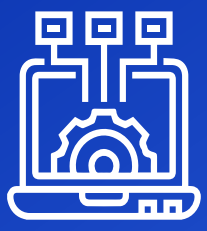
Cylum

CYBERSECURITY AS A SERVICE

Simplificamos la ciberseguridad

Soluciona tus necesidades de protección ante riesgos digitales. Cumple con la regulación.

Personal Experto



Tecnología

Cumplimiento normativo

Protección 24x7

Una solución de

FACTUM

15 años protegiendo empresas