# Taller SigmaCLI

## 1. Setup del entorno

Requisitos: Python 3.10+, acceso a terminal WSL o Linux y eventos de creación de procesos en Windows (por ejemplo con Sysmon).

### *Instala y verifica:*

```
sudo apt update
sudo apt install -y python3 python3-pip pipx
pipx ensurepath
export PATH="$HOME/.local/bin:$PATH"

pipx install sigma-cli

sigma version
sigma list pipelines
```

## 2. Ejercicio 1 — Validación y fortalecimiento de la regla base

Guarda el siguiente YAML como office_cmd_ps_download.yml. Valida con el linter y completa metadatos.

```
       # - 'tags' como string con comas (debe ser lista)
       # - 'falsepositives' como string (debe ser lista)
       # - regex sin comillas

       title: Office → CMD → PowerShell con descarga remota
(cadena sospechosa)
       id: 8d7a4b16-6f1f-4a54-9b7e-2f2d4c1e5a90
       status: test
       description: Detecta cadena típica de macro/phishing
donde Office lanza cmd y luego PowerShell con banderas
ofensivas y posible descarga de payload.
       author: Sergio Mazariego
       date: 2025/08/15

       tags: attack.execution, attack.t1204.002,
attack.t1059.001      # ❌ debe ser lista

       falsepositives: Scripts de IT o automatizaciones
legítimas que usen cmd/powershell con descargas   # ❌ debe
ser lista

       level: high

       logsource:
         category: process_creation
         product: windows

       detection:
         child_shells:
           Image|endswith:
             - '\powershell.exe'
             - '\pwsh.exe'
```

```
            - '\cmd.exe'

        office_parents:
          ParentImage|endswith:
            - '\winword.exe'
            - '\excel.exe'
            - '\powerpnt.exe'

        ps_args_offensive:
          CommandLine|contains:
            - '-noprofile'
          CommandLine|re: (?i)\-enc(?:odedcommand)?\s+[A-Za-
z0-9+/=]{20,}   # ✗ ponlo entre comillas al arreglar

        download_markers:
          CommandLine|contains:
            - 'Invoke-WebRequest'
            - 'curl http'
            - 'wget http'
            - 'bitsadmin /transfer'
            - 'certutil -urlcache -split -f'
          CommandLine|re: '(?i)https?://'

        cmd_chain:
          ParentImage|endswith: '\cmd.exe'
          ParentCommandLine|contains: '/c'

        condition: >
          office_parents and child_shells and
          (ps_args_offensive or download_markers or
cmd_chain)
```

### *Pasos:*

```
1) Guarda el archivo como office_cmd_ps_download.yml
2) Ejecuta: sigma check office_cmd_ps_download.yml3) Si hay advertencias,
   agrega o ajusta:
- modified: 2025/08/16
- references: URLs justificativas
- tags/status: según confianza tras pruebas
4) Repite 'sigma check hasta 0 errores
```

### *Criterios de aceptación:*

- La regla pasa 'sigma lint' sin errores.
- Metadata completa y coherente (title, id, author, date, modified, tags, references, level, status).

## 3. Ejercicio 2 — Variantes de sensibilidad (estricta y amplia)

Crea dos copias de la regla y modifica solo la condición para controlar sensibilidad y ruido.

### *Archivos:*

```
office_cmd_ps_download_strict.yml
office_cmd_ps_download_loose.yml
```

### *Condiciones:*

```
      # Estricta condition: office_parents and child_shells and ps_args_offensive and
      download_markers and cmd_c

      # Amplia
      condition: office_parents and child_shells and (ps_args_offensive or download_markers or
cmd_ch
```

### *Criterios de aceptación:*

- Ambas variantes pasan 'sigma check.
- Comentarios en YAML explican cuándo usar cada variante.

## 4. Ejercicio 3 — Tuning con allowlist en YAML

Añade exclusiones explícitas para reducir ruido (rutas y URLs corporativas conocidas).

### *Fragmento para incorporar en 'detection':*

```
      allowlist:
      CommandLine|contains:
          - 'https://intranet.ejemplo.local'      - 'C:\\HerramientasCorp\\scripts\\' condition:
>   office_parents and child_shells and (ps_args_offensive or download_markers or cmd_chain)   and
not allowlist
```

### *Criterios de aceptación:*

- La regla con allowlist pasa 'sigma check.
- El YAML documenta claramente qué se excluye y por qué.