Sigma Rules – *The “YAML of SIEMs”*

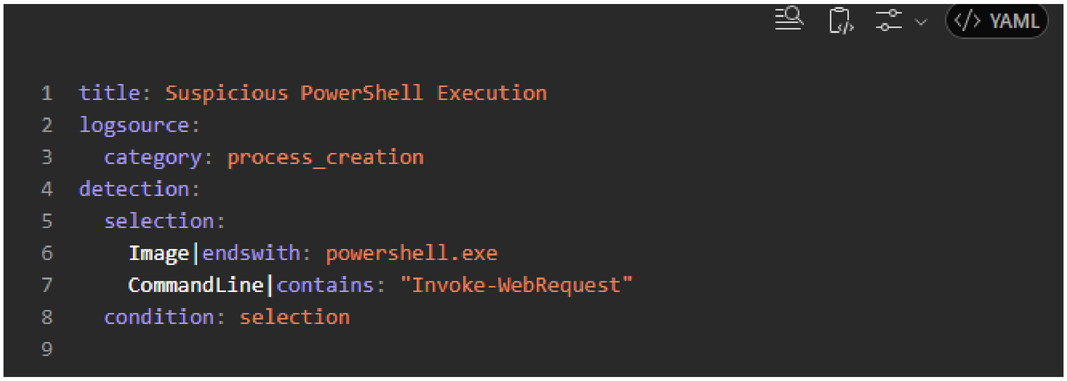
What Are They:

Sigma is a **generic and open detection rule format** for describing log-based detection logic. Think of it as the **“YAML for SIEMs”** — it lets you write one rule that can be converted into queries for different SIEM platforms (like Splunk, Elastic, Sentinel, etc.).

Use Case:

- Detect suspicious behavior in logs (e.g., PowerShell abuse, credential dumping)
- Write once, deploy anywhere (with a Sigma converter)

Example:



```yaml
title: Suspicious PowerShell Execution
logsource:
  category: process_creation
detection:
  selection:
    Image|endswith: powershell.exe
    CommandLine|contains: "Invoke-WebRequest"
  condition: selection

```

Show more lines

Tools:

- Sigma HQ GitHub
- sigmac – converts Sigma rules to SIEM queries

YARA Rules – *The "DNA of Malware"*

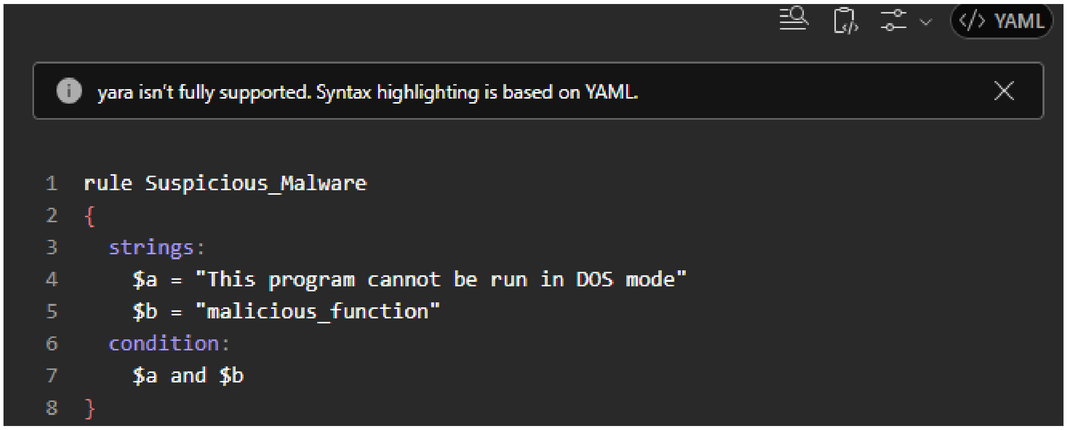
What Are They:

YARA is a tool used to **identify and classify malware** based on patterns (strings, byte sequences, file structure). It's often called the **"pattern-matching engine for malware"**.

Use Case:

- Detect malware in files, memory, or binaries
- Used in antivirus engines, sandboxes, and threat intel

Example:



yara isn't fully supported. Syntax highlighting is based on YAML.

```
rule Suspicious_Malware
{
  strings:
    $a = "This program cannot be run in DOS mode"
    $b = "malicious_function"
  condition:
    $a and $b
}
```

Tools:

- YARA GitHub
- Used in tools like VirusTotal, Cuckoo Sandbox, and Velociraptor

---

Sigma vs YARA – Quick Comparison

Feature	**Sigma**	**YARA**
Focus	Log-based detection	File/memory-based detection
Format	YAML	Custom rule syntax
Use Case	SIEM alerts, threat hunting	Malware detection, DFIR
Output	SIEM queries	Match results on files/memory