Sigma Rules

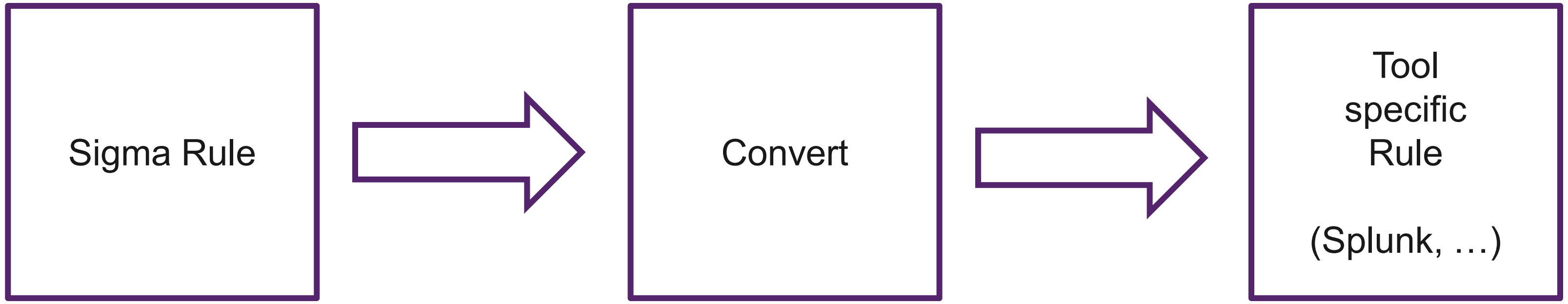
Hunting Rules

3 December 2024

OST
Eastern Switzerland
University of Applied Sciences

SIGMA

- Sigma is a generic and open signature format that allows you to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.
- Sigma is for log files what Snort is for network traffic and YARA is for files.



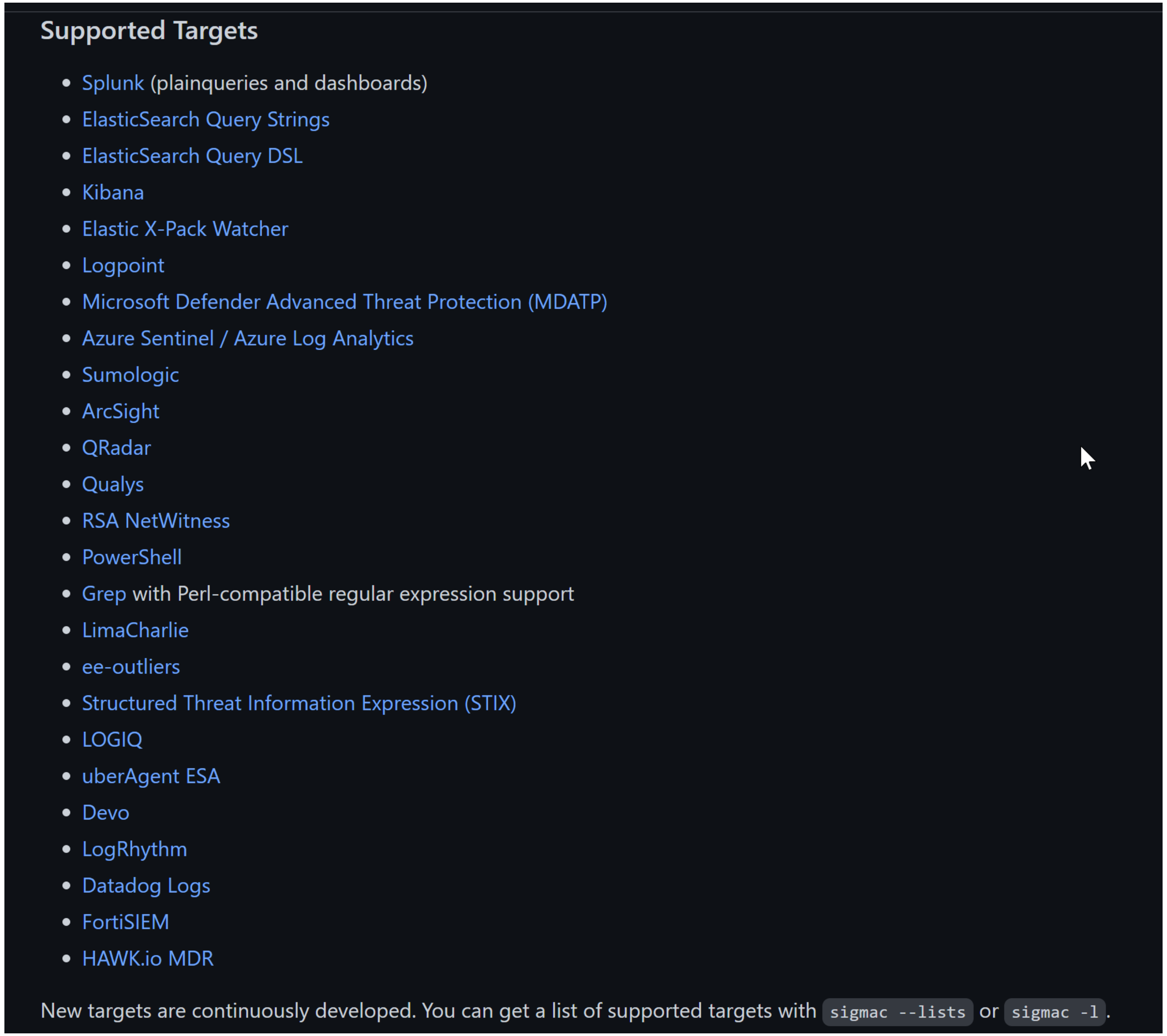
Detection Rules: Sigma

Sigma Rules

Widely accepted

Platform agnostic (avoid vendor lock in)

- Has tooling to convert to your environment
- Great library of rules
- Community driven!



Supported Targets

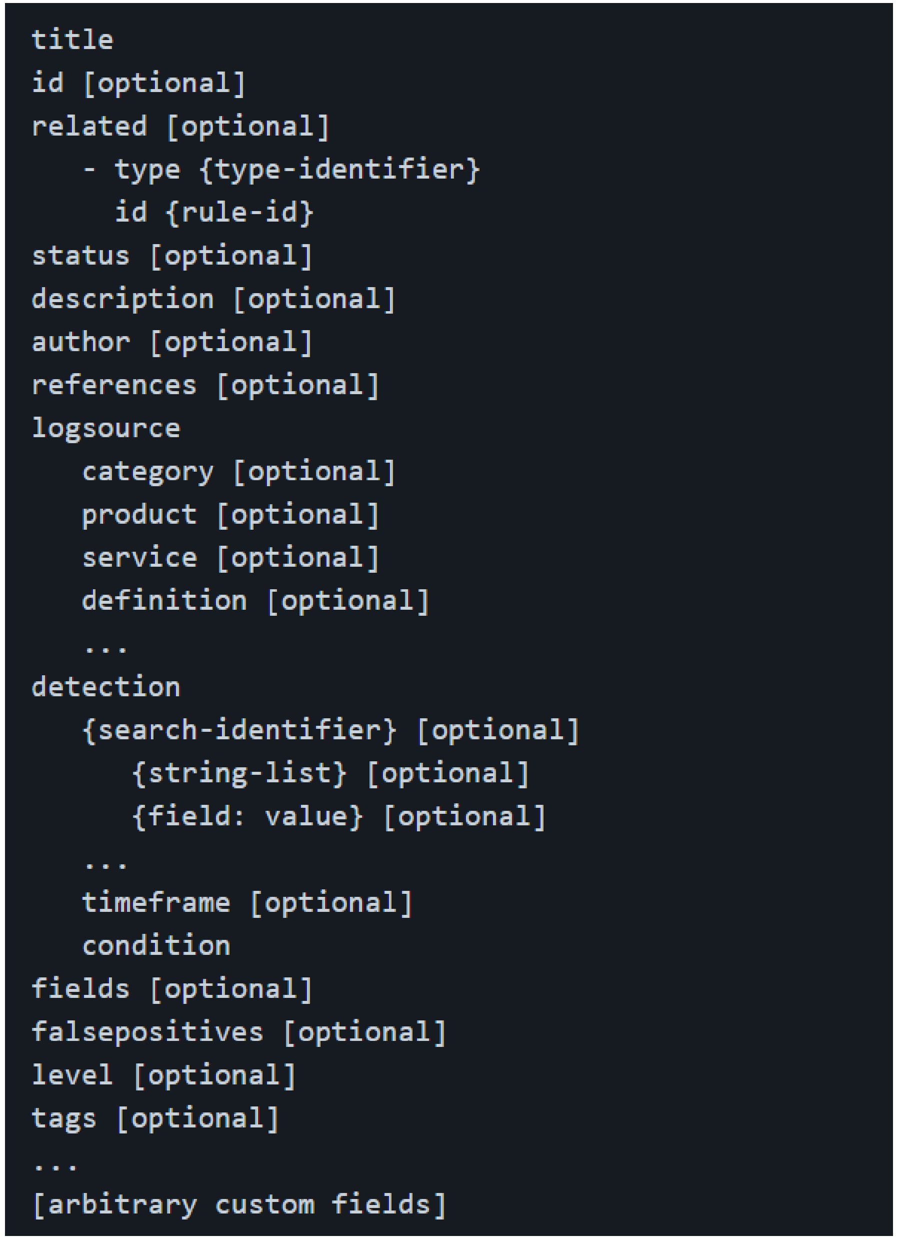
- Splunk (plainqueries and dashboards)
- ElasticSearch Query Strings
- ElasticSearch Query DSL
- Kibana
- Elastic X-Pack Watcher
- Logpoint
- Microsoft Defender Advanced Threat Protection (MDATP)
- Azure Sentinel / Azure Log Analytics
- Sumologic
- ArcSight
- QRadar
- Qualys
- RSA NetWitness
- PowerShell
- Grep with Perl-compatible regular expression support
- LimaCharlie
- ee-outliers
- Structured Threat Information Expression (STIX)
- LOGIQ
- uberAgent ESA
- Devo
- LogRhythm
- Datadog Logs
- FortiSIEM
- HAWK.io MDR

New targets are continuously developed. You can get a list of supported targets with `sigmac --lists` or `sigmac -l`.

https://github.com/SigmaHQ/sigma#supported-targets

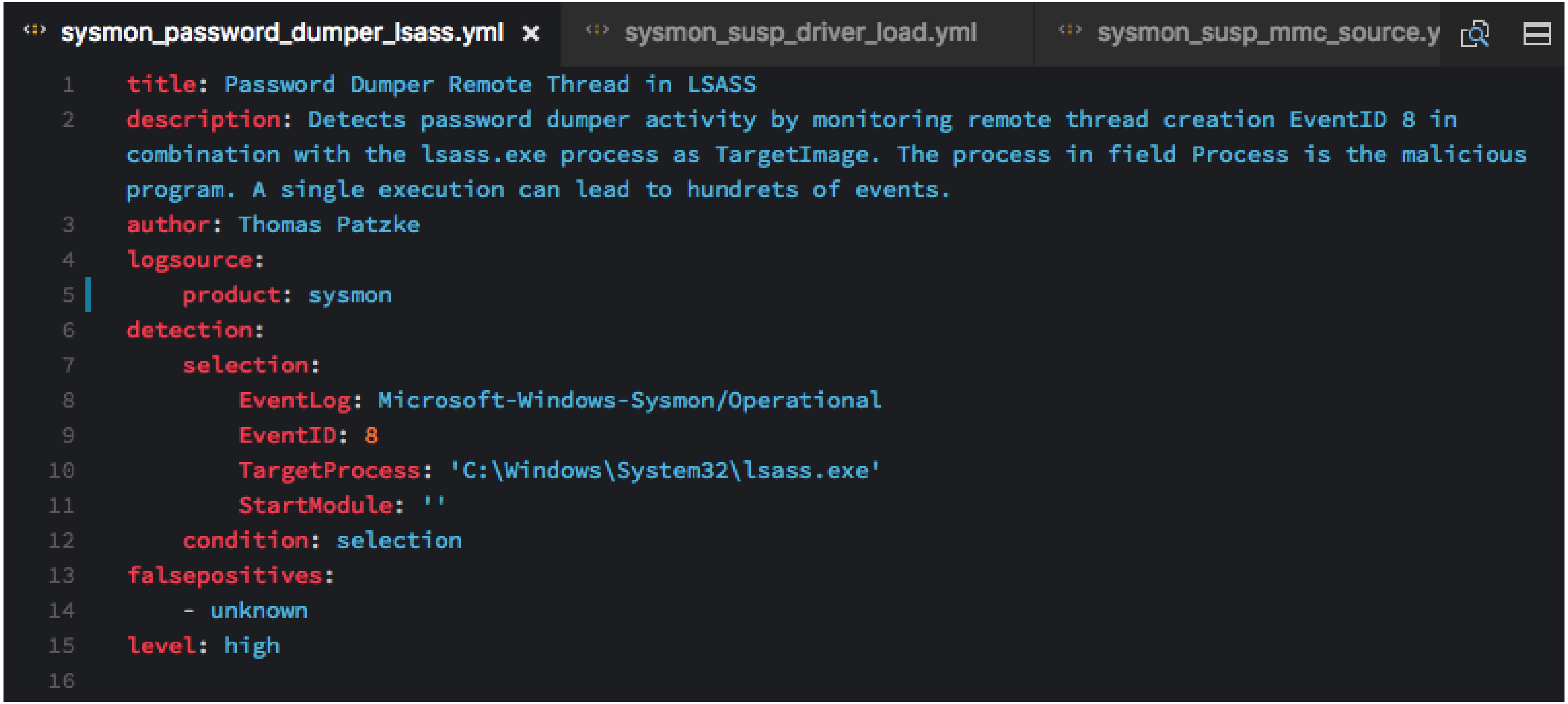
Sigma Rules - Structure

- It is relatively simple to use
- Yet very powerful
- Let’s look at the specification and then some examples!



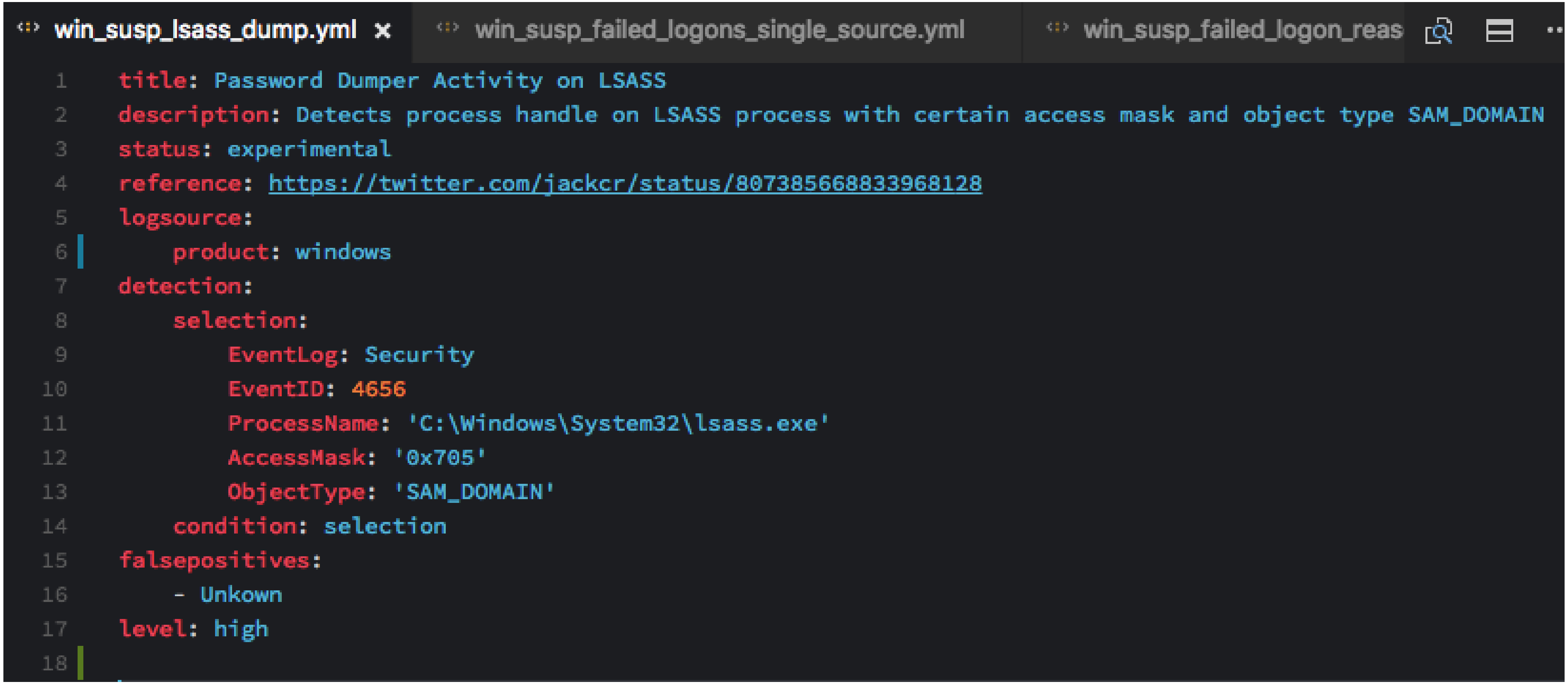
```
title
id [optional]
related [optional]
   - type {type-identifier}
     id {rule-id}
status [optional]
description [optional]
author [optional]
references [optional]
logsource
   category [optional]
   product [optional]
   service [optional]
   definition [optional]
   ...
detection
   {search-identifier} [optional]
      {string-list} [optional]
      {field: value} [optional]
   ...
   timeframe [optional]
   condition
fields [optional]
falsepositives [optional]
level [optional]
tags [optional]
...
[arbitrary custom fields]
```

Detection Rules: SIGMA


sysmon_password_dumper_lsass.yml ×
sysmon_susp_driver_load.yml
sysmon_susp_mmc_source.y

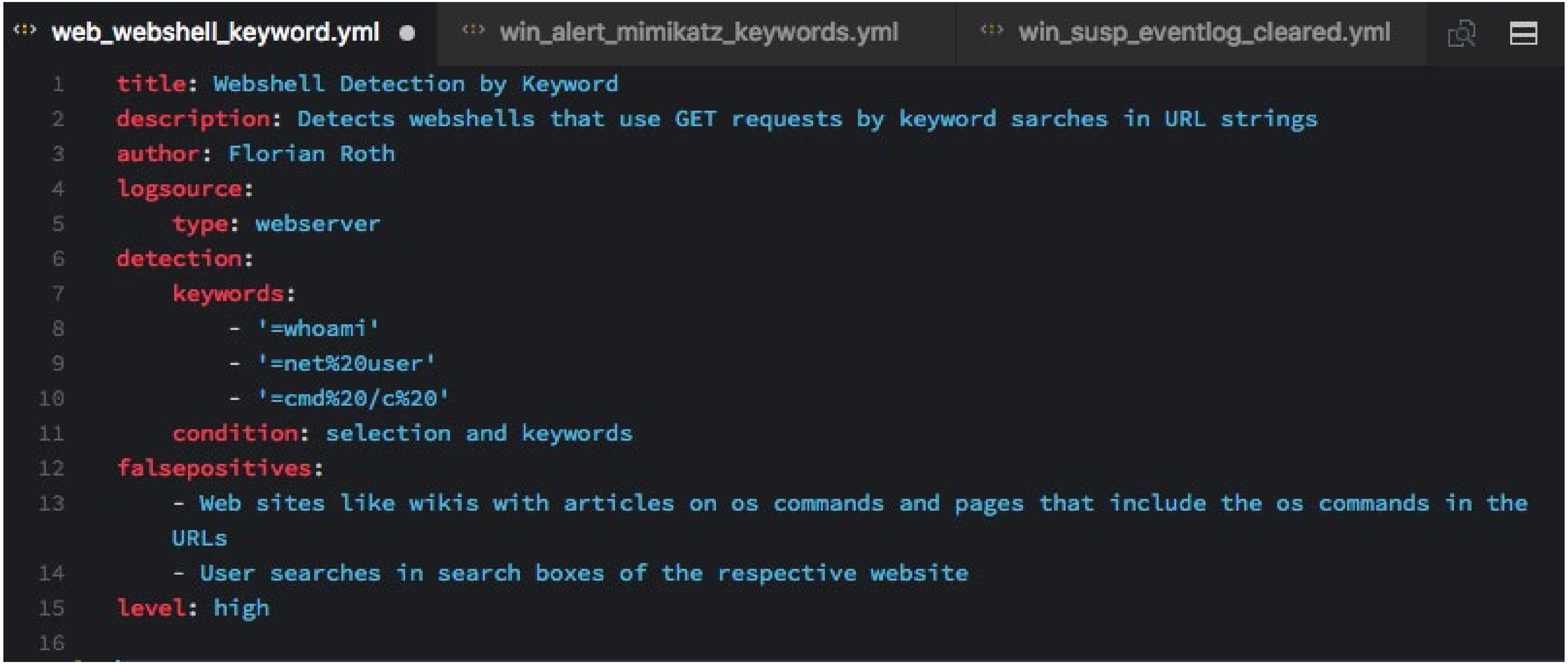
```yaml
title: Password Dumper Remote Thread in LSASS
description: Detects password dumper activity by monitoring remote thread creation EventID 8 in combination with the lsass.exe process as TargetImage. The process in field Process is the malicious program. A single execution can lead to hundrets of events.
author: Thomas Patzke
logsource:
    product: sysmon
detection:
    selection:
        EventLog: Microsoft-Windows-Sysmon/Operational
        EventID: 8
        TargetProcess: 'C:\Windows\System32\lsass.exe'
        StartModule: ''
    condition: selection
falsepositives:
    - unknown
level: high

```

Detection Rules: SIGMA


win_susp_lsass_dump.yml ×
win_susp_failed_logons_single_source.yml
win_susp_failed_logon_reas

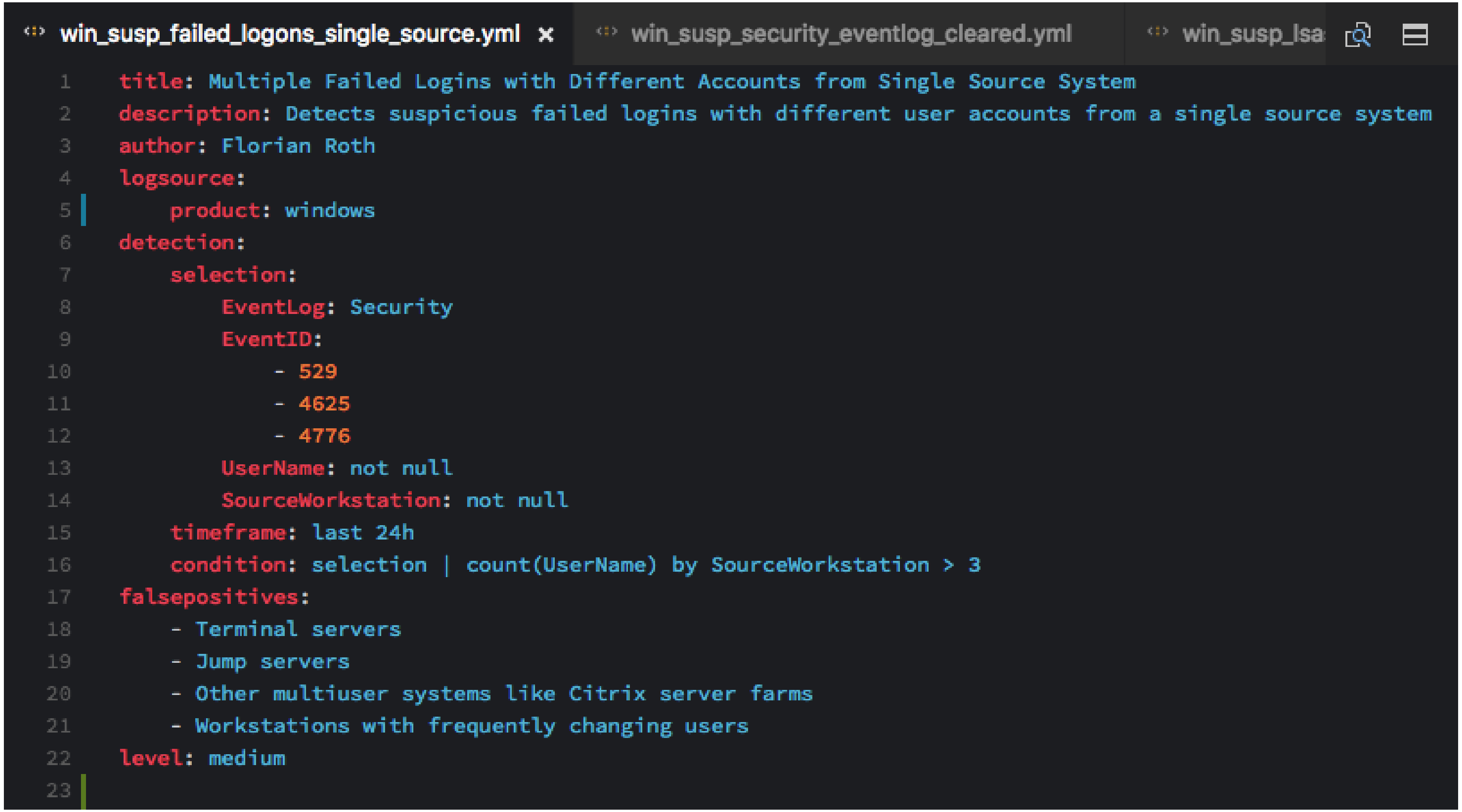
```yaml
title: Password Dumper Activity on LSASS
description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
status: experimental
reference: https://twitter.com/jackcr/status/807385668833968128
logsource:
    product: windows
detection:
    selection:
        EventLog: Security
        EventID: 4656
        ProcessName: 'C:\Windows\System32\lsass.exe'
        AccessMask: '0x705'
        ObjectType: 'SAM_DOMAIN'
    condition: selection
falsepositives:
    - Unkown
level: high
```

Detection Rules: SIGMA


web_webshell_keyword.yml
win_alert_mimikatz_keywords.yml
win_susp_eventlog_cleared.yml

```yaml
title: Webshell Detection by Keyword
description: Detects webshells that use GET requests by keyword sarches in URL strings
author: Florian Roth
logsource:
    type: webserver
detection:
    keywords:
        - '=whoami'
        - '=net%20user'
        - '=cmd%20/c%20'
    condition: selection and keywords
falsepositives:
    - Web sites like wikis with articles on os commands and pages that include the os commands in the URLs
    - User searches in search boxes of the respective website
level: high

```

Detection Rules: SIGMA


win_susp_failed_logons_single_source.yml
win_susp_security_eventlog_cleared.yml
win_susp_lsa

```yaml
title: Multiple Failed Logins with Different Accounts from Single Source System
description: Detects suspicious failed logins with different user accounts from a single source system
author: Florian Roth
logsource:
    product: windows
detection:
    selection:
        EventLog: Security
        EventID:
            - 529
            - 4625
            - 4776
        UserName: not null
        SourceWorkstation: not null
    timeframe: last 24h
    condition: selection | count(UserName) by SourceWorkstation > 3
falsepositives:
    - Terminal servers
    - Jump servers
    - Other multiuser systems like Citrix server farms
    - Workstations with frequently changing users
level: medium
```