50 Shades of Sigma

Describe and Share Generic Threat Detection Methods

Florian Roth

About Me

- Florian Roth
- Head of Research @ Nextron Systems
- IT Sec since 2000, Nation State Cyber Attacks since 2012
- THOR Scanner
- Twitter @cyb3rops
- Open Source Projects:
  - Sigma (Generic SIEM Rule Format)
  - LOKI (Open Source Scanner)
  - APT Groups and Operations Mapping
  - Antivirus Event Analysis Cheat Sheet
  - ...

Overview

- What is Sigma?
- Why Sigma?
  - Why do I believe that Sigma succeeds?
- Sigma – Quo vadis?
  - What is going to change?
- Shades of Sigma
  - STIX to Sigma
  - Sandbox Integration
  - Detect Unknown Threats

What is Sigma?

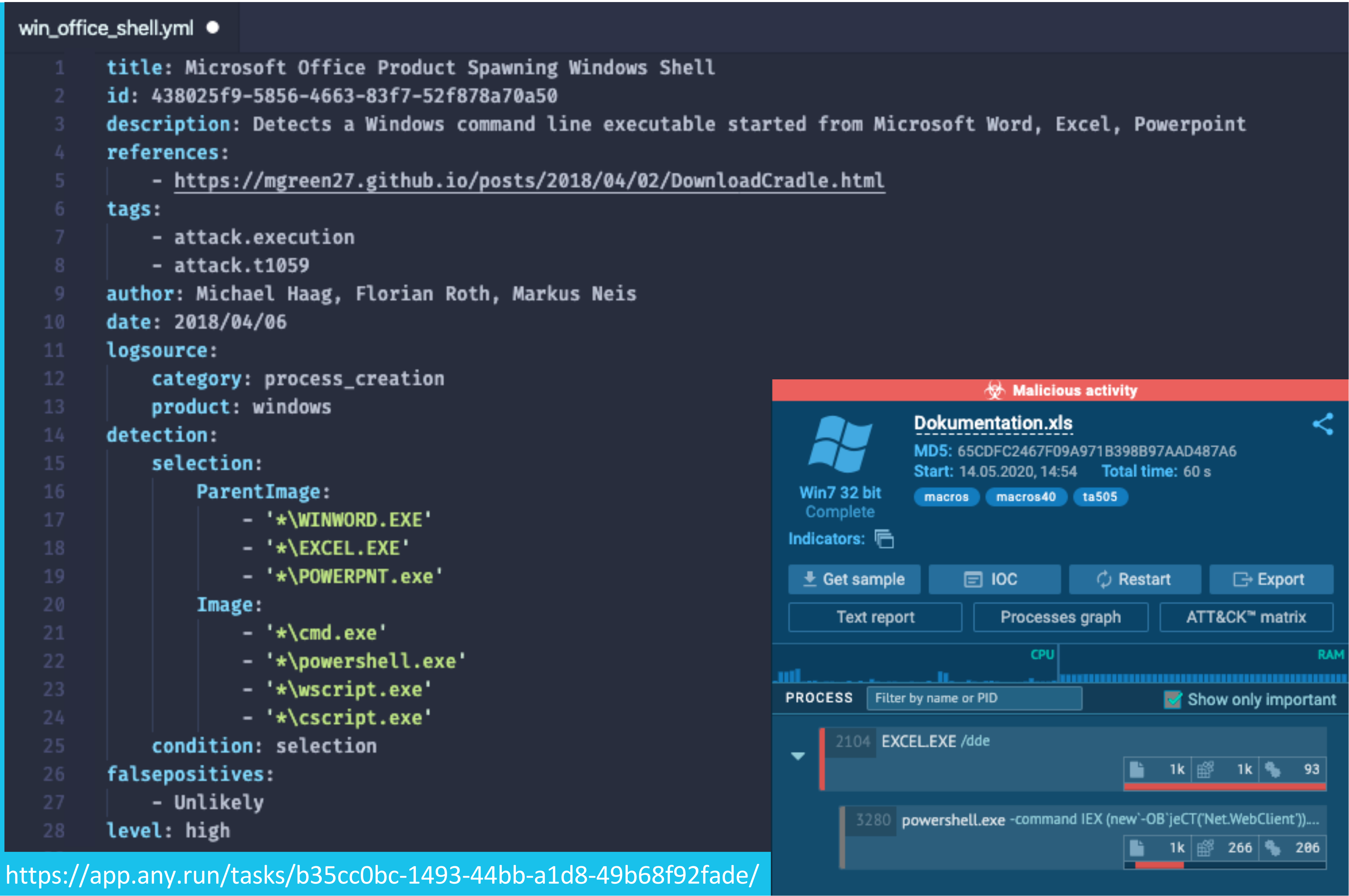
Sigma is for log data what
YARA is for files and
Snort is for network traffic .

What is Sigma?

Sigma is a generic rule format to express detection ideas on log data .

What does Sigma look like?

Example:
Microsoft Office program spawning a Windows executable



win_office_shell.yml ●

```yaml
title: Microsoft Office Product Spawning Windows Shell
id: 438025f9-5856-4663-83f7-52f878a70a50
description: Detects a Windows command line executable started from Microsoft Word, Excel, Powerpoint
references:
    - https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html
tags:
    - attack.execution
    - attack.t1059
author: Michael Haag, Florian Roth, Markus Neis
date: 2018/04/06
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        ParentImage:
            - '*\WINWORD.EXE'
            - '*\EXCEL.EXE'
            - '*\POWERPNT.exe'
        Image:
            - '*\cmd.exe'
            - '*\powershell.exe'
            - '*\wscript.exe'
            - '*\cscript.exe'
    condition: selection
falsepositives:
    - Unlikely
level: high
```

Malicious activity

Dokumentation.xls

MD5: 65CDFC2467F09A971B398B97AAD487A6

Start: 14.05.2020, 14:54 Total time: 60 s

macros macros40 ta505

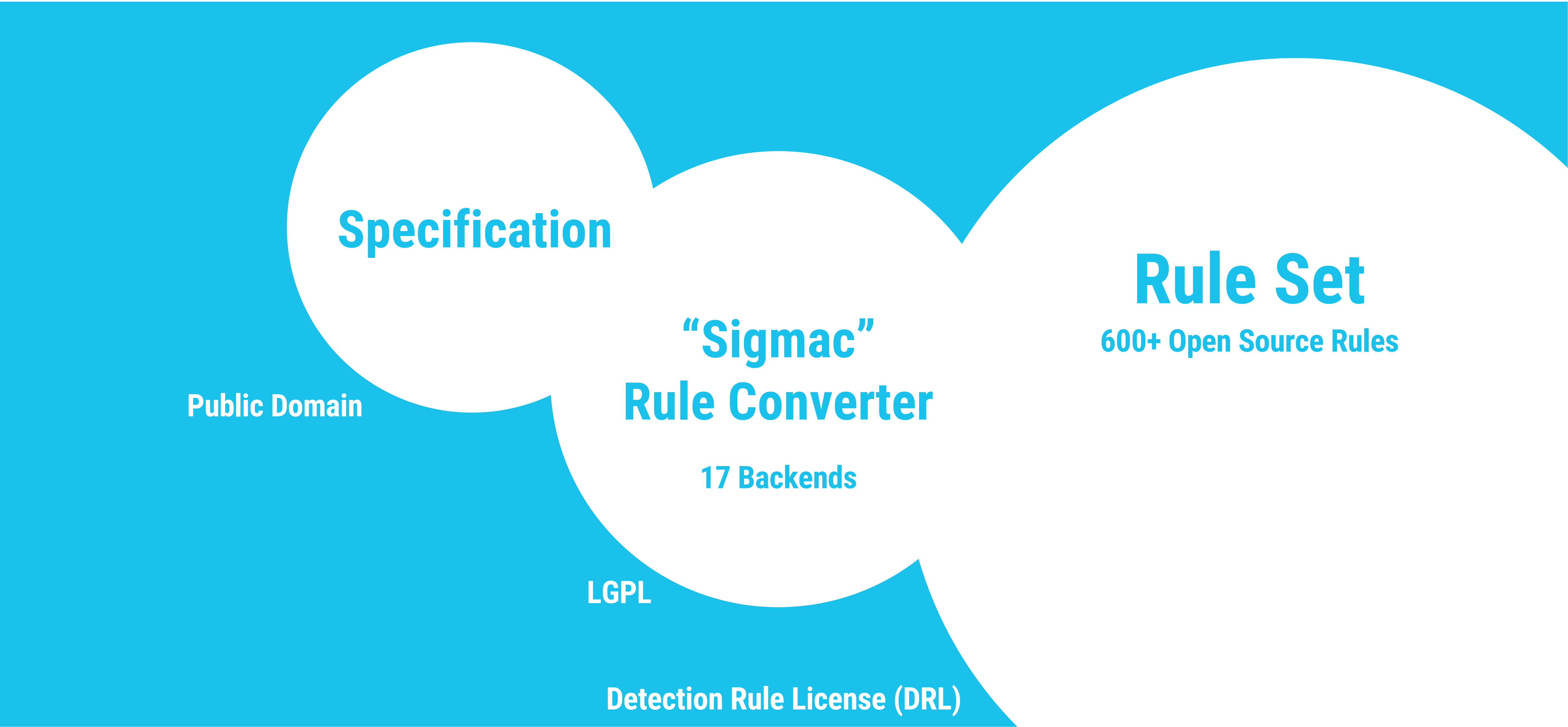
Win7 32 bit
Complete

Indicators:

```
2104  EXCEL.EXE /dde
      1k  1k  93
3280  powershell.exe -command IEX (new`-OB`jeCT('Net.WebClient'))....
      1k  266  206
```

https://app.any.run/tasks/b35cc0bc-1493-44bb-a1d8-49b68f92fade/

What does Sigma consist of?



Specification

Public Domain

“Sigmac”
Rule Converter

17 Backends

LGPL

Rule Set

600+ Open Source Rules

Detection Rule License (DRL)

Quote

Simplicity is the ultimate sophistication .

- Leonardo da Vinci

Why Sigma?

- Simplicity
  - Users like it: Easy to read and write
  - Developers like it: Manageable specs and expressions
- Immediate Benefit
  - Big rule base with more than 600 rules
  - Integrated converter for 17 backends (query generator)
- No Product-Specific Focus
  - No overreaching vendor
  - No SIEM specific expressions

Sigma - Quo Vadis?

- Adding Clarity
    - Better documentation
        - Which fields can I use?
        - How can I adjust it to my local field names?
        - How can I provide a new backend?
    - Improved test scripts
        - Why does my pull request fail?
        - Can I be sure that it doesn’t cause false positives?
- Ease of Integration
    - Rewrite Sigmac’s code base
    - Rule’s GPL license to Detection Rule License (DRL) 1.0
    - Convince more vendors for native support
- Gain Maturity
    - Automated rule testing
    - Releases, Roadmap, Web Page
    - Twitter account

sigma

Shades of Sigma

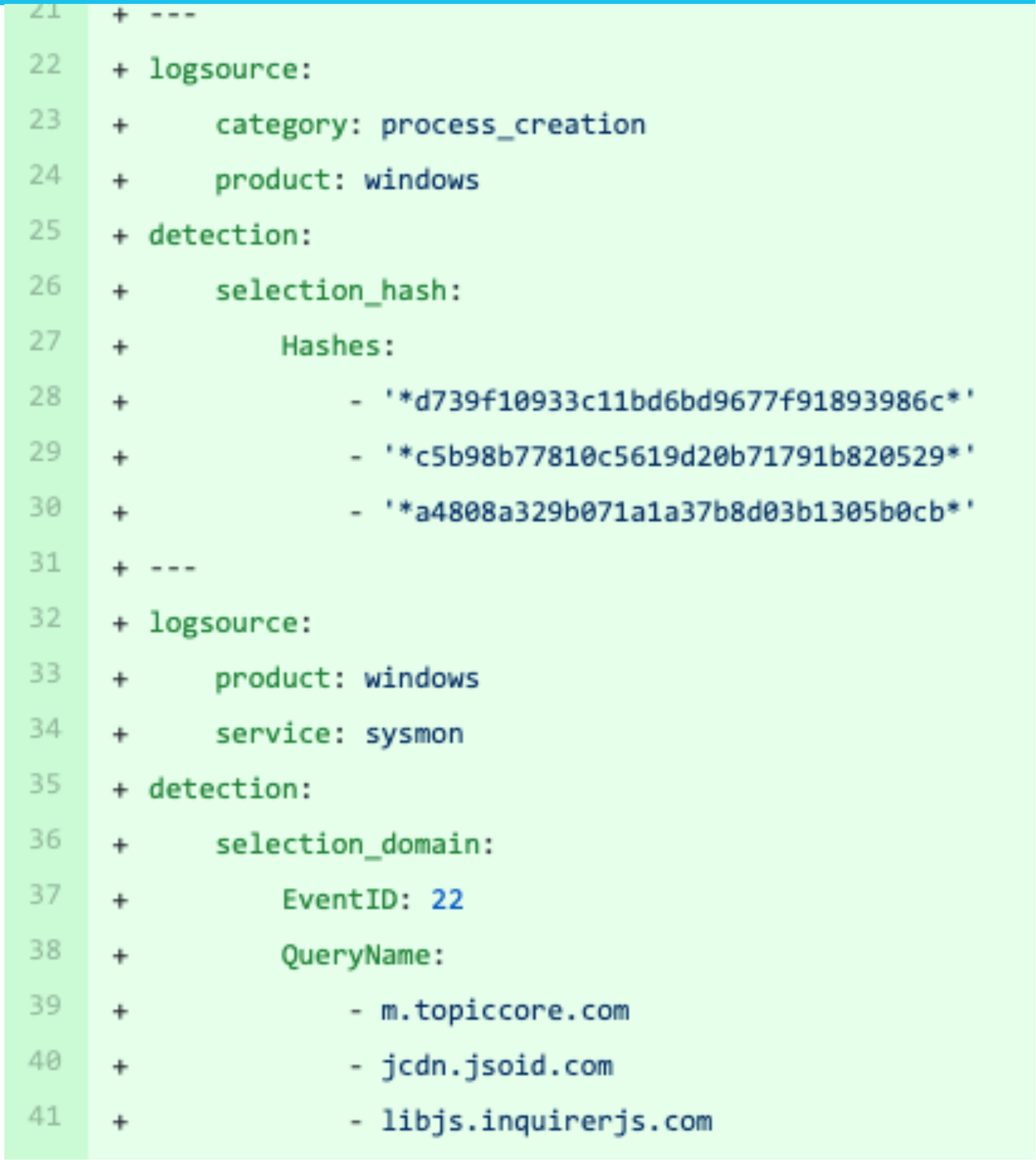
Ideas, Impulses, Use Cases

STIX to Sigma 1/2

- Sigma is designed to describe methods / techniques
- Users tend to include IOCs in Sigma rules
  - Why: Need to query IOCs
  - STIX and CSVs don't help > no native integration

- Project idea: STIX to Sigma converter

- as Web Tool
  - Like Google Translate or SOCPrime's uncoder.io
- as Library
  - to be used in MISP / OpenCTI / EclecticIQ



```
+ ---
+ logsource:
+     category: process_creation
+     product: windows
+ detection:
+     selection_hash:
+         Hashes:
+             - '*d739f10933c11bd6bd9677f91893986c*'
+             - '*c5b98b77810c5619d20b71791b820529*'
+             - '*a4808a329b071a1a37b8d03b1305b0cb*'
+ ---
+ logsource:
+     product: windows
+     service: sysmon
+ detection:
+     selection_domain:
+         EventID: 22
+         QueryName:
+             - m.topiccore.com
+             - jcdn.jsoid.com
+             - libjs.inquirerjs.com
```

STIX to Sigma

Here is a set of IOCs,

click on this button and

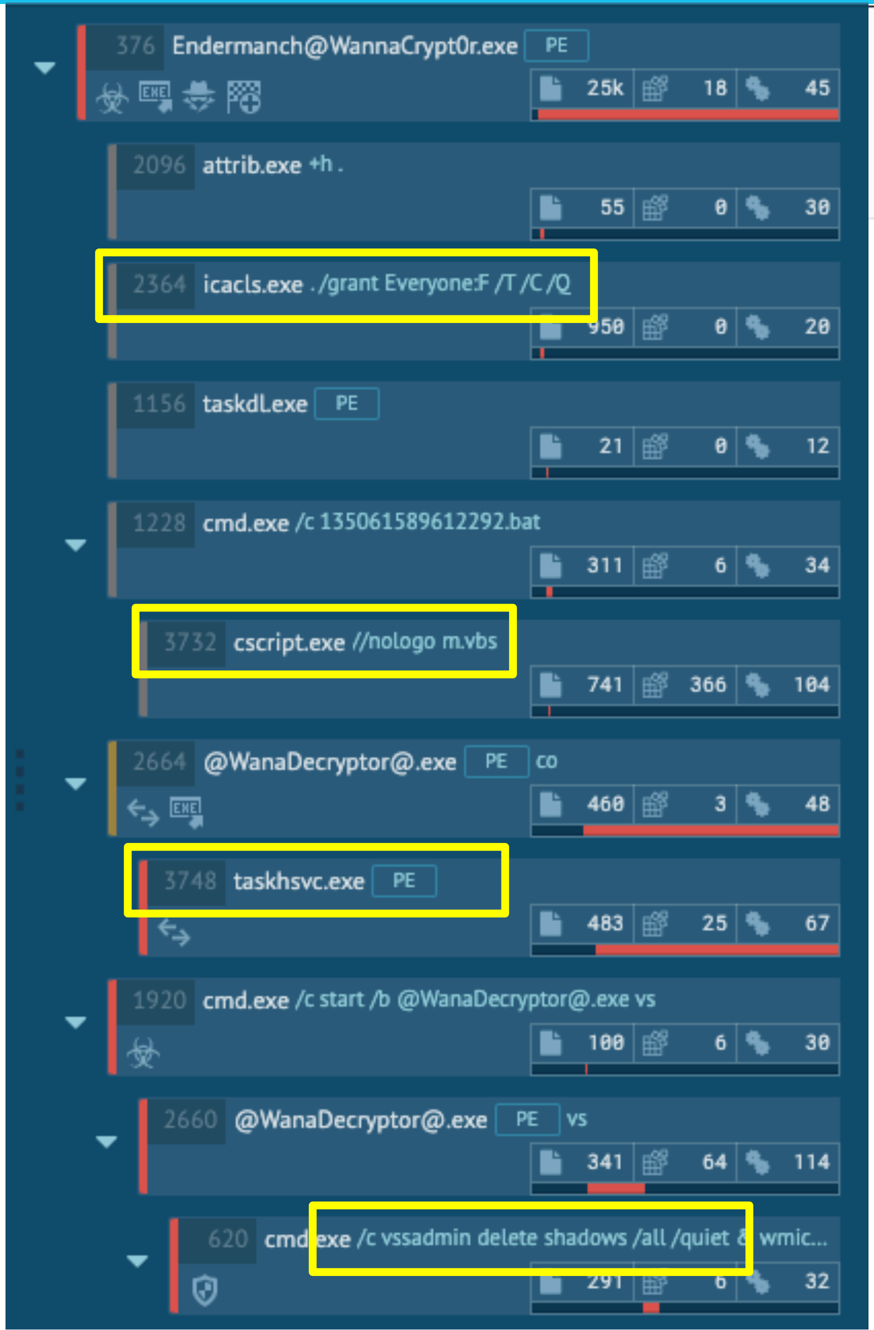
we open a new tab

with a SIEM query for these IOCs

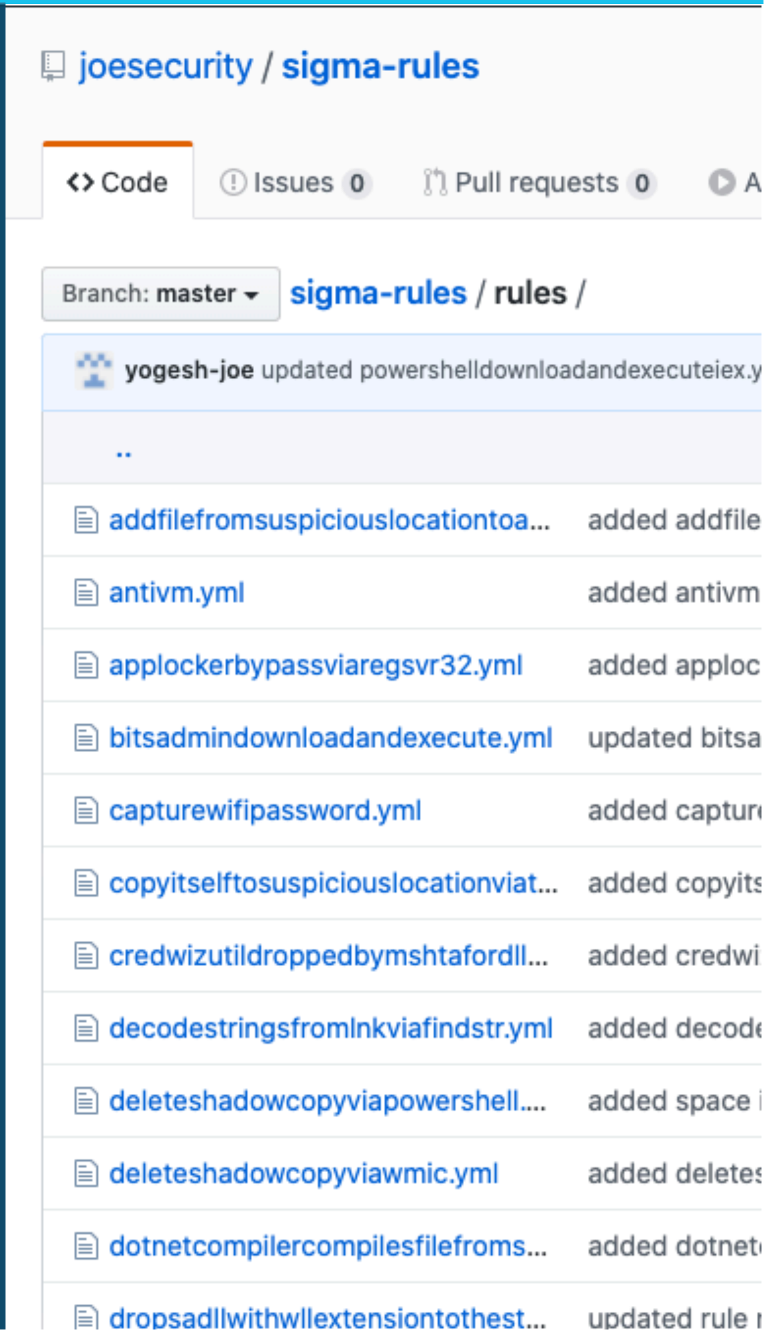
Sandbox Integrations 1/2

- Process command line, process tree, registry events, web request, file creation, …
- Apply Sigma rules to exported logs

- Stage 1: Show matches
- Stage 2: Allow searches using rule names
  - Show all samples with matching Sigma rule X
- Stage 3: Allow searches using custom(!) Sigma rules



```
376  Endermanch@WannaCrypt0r.exe  PE      25k   18   45
  2096  attrib.exe +h .                   55    0   30
  2364  icacls.exe ./grant Everyone:F /T /C /Q    950    0   20
  1156  taskdl.exe  PE                     21    0   12
  1228  cmd.exe /c 135061589612292.bat      311    6   34
    3732  cscript.exe //nologo m.vbs        741  366  104
  2664  @WanaDecryptor@.exe  PE  co         460    3   48
    3748  taskhsvc.exe  PE                  483   25   67
  1920  cmd.exe /c start /b @WanaDecryptor@.exe vs   100    6   30
    2660  @WanaDecryptor@.exe  PE  vs       341   64  114
      620  cmd.exe /c vssadmin delete shadows /all /quiet & wmic...   291    6   32
```



joesecurity / sigma-rules

Branch: master ▾ sigma-rules / rules /

yogesh-joe updated powershelldownloadandexecuteiex.y

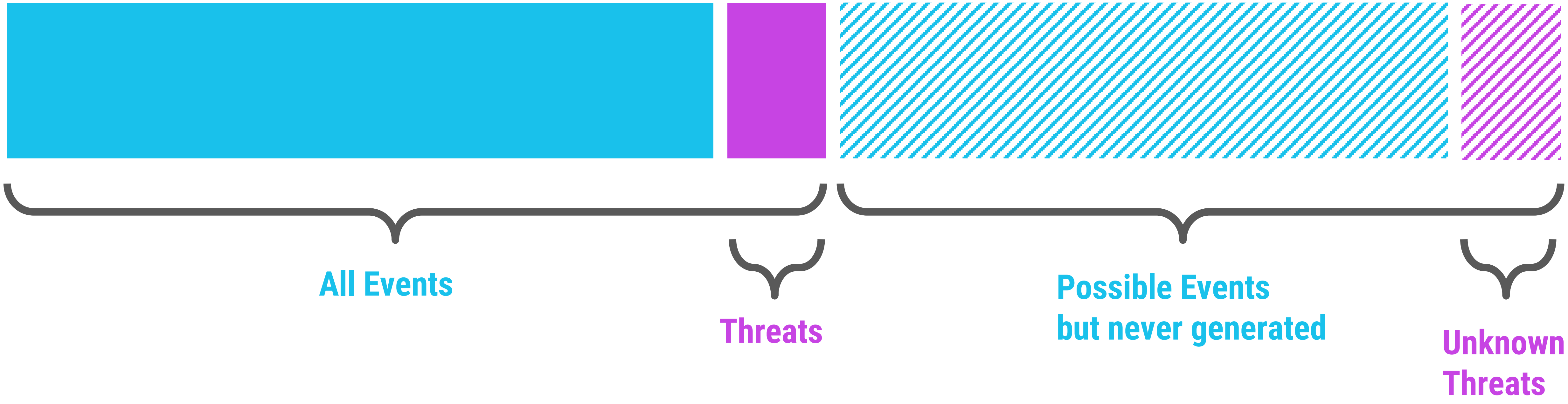
..

addfilefromsuspiciouslocationtoa...	added addfile
antivm.yml	added antivm
applockerbypassviaregsvr32.yml	added applοc
bitsadmindownloadandexecute.yml	updated bitsa
capturewifipassword.yml	added captur
copyitselftosuspiciouslocationviat...	added copyits
credwizutildroppedbymshtafordll...	added credwi
decodestringsfromlnkviafindstr.yml	added decode
deleteshadowcopyviapowershell....	added space
deleteshadowcopyviawmic.yml	added deletes
dotnetcompilercompilesfilefroms...	added dotnet
dropsadllwithwllextensiontothest...	updated rule

Sandbox Integrations

Here is your sandbox report,
this is a Sigma rule that triggered
and here are other samples triggering that rule
as well as a query for your SIEM.

Detect the Unexpected 1/3

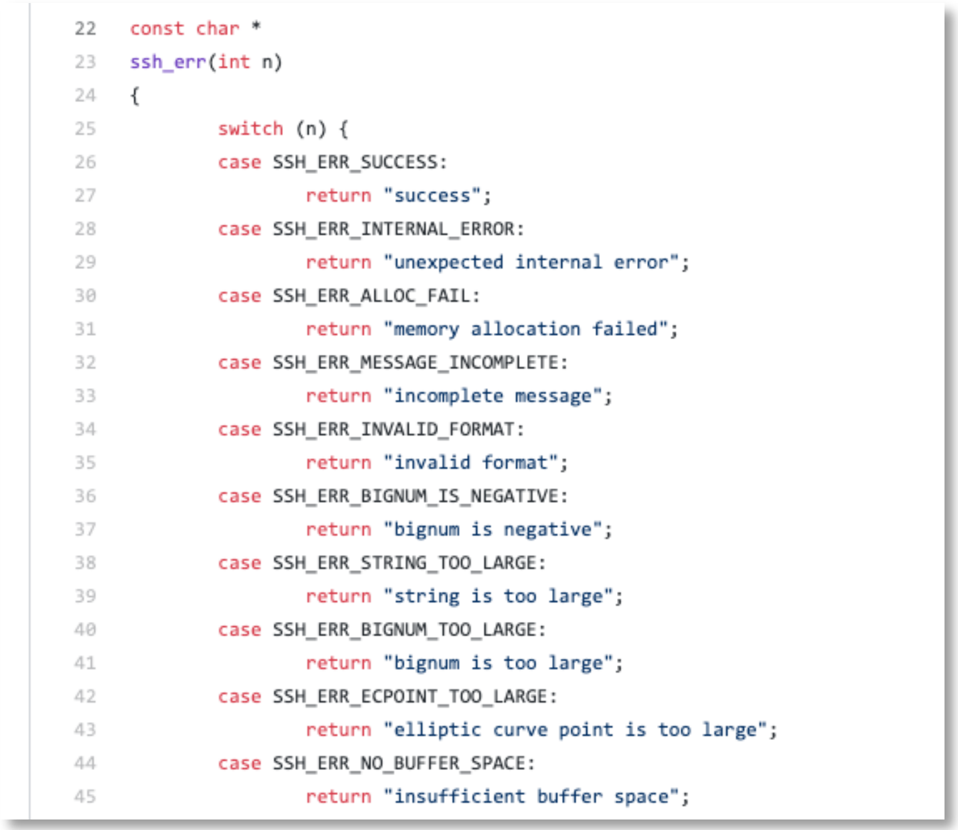


Analyst View

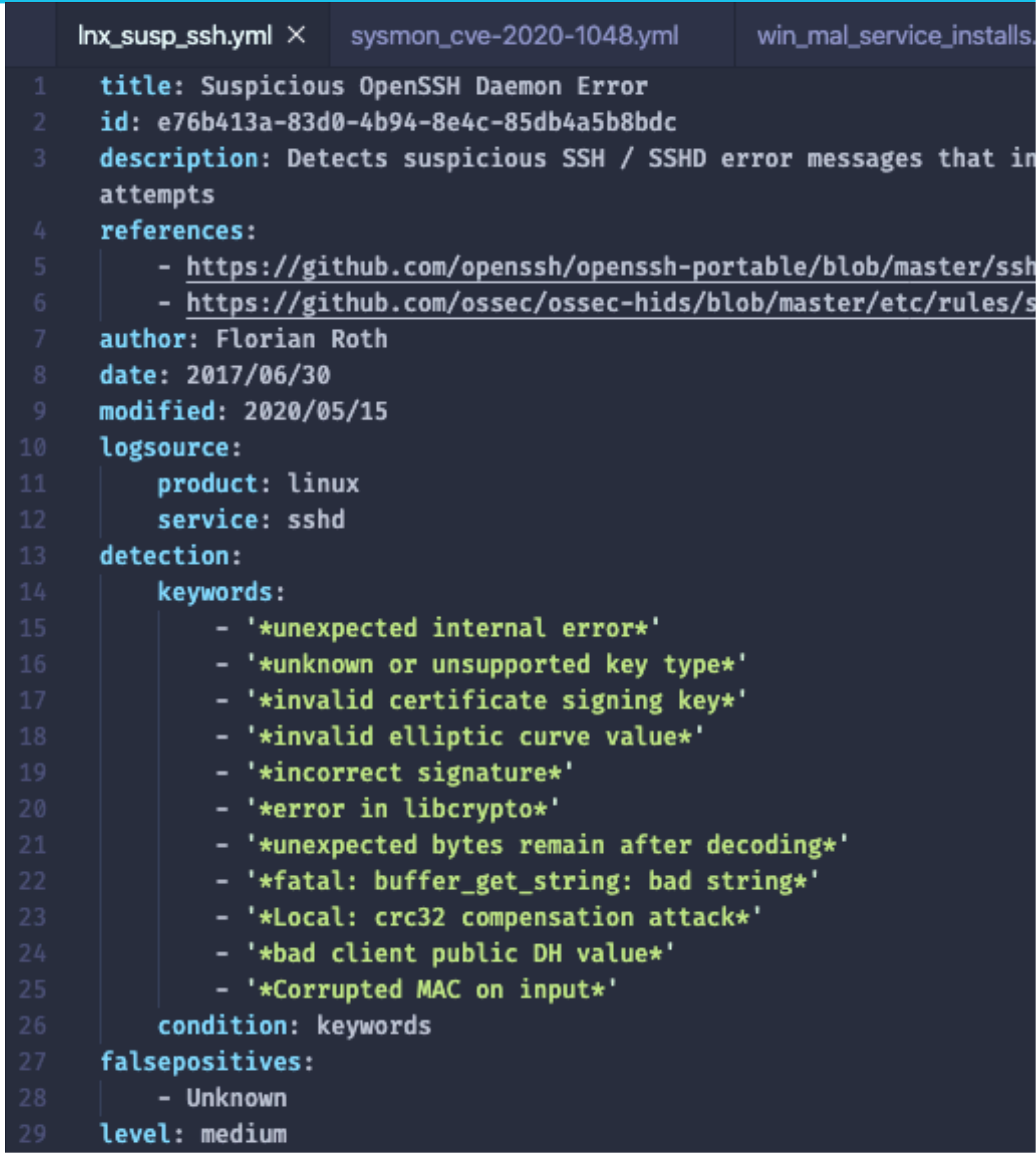
Developer View

Detect the Unexpected 2/3

- Exemplary rule 1: OpenSSH
- Exemplary rule 2: Django



```c
const char *
ssh_err(int n)
{
        switch (n) {
        case SSH_ERR_SUCCESS:
                return "success";
        case SSH_ERR_INTERNAL_ERROR:
                return "unexpected internal error";
        case SSH_ERR_ALLOC_FAIL:
                return "memory allocation failed";
        case SSH_ERR_MESSAGE_INCOMPLETE:
                return "incomplete message";
        case SSH_ERR_INVALID_FORMAT:
                return "invalid format";
        case SSH_ERR_BIGNUM_IS_NEGATIVE:
                return "bignum is negative";
        case SSH_ERR_STRING_TOO_LARGE:
                return "string is too large";
        case SSH_ERR_BIGNUM_TOO_LARGE:
                return "bignum is too large";
        case SSH_ERR_ECPOINT_TOO_LARGE:
                return "elliptic curve point is too large";
        case SSH_ERR_NO_BUFFER_SPACE:
                return "insufficient buffer space";
```



```yaml
title: Suspicious OpenSSH Daemon Error
id: e76b413a-83d0-4b94-8e4c-85db4a5b8bdc
description: Detects suspicious SSH / SSHD error messages that in
attempts
references:
    - https://github.com/openssh/openssh-portable/blob/master/ssh
    - https://github.com/ossec/ossec-hids/blob/master/etc/rules/s
author: Florian Roth
date: 2017/06/30
modified: 2020/05/15
logsource:
    product: linux
    service: sshd
detection:
    keywords:
        - '*unexpected internal error*'
        - '*unknown or unsupported key type*'
        - '*invalid certificate signing key*'
        - '*invalid elliptic curve value*'
        - '*incorrect signature*'
        - '*error in libcrypto*'
        - '*unexpected bytes remain after decoding*'
        - '*fatal: buffer_get_string: bad string*'
        - '*Local: crc32 compensation attack*'
        - '*bad client public DH value*'
        - '*Corrupted MAC on input*'
    condition: keywords
falsepositives:
    - Unknown
level: medium
```

Detect the Unexpected

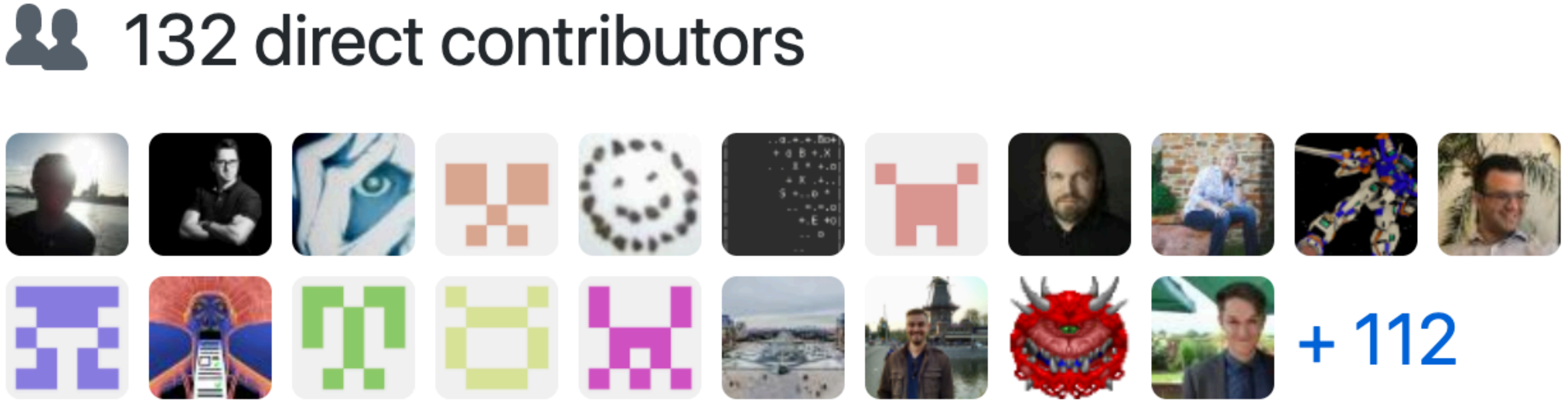
Here is our product,

and here is a set of Sigma rules

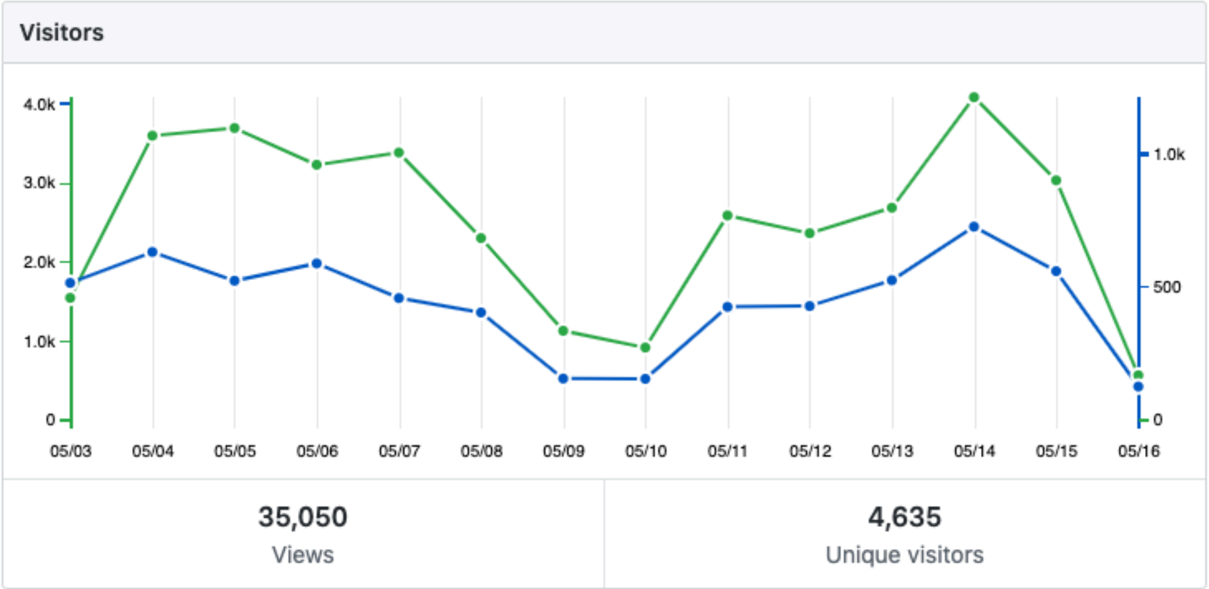
to detect events

that indicate dangerous conditions or threats.

Thanks to all contributors



132 direct contributors



Visitors

35,050
Views

4,635
Unique visitors

Rules: @cyb3rops me
Rule Converter: @blubbfiction Thomas Patzke
Twitter: @sigma_hq
Slack: siemexchange.slack.com (contact us for invites)
More information: https://github.com/Neo23x0/sigma