Sigma for Cloud With MITRE ATT&CK™?

by Andrii Bezverkhyi, SOC Prime

>_ whoami

Infosec since 2007

SOC Prime, Inc. since 2014

uncoder.io

https://github.com/socprime/SigmaUI

tdm.socprime.com

SOC PRIME
SECURITY QUALITY CONTROL

Tweet

Ihor Kravchuk
@ingvar_ua

Cloud is the place where everything is fast, API driven and has extremely good bandwidth. It takes only few minutes for an attacker to wipe out your infra or exfiltrate your data. If you not using autoremediation or near real time SOC for cloud security events - you doomed.

4:27 AM · Sep 9, 2019 · Twitter for iPhone

1 Retweet **3** Likes

Andrii Bezverkhyi @andriinb · Sep 9
Replying to @ingvar_ua
Agreed for 100%. Can I quote you in this?

1 1

Ihor Kravchuk @ingvar_ua · Sep 9
Sure!

SOC PRIME
SECURITY QUALITY CONTROL

Problems with cloud security monitoring

1. Cloud Logs are Veeeeery Reactive
2. MITRE ATT&CK is ~~Retrospective~~ Proactive for Cloud
3. In 2019 we mostly ~~talk~~ hunt on Sysmon

SOC PRIME
SECURITY QUALITY CONTROL

Cloud Logs are not real time

SOC PRIME
SECURITY QUALITY CONTROL

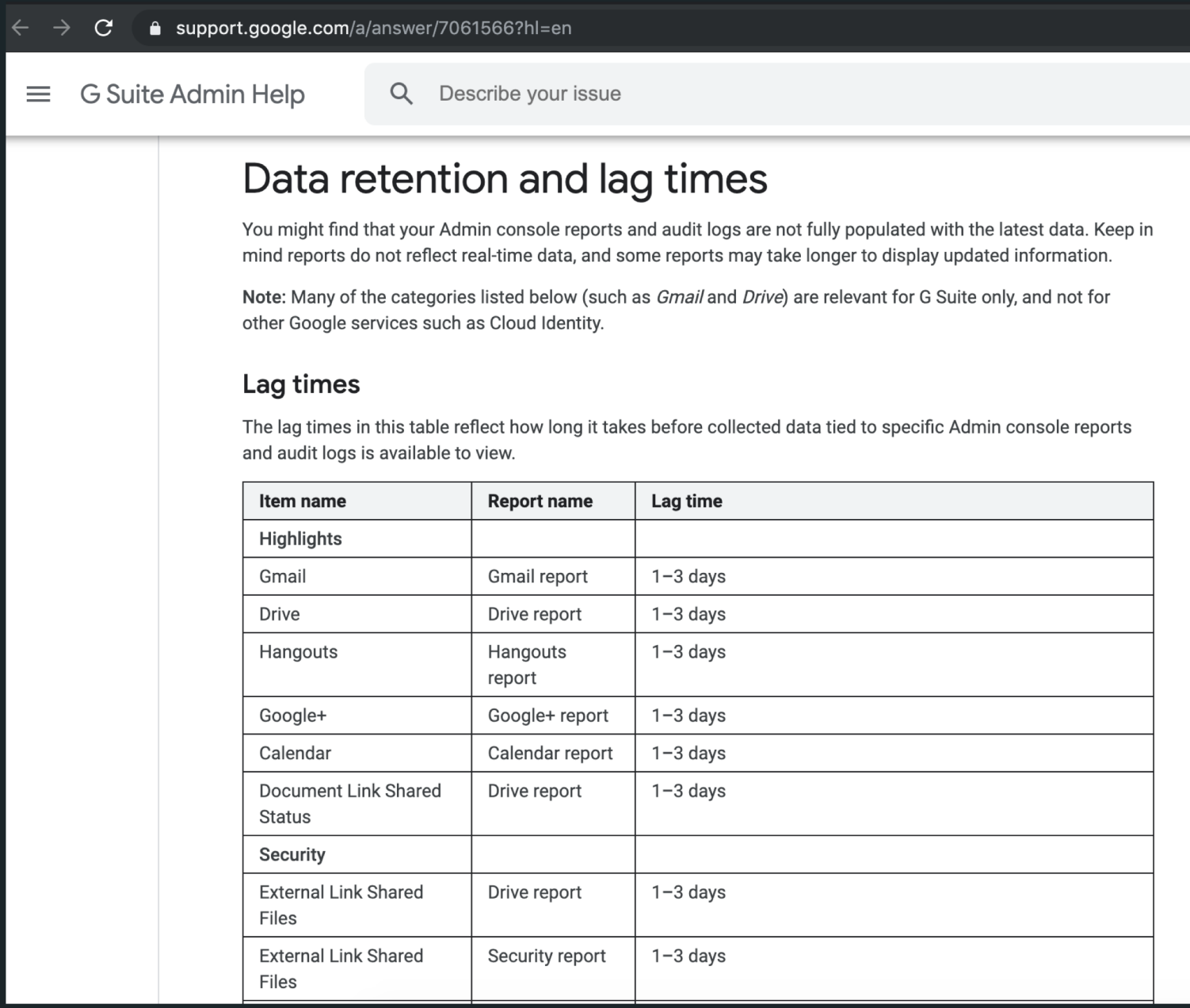
It can take up to 30 minutes or up to 24 hours after an event occurs for the corresponding audit log entry to be displayed in the search results. The following table shows the time it takes for the different services in Office 365.

Office 365 service	30 minutes	24 hours
Advanced Threat Protection and Threat Intelligence	✓	
Azure Active Directory (user login events)		✓
Azure Active Directory (admin events)		✓
Data Loss Prevention	✓	
Dynamics 365 CRM	✓	
eDiscovery	✓	
Exchange Online	✓	
Microsoft Flow	✓	
Microsoft Project	✓	
Microsoft Stream	✓	
Microsoft Teams	✓	
Power BI	✓	
Security & Compliance Center	✓	
SharePoint Online and OneDrive for Business	✓	

SOC PRIME
SECURITY QUALITY CONTROL

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance

https://support.google.com/a/answer/7061566?hl=en



Data retention and lag times

You might find that your Admin console reports and audit logs are not fully populated with the latest data. Keep in mind reports do not reflect real-time data, and some reports may take longer to display updated information.

Note: Many of the categories listed below (such as *Gmail* and *Drive*) are relevant for G Suite only, and not for other Google services such as Cloud Identity.

Lag times

The lag times in this table reflect how long it takes before collected data tied to specific Admin console reports and audit logs is available to view.

Item name	Report name	Lag time
Highlights		
Gmail	Gmail report	1–3 days
Drive	Drive report	1–3 days
Hangouts	Hangouts report	1–3 days
Google+	Google+ report	1–3 days
Calendar	Calendar report	1–3 days
Document Link Shared Status	Drive report	1–3 days
Security		
External Link Shared Files	Drive report	1–3 days
External Link Shared Files	Security report	1–3 days

SOC PRIME
SECURITY QUALITY CONTROL

ATT&CK for Cloud
Suggestions not from CTI

SOC PRIME
SECURITY QUALITY CONTROL

Technique: **Calendar Event Injection**
Tactic**: Initial Access**
There is a possibility for an attacker to create an important event in the Calendar (social engineering) and send invitation to target. The message may contain a phishing link or a malware link.
Ref: https://usa.kaspersky.com/blog/spam-through-google-services/17799/

Technique: **Publicly Shared Calendar**
Tactic: **Exfiltration**
There is a possibility to 'create an event' when replying to email from O365, Outlook or GSUITE. Such reply can leak up to 8000 bytes of email data. Text in reply is not logged. By using T1074/Data Staged attacker can prepare any number of events and exfiltrate them all by sharing Calendar Link or making it public. Remember delay of 24+ hours.
Ref: soon at SOC Prime blog

Adam [redacted]

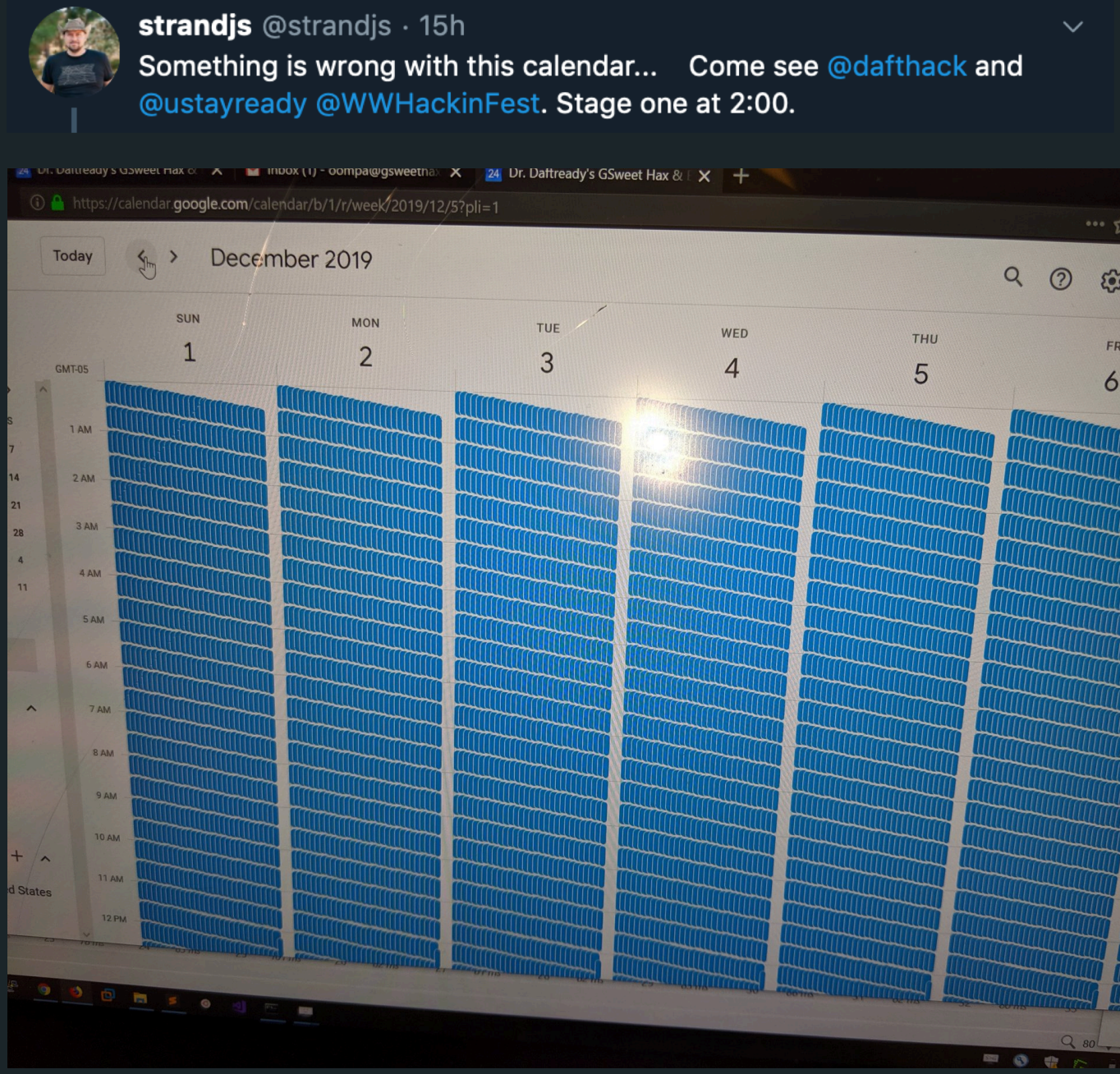
Looking forward to it!

On Mon, Oct 21, 2019 at 12:48 PM Adam Swan <[redacted]@gmail.com> wrote:
>
> Perfect! See you then.
>
> On Mon, Oct 21, 2019 at 12:48 PM Adam Swan <[redacted]@socprime.com> wrote:
>>
>> Cool. I can meet at 12pm EST on 10/23/2019 for lunch at Chipotle in Silver Spring
>>
>> On Mon, Oct 21, 2019 at 12:47 PM Adam Swan <[redacted]@gmail.com> wrote:
>>>
>>> Noon? Let's get it on our calendars!
>>>
>>>
>>>
>>> On Mon, Oct 21, 2019 at 12:46 PM Adam Swan <[redacted]@socprime.com> wrote:
>>>>
>>>> What time works for you?
>>>>
>>>> -Swan
>>>>
>>>> On Mon, Oct 21, 2019 at 12:45 PM Adam Swan <[redacted]@gmail.com> wrote:
>>>>>
>>>>> Sure!
>>>>>
>>>>> On Mon, ...

10 minutes before

Adam [redacted]

Going? Yes No Maybe


strandjs @strandjs · 15h
Something is wrong with this calendar... Come see @dafthack and @ustayready @WWHackinFest. Stage one at 2:00.
Dr. Daftready's GSweet Hax &
https://calendar.google.com/calendar/b/1/r/week/2019/12/5?pli=1
Today
December 2019
Week
SUN 1
MON 2
TUE 3
WED 4
THU 5
FRI 6
GMT-05
1 AM
2 AM
3 AM
4 AM
5 AM
6 AM
7 AM
8 AM
9 AM
10 AM
11 AM
12 PM

Technique: **Publicly Shared Calendar**
Tactic: **Exfiltration**
There is a possibility to ‘create an event’ when replying to email from O365, Outlook or GSUITE. Such reply can leak up to 8000 bytes of email data. Text in reply is not logged. By using T1074/Data Staged attacker can prepare any number of events and exfiltrate them all by sharing Calendar Link or making it public. Remember delay of 24+ hours.

ID: T1537
Tactic: Exfiltration
Platform: Azure, AWS, GCP
Permissions Required: User
Data Sources: Stackdriver logs, Azure activity logs, AWS CloudTrail logs, O365 Logs, GSUITE logs
Requires Network: Yes
Contributors: Praetorian, SOC PRIME ? ☺
Version: 1.0

Transfer Data to Cloud Account
An adversary may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.

SOC PRIME
SECURITY QUALITY CONTROL

SUBMISSION TO MITRE ATT&CK: IN PROGRESS

Sigma for Cloud MFA Bypass

SOC PRIME
SECURITY QUALITY CONTROL

action: global

title: Multi-factor authentication (2-step verification) disabled.

description: Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. The presence of an event leads to a mismatch with control. Recommended one day event search period. Sigma covers G Suite, AWS Console, Slack log sources.

references:
- https://www.cisecurity.org/controls/cis-controls-list/
- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
- https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- https://gdpr-info.eu/art-32-gdpr/
- https://developers.google.com/admin-sdk/reports/v1/appendix/activity/user-accounts
- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-aws-console-sign-in-events.html
- https://api.slack.com/docs/audit-logs-api

author: Alexandr Yampolskyi

status: stable
modified: 2019/08/15
detection:
  condition: selection
falsepositives:
- unknown

level: medium
tags:
- GDPR Art 32.1
- GDPR Art 32.2
- CSC16
- CSC16.3
- ISO 27002-2013 A.9.1.1
- NIST CSF 1.1 PR.AC-1
- PCI DSS 3.2 7.1
- attack.T1089
- attack.defense_evasion
- Attack.T1078
- Attack.initial_access

---

logsource:
  product: G Suite
detection:
  selection:
    events.name: 2sv_disable

---

logsource:
  product: AWS Console
detection:
  selection:

additionalEventData.MFAUsed: "No"

---

logsource:
  product: Slack
detection:
  selection:
    event.name: pref.two_factor_auth_changed
    Details: "")

MITRE ATT&CK
Sigma
Community
Marketplace

SOC PRIME
SECURITY QUALITY CONTROL

Threat Bounty

SOC PRIME
SECURITY QUALITY CONTROL

#threatbounty

Top | Latest | People | Photos | Videos

Andrii Bezverkhyi @andriinb · Oct 17

#threatbounty stats for September 2019 @SOC_Prime Threat Detection Marketplace:
minimum content threshold to get payout = 1 rule
average payout per developer per month = $510 (up from $400 in August)

You can do it!
my.socprime.com/tdm-developers/

14 33

Andrii Bezverkhyi @andriinb · Oct 4

#threatbounty payouts stats for August 2019 at @SOC_Prime Threat Detection Marketplace:
minimum content threshold to get payout = 1 rule
average payout per developer per month = $400

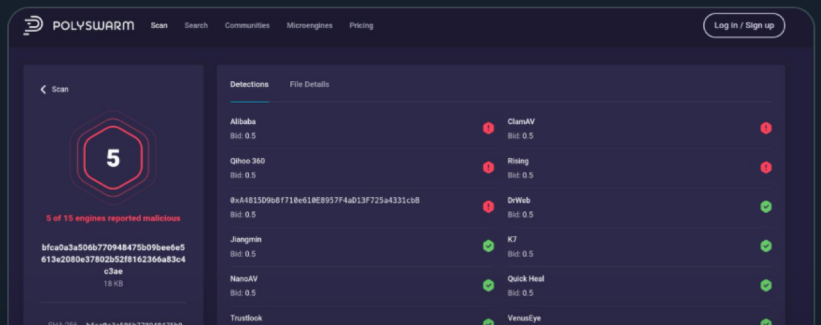
learn #sigma, earn money while you sleep
details at my.socprime.com/en/tdm-develop...

1 5 17

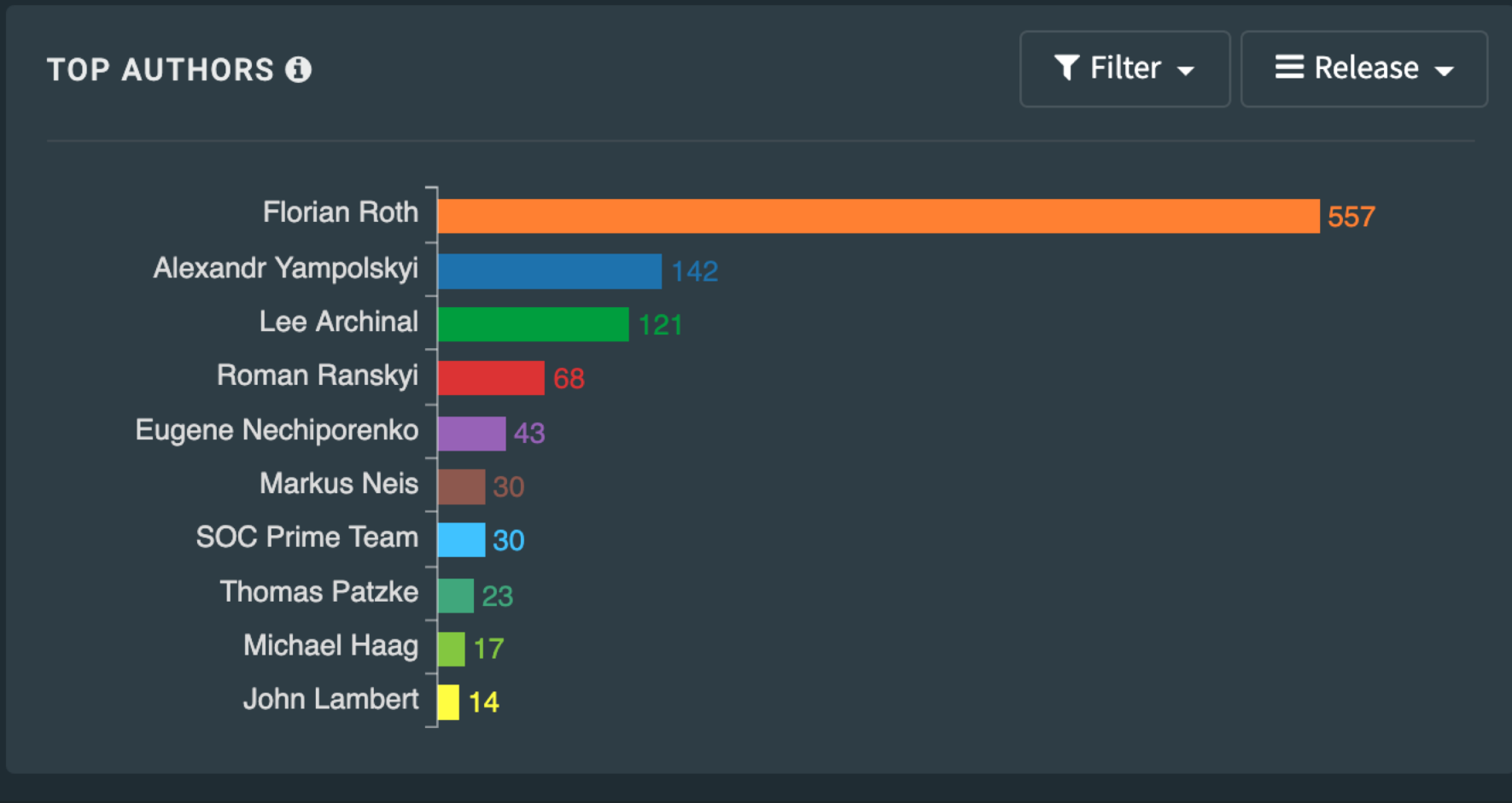
Show this thread

PolySwarm @PolySwarm · Oct 2

Looking for free analysis of #malware samples & URLs? Try PolySwarm: polyswarm.network where AV companies & #cybersecurity experts' scanning engines compete & are rewarded when right (#ThreatBounty bit.ly/threatbounty #VirusTotal alternative #infosec #threatintel #SoC

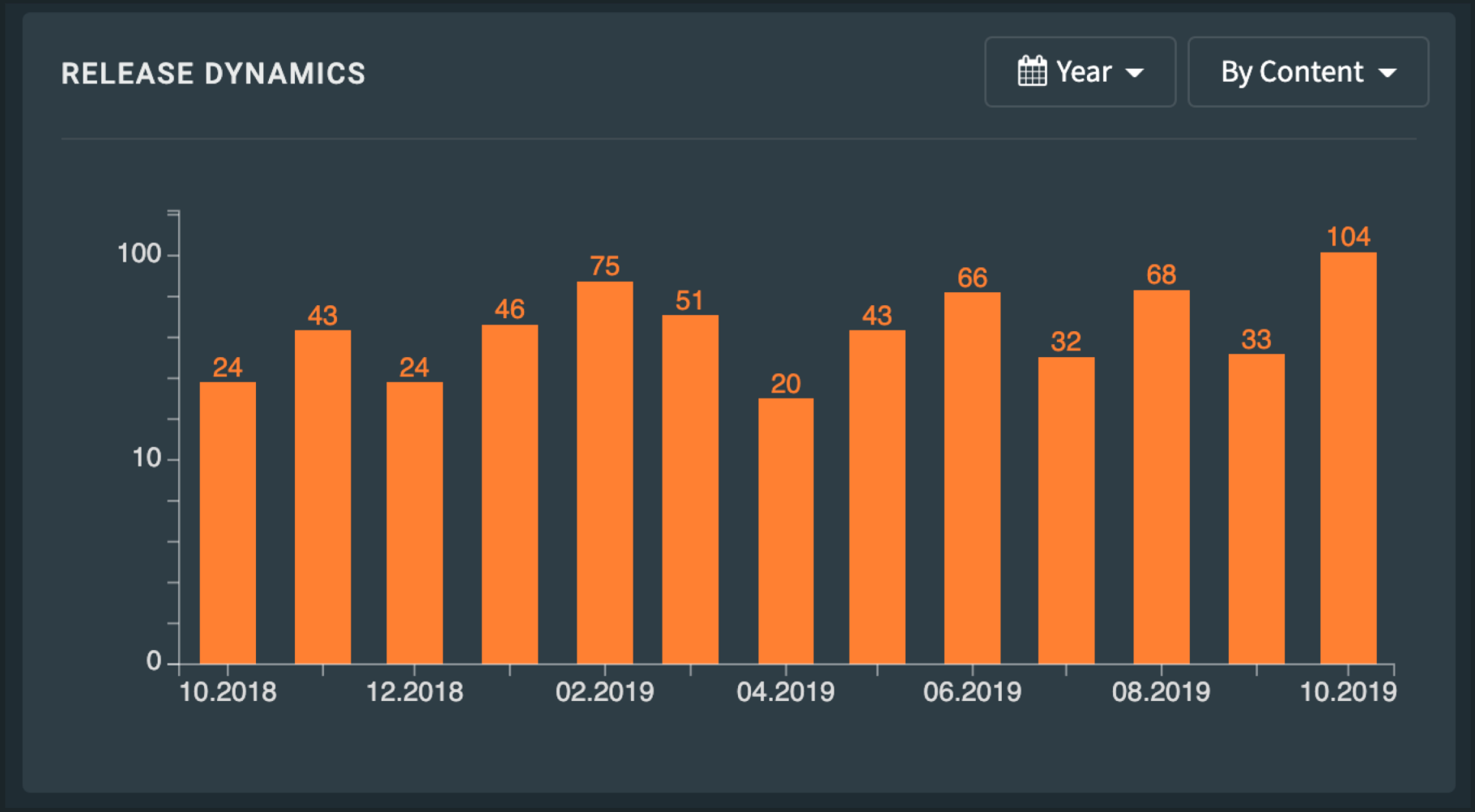


88 threat bounty hunters signed up since May 2019, some are on list



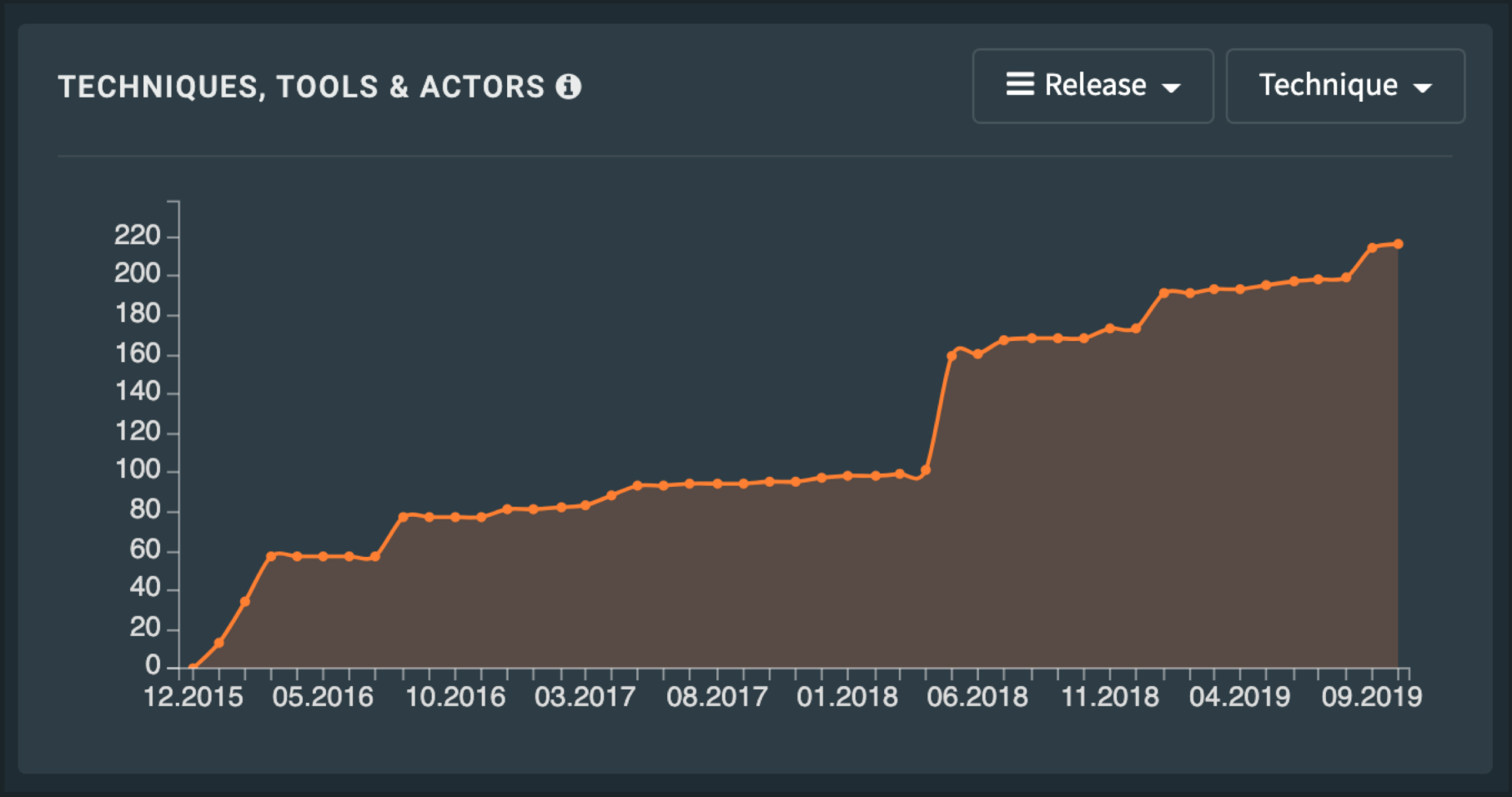
Source: leaderboards, threat detection marketplace

Unique detections per month



Source: leaderboards, threat detection marketplace

216 techniques coverage
811 sigma rules
33232 translations and native rules



Source: leaderboards, threat detection marketplace

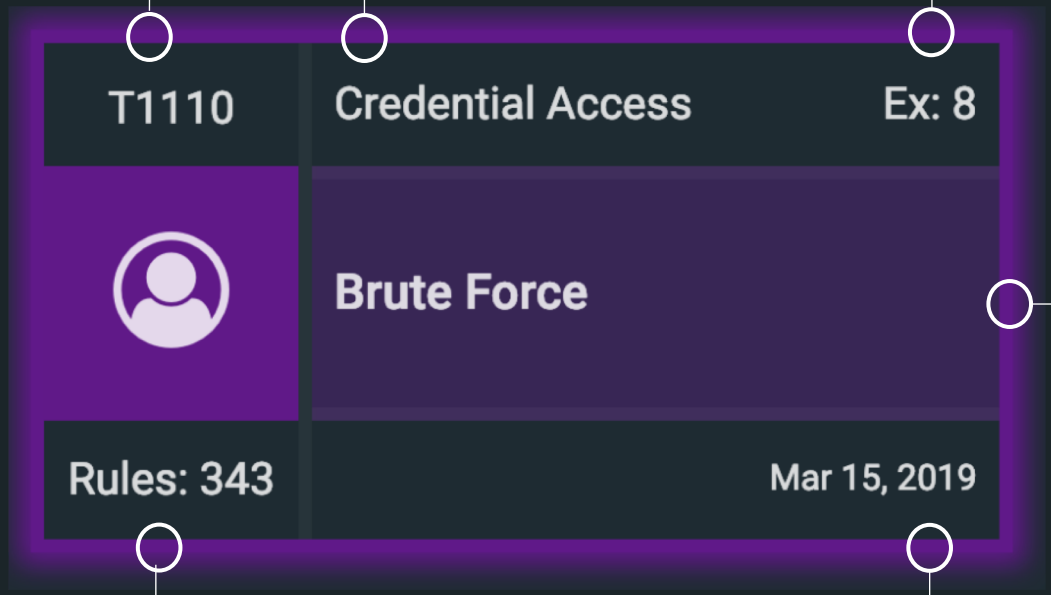
Periodic Table
Of Cyber Elements

SOC PRIME
SECURITY QUALITY CONTROL

Technique ID

Tactic
Adversary's tactical objective: the reason for performing an action.

Examples count
Number of the known Procedures, the exact ways an adversary or software implements a technique.



Technique
Techniques represent "how" an adversary achieves a tactical objective by performing an action.

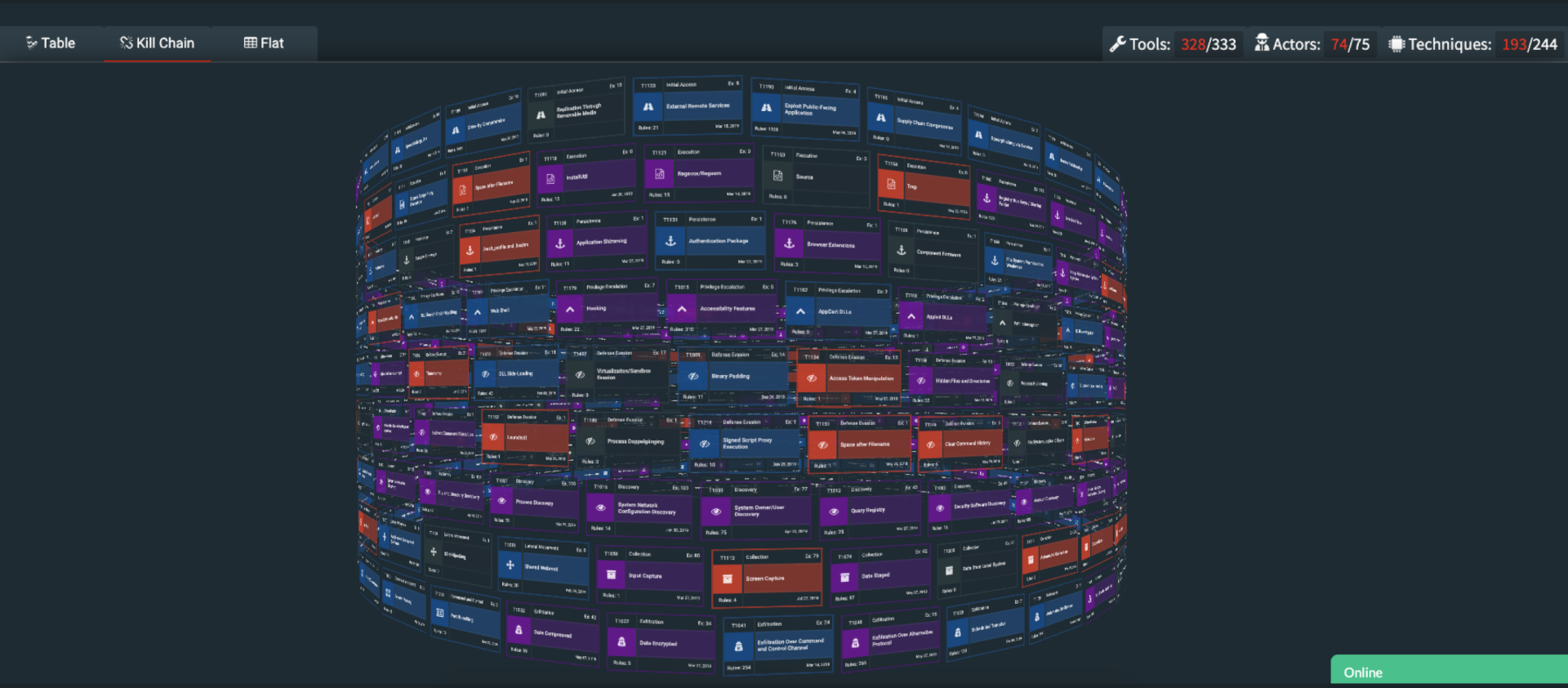
Rules count
Rules used for threat hunting, detection and testing of specific technique. Incudes Sigma, Yara, Snort, SIEM rules & Attack simulation tests.

Last update Date

SOC PRIME
SECURITY QUALITY CONTROL

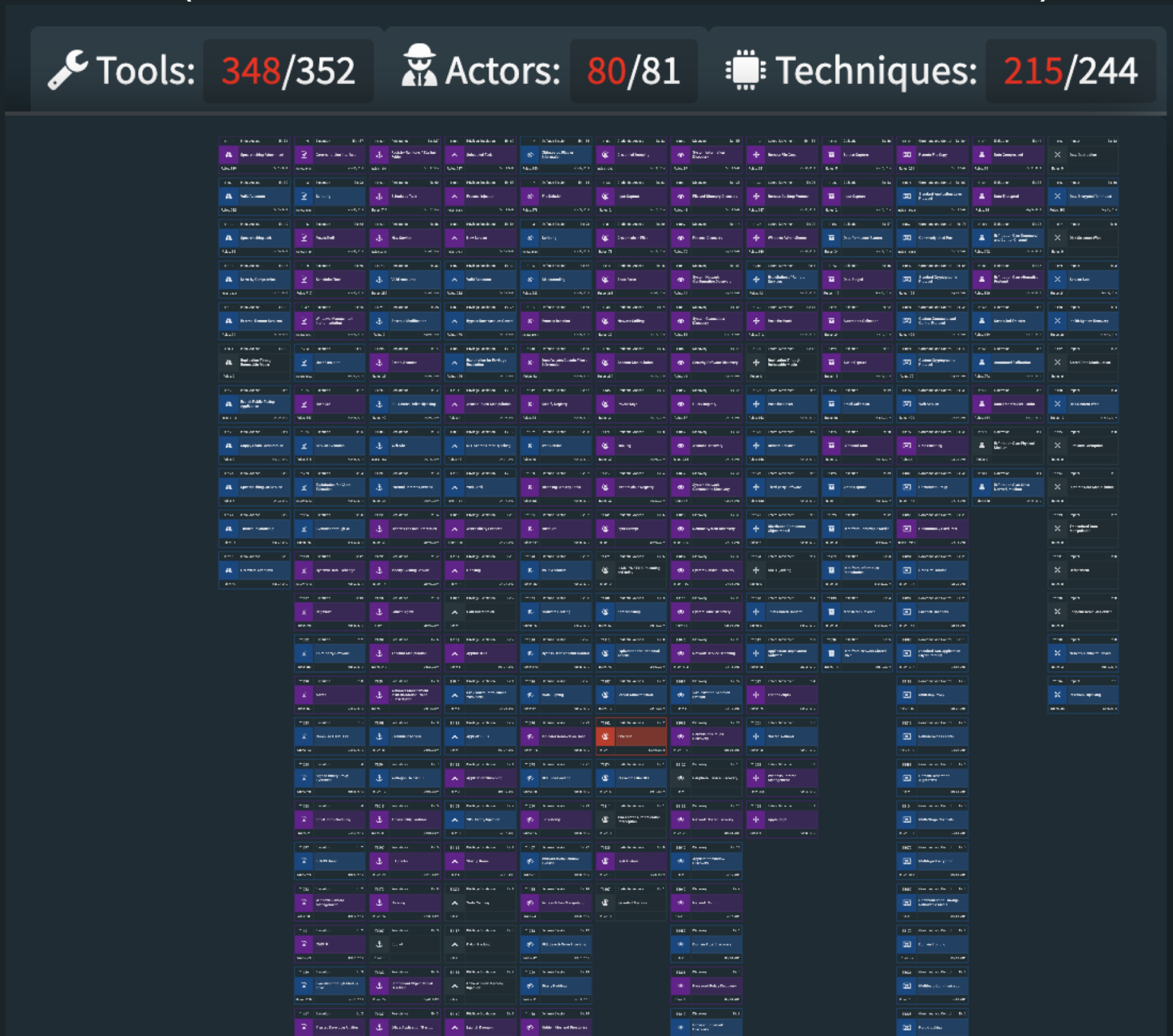
ATT&CK knowledge base: attack.mitre.org

Coverage May 2019 (EU ATT&CK COMMUNITY BRUSSELS)



SOC PRIME
SECURITY QUALITY CONTROL

Coverage OCT 2019 (EU ATT&CK COMMUNITY HACK.LU)

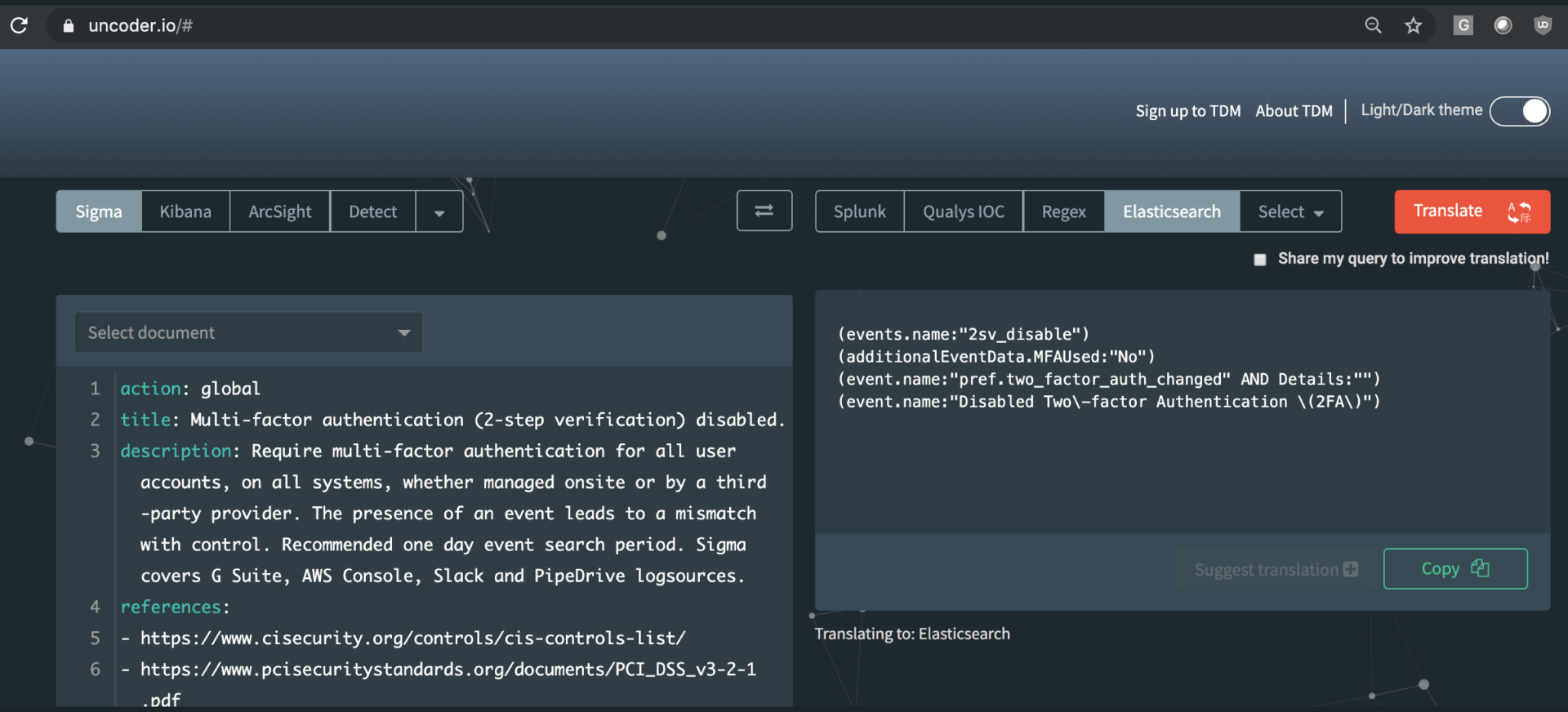


SOC PRIME
SECURITY QUALITY CONTROL

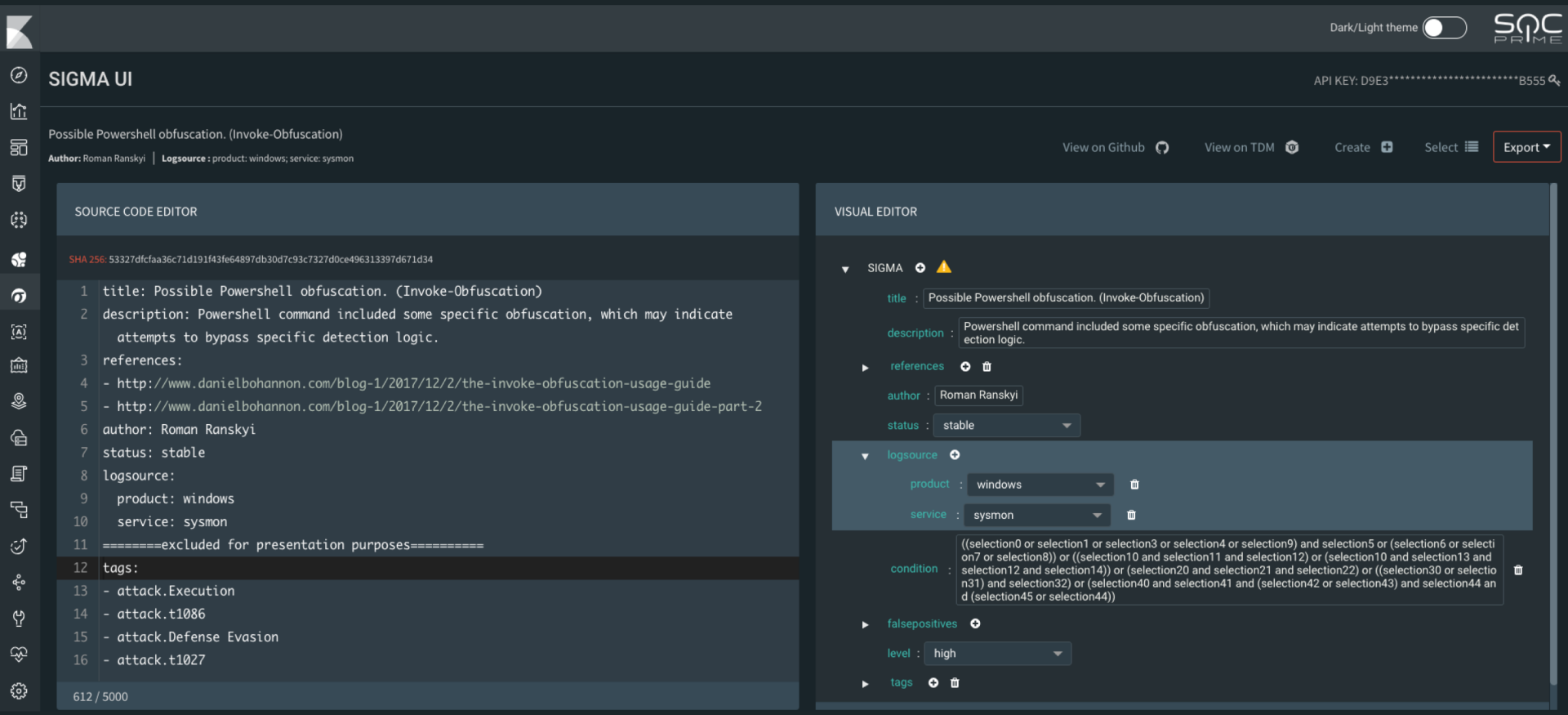
Threat Bounty needs You!

my.socprime.com/en/tdm-developers

SOC PRIME
SECURITY QUALITY CONTROL



https://uncoder.io



https://github.com/socprime/SigmaUI