



# The Magic of Cross-Platform Threat Detection



**Till Jäger**  
SOC Prime



Co-presented by:  
**Vini Engel**



- Security Professional at heart > 25 years in the field
- Living in the land of SIEM & Threat Detection (CA, ArcSight, HP, RiskIQ, Exabeam, SOC Prime)
- SOC Prime full-time since 2020
- CISSP since 2004
- Proud to be M.A.D. certified



# What?



The Challenge



SIGMA to the Rescue - The Revolution



Roota to Complement - The Evolution



Supporting OSS initiatives

# Cross-Platform? - Detection Engineers' Nightmare!

The abundance of security toolkits poses challenges for Detection Engineers, hindering collaboration & information exchange among experts who speak different query languages.



Microsoft  
Sentinel

Kusto



elastic

KQL, EQL, DSL,  
ESQL, Lucene



Radar®

AQL

splunk>

SPL



Chronicle

UDM



CROWDSTRIKE

LQL



Amazon Athena

SQL

LQL, VQL

Sharing? -> Difficult



ROOTA



SIGMA



## SIGMA

# 12,000+

SIGMA rules

- Invented in 2016, SIGMA has become the most popular cross-platform Detection Engineering language
- Used to describe any adversary TTP and translate it to any detection code
- Has revolutionized Threat Detection
- Designed to be the common denominator across all SIEM solutions
- Good for crafting atomic detections, still limited for more complex use cases
- Simple by design and relatively easy to learn due to its limited capabilities

## From the Detection Engineer's point of view:

- **Great for a top-down sharing approach but limited for bottom-up or peer-to-peer sharing**
  - DEs know their Platform and prefer the direct route, SIGMA challenging them as a new language to learn
  - DEs quickly adopt SIEM-specific functions for aggregation & correlation, which is limited or not supported in SIGMA
- **Perfect for threat research**
  - META language easily aligns with a hypothesis and allows modelling a META detection
  - But the Detection Engineer is focused on his platform
- **Single log source approach (changing in Sigma 2.0)**
  - Limited cross-device correlation
  - No functions support

## From the Backend Developer's point of view:

- Switch from Sigmac to pySigma has increased complexity
- More Backends are needed to increase the platform coverage





<https://roota.io>

<https://github.com/UncoderIO/RootA>

## ■ What?

- Open-source language for Detection & Response
- Not here to replace SIGMA but to **complement**

## ■ Why? - Accelerate Community Collaboration

- Very simple to learn, no dedicated QL
- Automated translation & reverse translation -> Easier to share
- DE can develop and share code in his preferred language
- Simplified architecture, hence easier to integrate

**Accelerate Threat Informed Defense!**

## Extensive Native Metadata

- MITRE ATT&CK at core
- Threat Actor Timeline & TI information
- Required log sources, service, audit information and instructions

## Flexibility

- Open Container format (Can potentially support “any” query language):

The “Splunk Detection Engineer” can easily share code with the “Sentinel Detection Engineer”!

- Native correlation & aggregation function mapping
- OCSF taxonomy support

## Beyond Detection

- Open for “Response as Code” in the future

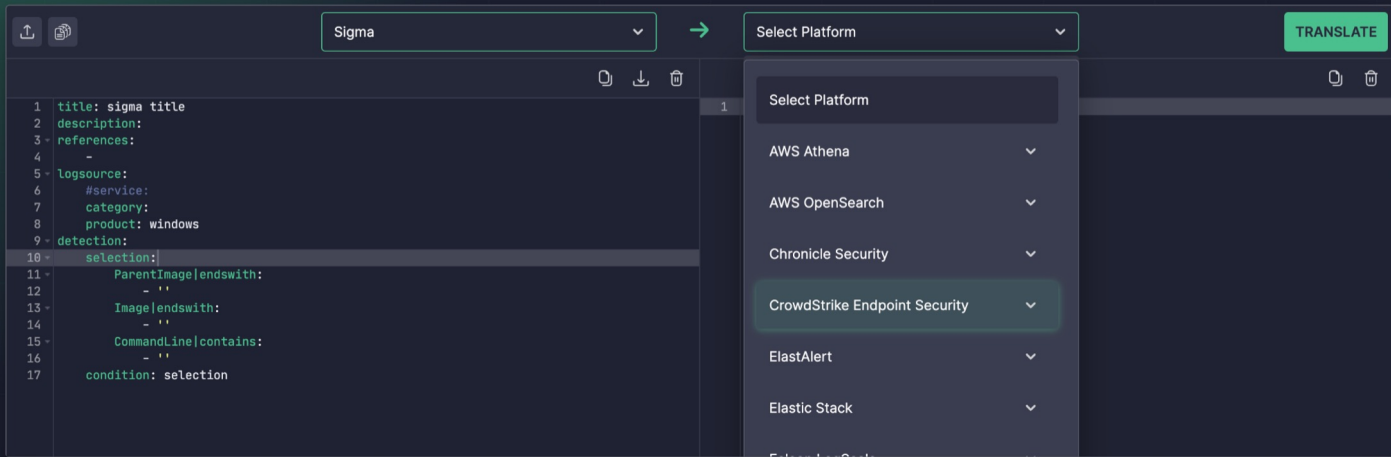


# Supporting OSS initiatives - Uncoder IO

**UNCODER.IO**

powered by SOC Prime, Inc.

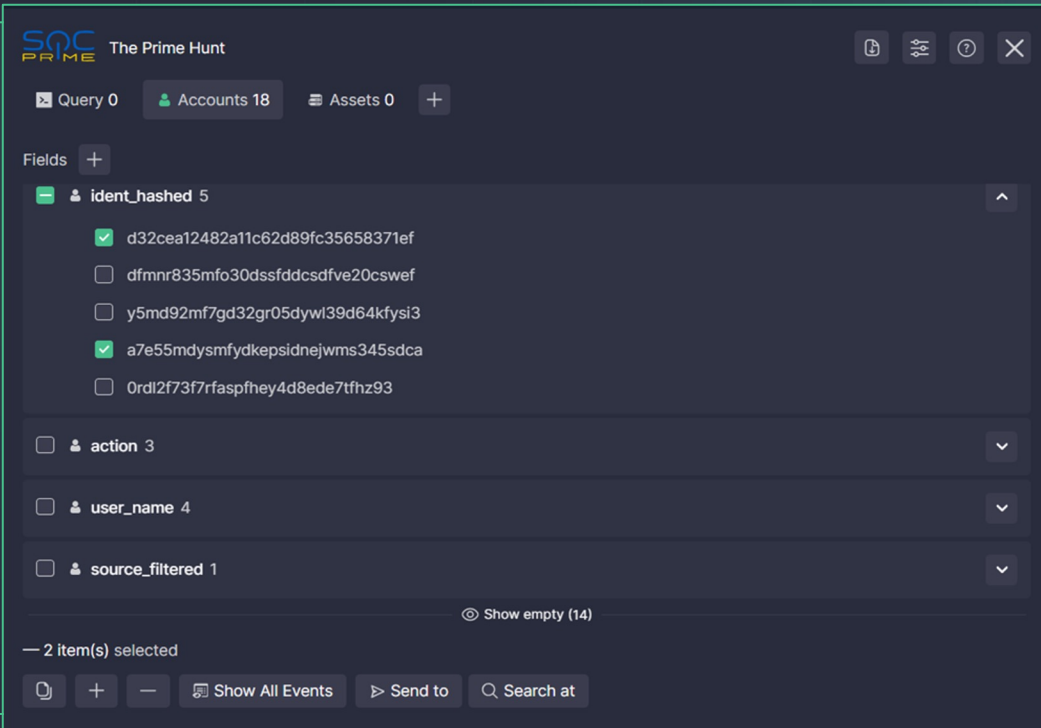
An IDE and translation engine for detection engineers and threat hunters. Be faster, write smarter, keep 100% privacy.



- An open-source IDE for Detection Engineers and Threat Hunters
- Fast, private, and easy-to-use online translation engine for Roota & SIGMA rules into specific SIEM, EDR, and Data Lake languages
- An open-source IOC packager from any non-binary format (PDF, text, STIX, or OpenIOC) to specific SIEM, EDR, and Data Lake languages
- Maintains 100% privacy of its users

<https://uncoder.io/> | [https://github.com/UncoderIO/Uncoder\\_IO](https://github.com/UncoderIO/Uncoder_IO)

- An open-source browser extension for threat hunting that provides one UI for different SIEMs/EDRs and simplifies investigation
- Detection sharing of native queries through Roota will be built-in
- Supports Chrome / Firefox / Edge
- Supported security platforms: MS Sentinel, MS Defender, Splunk, QRadar, Elastic (Kibana), ArcSight, Amazon Athena, Amazon OpenSearch, Falcon LogScale, Chronicle Security
- Supports multiple data schemas, including OCSF, CEF, ECS, LEEF, CIM, OSSEM



The screenshot displays the 'The Prime Hunt' browser extension interface. At the top, the title bar shows 'The Prime Hunt' with standard window controls. Below the title bar, a navigation bar includes 'Query 0', 'Accounts 18', 'Assets 0', and a '+' button. The main content area is titled 'Fields' and lists several fields with checkboxes and counts:

- ☒ **ident\_hashed** 5
  - ☒ d32cea12482a11c62d89fc35658371ef
  - ☐ dfmnr835mfo30dssfdcdsdfve20cswef
  - ☐ y5md92mf7gd32gr05dywl39d64kfysi3
  - ☒ a7e55mdysmfydkepsidnejwms345sdca
  - ☐ 0rdl2f73f7rfaspfhey4d8ede7tfhz93
- ☐ **action** 3
- ☐ **user\_name** 4
- ☐ **source\_filtered** 1

At the bottom of the field list, there is a link to 'Show empty (14)'. Below the field list, a status bar indicates '2 item(s) selected'. At the very bottom, there is a toolbar with buttons for 'Show All Events', 'Send to', and 'Search at'.

<https://github.com/socprime/the-prime-hunt>



Where does the name Roota come from?

**Hint:** explore the logo!

## Червона рута / chervona ruta -> red rue

Inspired by a Ukraine legend about a red rue symbolizing search and love. Since the cybersecurity industry has a lot of the former and somewhat lacking in the latter, we genuinely believe that the mission of Roota is to change that for the better by **driving collective cyber defense together**.



# ROOTA



# Thank you!

<https://github.com/UncoderIO/RootA>

<https://my.socprime.com/sigma/>

<https://github.com/socprime/the-prime-hunt>