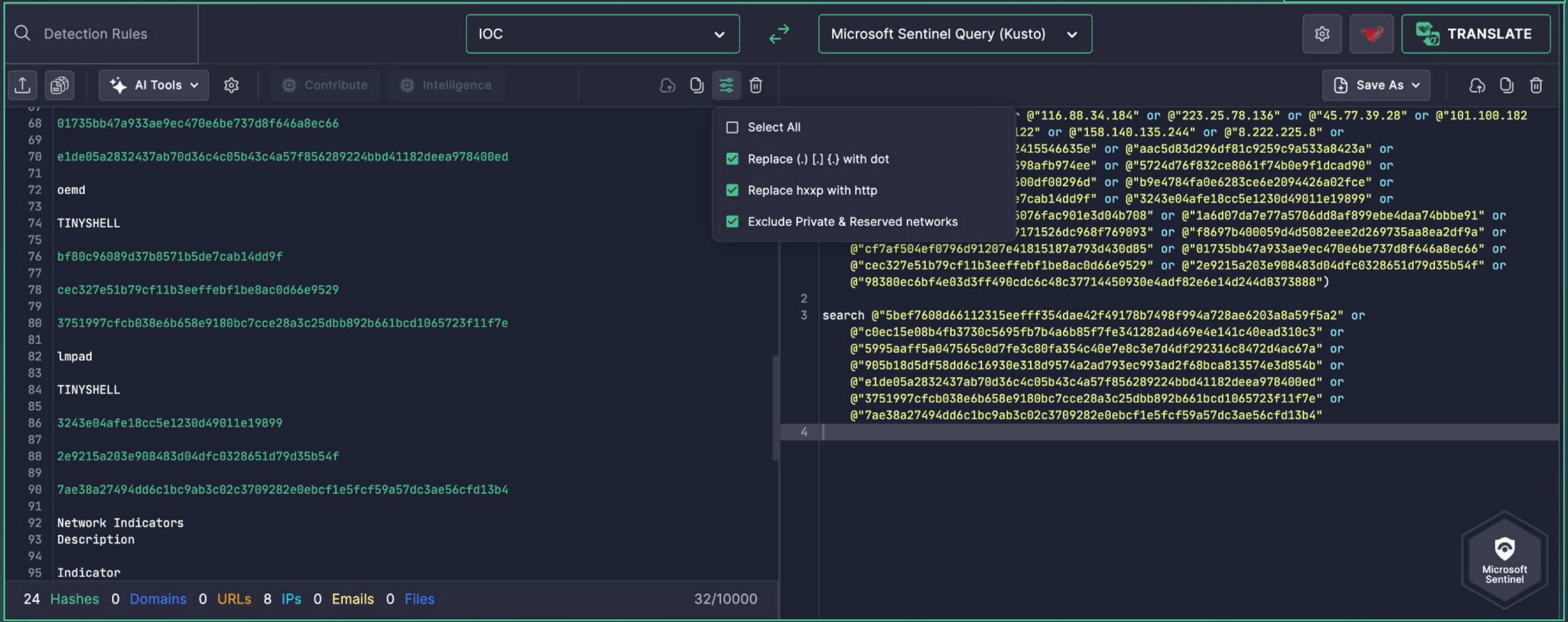
Generating IOC Queries from Threat Reports

Uncoder AI

Generating IOC Queries from Threat Reports

In production



```
01735bb47a933ae9ec470e6be737d8f646a8ec66

e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd41182deea978400ed

oemd

TINYSHELL

bf80c96089d37b8571b5de7cab14dd9f

cec327e51b79cf11b3eeffebf1be8ac0d66e9529

3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd1065723f11f7e

lmpad

TINYSHELL

3243e04afe18cc5e1230d49011e19899

2e9215a203e908483d04dfc0328651d79d35b54f

7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc3ae56cfd13b4

Network Indicators
Description

Indicator
```

24 Hashes 0 Domains 0 URLs 8 IPs 0 Emails 0 Files 32/10000

☐ Select All

☑ Replace (.) [.] {.} with dot

☑ Replace hxxp with http

☑ Exclude Private & Reserved networks

```
 @"116.88.34.184" or @"223.25.78.136" or @"45.77.39.28" or @"101.100.182
122" or @"158.140.135.244" or @"8.222.225.8" or
2415546635e" or @"aac5d83d296df81c9259c9a533a8423a" or
598afb974ee" or @"5724d76f832ce8061f74b0e9f1dcad90" or
500df00296d" or @"b9e4784fa0e6283ce6e2094426a02fce" or
e7cab14dd9f" or @"3243e04afe18cc5e1230d49011e19899" or
5076fac901e3d04b708" or @"1a6d07da7e77a5706dd8af899ebe4daa74bbbe91" or
9171526dc968f769093" or @"f8697b400059d4d5082eee2d269735aa8ea2df9a" or
    @"cf7af504ef0796d91207e41815187a793d430d85" or @"01735bb47a933ae9ec470e6be737d8f646a8ec66" or
    @"cec327e51b79cf11b3eeffebf1be8ac0d66e9529" or @"2e9215a203e908483d04dfc0328651d79d35b54f" or
    @"98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14d244d8373888")

search @"5bef7608d66112315eefff354dae42f49178b7498f994a728ae6203a8a59f5a2" or
    @"c0ec15e08b4fb3730c5695fb7b4a6b85f7fe341282ad469e4e141c40ead310c3" or
    @"5995aaff5a047565c0d7fe3c80fa354c40e7e8c3e7d4df292316c8472d4ac67a" or
    @"905b18d5df58dd6c16930e318d9574a2ad793ec993ad2f68bca813574e3d854b" or
    @"e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd41182deea978400ed" or
    @"3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd1065723f11f7e" or
    @"7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc3ae56cfd13b4"

```

Generating IOC Queries from Threat Reports

Operationalize Threat Intelligence by extracting Indicators of Compromise (IOCs) and applying them in practice to support threat hunting process and complement behavior-based detections. Uncoder AI natively parses IOCs from text and packs them into queries.

- Multiple languages supported
- Data doesn't leave SOC Prime's infrastructure
- Configurable settings including custom field mapping
- Automates a repetitive, error-prone task—manual extraction and query crafting—accelerating time-to-search post-threat intel ingestion
- Empowers Tier 1 and Tier 2 analysts to act on threat reports without deep knowledge of query languages across SIEMs
- Ensures consistent parsing and syntactically correct query generation, reducing false negatives due to human error or misinterpretation

Generating IOC Queries from Threat Reports

20 languages supported in production

- ArcSight
- OpenSearch
- Elastic Stack
- CrowdStrike Falcon LogScale
- CROWDSTRIKE
- FIREEYE
- graylog
- LOGPOINT
- Qualys
- Google Security Operations
- RSA NETWITNESS
- securonix
- QRadar
- Microsoft Defender for Endpoint
- Microsoft Sentinel
- SentinelOne
- snowflake
- splunk>
- sumo logic
- Carbon Black.

11 new languages added on April 16

- AWS Athena
- ANOMALI
- APACHE kafka
- DATADOG
- DEVO
- DNIF
- HUNTERS
- Sigma
- SQL
- SQLite
- STIX