

Threat Detection Marketplace

Stay ahead of cyber-security threats with the fastest cross-platform threat detection content built by incident responders for CISOs, SOC Managers and Analysts

8 Platforms

Supported for Integration and Enrichment with Attack and Threat Intelligence including Elastic stack, ArcSight, QRadar, Qualys, Splunk and Anomali ThreatStream

The #1 cross-platform SOC app store

Threat Detection Marketplace connects the dots for 3000+ rules and queries, MITRE ATT&CK, Threat Intelligence, Log Sources and Machine Learning

2000+ Organizations

Use Threat Detection Marketplace for SOC content & Sigma rules extended by IOC's from Anomali ThreatStream and mapped directly to MITRE ATT&CK

Detect 94+ Attacker Techniques

Available via API integration to stream the threat detection content which covers over 94 techniques based on MITRE ATT&CK.

Our content will help you to address the following use cases



Building and evolving Security Operation Centers



Real-time Threat Detection



Establishing Threat Hunting operations

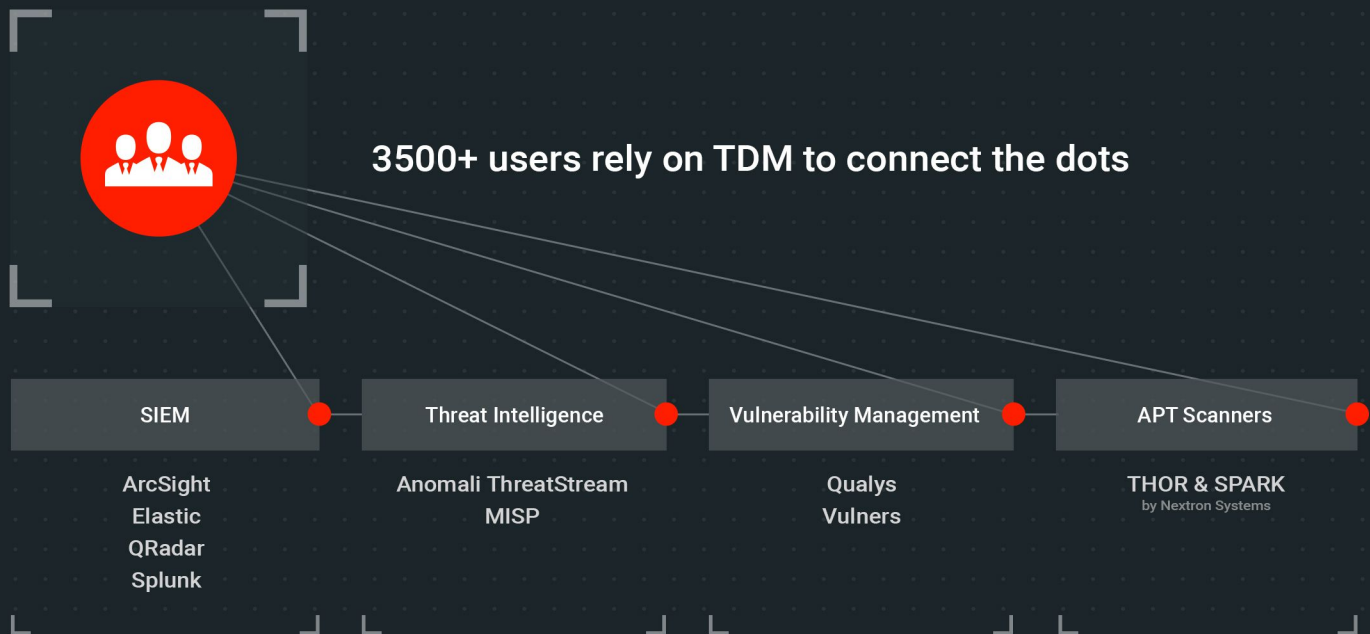


Digital and Cloud security monitoring

Evolving set of tools built by and for Blue teams



- Sigma rules and UI
- Data enrichers
- SOC and IR playbooks
- Parsers and configs
- Purpose-built Dashboards & Reports



One common language for cyber security

Sigma
Kibana
ArcSight
Detect

Splunk
Qualys IOC
Regex
Elasticsearch
Choose

Translate

VPNFilter Malware Detector (Hashes).

```

1 title: VPNFilter Malware Detector (Hashes).
2 description: VPNFilter Malware Hashes Detector.
3 references:
4 - https://blog.talosintelligence.com/2018/05/VPNFilter.html
5 author: Alexandr Yampolskiy, SOC Prime
6 status: testing
7 logsource:
8   product: windows
9   service: sysmon
10 detection:
11   selection:
12     | EventID: "1"
13     | file_hash:
14       - 50ac4fcd3fbc8abca766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
15       - 0e0094d9bd396a6594d8e21911a3982cd737b445f991581560d766759097d92
16       - 9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17
17       - d6097e942dd0fd1fb28ec1814780e6ecc169ec6d24f9954e7195aeebdc4c70e
18       - 4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b
19       - 9eb6c779dbad1b717caa462d8e048852759436ed79cc2172692339bc62432387
20       - 37e29b0ea7e9b97597385a12f525e13c0a7d02ba4161a6946f2a7d978cc045b4

```

[EventID:"1" AND file_hash: ("50ac4fcd3fbc8abca766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec" "0e0094d9bd396a6594d8e21911a3982cd737b445f991581560d766759097d92" "9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17" "d6097e942dd0fd1fb28ec1814780e6ecc169ec6d24f9954e7195aeebdc4c70e" "4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b" "9eb6c779dbad1b717caa462d8e048852759436ed79cc2172692339bc62432387" "37e29b0ea7e9b97597385a12f525e13c0a7d02ba4161a6946f2a7d978cc045b4" "0649fda8888d781eb2f91e6e0a5a2e2be714f564497c44a3813882ef8ff250b" "f8286e29f9a67ec765ae0244862f6b7914fc0de10423f96595cb84ad5cc6b344" "afd281639e26a717aead65b1886f98d6d6c25873601602304e590e3007348719"))]

Suggest translation

Copy

Translating to: Elasticsearch

A single search engine for the interlinked cyber data

- Actors, Techniques, Tactics from MITRE ATT&CK
- Vulnerability intelligence from Qualys and NIST
- Indicators of Compromise from MISP and Anomali
- Security incidents history archive handpicked from 300+ news outlets
- 500+ data sources and thousands of log event codes