SOC PRIME
SECURITY QUALITY CONTROL

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.

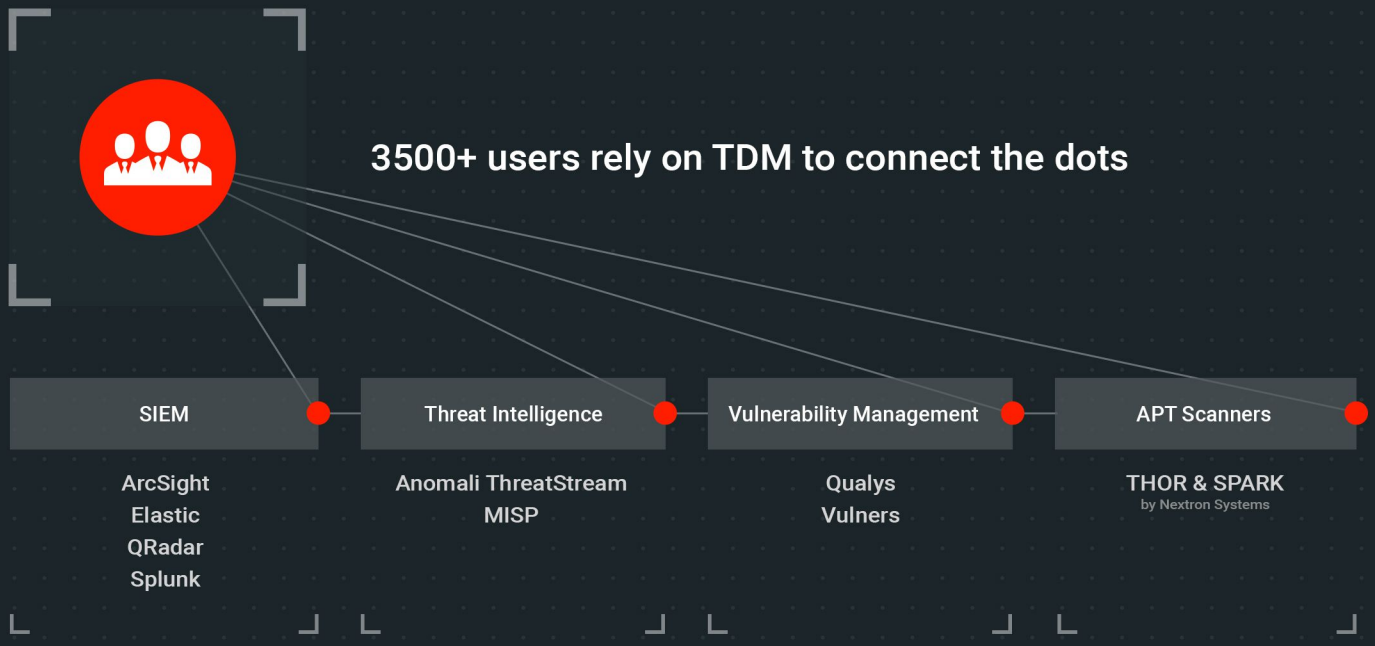
Our content will help you to address the following use cases

- Building and evolving Security Operation Centers
- Real-time Threat Detection
- Establishing Threat Hunting operations
- Digital and Cloud security monitoring

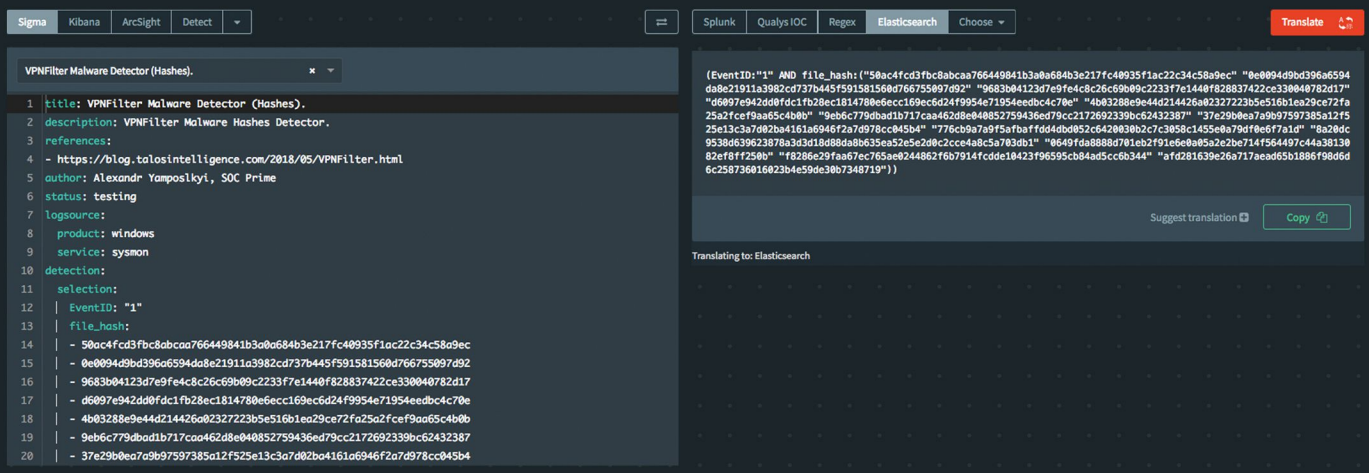
Evolving set of tools built by and for Blue teams

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

1.888.484.7555
+44.203.769.3384
sales@socprime.com
socprime.com



One common language for cyber security



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

1.888.484.7555
+44.203.769.3384
sales@socprime.com
socprime.com