Solution Brief

Threat Detection Marketplace: World's Largest Detection Content Repo

Overview: Threat Detection Marketplace

Threat Detection Marketplace empowers security teams with access to the world's fastest feed of security news, tailored threat intelligence, and the largest repository of curated 11,000+ Sigma rules continuously enriched with new detection ideas. Get started now to reach and download the latest behavioral detection algorithms and explore relevant context on any cyber attack or threat, including zero-days, CTI and ATT&CK references, and Red Team tooling.

Key Features

- **Detection Content**
  - **300K+** detection content items for cloud and on-prem tools
  - **11K+** behavior-based Sigma rules to describe any TTPs
  - **600+** expert content contributors
- **Strategic Detection Value**
  - Alignment with MITRE ATT&CK®
  - High focus on new & emerging threats
  - Log-source specific tagging
- **24/7/365 Detection Engineering Lifecycle**
  - **~400** detection algorithms released monthly
  - **24h** SLA for critical threats
- **Platform Compatibility**
  - Support for **28** SIEM, EDR, XDR & Data Lake platforms

Reduce Risk

24h

Access to the newly released detection code against emerging threats

Boost Detection Velocity

200%

Increase in threat investigation for streamlined detection operations

Improve Detection Quality

50%

Less false-positive rate with verified alerts

Optimize SOC Capacity

5 years

Saved of the Detection Engineering backlog

Threat Detection Marketplace Use Cases

Acting as an ultimate solution that can do it all, Threat Detection Marketplace lets you speed up detection capabilities and free up your security team tons of effort. Find emerging threats and detect cyber attacks faster than ever, accelerate threat investigation, or consolidate and manage all your detection code in an automated fashion from a single place.

- **Threat Intel & Detection Rules Search Engine.** Search for the latest ready-to-deploy behavioral detection algorithms and explore relevant context on any cyber attack or threat, including zero-days, CTI and MITRE ATT&CK references, and Red Team tooling.

- **Rule Feed on the Latest TTPs.** Browse through the world's largest rule feed on the latest TTPs used by adversaries in the wild, as well as proactive methods not yet linked to cyber attacks. Filter rules to get the most relevant to your industry and geography.

- **Central Content Management UI for Cloud-Native SIEMs.** Automate detection content deployment and management. Arrange detections in curated lists and push customized algorithms directly into your cloud SIEM. Centrally manage content deployed into multiple platforms and track the latest changes.

- **Custom Repo for Detection-as-Code Projects.** Create your custom repositories for Detection-as-Code projects smartly linked to ATT&CK. Save and manage any rules and queries supported by the SOC Prime Platform in a separate encrypted storage to boost the use case management lifecycle

Community-Driven Content Development

SOC Prime curates detections generated from two primary sources that combine to produce a monolithic body of knowledge giving any security team a significant advantage in their fight against adversaries:

- **SOC Prime's in-house team of content developers** connecting experts in Threat Hunting, Malware Reverse Engineering, and Detection Engineering. In addition to enriching and reviewing the quality of community contributions, SOC Prime's team places a high focus on new and emerging threats and overall coverage of the MITRE ATT&CK framework.
- **SOC Prime's crowdsourcing initiative, the Threat Bounty Program**, the world's largest and most diverse cyber defense bounty program enabling researchers to monetize their own threat detection content. The SOC Prime Threat Bounty Program connects over 600 researchers and threat hunters who actively contribute their own Sigma rules to the Threat Detection Marketplace.

Quality & Enrichment

Running a CI/CD lab for all supported technologies enables continuous testing and validation of the content quality. The recently developed detection rule is automatically checked for duplication and errors and is further enriched with the following metadata before being placed into another quality control queue:

- Relevant cyber threat intelligence, appropriate log sources, data sources, MITRE ATT&CK, CVE.
- Operation metadata, such as severity, rule status, and category, which allows security professionals to identify content that may be more suitable for use as a Query in Threat Hunting or as an Alert/Rule in Incident Response.

Curation & Filtering

After publishing content to the platform, user persona, log sources, user activity, collected feedback, and existing tags are continuously evaluated with various SOC Prime's recommendation algorithms to filter and sort content. In addition to searching based on all conventional tags, teams can also refine their detection results:

- Leveraging use case categories, such as Proactive Exploit Detection, Cloud, or Active Directory.
- Through platform configuration features, such as Search Profiles, which allow defining what analytics platforms are in use and what log sources are being collected.

Privacy

Trust, transparency, and privacy are inherent values SOC Prime delivers throughout all security operations, processes, and procedures to their customers. As a security-conscious organization dedicated to data protection and privacy, SOC Prime collects and processes all user data within the scope of the GDPR driven by a single purpose to improve the customer experience with the Detection as Code platform. All the projects are run by the in-house SOC Prime Team, which ensures privacy protection and no access for third parties to the platform functionality.

Being a trusted security-minded organization, SOC Prime regularly completes the Service Organization Control (SOC) 2 Type II auditing procedure verifying its compliance with the high standards of excellence in cybersecurity.

Trusted by the Best

More than 8,000 enterprises, including 42% of Fortune 100, 21% of Forbes Global 2000, 90+ public sector institutions, and 300+ MSSP and MDR providers rely on SOC Prime as a trusted partner.

Gartner peerinsights™

Customer Experience & Product Capabilities

4.9/5

Safeguard your organization with the best-in-class technology and professional support. Join the world's first platform for collective cyber defense. Let's build a secure tomorrow, together.

START NOW