Threat Detection Marketplace

World's Largest Detection-as-Code Library of Rules & Real-Time CTI

Threat Detection Marketplace empowers security teams with access to the world's largest Detection-as-Code library of rules and real-time threat intelligence. Get started now to reach and download the latest behavioral detection algorithms from 13,000+ Sigma rules continuously enriched with new detection ideas and explore relevant context on any cyber attack or threat.

Highlights

Detection-as-Code Library

- **500K+** detection content items for cloud and on-prem tools
- **13K+** behavior-based Sigma rules to describe any TTPs
- **Ultra-fast** search engine to find CTI & detections in 0.5 seconds

Active Threats Feed

- **60 seconds** to understand any threat and its full context
- AI-enriched context, including info on attribution, ATT&CK techniques, geo of attacks
- Relevant behavior rules based on TTPs for each active threat

Strategic Detection Value

- Alignment with MITRE ATT&CK®
- High focus on new & emerging threats
- Log-source specific tagging

Platform Compatibility

- Support for **30+** SIEM, EDR & Data Lake platforms

24/7/365 Detection Engineering Lifecycle

Reduce Risk

24-hour

Access to the newly released detection code against emerging threats

"DIRECTV Latin America relies on SOC Prime's follow-the-sun detection engineering operations that ensure round-the-clock protection and proactive defense."

SOC Prime & DIRECTV Latin America Success Story

Optimize SOC Capacity

5 years

Saved on the Detection Engineering backlog

"With SOC Prime, LTIMindtree's clients can continuously stream up-to-date detection algorithms directly into their environment."

SOC Prime & LTIMindtree Success Story

Improve Detection Quality

50%

Less false-positive rate with verified alerts

"Neurosoft has significantly improved MTTD and MTTR and cut down the false positive rate by up to 50% over the first 6 months of using the Platform."

SOC Prime & Neurosoft Success Story

Boost Detection Velocity

200%

Increase in threat investigation for streamlined detection operations

"This allowed Deloitte Brazil to maximize available threat hunting resources while increasing the speed of threat detection operations, including a 200% increase in identification to expedite investigation and remediation."

SOC Prime & Deloitte Brazil Success Story

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 detection algorithms and explore relevant context on any TTP, cyber attack or threat, including zero-days, CTI and MITRE ATT&CK references, and Red Team tooling. Search privately across 12,000+ tailored data labels within SOC Prime's private AWS SOC 2 Type II certified cloud. Apply AI-powered search, transforming any human language prompt into a corresponding query, to find exactly what you need in the world's largest Detection-as-Code library.
- **Complete CI/CD workflow for threat detection.** Automate detection logic streaming directly into your SIEM instance. Centrally manage content deployed into multiple platforms and track the latest changes to the content in production. Download content translations via API to on-prem and cloud environments. Save and manage detection code in a separate encrypted storage.
- **Community-Driven, AI-Powered Cyber Threat Intelligence.** Rely on a unified source of real-time threat intelligence, relevant detection rules, and AI-enriched context to take action on any threats challenging your business in under 60 seconds. Prioritize security operations and timely apply relevant mitigation strategies while improving the overall cybersecurity posture. Get actionable data to make informed decisions.

Content Development Life Cycle

SOC Prime Platform acts as a single point to access Detection-as-Code content – both open-source and proprietary. Each piece of content from Threat Detection Marketplace follows a life cycle of continuous quality enhancement backed by feedback from over 11,000+ companies and 50,000+ users.

SOC Prime's in-house team of content developers connects 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 under a 24-hour SLA. Also, we integrate external open-source repositories maintained by market leaders while adding critical security context, threat intelligence, and MITRE ATT&CK tags since 2018. Rely on Threat Detection Marketplace to get high-quality feeds for a wide range of cybersecurity use cases, including edge and cloud.

Content Utilization & Management

After publishing content to the platform, detection algorithms need to be prioritized before being deployed in iterative phases to the customer's SIEM, EDR, or Data Lake. Leveraging Attack Detective, security teams can address the content prioritization hurdle by obtaining ready-to-deploy and easily customizable rules and queries most relevant to their industry, geography, and threat profile.

In addition to manual content deployment capabilities, Threat Detection Marketplace enables automated detection logic streaming directly into the customer's SIEM instance. Once deployed, centrally manage detections via a single UI or API and track the latest changes to the content in production. To foster content quality improvement, detection algorithms undergo performance checks in Attack Detective, enabling defenders to prioritize the content selection:

- **Obtain SIEM use cases for high-fidelity alerting**
- **Have verified hunting queries always at hand**

Leveraging Uncoder AI, security teams can tune detection logic and customize content to match current security needs. Once updated, refined detection code can be instantly saved in separate encrypted storage to help keep all content in sync and streamline its management from a single place.

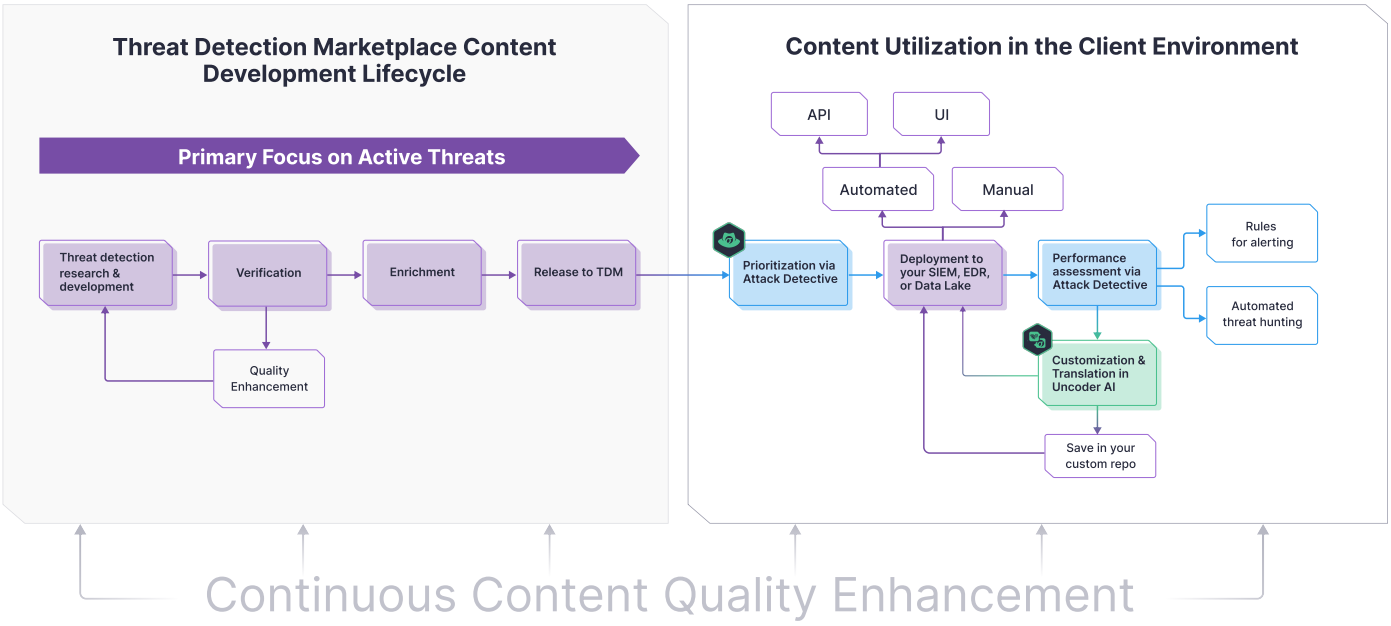

Figure 1. Detection Content Development & Utilization Lifecycle Backed by Threat Detection Marketplace

Privacy

Trust, transparency, and privacy are inherent values SOC Prime delivers throughout all security operations, processes, and procedures to its 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 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.

SOC Prime delivers AI-powered threat detection that enhances SIEM, EDR, and Data Lake systems while prioritizing privacy. Through on-premise training, we keep data private and secure by relying on NIST-AI-600-1 NIST AI Risk Management Framework (AI RMF 1.0)[1]. We use different models for different tasks like META's LLama, OpenAI's GPT, etc.—letting SOC Prime users always stay in control of their interaction with AI.

[1] NIST-AI-600-1 NIST AI Risk Management Framework (AI RMF 1.0)

Privacy Highlights

- One-time password (OTP) and multi-factor authentication options
- Security logging (audit trail)
- Hosted on Amazon AWS
- Web Application Firewall (WAF) protection
- Overall Rating A+ according to Qualys SSL Labs
- Single Sign-On (SSO) authentication & role-based access control (RBAC)
- Privacy-first AI completely under user control

Trusted by the Best

More than 11,000 enterprises, including 42% of Fortune 100, 21% of Forbes Global 2000, 90+ public sector institutions in key NATO countries, and 300+ MSSP and MDR providers rely on SOC Prime as a trusted partner.

Gartner peerinsights™

Customer Experience & Product Capabilities

4.6/5 ★★★★½

Empower your cybersecurity strategy with the complete product suite for AI-powered Detection Engineering, Automated Threat Hunting and Advanced Threat Detection to smartly resolve your existing challenges with a single end-to-end workflow.

Start Now