Data Sheet

Key Features

- Curated SOC Content
- Accelerated Threat Detection
- Automated Content Delivery
- 100k+ Detection Rules
- 2,800+ Behavior-Based Sigma Detections
- 95% MITRE ATT&CK® Coverage
- Leading SIEM, EDR, & NTDR Vendors Supported

Threat Detection Marketplace

SOC Prime Threat Detection Marketplace is the world's largest Detection as Code platform for SOC content connecting over 14,000+ security experts from 150+ countries.

We help organizations accelerate their cyber defense capabilities by delivering SOC content, such as queries, parsers, SOC-ready dashboards, YARA and Snort rules, Machine Learning models and Incident Response Playbooks mapped to the MITRE ATT&CK(™) framework. Threat Detection Marketplace enables full Continuous Integration (CI) / Continuous Delivery (CD) workflow for your detection procedures by providing automated delivery, deployment, and customization of cross-tool SOC content directly into your SIEM instance or other security environment. The platform capability to continuously deliver detection content matching the organization's SIEM and XDR stack fits the innovative approach to threat hunting known as "Detection as Code."

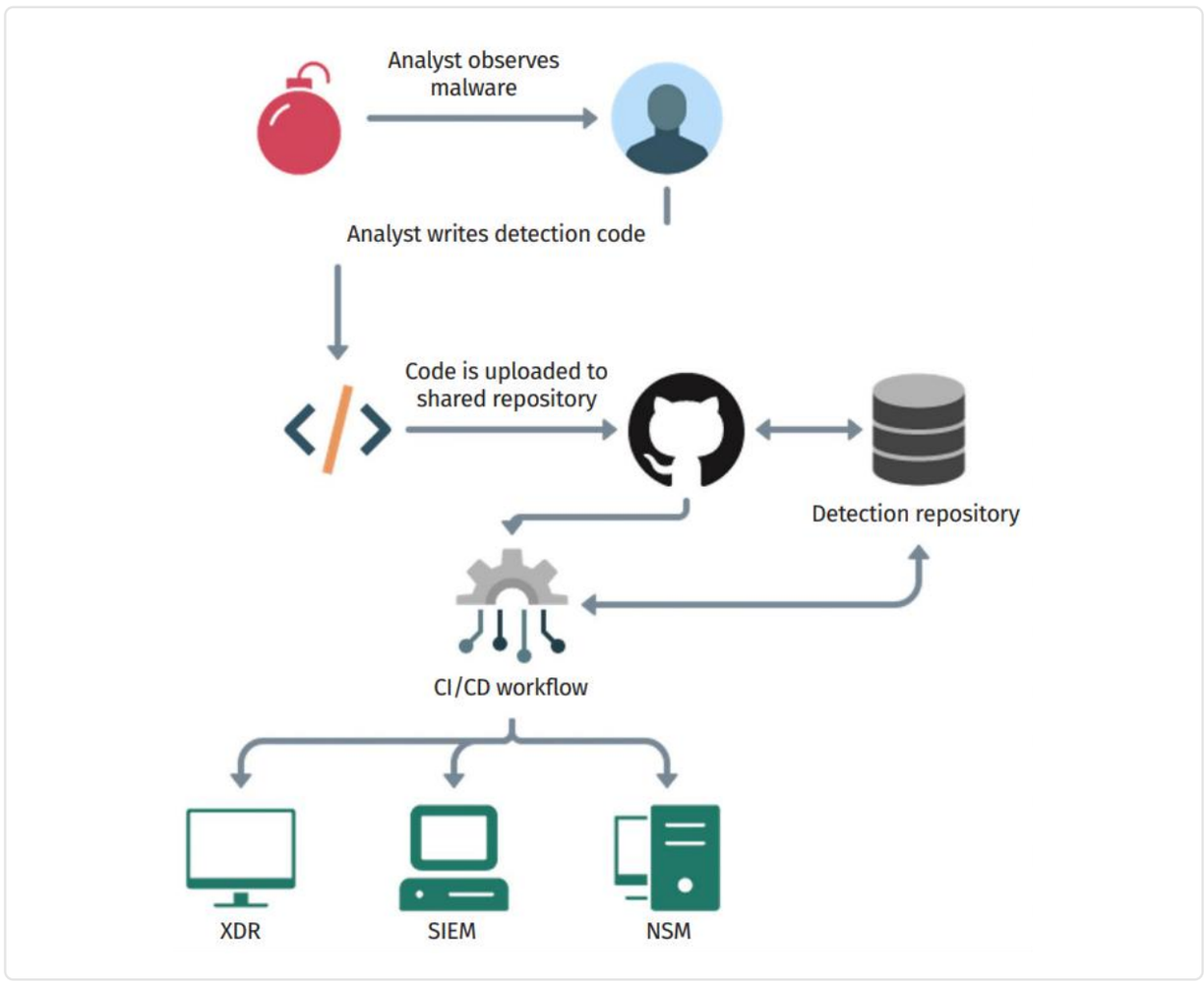

Figure 1. Detection as Code from Anton Chuvakin

By automating the integration processes Threat Detection Marketplace provides continuous streaming of detection and response algorithms to analytic-based SIEMs and 20+ leading security tools.

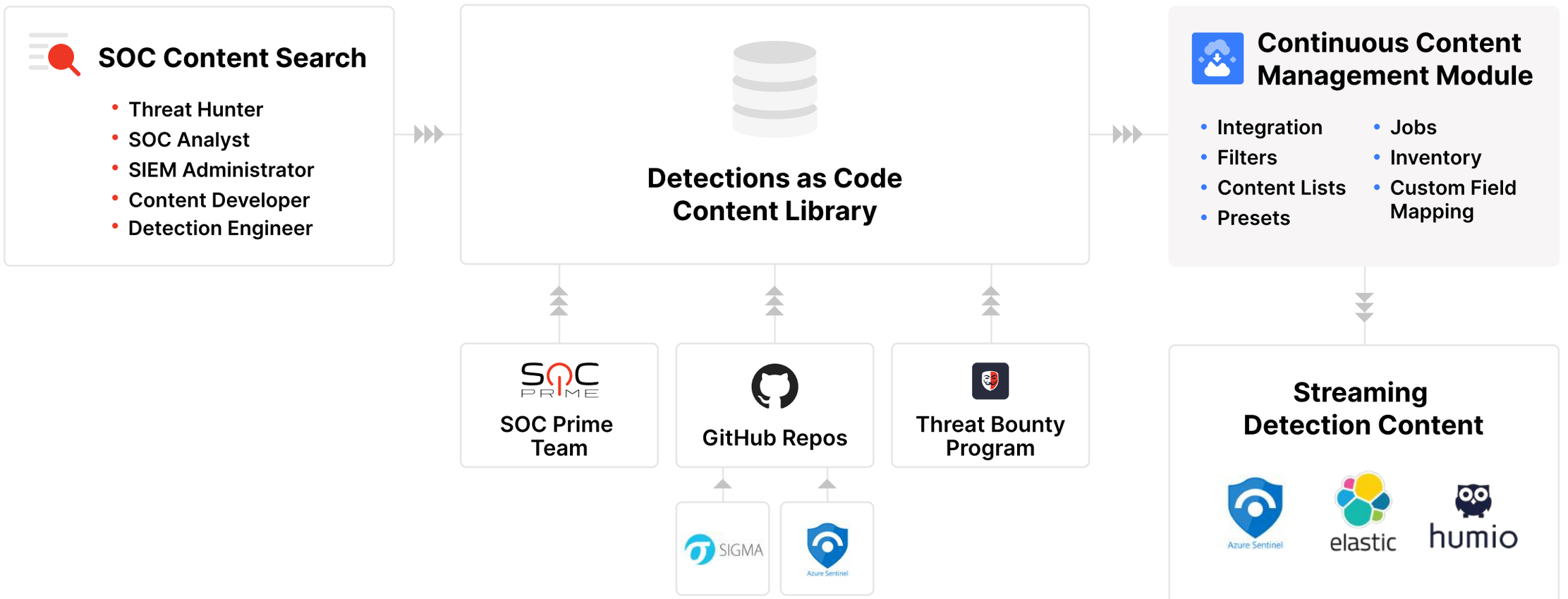

Figure 2. SOC Prime's Detection as Code platform enables continuous threat coverage and automated content streaming

Key Benefits

- Increase SOC team productivity by optimizing rule & query building
- Reduce risk with more accurate data and faster threat detection & response
- Tailor use cases matching your company's threat profile
- Make security content portable simplifying SIEM migrations
- Cost-efficiency and continuous threat coverage
- Reduced MTTD and MTTR

Learn More

To learn more or explore our MDR and MSSP Partnership options, contact your local sales representative today or sign up for Threat Detection Marketplace.

Cross-Platform Language Format

Threat Detection Marketplace supports on-the-fly translations from generic languages, like Sigma and Yara-L formats, as well as content written in the SIEM-native languages.

Threat Bounty Program

The Threat Bounty Program is a 300+ strong content developer community actively contributing Sigma rules to Threat Detection Marketplace.

Proactive Automated Threat Search, Detection & Response

Reduce MTTD and MTTR with streamlined search within a fully automated system of content management. Threat Detection Marketplace helps organizations proactively defend against emerging company-specific threats.

Role-Based Platform Experience

SOC Prime offers role-based experience using Threat Detection Marketplace for CISOs, SOC Managers, Threat Hunters, Red Team Specialists, and SOC Analysts. Filtering enables streamlined content search experience according to the pre-configured user profile.