Solution Brief

Privacy

Trust, transparency, and privacy are the core values when it comes to the security operations, processes, and procedures the companies seek to obtain from their partnership with SOC Prime.

GDPR Compliance

As a GDPR-compliant organization, we are dedicated to protecting the privacy of our customer data. The data we collect about our users is protected by GDPR controls. SOC Prime does not store any user data on a perpetual basis and does not share it with any third parties except for third-party processors with whom we have signed data processing agreements that help us provide and improve our services to the end users. We collect the user data within the scope of the GDPR regulations driven by a single purpose to improve the platform experience and thus, follow our mission to enable collective cyber defense against attacks of any sophistication.

According to GDPR, we are compliant with "the right to erasure" ("right to be forgotten"), which states that users can demand to have their personal data erased if they have withdrawn their consent or object data processing. Upon the user erasure request, we are responsible for telling our processors to delete the related Personally Identifiable Information (PII) data, both from productive live systems and backup archives.

Privacy and Ownership Concerns

Obtaining detection content from third-party vendors involves granting full access to the organization's SIEM, EDR, or Data Lake environment, including the data sources and alert outcomes, which raises high concerns about data privacy protection. At SOC Prime, we have adopted our own content development maturity aimed at mitigating the privacy risks of our customers. Along with the data privacy imperative, SOC Prime recognizes and respects content ownership and Intellectual Property (IP) rights. Detection content made in the customer's infrastructure based on the customer's logs shall belong to the customer only.

Data privacy protection and ownership concerns guide our development procedures and are reflected in SOC Prime's products that process user data. The in-house SOC Prime Team runs all the projects powered by our collective cyber defense platform, which ensures privacy protection and no access for third parties to the platform functionality. All the data is encrypted by industry standards — data at rest by the AES-256 encryption algorithm and in transit by the TLS 1.2 protocol. SOC Prime's information security practices, policies, operations, and procedures meet the relevant standards for secure data management, which is reflected in the dedicated Service Organization Control (SOC) 2 Type II auditor's report.

Zero-Trust Security

According to Gartner, by 2026, 10% of large enterprises will have a mature, measurable zero-trust program, a significant rise from less than 1% today. Zero-trust architecture (ZTA) replaces implicit trust with dynamic, risk-based authentication and continuous verification, adapting security postures in real time.

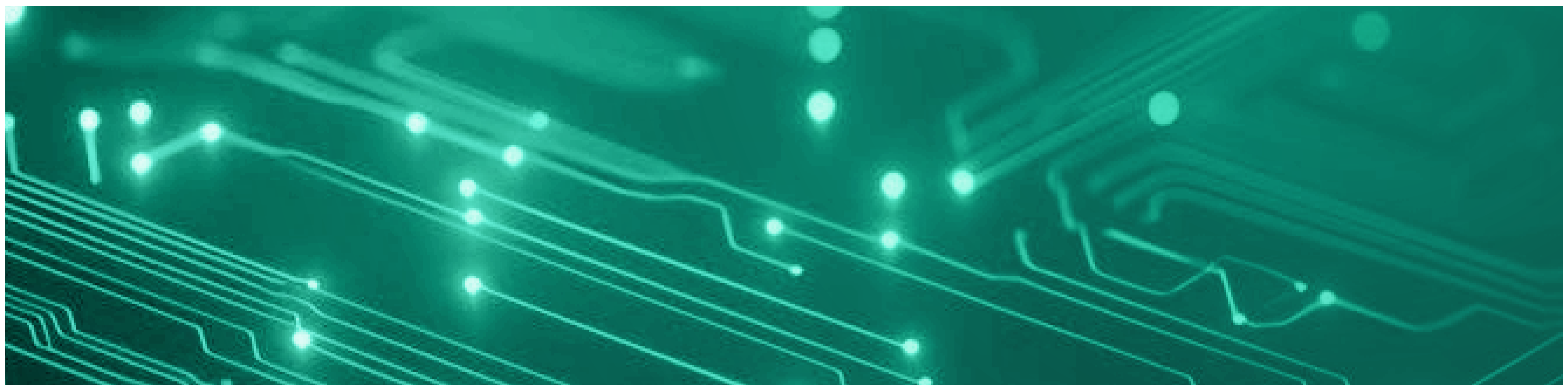
As per NIST SP 800-207 guidelines, no single vendor can provide a complete zero-trust solution, and relying on one may introduce vendor lock-in risks. Interoperability is crucial both at the time of adoption and throughout the lifecycle of security systems. Operating on ZTA, SOC Prime ensures compliance with the least privilege and data access controls to minimize the risk of breaches. By separating the data and control planes, SOC Prime follows NIST 800-207 guidelines, ensuring role-based access without storing, transferring, or inheriting SIEM, EDR, or Data Lake credentials or other sensitive data.

Privacy-First & Responsible AI

AI in cybersecurity is powerful—but only when used with control and precision. At SOC Prime, we believe that cybersecurity is more critical than ever, and we need defenders to have more control, transparency, predictability, and privacy. SOC Prime delivers AI-powered threat detection that enhances SIEM, EDR, and Data Lake systems while prioritizing privacy. Users control their data, ensuring security without extra costs. By fusing human expertise with AI, we boost detection accuracy and speed, staying ahead of emerging threats.

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). We also continuously work on optimizing compute efficiency to reduce CPU strain and environmental impact, supporting ethical and green AI practices.

In the world of AI model training, private high-quality dataset is the only technical advantage that gives a competitive edge. 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. SOC Prime users are the ones who decide what to send, when to send it, and whether to enable AI functionality at all.

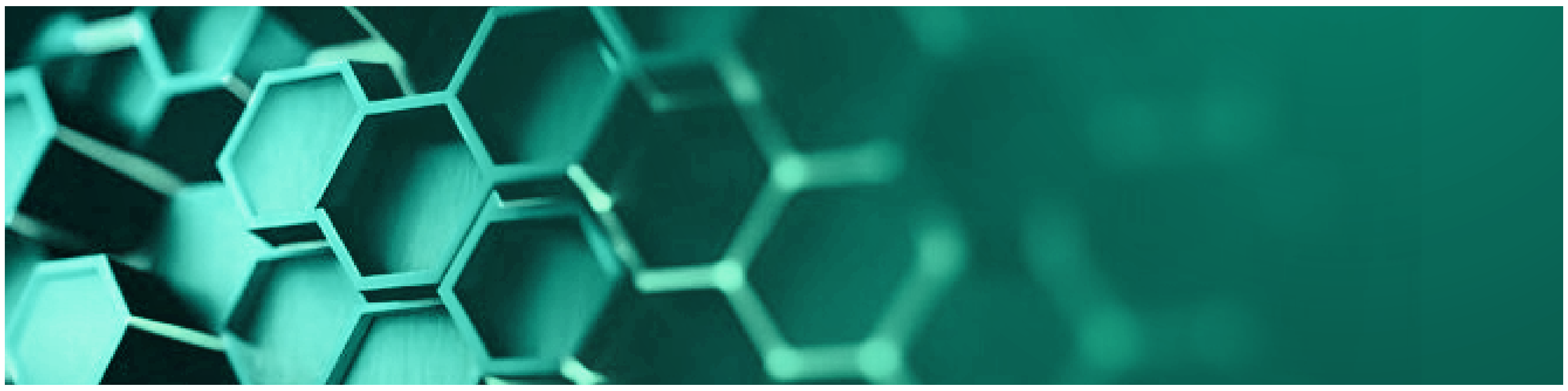


Threat Detection Marketplace

Powered by SOC Prime Platform for collective cyber defense, Threat Detection Marketplace is the world’s largest library of behavior-based Sigma rules and native rules for SIEM, EDR, and now Data Lakes, enriched with tailored intelligence, documented and mapped to the MITRE ATT&CK® framework.

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)



Attack Detective

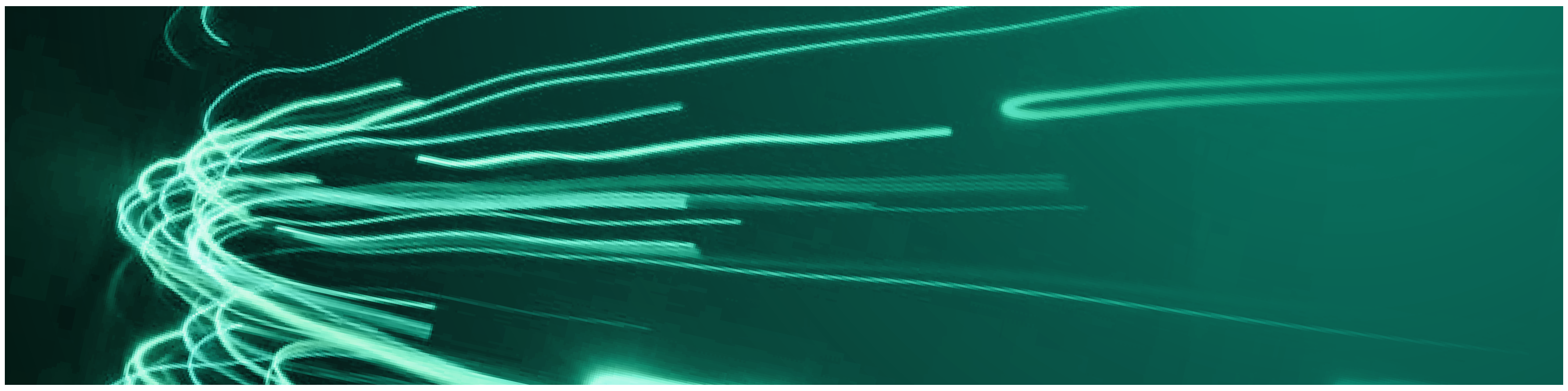
Attack Detective is an industry-first SaaS serving a real-time, researched, and packaged threat detection & hunting capability to quickly identify and tackle cyber threats before they escalate. It provides real-time data and content audits for comprehensive threat visibility and improved detection coverage, equips security teams with low-noise and high-quality rules for alerting, and enables automated threat hunting.

Attack Detective stores only aggregated information about the triggered rules, like hit count grouped by 1-hour bins and unique hashes (SHA256) for usernames and hostnames to show asset and account counts in the triggered queries. No SIEM log source data is collected or stored in Attack Detective.

Attack Detective is built on the ZTA milestones enabling organizations to risk-optimize their cybersecurity posture. It provides complete visibility based on the organization-specific logs to query data in its native location.

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
- Queries data in its native location avoiding data duplication or distribution and possible permission inconsistency
- Clear segregation between the control plane and the data plane according to NIST 800-207
- Single Sign-On (SSO) authentication & role-based access control (RBAC)



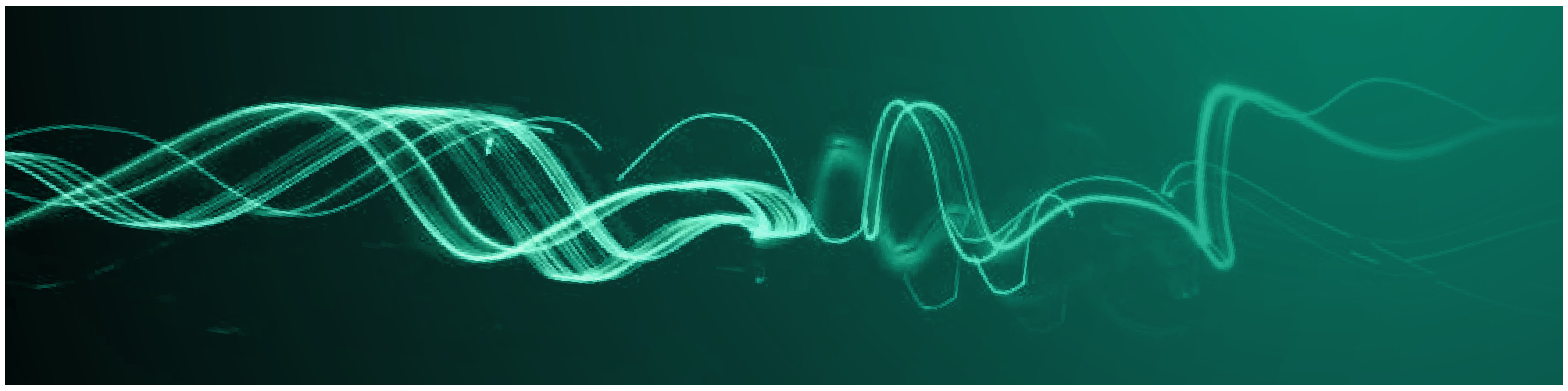
Uncoder AI

Uncoder AI acts as an industry-first integrated development environment (IDE) and co-pilot for threat-informed detection engineering enabling seamless algorithm creation, exchange, translation, and improvement in a trusted environment while protecting the intellectual property of threat researchers. Using Uncoder AI, security professionals can create, customize, and translate detection code into multiple SIEM, EDR, and Data Lake native languages or open-source language formats like Roota & Sigma. Additionally, Uncoder AI leverages Artificial Intelligence LLM and Augmented Intelligence datasets to deliver relevant CTI, provide detection engineering context, and ensure triage information enrichment. Powered by market-leading public LLMs, such as OpenAI, Gemini, DeepSeek, and Llama along with SOC Prime's private Machine Learning models trained on the world's largest dataset of 1,000,000+ detection rules and queries, along with 13,000+ labels and running on SOC Prime's private cloud, Uncoder AI provides broad options for detection code mastering.

Uncoder AI takes a privacy-first approach, offering cutting-edge open-source and private LLMs as optional opt-in plugins—completely under your control. With Uncoder AI, every byte sent to an LLM is first verified by the user.

Highlights

- One-time password (OTP) and multi-factor authentication options
- Unlimited AI/LLM capabilities completely under your control
- Security logging (audit trail)
- Hosted on Amazon AWS
- Web Application Firewall (WAF) protection
- Overall Rating A+ according to Qualys SSL Labs
- No data sharing with third parties or AI
- Single Sign-On (SSO) authentication & role-based access control (RBAC)



Uncoder IO

Uncoder IO is an open-source version of its AI co-pilot version Uncoder AI. It acts as a fast, private, and easy-to-use online translation engine supporting conversion of Sigma & Roots rules into multiple SIEM, EDR, and Data Lake query formats. Additionally, Uncoder IO supports IOC packaging from any non-binary format such as PDF, text, STIX, or OpenIOC into performance-optimized queries tailored to your security stack in use.

Highlights

- Fully anonymous: no registration, no authentication, no logging
- All data kept session-based, stored in memory, no presence on server disks
- Microservice-based architecture and Amazon AWS hosting
- Based on the community-verified project “sigmac”
- Overall Rating A+ according to Qualys SSL Labs

The Prime Hunt

The Prime Hunt is an open-source browser extension that acts as the industry-first platform-agnostic UI for all threat hunters, no matter what SIEM or EDR they use. The tool enables security engineers to quickly convert, apply, and customize detection code across the widest stack of SIEM and EDR — directly within their Chrome, Firefox, or Edge browser.

Highlights

- Fully anonymous: no logging, no third-party access to user data
- Relevant access rights and permissions for each security analytics per each SIEM, EDR, or Data Lake platform via existing authentication and authorization mechanisms

Enhance 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 via a single end-to-end workflow.

START NOW ↗