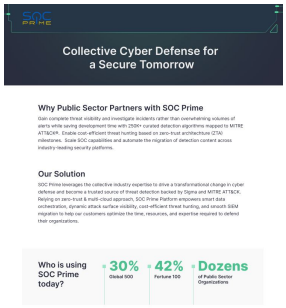


Collective Cyber Defense for a Secure Tomorrow

Case Study

Thank you for downloading this SOC Prime Case Study. Carahsoft is the official government distributor for SOC Prime cybersecurity solutions.

To learn how to take the next step toward acquiring SOC Prime solutions, please check out the following resources and information:

For additional resources:
carah.io/SOCPrimeResources

To request a quote:
carah.io/requestaquote

For additional solutions:
carah.io/SOCPrimeSolutions

For additional Cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
SOCPrime@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/SOCPrimeContracts

Collective Cyber Defense for a Secure Tomorrow

Why Public Sector Partners with SOC Prime

Gain complete threat visibility and investigate incidents rather than overwhelming volumes of alerts while saving development time with 250K+ curated detection algorithms mapped to MITRE ATT&CK®. Enable cost-efficient threat hunting based on zero-trust architechture (ZTA) milestones. Scale SOC capabilities and automate the migration of detection content across industry-leading security platforms.

Our Solution

SOC Prime leverages the collective industry expertise to drive a transformational change in cyber defense and become a trusted source of threat detection backed by Sigma and MITRE ATT&CK. Relying on zero-trust & multi-cloud approach, SOC Prime Platform empowers smart data orchestration, dynamic attack surface visibility, cost-efficient threat hunting, and smooth SIEM migration to help our customers optimize the time, resources, and expertise required to defend their organizations.

Who is using SOC Prime today?

30%
Global 500

42%
Fortune 100

Dozens
of Public Sector Organizations

SOC Prime in Numbers

250K+
detection algorithms against current & emerging threats

10K+
vendor-agnostic Sigma rules for any TTP or attack behavior

94%
detection content mapped to MITRE ATT&CK v12

27+
supported SIEM, EDR, and XDR platforms

600+
security experts contributing detection algorithms daily

24 hours
SLA for emerging threats

33K+
cyber defenders providing actionable feedback on detection algorithms

85%
faster cross-SIEM content translation and fine-tuning

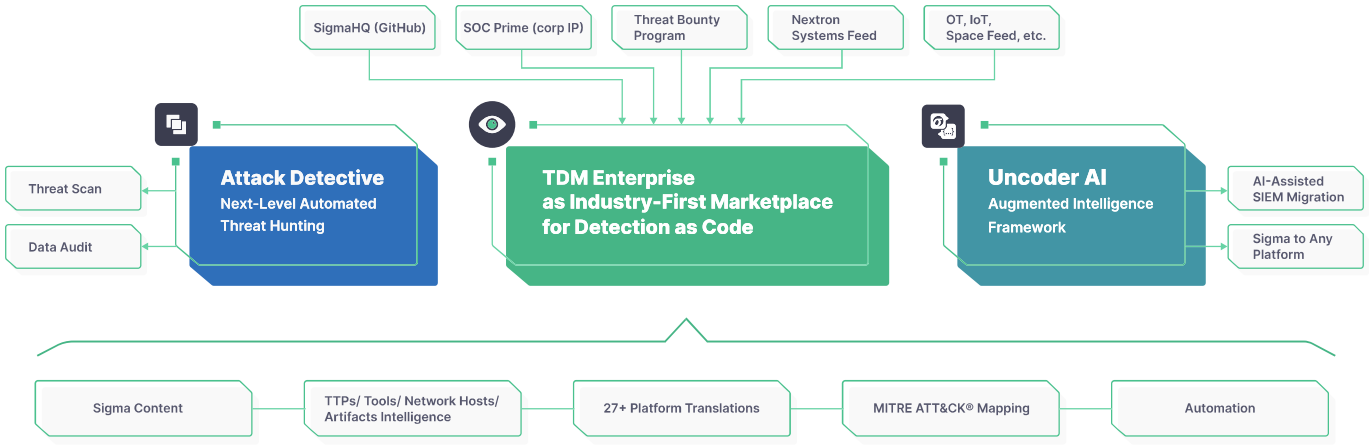
SIGMA

SOC Prime is the single largest commercial contributor to the SIGMA open source project. SIGMA acts as one common language for cybersecurity to describe any adversary TTP and translate it to any detection code. Since its invention in 2016, Sigma has become an agnostic way of sharing detection logic between security practitioners regardless of maturity level and the tech stack in use.

- Sigma – generic format for SIEM systems
- Ranked #7 in the list of best open-source security projects
- Recommended as an effective way to identify cyber threats by CISA, FBI, and NSA
- Enables expressing threat detection by focusing on behavior and the algorithm itself
- Convertible to 27+ SIEM, EDR, or XDR solutions

Driving Cost-Efficient, Zero-Trust, and Multi-Cloud Security Backed by Collective Expertise

SOC Prime operates the world's largest and most advanced platform for collective cyber defense that cultivates collaboration from a global cybersecurity community and curates the most up-to-date Sigma rules compatible with over 27 SIEM, EDR, and XDR platforms. SOC Prime's innovation, backed by the vendor-agnostic and zero-trust cybersecurity approach, and cutting-edge technology leveraging Sigma language and MITRE ATT&CK® as core pillars are recognized by the independent research companies, credited by the leading SIEM, XDR & MDR vendors, and trusted by 8,000+ organizations.



SOC Prime's 3-Pronged Approach to Future-Proof Cyber Defense

Threat Detection Marketplace

SOC Prime's Threat Detection Marketplace acts as a trusted source of threat detection covering emerging threats in a matter of hours and offering Concierge Support with a 24h SLA on the latest threats. By fusing Sigma and MITRE ATT&CK, we created a reliable knowledge base that is updated every minute and is searchable at sub-second performance to help security teams address the challenges of building advanced and threat-specific detections, organize and execute around strategic detection objectives, and manage the deployment of content at scale across 27 SIEM, EDR and XDR platforms.

Attack Detective

SOC Prime's Attack Detective enables smart data orchestration and empowers security teams to identify cyber defense gaps and eliminate blind spots to continuously improve visibility into the organization-specific threats, CVEs, and adversary TTPS that can be used in cyber attacks.

Uncoder AI

SOC Prime's Uncoder AI is an Augmented Intelligence framework that fuses cyber threat intelligence, indicators of attacks, and over 10,000 Sigma rules mapped to MITRE ATT&CK® backed by collective cybersecurity expertise and generative AI engines to timely notify users of emerging threats, enable them to proactively develop and update detection algorithms, and gain aggregated context on any cyber attack. AI-assisted capabilities of Uncoder AI enable 85% faster cross-SIEM content translation & fine-tuning while saving development time and reducing SIEM migration costs.