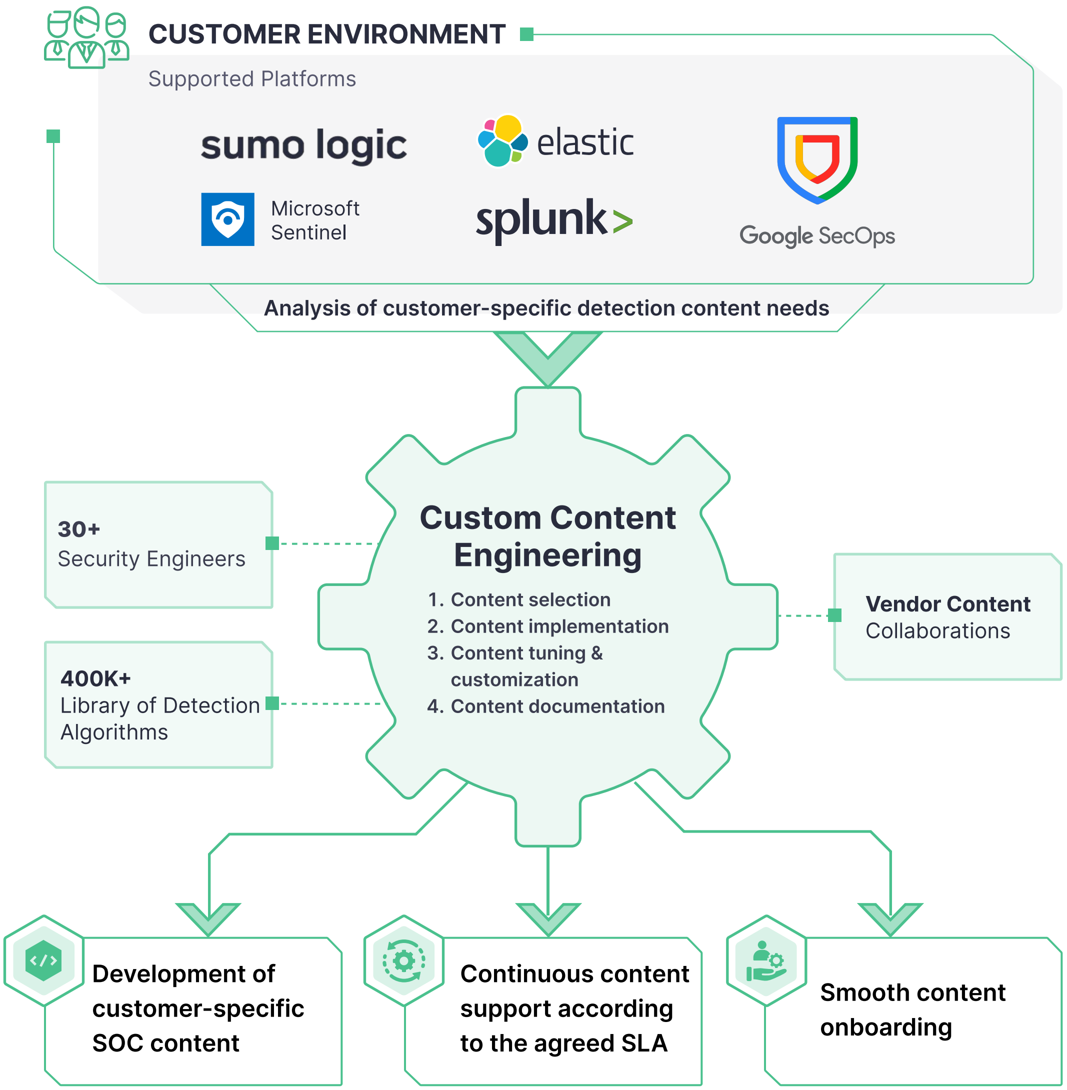
Data Sheet

Custom Content Engineering

Adopt out-of-the-box detection engineering capability to proactively defend against emerging cyber threats most challenging your business. Rely on our expert team to create, implement, and operationalize custom detection content directly in your SIEM and EDR environment.



CUSTOMER ENVIRONMENT

Supported Platforms

sumo logic

elastic

Microsoft Sentinel

splunk>

Google SecOps

Analysis of customer-specific detection content needs

30+
Security Engineers

400K+
Library of Detection Algorithms

Custom Content Engineering

1. Content selection
2. Content implementation
3. Content tuning & customization
4. Content documentation

Vendor Content Collaborations

Development of customer-specific SOC content

Continuous content support according to the agreed SLA

Smooth content onboarding

24-h SLA

for detection content against emerging threats

30+

SIEM, EDR, and Data Lake platforms we are experts in

50%

Reduced MTTD & MTTR to ensure no attack goes undetected

Highlights

- Eliminate gaps in your detection coverage
- Adopt advanced Detection Engineering capability
- Make your SIEM and EDR use cases portable
- Save development time and migration costs
- Address content management challenges with continuous guided support

Fast-Tracked Content Delivery

Development of customer-specific SOC content:

- Rules and rule packs
- Parsers and configs
- Incident Response Playbooks
- SOC-ready dashboards and reports

Enhanced Content Support

Continuous content support according to the agreed SLA:

- Initial configuration and deployment
- Fine-tuning
- Content updates
- Transition of customer-specific use cases to a different environment

Expert Content Onboarding & Training

Smooth content onboarding backed by training sessions:

- Training in content deployment and customization
- Live demos upon request
- Extended documentation support

SOC Prime Expert Team

30+
Seasoned experts

400K+
Detection rules & queries

The SOC Prime team is the creator and maintainer of the world's largest library of detection content. Our engineering expertise encompasses a diverse skill set, including Threat Hunting, Detection Engineering, Incident Response, Forensics, and Risk Assessment.

About Us

SOC Prime operates the industry-first modular platform for collective cyber defense against attacks of any sophistication and fast attribution. The Platform is backed by the world’s largest library of detection algorithms and tailored threat intelligence powered by our mature engineering team, global CERTs, third-party consultancy, and the global crowdsourcing program for cyber defenders. We have established a dedicated Professional Services team to help our enterprise clients maximize their security investments and turn their strategic vision into an actionable roadmap for long-term success.

Reach out to your local sales representative at sales@socprime.com to explore the full list of SOC Prime Professional Services.