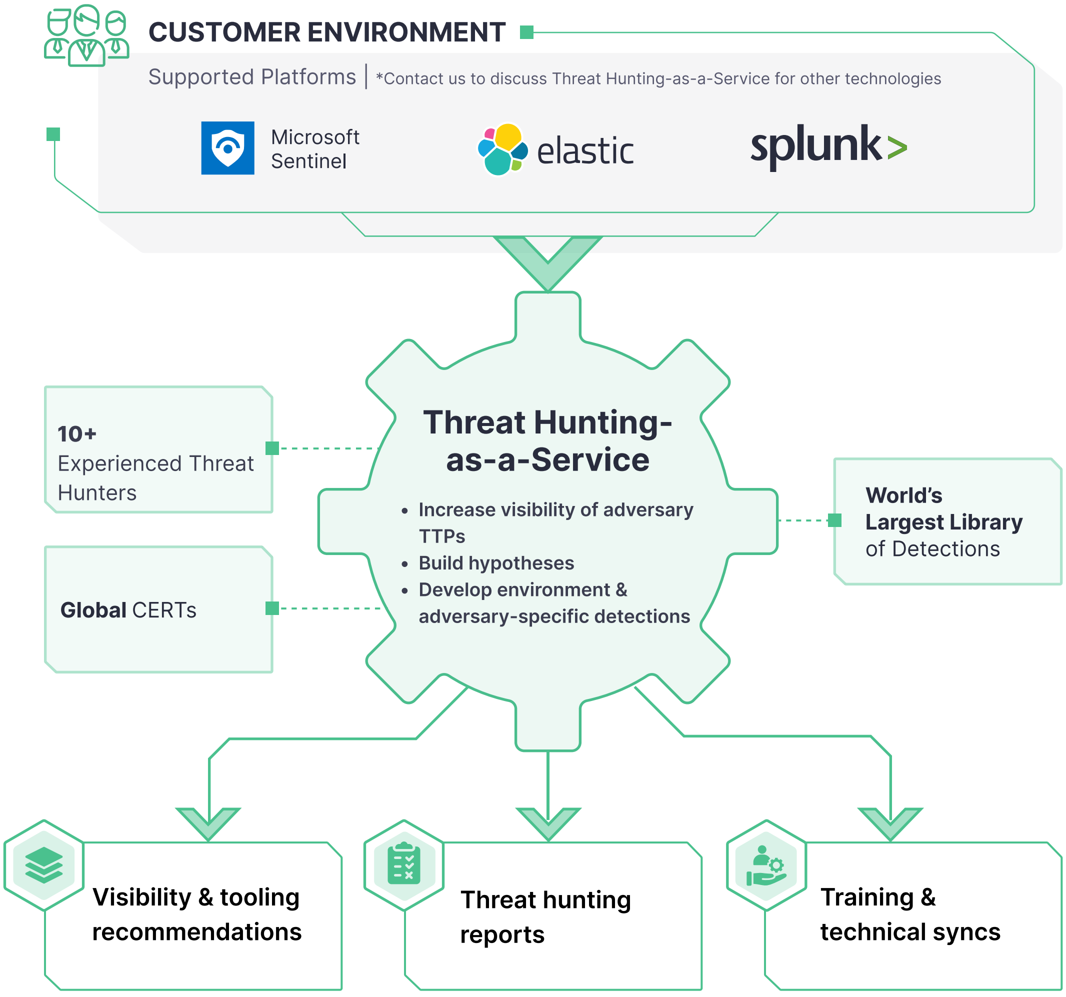
SOC PRIME

Data Sheet

Threat Hunting-as-a-Service

Significantly boost your cybersecurity posture and strengthen native defense capabilities with SOC Prime's exclusive Threat Hunting-as-a-Service. Our expert team proactively hunts for both insider threats and external attackers, while enhancing your security operations and optimizing detection and logging for a more resilient cyber defense.



CUSTOMER ENVIRONMENT

Supported Platforms | *Contact us to discuss Threat Hunting-as-a-Service for other technologies

Microsoft Sentinel

elastic

splunk>

10+ Experienced Threat Hunters

Global CERTs

Threat Hunting-as-a-Service

- Increase visibility of adversary TTPs
- Build hypotheses
- Develop environment & adversary-specific detections

World's Largest Library of Detections

Visibility & tooling recommendations

Threat hunting reports

Training & technical syncs

Threat Hunting-as-a-Service primarily uses the customer's existing tooling and requires full remote access over either VPN, VDI, or equivalent means

400,000+

Library of rules & queries

24-h SLA

for detection content against emerging threats

50%

Reduced MTTD & MTTR to ensure no attack goes undetected

Highlights

- Uncover hidden threats and stop attacks at early stages
- Adopt expertly-packaged threat hunting capability
- Identify threats that tools can't
- Reduce investigation time & boost incident response efficiency
- Enhance detection accuracy while minimizing false-positive rate

Deliverables

Visibility & Tooling Recommendations	Threat Hunting Reports	Training & Technical Syncs
■ Identifying and addressing critical gaps to ensure hunts are executed on viable log source ■ Actionable improvement recommendations ■ Collaboration with non-security engineers to resolve visibility & engagement issues	■ Summary and intention of the hunt ■ Analytic overview ■ Overview of limitations and recommendations (e.g., enrichments, visibility) ■ Outcomes of the hunt ■ List of detections based on the outcomes	■ THAAS results overview detailing real-life, industry-specific attack scenarios ■ Threat hunting skills improvement for targeted threat mitigation

SOC Prime Expert Team

10+

Seasoned Threat Hunters

SOC Prime's engineering expertise includes a diverse skill set ranging from Threat Hunting, Detection Engineering, Incident Response, Forensics, and Risk assessment. Our team involves certified experts, including GREM, GCFE, CISSP, CEH, Security+ recognized professionals and MITRE ATT&CK Defenders.

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.