Member of
Microsoft Intelligent
Security Association

Microsoft

SOC Prime's Detection as Code Platform and Microsoft Sentinel

SOC Prime's Detection as Code platform allows organizations to stay ahead of emerging threats by supercharging SOC operations with the world's largest collection of detection content to enrich any security solution in use. Equip your team with Microsoft Sentinel-native solutions customized to your environment and business needs. SOC Prime's strong partnership with Microsoft and MISA membership yields unparalleled industry expertise capable of addressing any custom use case.

Benefits & Capabilities

- Enhance threat hunting capabilities by accelerating your proactive and retrospective Threat Hunting with behavior-based detections and Cyber Threat Intelligence. Focus on real threats most relevant to your business to instantly run high-quality hunts customized to your environment needs.

- Maximize the efficiency of your cyber defense by tracking your team's threat detection progress and apply measures to gauge ROI, benchmark against industry peers, and illustrate MITRE ATT&CK® coverage. Execute around strategic detection objectives and fill potential gaps to drive more productivity and team collaboration.

- Enable continuous threat coverage by automating your content deployment and management from a single place with no time wasted on complex configuration and fine-tuning. Stream customized, deployment-ready detection content created through the collaboration of the global experts directly into your SIEM, EDR & XDR environment.

View the Customer Success Stories of our clients leveraging the Microsoft Sentinel solution:

- https://socprime.com/customer-success-stories/mssp/sorint-sec/
- https://socprime.com/customer-success-stories/mdr/quzara-cybertorch/
- https://socprime.com/customer-success-stories/mssp/entelgy-innotec-security/

SOC Prime and Microsoft Sentinel:
Expertise in Numbers

Save up to 5 years of R&D effort on SIEM-native content development tailored to the needs of both large-scale enterprises and MDRs. SOC Prime's mature partnership with Microsoft offers broad customization options for Sentinel-native content accessible right from your SIEM instance.

Data Connectors

69 Products

Automation

30 Playbooks
10 Logic Apps

Workbooks

34 Products

Analytics

340+ rules
340+ queries

Accelerated Detection and Response Powered by SOC Prime and Microsoft Sentinel

Sentinel-native content development

Obtain out-of-the-box use cases, including SIEM-native Workbooks, Playbooks, Logic Apps, and Data Connectors.

Cost-efficient support and maintainance

Have all data normalized and parsed with no extra costs for content development, integration, and fine-tuning.

Full threat context and ATT&CK® alignment

Get ready-to-use rules & queries mapped to ATT&CK with threat context on any alert triggered and query matched.

Automated content streaming

Automatically push detections that can instantly kick off SOAR Playbooks in Logic Apps directly in your environment.

On-Demand Microsoft Sentinel Expertise

SOC Prime's Detection as Code platform ensures complete threat visibility with your Microsoft Sentinel solution to keep your SIEM continuously updated on the latest threats.

Smooth Migration of Use Cases

Find more threats in less time by migrating all your existing detections to Microsoft Sentinel. We support multiple languages to transition to KQL compliant with the ASIM data schema.

Log Source Integration

SOC Prime provides support for the development, implementation, and integration of all available custom log sources. Even the log sources currently not supported out of the box will be covered using custom Function Apps.

Incident Response Coverage

Microsoft Sentinel offers a broad collection of incident response scenarios, with 65+ available in SOC Prime's platform. Incident Response Playbooks boost cyber response capabilities and reduce MTTR.

Sentinel Centric Engineering Suite

SOC Prime's engineering expertise includes a diverse skill set ranging from Azure administration, Sentinel operations, Data Connectors, custom Logic Apps & Playbooks development, and fine-tuning.

Seasoned & Certified Team of MITRE ATT&CK Defenders