

# AI SOC Ecosystem

SOC Prime brings together innovative cybersecurity technologies into a powerful, vendor-agnostic ecosystem with privacy, performance, and efficiency at its core. Partnering with the market-leading security innovators, SOC Prime curates a platform that delivers autonomous SOC to enterprises, MSPs, MDRs, and MSSPs. Together, we create a dynamic network to optimize and revolutionize cybersecurity operations.

# **About AI SOC Ecosystem**

Leading the way in Detection-as-Code, Al-powered detection engineering, and automated threat hunting, SOC Prime operates an industry-first platform for collective cyber defense, offering three core products – Threat Detection Marketplace, Attack Detective, and Uncoder Al. With a vendor-agnostic approach at the core, we collaborate with top vendors to help security teams outscale evolving cyber threats and strengthen their detection and response capabilities. We shape a dynamic ecosystem fusing SOC Prime technology driven by Al and augmented by collective cybersecurity expertise with our partners' innovations to deliver unparalleled cyber defense capabilities.





# **Privacy-First**

We've built a platform that surpasses security standards to protect the minimal personal data we collect from you. You can exercise your right to be forgotten at any time, no matter where you are. With a privacy-first approach, we provide advanced AI tools that are fully under your control, allowing you to choose what data to share or whether to share it at all. By relying on AI SOC Ecosystem, organizations can outscale cyber threats, without surrendering their data.

#### **Zero-Trust Architecture**

Operating on a Zero-Trust Architecture, the SOC Prime Ecosystem 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 <a href="NIST 800-207 Special Publication">NIST 800-207 Special Publication</a>, ensuring role-based access without sharing SIEM, EDR, or Data Lake credentials. Our solutions integrate natively with zero-trust principles, leveraging proper access rights and permissions for each platform using existing authentication mechanisms.

# **Responsible & Green Al**

SOC Prime Ecosystem delivers Al-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 Al, we boost detection accuracy and speed, staying ahead of emerging threats. Through on-premise training, we keep your data private and secure, while optimizing compute efficiency to reduce CPU strain and environmental impact, supporting ethical and green Al practices.

#### **Highlights**

- Automation. Streamline SOC and Incident Response processes
- Advanced Threat Detection. Adopt faster, more accurate threat detection across multiple security vendors
- Scalability. Process more telemetry, add context, and expand capabilities
- Faster Incident Response. Reduce dwell time and accelerate mitigation
- Efficient Staffing.
  Optimize human
  resources with Al-driven
  insights
- Training & Information Sharing. Benefit from knowledge exchange for continuous improvement
- Working with Local Innovators. Supporting regional cybersecurity advancements



# **Unlock the Fusion of Technologies**

We curate advanced tools for threat detection and hunting, offering data audits, rule sourcing, and deployment—all without retrieving any data, unlike other vendors. SOC Prime enriches its AI SOC Ecosystem by integrating with open-source repositories and supporting vulnerability management systems to prioritize detection rules based on the latest exploits. This is further enhanced by support for threat intelligence platforms (TIPs) to create a new layer of CTI, enrich detection rule context, and streamline IOC-to-query conversion. By connecting with market leaders through Git protocol and open-source projects like OpenTIDE, we accelerate the Detection-as-Code workflow and automate ticket creation for identified threats.

#### **Data Planes**

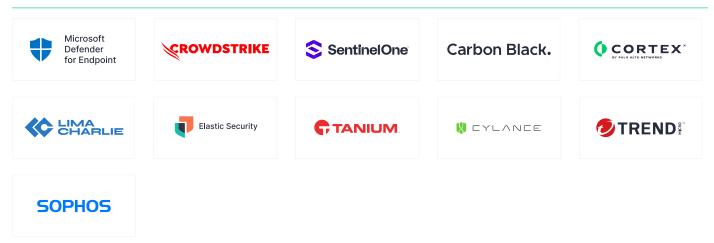
SOC Prime treats SIEM, EDR, and Data Lake platforms as Data Planes in line with the NIST SP 800-207 Zero Trust Architecture standard. We never store, transfer, or inherit SIEM, EDR, or Data Lake data, prioritizing security and trust.

#### SIEM

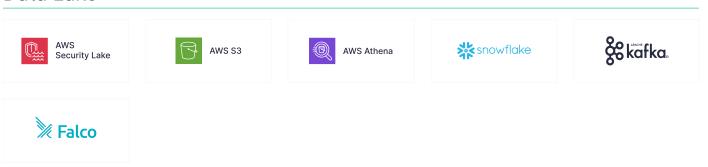




#### **EDR**



#### Data Lake



## CI/CD

SOC Prime supports its Ecosystem by connecting with market leaders leveraging Git protocol and open source projects adopted worldwide, as well as cutting-edge OpenTIDE framework for threat-informed detection engineering.





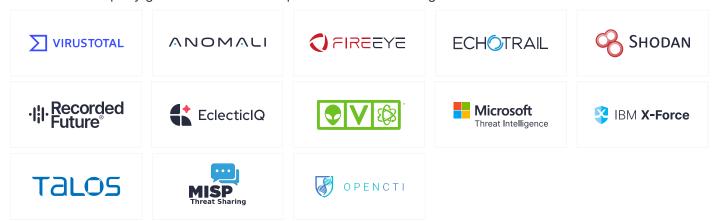
### **Detection Rule Repositories**

SOC Prime Platform acts as a single point to access Detection-as-Code content-both open-source and proprietary. We integrate external open-source repositories maintained by industry leaders while adding critical security context, threat intelligence, and MITRE ATT&CK tags since 2018. Our AI SOC Ecosystem allows getting high-quality feeds for a wide range of cybersecurity use cases, including edge and cloud.



## **Threat Intelligence**

By integrating with TIPs, we generate a new layer of threat intelligence and enrich detection rule context. Also, we enable IOC guery generation based on open-source and leading commercial vendor data.



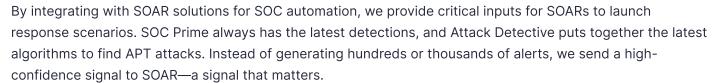
# **Vulnerability Management**

SOC Prime integrates with vulnerability management systems to prioritize detection rules against the latest exploits as reported by vendors and generate a new layer of intelligence that combines Detection-as-Code and vulnerability intelligence. This ensures that in addition to the detection itself, you are all set in terms of priority, compliance, and patching.





#### SOAR





#### **CMDB**

SOC Prime supports integrating with CMDB software to support the Detection-as-Code process in terms of workflow governance and management for detection rule development, tuning, and deployment, as well as automatic ticket creation in case of detecting APT threats with Attack Detective, thus completing threat hunting process.











Confidential and Proprietary. Do not distribute without consent. © 2025 SOC Prime, Inc. All Rights Reserved

#### **How to Become A Partner?**

Contact Sales at <a href="mailto:sales@socprime.com">sales@socprime.com</a> to learn more about the benefits of Al SOC Ecosystem and discover how our projects can elevate your security operations. You can also get in touch with us to explore partnership <a href="mailto:opportunities">opportunities</a> and drive the future of cybersecurity together.

Become a Partner