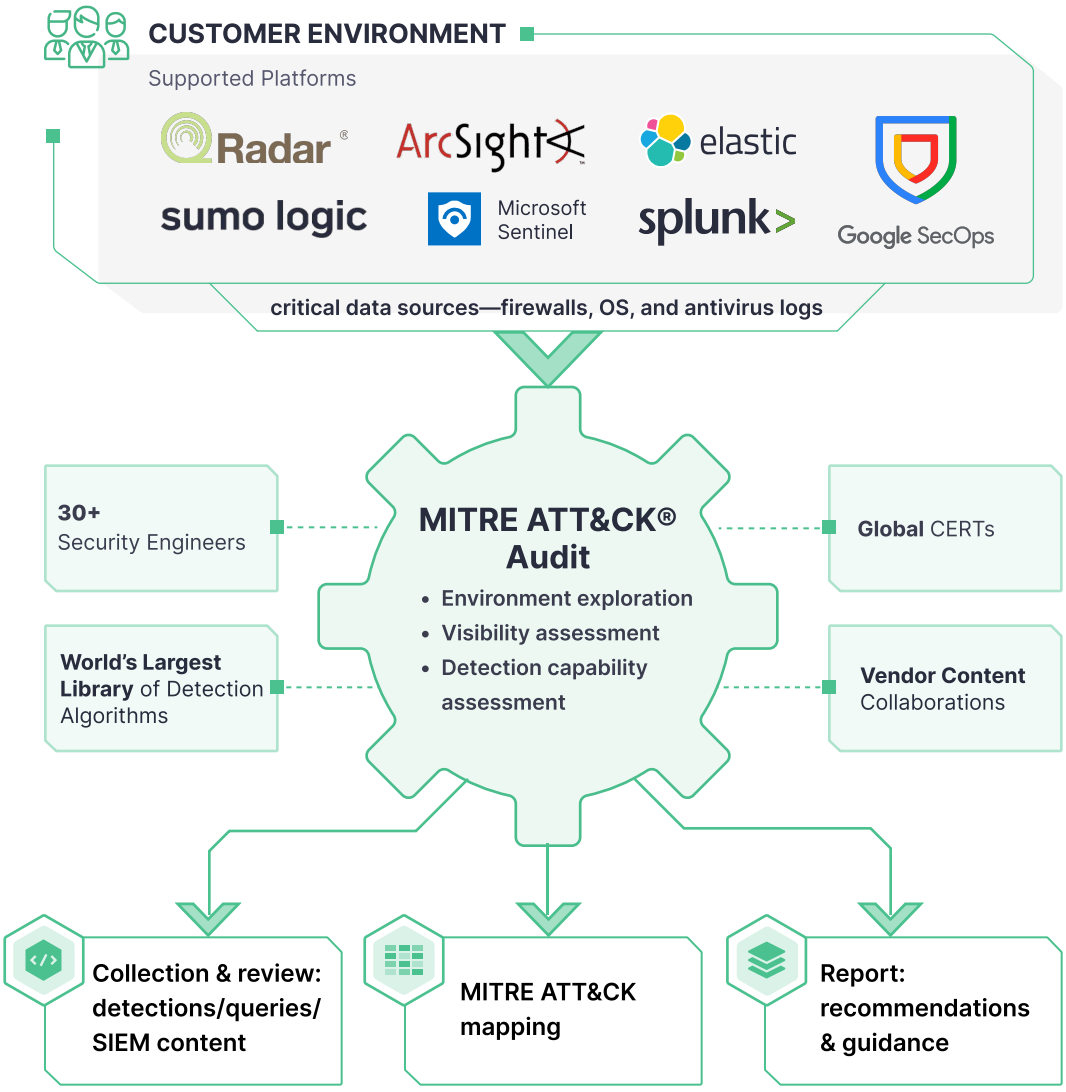
MITRE ATT&CK® Audit

SOC Prime's Professional Services team takes a data source-centric approach to delivering the MITRE ATT&CK audit. Our experts ensure your critical data sources—firewalls, OS, and antivirus logs—are optimized for maximum security performance and readiness.



150+

MITRE ATT&CK audits delivered

30%

Boost in log source & detection coverage as per ATT&CK within the 1st month

5+

Years of experience in MITRE ATT&CK auditing

Highlights

- Improve log source & detection coverage as per ATT&CK
- Enhance attack surface visibility tailored to business-specific threats
- Gain actionable recommendations on addressing existing security gaps
- Maximize the ROI of your cybersecurity tool investments

What it Covers	Results
General visibility of MITRE ATT&CK	■ Organization has comprehensive visibility of data for detection and response
Availability of data sources	■ Events make it into the SIEM & EDR environment from a relevant data source ■ All possible agents report to the SIEM & EDR environment ■ Filtering of data sources is appropriate
Usability of data sources	■ Data sources are parsed into appropriate fields ■ Additional fields are added to be used by SOC Analysts ■ Data source follows a common data schema

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. In 2018, the SOC Prime Team pioneered tagging Sigma rules with MITRE ATT&CK, and in 2023 the company became the world's first MITRE ATT&CK Benefactor.

SOC Prime Expert Team

30+

Seasoned experts

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.

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