Autonomous SOC

for MSPs, MDRs, MSSPs, and Enterprises

SOC Prime, a long-established and respected leader in the Security Operations industry, curates a platform that delivers an autonomous SOC to MSPs, MDRs, MSSPs, and enterprises to help them address the most pressing security challenges.

SOC Prime Ecosystem

Threat Detection Marketplace

World's largest library of detection rules and actionable threat intelligence

Attack Detective

Industry-first SaaS serving real-time, researched, and packaged threat detection & hunting capability

Uncoder AI

Integrated development environment and co-pilot for detection engineering

SOC Prime ECOSYSTEM | DataHelix AI | SOC Prime ECOSYSTEM

DataHelix AI - Rule-Less Logic

Machine learning algorithms and models that do not rely on platform-specific rules are added to the detection stack to discover and hunt for threats that would not otherwise be detected by traditional rule-based use cases.

SOCs Challenges:

- Multiple attack surfaces due to multiple clouds, OT, DevSecOps, etc.
- High volumes of mundane, repetitive tasks
- Need for additional sources on data ingestion to assemble the necessary telemetry and make informed decisions

SOCs Challenges:

- Evolving attackers' toolkit and skillset to circumvent traditional SOC approaches
- Excessive alerts, weak correlation, missing context, and increased false positives complicate detection
- Response and containment is often simply not fast enough
- Significant pressure on human resources, skill levels, and training

Autonomous SOC Approach

The next-gen SOC approach fuses traditional threat detection with AI and machine learning, distributed multi-tier automation, and real-time threat intelligence to automate and scale cybersecurity workflows. While typically SIEMs miss 80% of logged data, organizations can automate as many security operations processes as possible to enable an MDR to scale with an autonomous SOC approach backed by DataHelix AI as part of SOC Prime ecosystem.

Benefits

- **ML-Enriched Detection:** Combines traditional rule-based detections with ML-based techniques
- **Platform-Agnostic:** Apply ML-based detections to any dataset or data plane—logs, email, web, network traffic, SD-WAN, etc.
- **MDR Creates Its Own Threat Intelligence Cloud:** The ability to threat hunt all data planes enables new Sigma rules to be propagated through to the SIEM and to other customer environments
- **Resource Scaling:** Automate SOC T1–T3 Analyst work
- **New Services:** Automation means new monetized services can be rolled out with minimum cost—e.g., Threat Hunting and Phishing Detection Service

DataHelix AI: Next-Gen Autonomous SOC Solution

DataHelix AI represents a next-gen autonomous SOC solution that leverages automation at multiple layers within the SOC. A key feature of the platform is that it is completely data-agnostic, meaning it can support any data plane, including logs, API calls, databases, network packets/traffic, email, web proxies, SIEMs, SD-WANs and bespoke applications.

DataHelix applies the same detection logic and threat-hunting algorithms to all data planes, ensuring that “no stone is left unturned.” The platform is available as an on-premises solution (ideal for air-gapped customers), a hybrid solution, or a cloud-based solution. The MSP version is designed to be installed and operated within MSP’s own cloud infrastructure, enabling them to brand their own Autonomous SOC solution.

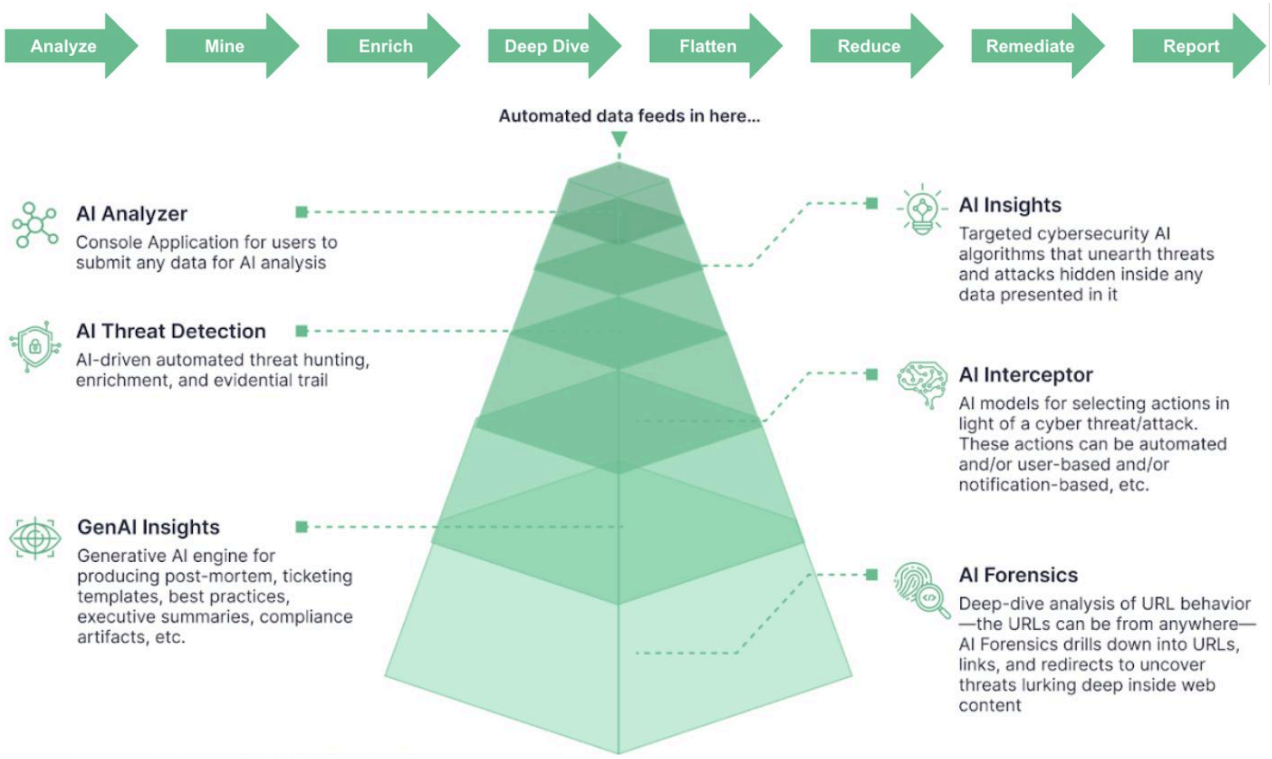
Highlights

- DataHelix AI flattens and evidences **100,000s** of bad things that SIEM rules miss
- **10-100s** of alerts prioritized by criticality and auto-remediate breakdown
- Over **95%** reduced workload on SOC teams coupled with increased efficiency & scalability
- Of many of the alerts DataHelix AI detects, **99%** of these are not, and would not be captured by the SIEM rule set
- Hidden threats that may not emerge immediately, continuously threat hunted and detected over longer periods of 3–6 months
- MSPs encourage customers to log more and charge for this “Data Lake” threat-hunting service, ideally stored within the MSP cloud

Powered by Multi-Layered Machine Learning and AI

The multi-layered use of AI and machine learning enables DataHelix AI to process vast data volumes, providing MSSPs and MDRs with the ability to ingest more data for a clearer security view. Unlike traditional SOCs that limit logs due to cost and complexity, its autonomous engine handles massive datasets, delivering actionable insights and automated triage. The platform supports MSP-hosted data lakes for extended storage and continuous threat hunting, detecting hidden threats over months. Being platform-agnostic, it also analyzes bespoke applications, offering MSPs a valuable service for diverse industries.

The Six Levels of SOC Prime DataHelix AI – Multilayer Machine Learning and AI

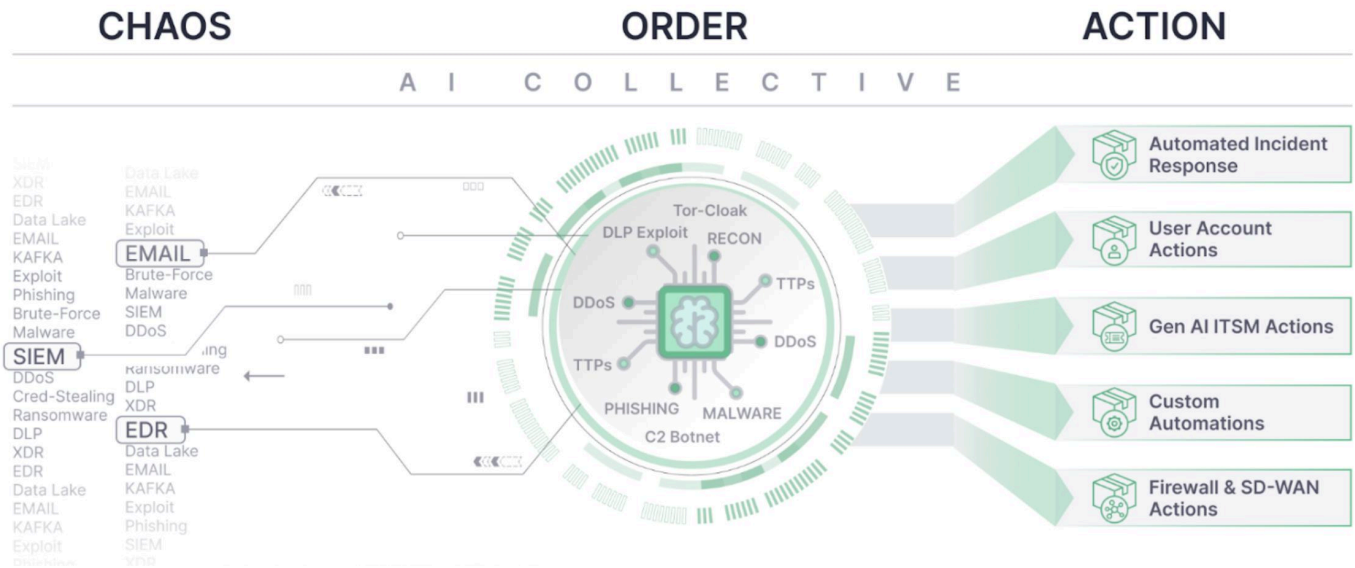


Different Feeds & Formats Analyzed at Scale

DataHelix AI surfaces real-time Indicators of Compromise (IOCs) and threat intelligence information gathered from global feeds, such as email, web traffic, and network packet capture. This real-time IOC information is then automatically packaged into detection rules that can be applied within the SIEM, EDR, CASB, and email configurations to further threat-hunt the estate and improve on “Lessons Learned.” In MDR environments, this can be applied across multiple customers, with all benefiting from the MSP-branded Cyber Collective, effectively creating the MSP's own Cyber Threat Cloud.

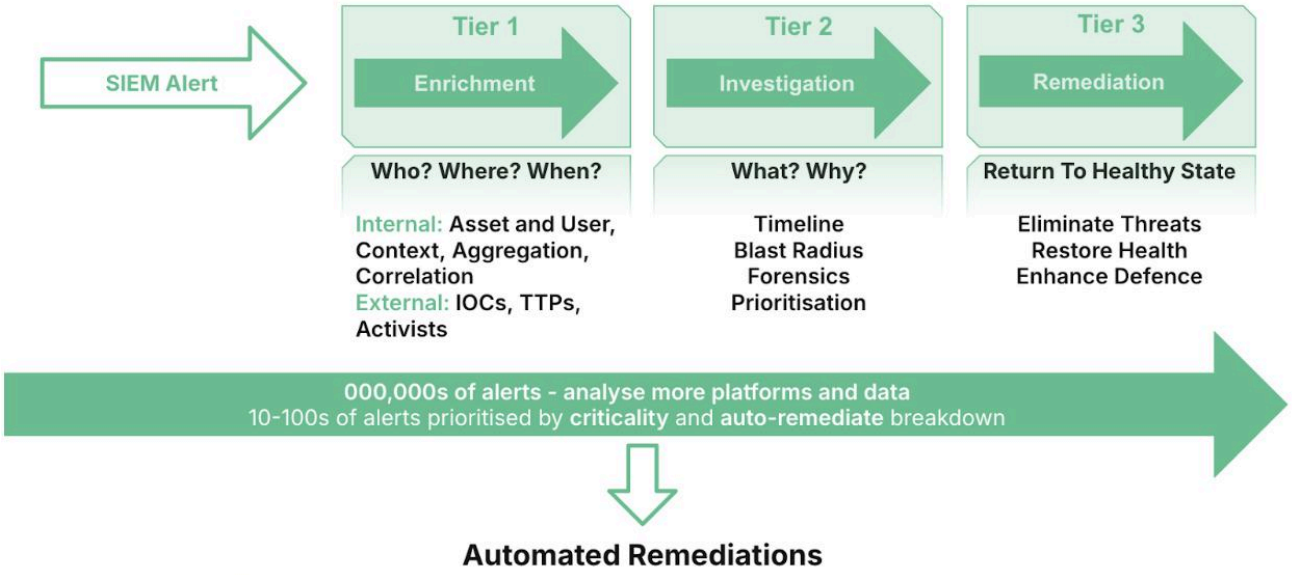
Different Feeds and Formats Analysed at Scale

We analyse the morass of telemetry to include ALL SIEM, EDR and other security & infrastructure alerts and logs and detect threats at scale. The DataHelix AI logic is behavioural and constantly updated with emerging threat intelligence



Resource Scaling

DataHelix AI does more than detect; it also automates the SOC Tier 1–3 Analyst tasks. Once it has processed the data, correlated, and flattened security alerts into real incidents, it categorizes their priority. The platform then provides the option to automate most of the remediations or mitigations. This significantly reduces the workload on the SOC by up to 95–99%.



Start applying AI and Automation to your SOC now, with expert guidance from us! For more details on the Autonomous SOC approach powered by DataHelix AI, reach out to your local sales representative at sales@socprime.com or kick off your journey with SOC Prime at https://socprime.com/.