Autonomous SOC Services

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.

SOC Prime Ecosystem

Threat Detection Marketplace

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

SOC Prime ECOSYSTEM

Attack Detective

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

DataHelix AI

Uncoder AI

Integrated development environment and co-pilot for detection engineering

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.

DataHelix AI: Next-Gen Autonomous SOC Solution

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

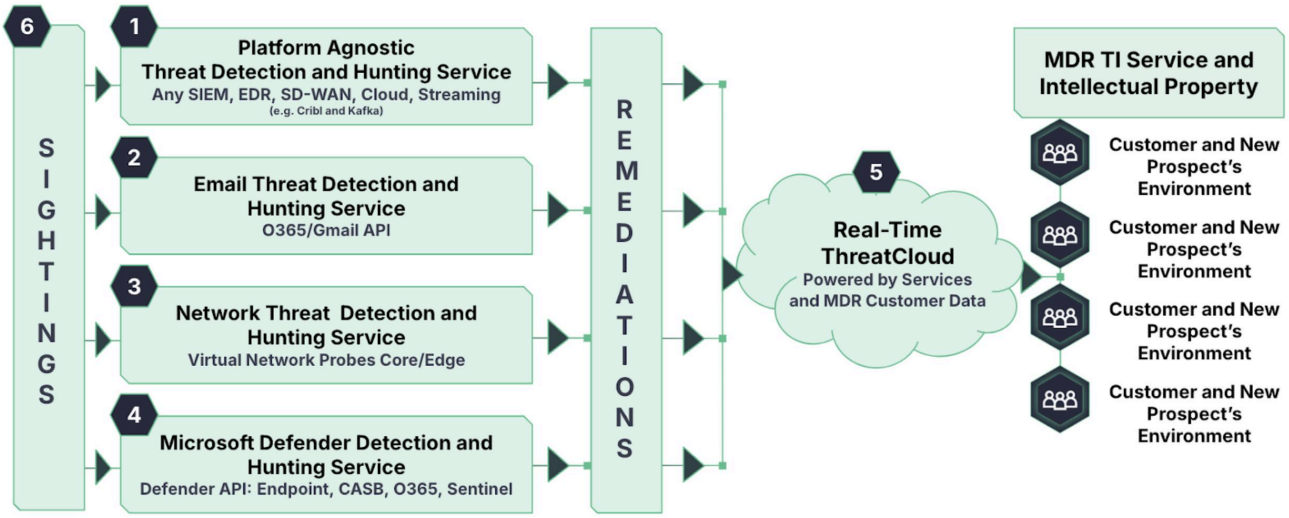
- **ML-Enriched Detection:** Combines traditional rule-based detections with ML-based techniques
- **Platform-Agnostic:** Apply ML-based detections to any dataset or data plane—logs, email, web, network traffic, SD-WAN, etc.
- **MDR Creates Its Own Threat Intelligence Cloud:** The ability to threat hunt 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 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. 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.

Autonomous SOC Services

For service providers, the autonomous SOC approach opens the door to the following service offerings:

- Native SOC Service – with a SIEM or without
- Email Threat and Phishing Detection App
- Network Detection and Response (NDR)
- Microsoft Advanced Threat Hunting App
- Threat Cloud
- Threat Intelligence (TI) Sightings-powered detections & Threat Hunting



Native SOC Service

DataHelix AI augments existing SIEM architectures, enhancing detection across all security tools while automating SOC processing and remediation. This drives significant resource savings for MSSPs and ensures 100% retention of log and storage costs in-house. Additionally, its ThreatCloud, generated from customer data, forms proprietary IP that can be targeted at vertical-specific markets (e.g., Emergency Services). This enables MSSPs to offer an automated SOC & Threat Hunting service—such as an “Advanced Data Lake SOC” (ADLS) or “Total Infrastructure Hunting Service” (TIHS)—that is scalable and cost-efficient, unlike traditional MDR and SIEM solutions.

Email Threat and Phishing Detection App

DataHelix AI’s Phishing Detection & Response (PDR) seamlessly integrates via API with popular email platforms such as Microsoft 365 Copilot and Gmail. It applies DataHelix AI’s threat detection and hunting algorithms to all email content, including attachments and, more importantly, embedded web links within emails, to detect all phishing attacks targeting the organization. This Phishing Protection service could be the first offering that an MDR launches to its customer base, quickly followed by the traditional DataHelix AI SOC service, as mentioned earlier.

Network Detection and Response (NDR)

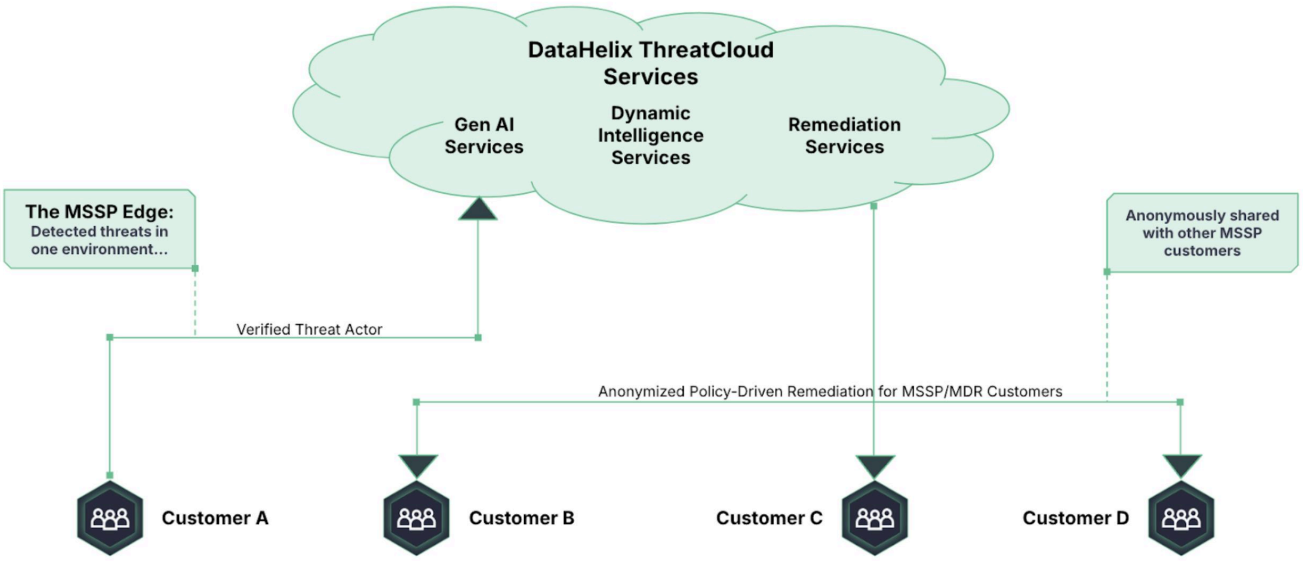
Most SOCs lack comprehensive network telemetry, limiting their ability to analyze the full kill chain of incidents. DataHelix AI’s Network Detection & Response (NDR) solution addresses this with virtual probes that inspect all internal and external traffic using ML-driven threat detection. These probes, deployed across multiple network segments, generate real-time IOC data, which is automatically integrated into the latest threat detection rules. These rules are then fed into the SIEM, EDR, and MSP Threat Cloud, enabling MSPs to conduct proactive threat hunting across all customer infrastructures.

Microsoft Advanced Threat Hunting App

DataHelix AI provides advanced enrichment and SOC automation to the Microsoft Defender platform. DataHelix AI and SOC Prime Threat Detection Marketplace connect via API to a suite of detection tools from Microsoft—Defender for Endpoint, O365, Cloud, Sentinel, and more—to uncover threats the Microsoft stack alone may miss. Additionally, DataHelix AI adds context, corrects miscategorized incidents, and streamlines triage for more accurate threat management. Beyond detection, DataHelix AI adds context, corrects miscategorized incidents, and streamlines triage, ensuring accurate and efficient incident management across all Defender tools.

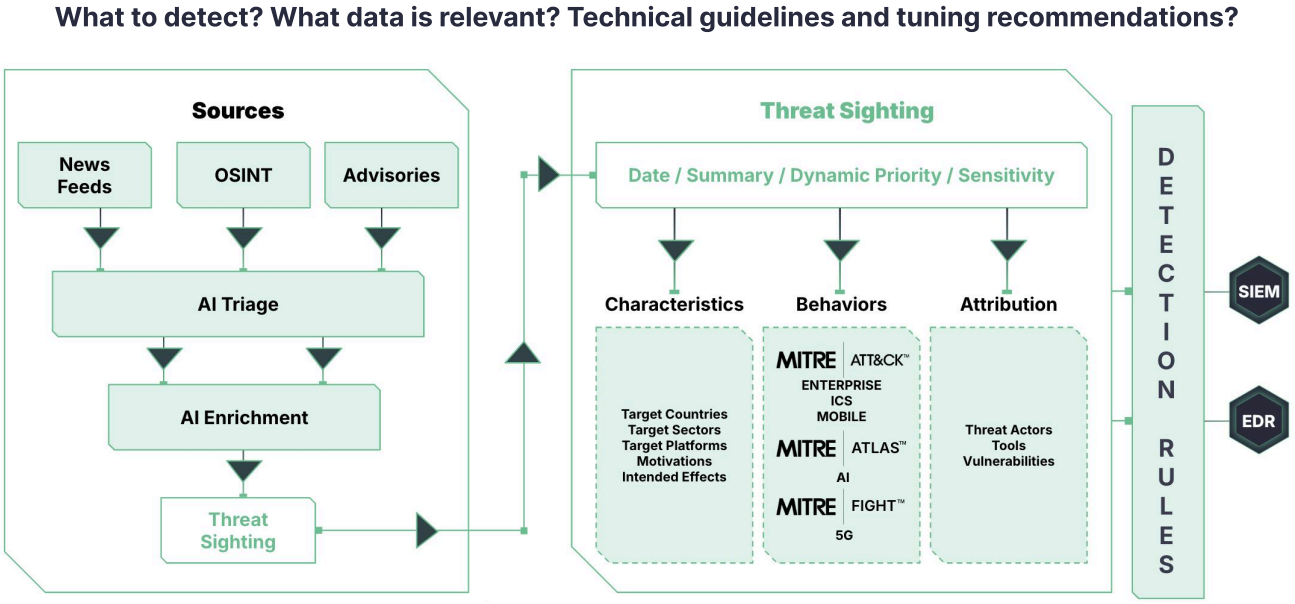
ThreatCloud

As MSPs deploy services to multiple customers, they gather valuable threat intelligence through DataHelix AI, analyzing emails, attachments, web traffic, and logs to detect real-time threats. With DataHelix ThreatCloud, MSPs can create their own branded Threat Intelligence service, hosted within their cloud tenancy, and deliver it to all customers, even those without a full SOC offering. This not only enhances service portfolios but also builds the MSP's brand and intellectual property.



Sightings-Powered Detection

DataHelix Sightings analyzes external threat intelligence, offering real-world insights based on industry, geolocation, TTPs, and specific adversaries, then applying them to your automated SOC. While IOCs like IPs and hashes help counter immediate threats, they often lack strategic context for executive decision-making. By tracking adversaries, tools, and associated techniques, customers can better identify and prioritize risks, but traditional methods miss key context—such as when a technique was last used—making it harder to assess and act effectively.



Data-Driven Insights

DataHelix Sightings monitors over 300 news feeds, including regional news, government CERTs, and open-source intelligence. Powered by AI, it then triages and enriches these feeds, linking them to relevant sectors, motivations, and attack locations.

Benefits & Capabilities

- **Behavioral Analysis:** Each article is enriched with techniques, adversary, and tool attribution, creating a comprehensive picture of the threat landscape. Supporting MITRE ATT&CK®, ICS, Mobile, Atlas, and many more.
- **Dynamic Prioritization:** Sightings are prioritized based on their relevance over time. Unlike static lists, Sightings dynamically adjusts priorities, ensuring your organization focuses on the most relevant threats.
- **Automation Workflow:** Sightings and TDM enable programmable customization of threat sighting priorities, to activate relevant use cases covering flagged TTPs.

This smart use of threat intelligence is very powerful as it allows MSPs to now have verticalized threat-hunting services that they can apply to their customer base while essentially adding even more intellectual property to the MSP cybersecurity stack.

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/.