Network Detection & Response

Key Component Within an Autonomous SOC

The trend in the Managed Detection and Response (MDR) marketplace is moving towards a fully automated or Autonomous Security Operations Centre (ASOC) model using AI/ML to automate as much as possible, including ingestion, processing, and remediation. SOC Prime and its Ecosystem partners, like SOCAutomation serving DataHelix AI, work together to deliver an autonomous SOC to MSPs, MDRs, MSSPs, and enterprises. Together, we focus on automating key pain points that all SOCs encounter, including SIEM/EDR, Email & Phishing Triage, and Network Traffic Analysis.

Network Detection & Response (NDR)

Network logs provide detailed records of network traffic, including connections, applications, and protocols across the network. They are essential for detecting malicious activity, often seeing attacks early in the kill chain. However, network logs generate an immense volume of data that could overwhelm any SIEM. Instead of tuning network data and risking the loss of critical security metrics, the “brain” engine, DataHelix AI, processes ALL network telemetry data at scale. It applies SOC Analysis Processing and workflows, including enrichment, tuning, correlation, and alert flattening, to produce highly tuned Incidents.

Virtual network probes (NDR Probes) can be configured at ingress/egress points, core switches, branch locations, cloud environments, and SD-WAN architectures, ensuring full network visibility at scale. However, the platform goes beyond visibility—it also remediates many of the incidents it receives. This capability is a game-changer, as most SOCs already struggle with alert fatigue, and processing additional telemetry without automation would be a significant challenge.

True Threat Intelligence (TTI)

What makes DataHelix AI unique is its ability to automatically leverage real threat data within NDR, combining it with threat intelligence (TI) from multiple sources—third-party vendors, vertical industry insights, CERTs, Bulletins, and TI platforms. This approach provides a real-time answer to the critical question: "What is attacking me right now?" Unlike traditional threat intelligence, which often relies on hypotheses, True Threat Intelligence (TTI) is derived from real production events and live network traffic, delivering security insights based on facts.

DataHelix AI and its advanced models provide a comprehensive view of infrastructure security, while its natural language capabilities allow users to interact with their security data intuitively. Now, any IT or Compliance team member can query the organization's security posture in real time covering the following:

- List all phishing attacks detected in my environment last month and their current status
- Show me trending vertical industry attacks that have impacted us
- Which security tools are generating alerts, and which are not?

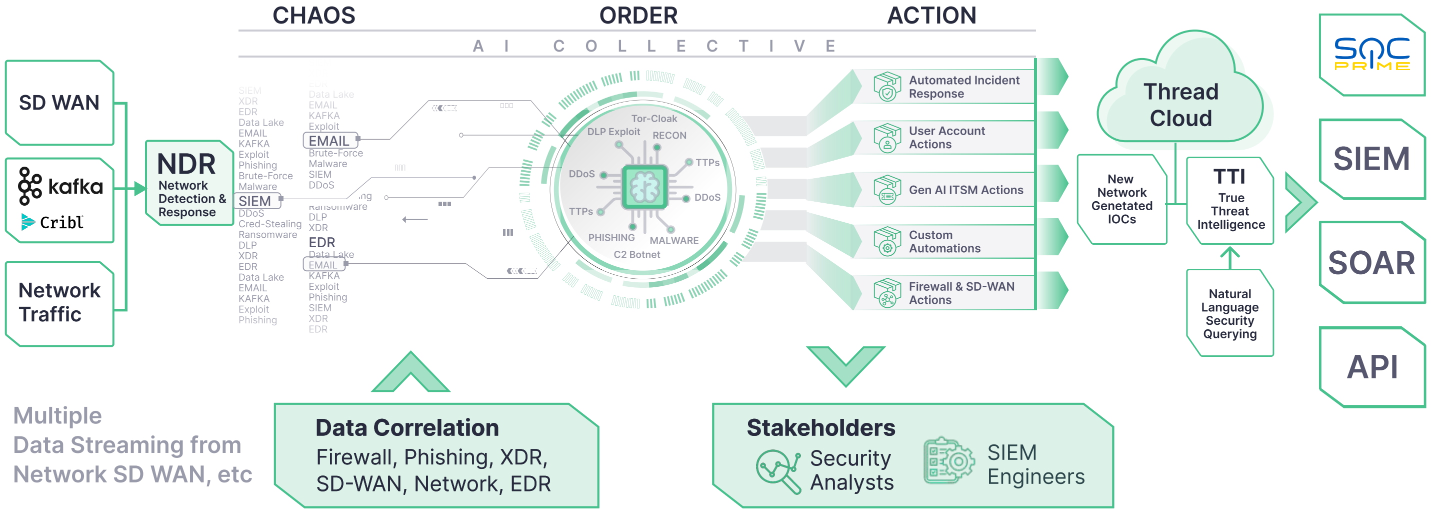
With DataHelix AI, security insights become accessible, actionable, and rooted in real-world data, empowering organizations to make informed decisions with precision.

AI-Driven Security Operations and Response (AI SOAR)

The incidents generated by True Threat Intelligence (TTI) can be automatically remediated through the platform’s automated SOAR capability. A key advantage is that the same detection logic seamlessly applies across any dataset—whether email, web, logs, endpoint, or other telemetry sources.

The platform not only illustrates the volume and variety of telemetry that the SOC can now handle but also reduces the overall workload. While incident volumes may increase, much of the remediation process is automated, allowing SOC teams to focus on more critical security challenges.

Machine learning across network traffic generates new IOCs that automatically generate Sigma rules to query the whole MDR infrastructure. Can be run on-premises, hybrid or cloud, and can be hosted within an MSP to service their customers.



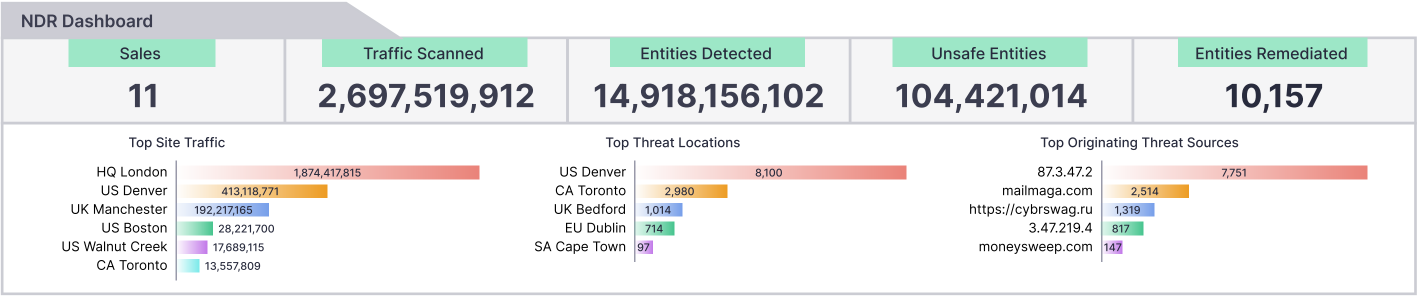
Multiple Data Streaming from Network SD WAN, etc

Data Correlation
Firewall, Phishing, XDR, SD-WAN, Network, EDR

Stakeholders
Security Analysts
SIEM Engineers

Analyze → Mine → Enrich → Deep Dive → Flatten → Reduce → Remediate → Report

NDR Dashboard


NDR Dashboard

Sales	Traffic Scanned	Entities Detected	Unsafe Entities	Entities Remediated
11	2,697,519,912	14,918,156,102	104,421,014	10,157

Top Site Traffic

HQ London	1,874,417,815
US Denver	413,118,771
UK Manchester	192,217,165
US Boston	28,221,700
US Walnut Creek	17,689,115
CA Toronto	13,557,809

Top Threat Locations

US Denver	8,100
CA Toronto	2,980
UK Bedford	1,014
EU Dublin	714
SA Cape Town	97

Top Originating Threat Sources

87.3.47.2	7,751
mailmaga.com	2,514
https://cybrswag.ru	1,319
3.47.219.4	817
moneysweep.com	147

Benefits

- **End-to-End Platform:** Threat Intelligence, Detection, SOC Analysis, and Remediation
- **Virtual Probes:** Monitor internal, external, cloud, and SD-WAN traffic
- **Automated Processing:** Scales enrichment, tuning, correlation, and alert flattening into highly tuned incidents
- **True Threat Intelligence (TTI):** Based on real-world production events and network traffic
- **SOC Automation:** Automated Tier 1-3 SOC analysis integrated into Incident Response
- **Incident Auto-Remediation:** Reduces manual workload for SOC teams
- **Natural Language Querying:** Easily assess infrastructure's security posture
- **Enterprise Threat Cloud:** Created and maintained to be used in Threat Hunting and defense against longer-term "Living-off-the-Land" attacks

Start applying AI and Automation to your SOC now, with expert guidance from us! For more details on NDR 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/.