SOCAutomation

DATA SHEET

DataHelix™

Cross Platform Detection and Response

SOCAutomation's DataHelix platform is powered by an advanced AI Data Interrogation engine which is designed to seek out hidden threats, inside any data.

DataHelix™ leverages Artificial Intelligence and Machine Learning to detect and hunt advanced threats, employing sophisticated decision making using statistical analysis, networking, indexing and cross correlation techniques to deliver logic that mimics a SOC Analyst's eyes and knowledge re: processing alerts, email, and data to identify attacks. These machine eyes act like Cyber Security experts…at scale.

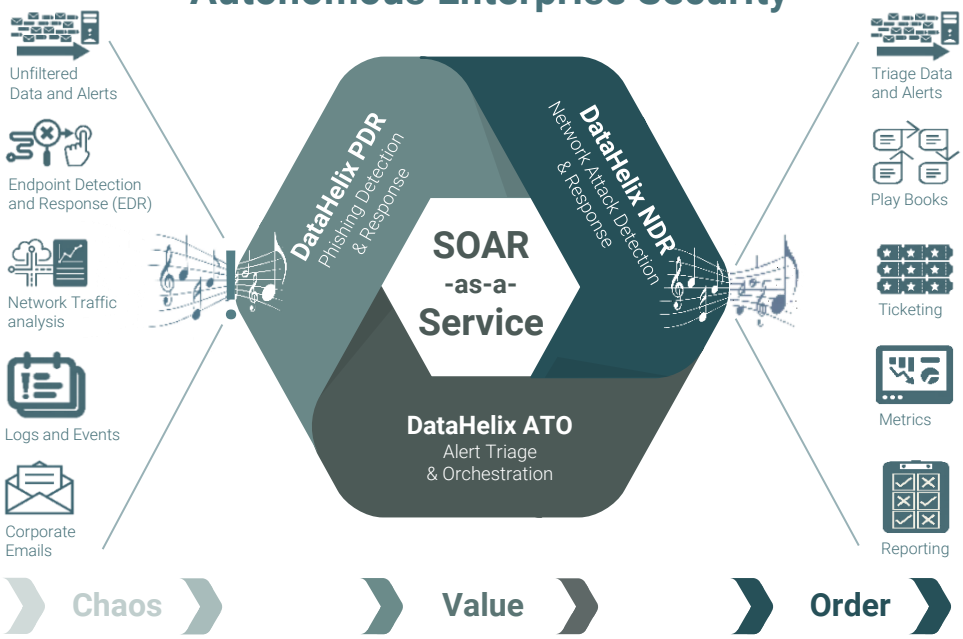
Data Centric Threat Hunting

DataHelix is a highly distributable data interrogation engine that can be deployed at the edge rather than bringing all the data into a centralised log store or SIEM.

Threat Hunting of; data, emails, events, alerts, files, and network packets can be carried out locally at speed and with agility, working with any infrastructure or security platform. The value here is that it can detect security threats using whatever existing security controls and tooling a customer already has in place.

In addition, if the customer is missing any key detection components such as Network Traffic Analysis or a SIEM, DataHelix can be configured to automatically create instances of these to plug gaps quickly for a customers' security monitoring visibility.

Autonomous Enterprise Security



So Why DataHelix?

DataHelix detects multitudinal threats and automates Incident Response across all security planes, with functionality covering the following areas;

- Cross Platform Detection & Response–XDR
- A SIEM Data-Lake
- Security Orchestration & Response SOAR
- Breach Attack Simulation (BAS)
- Threat Intelligence TI

The Benefits

- Faster than a SIEM Edge compute model gives immediate threat hunting results
- Combines XDR + SIEM Data Lake + SOAR + BAS + TI
- SaaS, On-premises or Hybrid deployment options
- In-built Automations 'security apps' for security operational tasks
- Advanced-automated threat hunting & compliance platform–always on-duty, hunting and preventing
- Utilising automation and orchestration throughout the investigation and triage stage
- Performs to Scale

socautomation.com
+44(0)1582 369330