SOCAutomation

DATA SHEET

DataHelix™ NDR

Network Detection and Response

DataHelix NDR, Network Detection & Response detects sophisticated attacks by diving into the depths of raw unstructured network traffic.

DataHelix NDR 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.

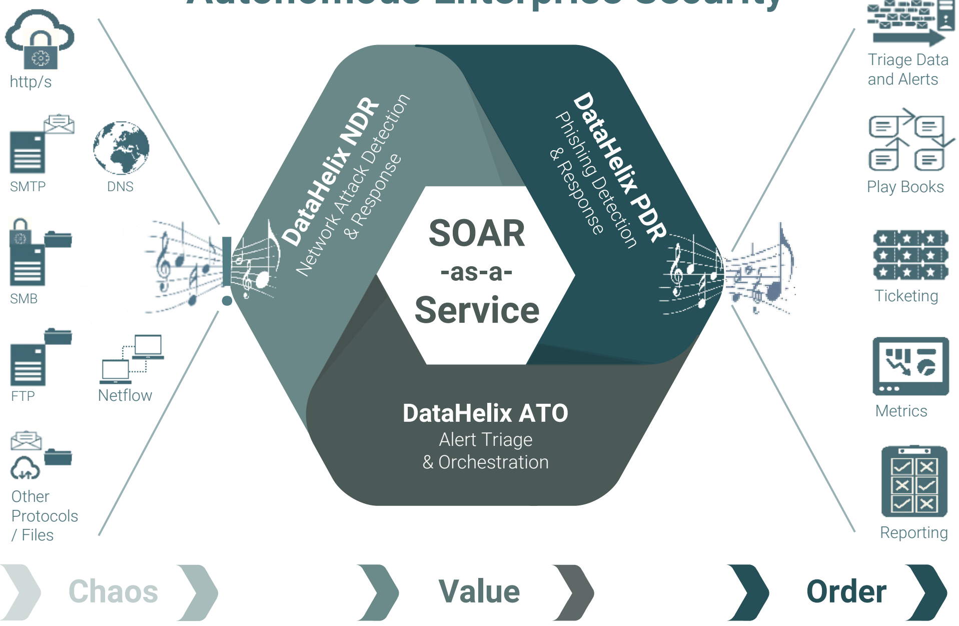
DataHelix NDR

Hidden within the morass of data flowing in and through your network, both cloud and on-premise, DataHelix NDR provides a level of security visibility not possible until now.

With DataHelix NDR suspicious content is detected in machine-time, triggering real-time automated responses. Incident Response playbooks can be auto-triggered to execute tasks such as ticketing integration and multi-security tool orchestration or even threat hunting across other platforms/tools based on NDR detection findings.

The network and network data provides invaluable context for incident response and threat hunting and is typically a missing component within a cybersecurity Investigation. Network probes can be difficult and costly to correctly configure to 'see' all relevant traffic processing the network traffic at source.

Autonomous Enterprise Security



Why DataHelix NDR?

- Fleshes out unusual suspicious behavour with network traffic
- Provides invaluable context for incident response and threat hunting
- Covers all network protocols, files, and applications
- Distributed deployment options enable data inspection to be applied on remote sensors and third party network data stores

The Benefits

- DataHelix NDR probes can be spun up as needed in the cloud
- On Premise or Hybrid Environments
- Processing Network Traffic at source
- Reduction in shipping across costly bandwidth
- Covers vast amounts of network protocols using State-of-the-Art Network Attack Detection
- Sends only surfaced detections and alerts to the Automation portal or console
- Performs to Scale

socautomation.com
+44(0)1582 369330