SOCAutomation

DATA SHEET

DataHelix™ ATO

Alert Triage and Orchestration

Maximize your security investment with DataHelix ATO Alert Triage and Orchestration. Automate your security tools and processes – Quickly and Easily.

DataHelix ATO connects all your security technologies, tooling, and security processes into a unified holistic security machine to deliver round-the-clock cyber security surveillance at scale. Finally, your security staff can get on with security, rather than tweaking endless systems and tuning down alerting to fit. Now your team can handle any amount of alerting because ATO is handling the drudge work by triaging and executing qualification, freeing your staff to do real security work.

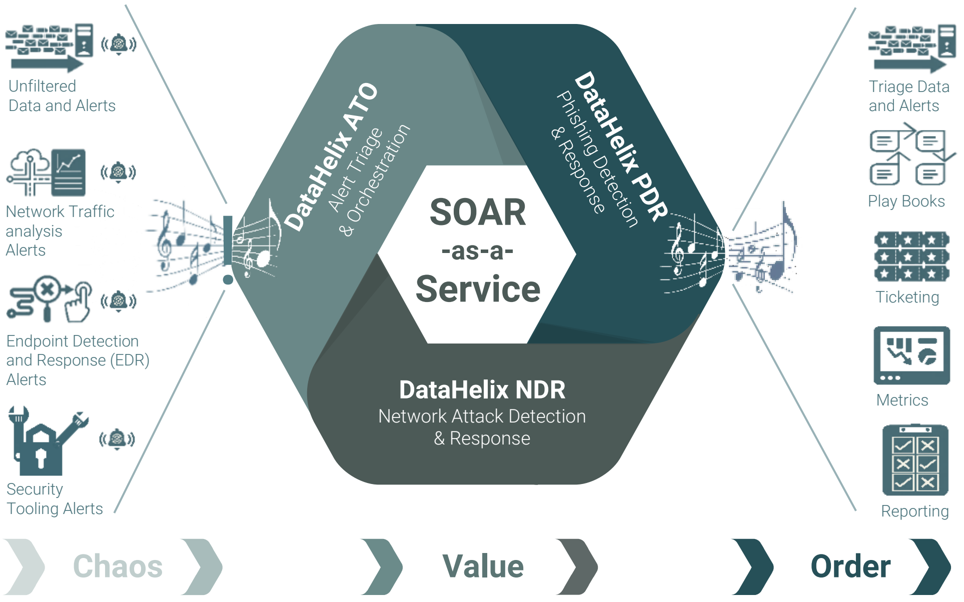
DataHelix ATO

DataHelix ATO collects 'unqualified' and 'uncontextualised' alerts from existing security tools and applies machine learning and logic to ascertain whether they are valid and not false positives, essentially doing the work of a security analyst, but at scale and benefits from being always on, 7/24/365 days a year.

DataHelix ATO uses the power of all security and infrastructure tools an organisation possesses, chaining them together to perform Cross-Platform Detection & Response (XDR) enriching this with contextual data from a company's asset/stakeholder application feeds and threat intelligence sources.

This 'SOC-in-a-BOX' approach enables your security team to process ALL alerts coming in from their security tooling, so no alert is ignored or 'tuned out', enabling them to focus on true incidents and security work.

Autonomous Enterprise Security



Why DataHelix ATO?

- Does not tune out alerts, processes them all to ensure full visibility
- Automatic content enrichment, decision making, response and triage
- Allows security team focus on true critical incidents and investigations
- Cross platform detection and response (XDR)

The Benefits

- Allows security teams to scale to respond to ever increasing alerts
- 7x24x365 alerting and incident response 'Always On'
- Works with all security and infrastructure platforms, on premise, cloud or hybrid
- Maps and integrates with an orginisation's incident response playbooks, processes and ticketing systems
- Captures alerts from all security and infrastructure tools to enhance the power of these technologies to deliver holistic security across the organisation and cloud
- Performs to Scale

socautomation.com
+44(0)1582 369330