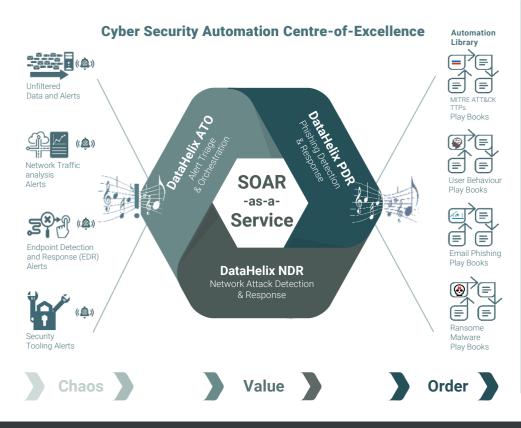# SOCAutomation

SOAR-as-a-Service

Autonomous Enterprise Security

Security Orchestration & Response (SOAR) tools are time consuming to design and configure and typically utilises much of a security teams' precious resources by engaging in systems engineering work rather than security analysis.

SOCAutomation SOAR-as-a-SERVICE

The SOCAutomation SOAR-as-a-Service platform delivers 'off the shelf' SOAR 'apps' as a fully managed SaaS/hybrid solution to automate your entire security infrastructure and your Security processes, delivering a Center-of-Excellence to your security landscape.

Now you can realise the full benefits of automation and orchestration without the stratospheric costs of an off-the-shelf manual SOAR toolkit. The huge library of apps includes Phishing Forensics, Network Detection and Response, Endpoint Threat Hunting, Vulnerability Management with Stakeholder Mapping Workflow, Bi-Directional Ticketing System Integration, all of which can be customised as part of the Service without any additional cost or customer resources required.

SOAR-as-a-SERVICE Main Features

- End to End Automation of the whole cybersecurity detection and response lifecycle
- SOC App library – 'off the shelf' SOAR 'apps' automating much of the day-to-day SOC work
- Pre-built Playbooks for orchestration of incident response tasks
- Cyber Security Automation Centre-of-Excellence – UK's first 'Security Automation Team'

The Benefits

- Automates detection and response, providing an 'Automated SOC'
- Scales to cover the ever increasing Cyber Security alert volumes
- Automation library and automation Centre of Excellence enable customers to focus on real security, not systems engineering and tooling
- Play Books enable a consistent approach to Incident Response across teams, tooling and processes
- Covers on premise, cloud and hybrid environments

Cyber Security Automation Centre-of-Excellence

Unfiltered Data and Alerts
Network Traffic analysis Alerts
Endpoint Detection and Response (EDR) Alerts
Security Tooling Alerts

DataHelix ATO — Alert Triage & Orchestration
DataHelix PDR — Phishing Detection & Response
DataHelix NDR — Network Attack Detection & Response

SOAR -as-a- Service

Automation Library
MITRE ATT&CK TTPs Play Books
User Behaviour Play Books
Email Phishing Play Books
Ransome Malware Play Books

Chaos ＞ Value ＞ Order