SOCURA

Managed Detection and Response

24/7 threat containment

Service Definition

hello@socura.co.uk

Table of Contents

Managed Detect and Response Service (MDR)

Socura's Managed Detection and Response (MDR) service offers a 24x7 proactive threat detection, hunting and response capability that identifies and contains cyber threats in near real-time. The service is designed to protect customers from data breaches, reduce attacker dwell time and defend against loss of business operations through malicious activity.

Service Features

- 24/7/365 Threat monitoring & detection
- Threat and breach containment
- Incident management, remediation advice
- Unlimited security data ingestion - fixed price, full visibility
- Endpoint, Network and Cloud Monitoring
- Threat Intelligence
- Threat Hunting
- Security Incident Reporting
- Use Case Development
- Vulnerability monitoring
- Service portal including dashboards and incident management
- Dedicated Customer Success manager and Senior Security Analyst Champion
- Monthly or Quarterly Service Review

Service Benefits

- Reduced risk of data breach and business impact of attack
- Proactively detect malicious activity
- Reduce attacker dwell time from months to minutes
- Latest cyber technologies used to improve detection and response
- Subscription based service, reduced capital expenditure
- Complement in-house capability with our cyber experts, in a true partnership
- Unlimited Data Ingestion, no need to compromise on data sources
- Latest Global Threat Intelligence

Implementation Plan and Onboarding support

Provision of the service is conducted in 4 phases:

Phase 1: Planning and Requirements Gathering

The first phase of the Socura MDR deployment process is focussed on understanding the client's environment, business processes and key information assets. This information is gathered in a joint workshop with the customer. With this information, Socura will develop a deployment plan in conjunction with the client which is agreed by both parties before Phase 2 can begin.

Phase 2: Deployment

Socura will work with the client to deploy any necessary technology into the customers' environment to allow the monitoring, security telemetry and pro-active action to take place. Socura will conduct this work remotely, working in collaboration with the customer.

Phase 3: Tuning

Socura will implement tuning of the technologies deployed in a controlled way to ensure there is no adverse effect to the detection capability or business impact. This will be done in conjunction with the client. Socura will continue to tune the rulesets in this phase with the customer.

Phase 4: Service Go-Live

A service acceptance meeting will be held to review the progress made in all previous stages. If both the Customer and Socura agree that all acceptance criteria have been met, the service will now move into a live 24/7 service state under the full SLA.

Security Incidents will now be raised to the customer as they happen and regular service review meetings will take place to ensure the service is operating as planned.

Service Level - Security Incident Response

Security alerts are initially prioritised based on severity by the platform responsible for processing the security event data from the client environment. The Socura analyst team will then adjust the prioritisation as required based on their investigation.

Socura commits to having an analyst take named ownership of each alert within the following timeframes, once received by Socura systems:

SLA	Timeframe
Security Incident Response	< 1hr

Service Level - Service Availability

Socura's service is guaranteed to be available against this SLA:

Service	Monthly Availablity Service Level
Managed Detection and Response	99.9%

Business Continuity and Backup

All services are delivered from the cloud in a high availability configuration and are continually backed up, providing excellent levels of availability (99.9%). Data is provided online (hot) for customers for a minimum of 12 months, with greater retention periods available on request.

Service Constraints - Maintenance

All significant upgrades or changes to the Socura solution will be notified to the client 7 days prior to the change. Emergency changes will be notified to the client as soon as possible.

Most changes to the service require no downtime. If it is deemed downtime is required, then the client will be notified, and downtime will not exceed 4 hours in any single calendar month.

Service Levels will not apply during maintenance windows.

Ordering and Invoice Processes

Orders can be placed by completing the G-Cloud ordering process. We encourage customers to contact us using the details contained within our G-Cloud page to allow us to support you with any queries.

Invoicing will take place annually in advance based on the agreed contract that has been put in place between the customer and Socura Ltd. Invoices are payable within 30 days.

Termination

Termination of services will be in line with the expiry of the agreement, or through client request in accordance with the termination clause in the Terms and Conditions.

Socura will ensure that an orderly cessation of service is achieved, along with the removal of any deployed capability and any data destroyed in line with the agreed security principles.

The minimum commitment for services is twelve months.

After-sales support

Each client is assigned a customer success manager (CSM) as part of the service. The CSM is responsible for ensuring the client is satisfied with the service and is the first point of escalation for any service performance related issues or any client driven service change requests.

A formal review of the service performance will be conducted on a quarterly basis and will provide the client with the opportunity to identify and discuss any changes in business strategy which may impact the service delivery.

Technical Requirements

To enable Socura to collect the required security telemetry and respond to incidents, two pre-configured virtual machines (VM) will be provided to deploy into the customers network.

The VM appliance compute requirements (CPU, memory and storage) will vary depending on the size of the environment to be monitored. This will be clarified as part of the scoping process.

Socura will also collect security telemetry from cloud services via any available APIs.

In some cases, an endpoint agent will also need to be deployed to client devices. This is a small, self-contained installation package that can be deployed in the same way as any other enterprise software (SCCM, JAMF etc). Once installed, it will connect to the Socura service over the public internet using a secure, encrypted channel.

The Socura team will support the customer with these steps as part of the onboarding process.

Pricing

Pricing is per the pricing sheet available on the Socura G-Cloud page.

Further Information

If further information, or clarification is required, please contact hello@socura.co.uk

SOCURA

14 Shepherdess Walk, Hoxton, London N1 7LB

socura.co.uk