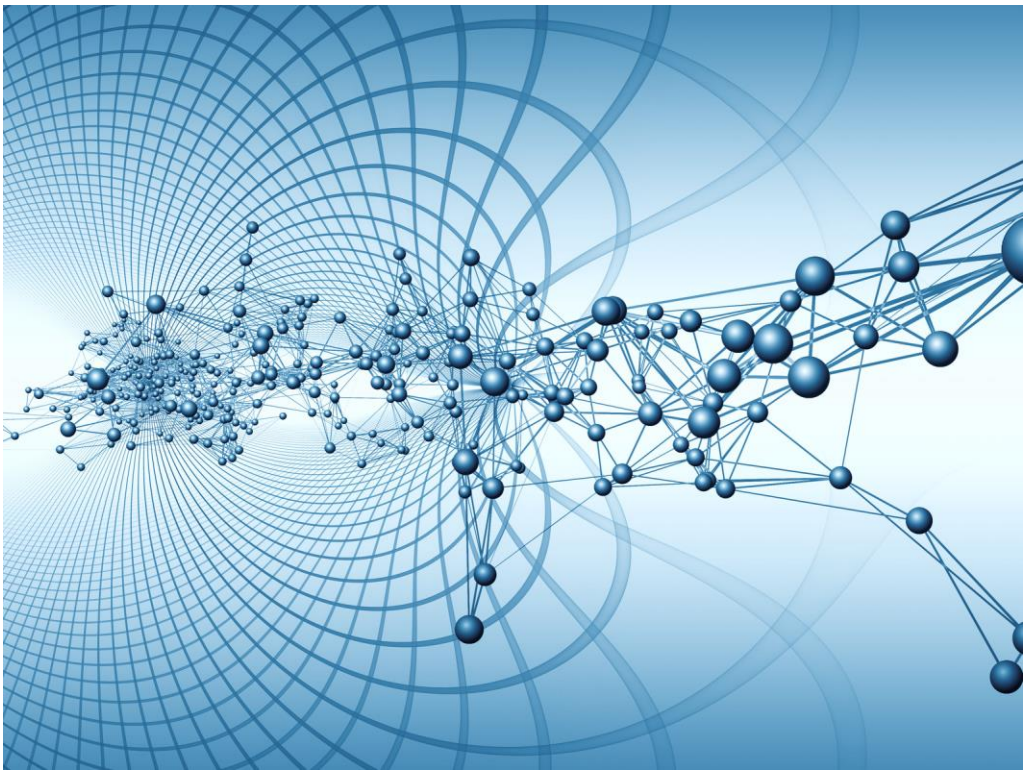
research·series
...founded on research

Virtual Cyber Security Operations Centre (vSOC) Service



Service Pricing

Issue Number	V1.5
Document Date	7th May 2018
Author	Research Series Ltd
Marking	OFFICIAL
G-Cloud	G-Cloud 10

Accreditations & Certifications

CESG Certified Professional

iisp

CSP A CATALYST FOR COLLABORATION

CYBER ESSENTIALS

Registered Office: 1 Meadway, Woodford, London, IG8 7RF.
Company Registered in England & Wales, No: 6633403
Website: http://www.research-series.com Email: info@research-series.com

e:(security·group)
Information and Security Assurance

Introduction

Our virtual cyber security operations centre (vSOC) service pricing is simple and easy to understand, making it totally transparent, and affording significant cost savings to the client.

The service is priced in four workstreams, the first and the fourth workstreams are optional.

Workstream 1 (optional): Requirements Gathering

This is a consultancy service we provide to our clients, to help them gather their SIEM or SOC requirements to ensure that their needs or requirements are met, and that they are focusing on the most important aspects of the service they require. This consultancy service is ensuring a risk-based, risk-prioritised and user-needs focused approach to requirements gathering for the client so that they know where to focus their effort, to categorise their assets, criticality and risk so that the protective monitoring is tailored to meet these requirements.

The rate / charge is based on the experience level, role and expertise of the personnel.

Table 1: Requirements Gathering Consultancy

Personnel/ Roles	Rate (per day)
Business Analyst	£680
Lead Security Architect	£1,500
Lead Security Information & Risk Advisor	£1,200
Project Manager	£1,200

Workstream 2: Implementation and Onboarding

Implementation and onboarding are focused on:

- Setting up of the sensor for the client to onboard the assets and environments to be monitored.
- configuring the log sources to send their security and event logs to our collector in real-time so that event can be analysed, correlated and assessed in real-time to identify, detect and mitigate risk, IoCs, threats and malware or policy violation.
- configuring netflow, heartbeat and snmp so that indicators of compromise in the information stream can be detected in real-time, and that monitoring is not just focused on

Registered Office: 1 Meadway, Woodford, London, IG8 7RF.
Company Registered in England & Wales, No: 6633403
Website: http://www.research-series.com Email: info@research-series.com

analysis of logs only.

- conducting asset discovery, vulnerability scanning to determine the assets in the monitored environment and any vulnerabilities that may exists in those assets.
- Configuring Open Threat Exchange (OTX) threat intelligence feeds that are downloaded and correlated against the data feed in real time.
- configuration, testing, and onboarding. Implementation and onboarding is a one-off charge for these set of deliverables as shown in table 2.

Table 2: Implementation and Onboarding Charges

Service Onboarding	Cost
Small (up 50 log sources or 500 EPS[1])	£15,000.00
Medium (up to 100 or 1000 EPS)	£30, 000.00
Large (up 250 or 2500 EPS)	£60,000.00

Workstream 3: Security Monitoring (Monthly Service Charges)

Security monitoring is a continuous monitoring of service based on the SLA of 9:00 to 17:00 Mondays through Fridays real-time monitoring, raising of alerts, correlation of logs, and cyber security incident response, reporting and escalations, ticketing and customised service reporting. This charge is monthly, as shown on table 3.

Table 3: Security Monitoring Monthly Service Charges

Security Monitoring	Rate (per day)	Monthly Charges[2]
Small (up 50)	£200	£4,600
Medium (up to 100)	£120	£2,760

[1] EPS – Event Per Second – a measure of the event produced by the different Log Sources/Assets

[2] An average of 23 days per month

Registered Office: 1 Meadway, Woodford, London, IG8 7RF.
Company Registered in England & Wales, No: 6633403
Website: http://www.research-series.com Email: info@research-series.com

Large (above 250)	£80	£1,840
Threat Intelligence Subscription	£66	£1,518
Security Incident Response	£75	£1,725
Yearly Support and Renewal Threat Intelligence Subscription Cost		£2,518

Workstream 4: Off-boarding & Contract Closure (Optional)

Prior to contract closure, historical logs may be off-boarded to the customer on request, otherwise, on contract termination, exit or expiry, then client event logs will be securely destroyed by the supplier.

Where historical logs or events are requested by the client/customer:

- The customer will be responsible for ensuring that storage media, links and communication network required to off-board historical logs are provided to the supplier.
- The supplier will ensure that historical logs are made available to the client in open data format and are copied to the customer provided storage media and after off-boarding is complete that data resident in the supplier's kit are securely destroyed.

The charges for these activities are shown in table 4 below.

Security Monitoring	Rate (per day)
Small (up 50 Log Sources)	£200
Medium (up to 100 Log Sources)	£120
Large (up to 250 Log Sources)	£80

Registered Office: 1 Meadway, Woodford, London, IG8 7RF.
Company Registered in England & Wales, No: 6633403
Website: http://www.research-series.com Email: info@research-series.com
e:(security·group) Information and Security Assurance