SPECIFICATION (READ-ONLY)

FOR THE PROVISION OF A SECURITY OPERATIONS CENTRE (SOC) AND A SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) TOOL

Overview

Staffordshire County Council (SCC or the Council) recently engaged the services of a security consultancy organisation to perform a Security and Threat Assessment and to help the council produce a Target Operating Model aligned to their findings and the council's ambition to improve its Cyber Security arrangements.

Regarding the implementation of a SOC/SIEM capability, the recommendation from that report was:

"If SCC were to focus on one deliverable in terms of technical controls, this would be the key area to prioritise in order to uplift the security maturity."

It was also a recommendation of the report that the SOC/SIEM service should be outsourced in order to get maximum value:

"A full balanced scorecard evaluation has been conducted to identify the most efficient and effective delivery of SOC and SIEM capability to SCC and conclusively it has been evaluated that this should be a third-party provision."

This document comprises the specification for the provision of a Security Incident and Event Monitoring (SIEM) service, along with the provision of a Security Operations Centre (SOC) function who will monitor, support and manage the SIEM solution interacting with council staff to proactively identify threats, reduce risks and continuously improve the council's cyber security defences.

The Council is seeking to arrange for the implementation and monitoring of a SIEM solution to improve the security of the ICT estate against an evolving threat landscape.

The Council would expect to have shared access, along with the Service Provider, to a central instance of aggregated data, providing a dashboard of analytical data in a 'single pane of glass' view which represents the entire enterprise ICT environment.

The Council has a budget of: £40,000.00 in order to procure and implement a solution and would expect to sustain annual service costs of no more than: £125,000.00

Definitions:

A security operations center (**SOC**) is a facility that houses an information security team responsible for monitoring and analysing an organization's security posture on an ongoing basis.

In the field of cyber security, security information and event management (**SIEM**) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

The council is seeking to procure a SIEM service with associated support, a dashboard providing the supplier with a high-level view of threats, risks and potential concerns will be accessible to the councils ICT and Information Governance staff, with monitoring, alerting and initial response services provided by the SOC.

Background:

The client computing estate is made up of approximate 3200 laptops, 1600 desktops and 400 thin clients.

The council currently has two data centres (classified as primary and secondary) located approximately 13 miles apart. Between the two sites we run in the region of 770 virtual servers based on Cisco UCS architecture. The council also has an extensive number of applications that are delivered using Software as a Service (SAAS) and continue to investigate the Business Case for Infrastructure as a Service. This may well happen within the duration of this contract.

Specification:

The council is seeking to arrange for the implementation and monitoring of a SIEM service to improve the security of the ICT infrastructure against an evolving threat landscape.

Following the guidance issued by the National Cyber Security Centre, as a minimum we would expect any service to provide monitoring of:

- Business traffic crossing a boundary
- Activity at a boundary
- Internal workstations, servers and devices
- Internal network activity
- Network connections
- Session activity by user and work stations
- Alerting on events
- Accurate time in logs
- Data backup status

Additionally, we would expect the service to provide:

- Enhanced, data analytics and threat intelligence collected from global networks
- Professionally qualified staff in cyber security, threat analysis, incident response
- 24x7 Detection & Analysis Service
- Continuous Vulnerability Management
- Regular reporting with user accessible dashboards and monthly/quarterly service reviews
- Compliance with regulatory / Standards requirements

- Emergency support in the event of a major incident\compromise
- Periodic searches of the clear and dark web for SCC information, login credentials and sensitive materials

The council reserves the right to add two additional lots into the procurement, these would represent additional goods/services that would be delivered by the successful bidder (or by a partner).

- Availability & Health Monitoring (Lot 2)
    - To encompass the monitoring of the status of selected data centre infrastructure and alerting of third-party maintainers in the event of an incident or outage in line with an SLA to be agreed.

- A managed IDS/IPS service (Lot 3)
    - To encompass monitoring of traffic at all perimeter devices, a proposed solution should allow the council to track users, report on activity and provide deep packet inspection of traffic anywhere on our network.

As a result of commissioning this service, we would expect to benefit from:

- Enhanced protection from internal / external threats
- Enabling the secure use of Cloud services
- Reduced complexity and improved effectiveness of protection
- Underpin a security improvement programme
- Reduce risk of security incidents
- Enabling in-house security operations teams to focus on what matters
- Improved threat detection and visibility of current and evolving threats
- Reduce the impact of security incidents
- Define priorities in terms of risk and threat intelligence
- Business focused alerting and reporting
- Able to make well informed risk-based decisions
- Services are vendor agnostic, interfacing with all standard security frameworks
- 24x7 security monitoring with predictable costs

Any economic operator interested in providing this service is directed to see the ‘Request for Information’ (RFI) which has been issued in conjunction with this document.

The council is seeking responses to the RFI, based on the specification above, in order to allow the specification to be refined, if necessary, following feedback.