



## **Statement of Work**

### **Security Event Management Services**

#### **1. Background**

The International Atomic Energy Agency (“IAEA” or “Agency”) is the world’s centre of cooperation in the nuclear field. The IAEA is established as a specialized organization under the umbrella of the United Nations family. It works together with its Member States and multiple partners worldwide to promote a safe, secure and peaceful use of nuclear technologies.

The IAEA Information and Communication Technology (ICT) infrastructure and computing environment consists of state-of-the-art hardware and software platforms. The threats to the ICT infrastructure of the IAEA are consistent with those of an entity with high international visibility that handles sensitive and highly sensitive information.

The IAEA relies on Security Event Management to fill a critical role in a broader defence-in-depth and continuous monitoring security strategy. Security event management systems are currently deployed across the IAEA and relied upon to generate alerts, produce reports, act as a repository of information to support investigations, enforce accountability, identify operational and security issues within the environment, provide a centralized view of the environment and to provide a sense of situational awareness.

#### **2. Scope**

This Statement of Work (SOW) describes the IAEA’s requirements for Security Event Management Services. These services are meant to both complement the IAEA’s in-house capabilities where they may already exist and provide additional capabilities where gaps may exist. These services may also be called upon during periods of high activity, in order to supplement existing resources and expertise.

The Contractor shall provide the following Security Event Management (SEM) Services:

- HP ArcSight ESM, ArcSight Express & ArcSight Logger Support and Professional Services; and
- ELK Support and Professional Services.



### 3. Applicable Documents

The following documents shall be applicable for the work to the extent specified hereinafter:

- NIST Special Publication 800-137 - Information Security Continuous Monitoring (ISCM);
- NIST 800-92 - Computer Security Log Management; and
- ISO/IEC 27001:2013-- Information security management systems — Requirements.

In the event of conflict between the documents listed above and the content of this SOW, the content of this SOW shall take precedence to the extent of the conflict.

### 4. Definitions, Acronyms, and Abbreviations

The following definitions, acronyms, and abbreviations shall apply throughout this SOW unless defined otherwise hereinafter:

- ELK means Elasticsearch, Logstash, and Kibana applications or platforms;
- ISO means International Standards Organization;
- NIST means National Institute of Standards and Technology;
- NDA means Non-Disclosure Agreement; and
- SEM means Security Event Management.
- API means Application Programming Interface



## 5. Requirements

5.1 The Contractor shall provide the following services as and when required by the IAEA using an industry recognized and accepted “process based” methodology:

- Guidance on architecting scalable security event management systems;
- Guidance on architecting reliable security event management systems;
- Guidance on collecting events from a diverse set of sources, including MS Windows clients and servers, Linux systems and applications that log into flat files or databases;
- Identification of cyber security and compliance use cases;
- Design of correlation and alerting rules;
- Development of custom parsers;
- Development of dashboards;
- Development of security operations reports;
- Guidance on accessing the SEM systems exposed API's by software developers; and
- Installing, upgrading and supporting SEM systems and all their various components (databases, connectors, rules, alerts, parsers, reports).

5.2 The IAEA shall clearly identify the priority of all service requests. The Contractor shall respond to service requests with the following response times:

Priority	IAEA Request to Contractor Response Time	Schedule Time (time frame for initiating work request)
High	4 hours	48 hours from response
Normal	24 hours	5 days from response

### 5.3 Onsite and Offsite Services

5.3.1 The Contractor, in its response to the IAEA service request, shall clearly define costs, methodologies and definitions of the onsite and offsite Services.

5.3.2 The IAEA shall determine whether a requested task is suited to be performed on-site or off-site.

5.3.3 In case of onsite services, the Schedule Time under Paragraph 5.2 shall be considered as the time for the Contractor to be at the IAEA premises (Vienna).

#### 5.4 Tools and licenses

The Contractor shall perform all the Services at the agreed rates. There shall be not charges for tools, devices, or licenses unless previously agreed upon by the IAEA.

#### 5.5 Contractor Experience & References

The Contractor's staff shall meet the following requirements for working on IAEA tasks:

- A minimum of three years of experience;
- Experience providing consulting services in a highly confidential environment;
- Ability to read and write fluently in the English language;
- Industry certifications or similar qualifications appropriate to the services provided; **such as any 2** of those listed below:

- HP Master ASE - ArcSight Security V2;
- HP ASE - ArcSight Administrator V1;
- HP ASE - ArcSight Analyst V1;
- HP ASE - ArcSight Logger V1;

And preferably possess the expertise commensurate of two of the below trainings:

- Core Elasticsearch: Developer;
- Kibana 4 Workshop;
- Core Elasticsearch: Operations; and
- Elasticsearch, Logstash, and Kibana Workshop.

5.6 The operating language of the IAEA is English. The Contractor shall provide all documentation, reports, presentations and conference calls in English.

#### 5.7 Information handling

5.7.1 The Contractor shall sign the IAEA NDA and ensure that all personnel providing services or having access to information related to the services provided under the Contract have signed either the IAEA NDA or a similarly restrictive NDA with the Contractor.

5.7.2 Transmission of requests for services or reports and other output that contain sensitive information shall be encrypted during transmission between the Contractor and the IAEA. The method of encryption and management of key material shall be agreed upon by both Parties.

5.7.3 Storage of sensitive information relating to current or past vulnerabilities or IT security incidents at the Contractor's site shall be encrypted during storage and purged at the conclusion of the activity to minimize any risks associated with the unauthorized release of information. After providing a copy of all information related to a specific request for services, the Contractor shall provide assurance to the IAEA



that all sensitive information related to the service request has been permanently removed.

## **6. Deliverable Data Items**

For each individual engagement, a “documentation package” containing the following items shall be submitted by the Contractor to the IAEA, for review and acceptance, within 7 days of the conclusion of the engagement. The “documentation package” shall include the following:

- a) A detailed summary of the work that was performed along with an accounting of the time spent in hours, identifying whether the task has been completed, cancelled or rescheduled; and
- b) An additional “product” documentation related to the work performed or product that was delivered. For example if the work performed was a software development task (custom parser, dashboard, rule or alert) the configuration information shall be documented. If the task requested was related to installations or upgrades, (connector upgrades, new Logger installation) documentation of the installation/upgrade parameters and configuration selections chosen during the process shall be documented and provided as part of the package.