دائرة اللوازم والمشتريات

عطاء رقم T18-2024.25

Logging and Reporting Solution

2024-2025

Logging and Reporting Solution

وثائق العطاء:

أ- الجزء الأول:

(1) دعوة العطاء

(2) الشروط والتعليمات التنظيمية للعطاء

(3) طريقة الدفع

ب- الجزء الثاني:

(1) جدول الكميات والمواصفات الفنية

الجزء الأول (1)

إعلان طرح عطاء رقم T18-2024.25

Logging and Reporting Solution

تدعو الجامعة العربية الأمريكية الشركات المختصة الى المشاركة في العطاء المذكور أعلاه.
يمكن الاستفسار أو الحصول على وثائق العطاء من دائرة اللوازم والمشتريات في الجامعة/ مبنى الدوائر الإدارية الطابق الثاني، هاتف- 2418888 04- تحويلة 1488 فاكس 2510972 04 بريد الكتروني pnp@aaup.edu
مقابل مبلغ غير مسترد مقداره (50 دولار) تدفع في إحدى البنوك المعتمدة وذلك اعتباراً من يوم (الاربعاء) 2025/4/9.

ملاحظات :

1. تقديم عرضين: فني ومالي، وسيتم دراسة العروض فنياً ومالياً لاختيار العرض المناسب.
2. آخر موعد لتسليم العطاءات هو في تمام الساعة الثانية من يوم(الاربعاء) 2025/4/23 ولنفس المكان.
3. يجب تقديم كفالة دخول عطاء 5% من قيمة العطاء على شكل كفالة بنكية أو شيك بنكي مصدق لصالح الجامعة العربية الأمريكية .
4. الأسعار (بالدولار) وتشمل جميع الضرائب بما فيها ضريبة القيمة المضافة وعلى المورد تقديم الفواتير الضريبية وشهادة خصم المصدر.
5. الجامعة غير ملزمة بأقل الأسعار وبدون إبداء الأسباب.
6. رسوم الاعلان على من يرسو عليه العطاء.
7. بإمكانكم الاطلاع على النظام الداخلي لدائرة اللوازم والمشتريات من خلال زيارة صفحة الجامعة العربية الامريكية على الانترنت. www.aaup.edu

(2) الشروط والتعليمات التنظيمية للعطاء

1. على جميع المشاركين في العطاء الالتزام التام بهذه الشروط والتعليمات، وهي تعتبر جزءاً لا يتجزأ من أي أمر شراء أو عقد يبرم مع المشارك الفائز ما لم ينص صراحة على خلاف ذلك في أمر الشراء أو العقد.
2. في هذه الشروط والتعليمات يرمز إلى "الجامعة العربية الامريكية بالاختصار (AAUP).
3. يجب أن تكون الشركة المتقدمة للعطاء مسجلة رسمياً ومشتغلاً مرخصاً.
4. **تقدم الأسعار (بالدولار) شاملاً لجميع الضرائب** بما في ذلك ضريبة القيمة المضافة (VAT).
5. يلتزم المشارك الفائز بتقديم شهادات خصم المصدر والفواتير الضريبية اللازمة وأية مستندات قانونية أخرى تغطي عملية الشراء.
6. يجب أن تشتمل الأسعار على جميع المصاريف المطلوبة من النقل والتركيب والتشغيل والفحص **والصيانة والتدريب** في المواقع المحددة في جدول المواصفات والكميات المرفق.
7. يجب أن تكون الأسعار المقدمة سارية المفعول لمدة لا تقل عن (90) يوماً من تاريخ تقديم العرض.
8. على المشارك الفائز تقديم كفالة حسن تنفيذ خلال أسبوع من تاريخ الاتفاقية بحيث تعادل (10%) من قيمة الاتفاقية على شكل كفالة بنكية صادرة عن إحدى البنوك العاملة في فلسطين أو شيك مصدق صادر لصالح "الجامعة العربية الامريكية".
9. إذا تخلف المناقص الفائز عن تقديم كفالة حسن التنفيذ عن الموعد المحدد في البند السابق فإنه يحق لـ (AAUP) إلغاء الإحالة.
10. إذا تخلف المناقص الفائز عن التوقيع على عقد التنفيذ و تسليم الكفالات والتأمينات المطلوبه منه خلال أسبوع من تاريخ قرار الاحالة، يعتبر مستنكفا عن تنفيذ العطاء ويصادر مبلغ الكفالة أو التأمين دخول العطاء بالاضافة الى ذلك يتحمل فرق السعر و/أو اي أضرار أخرى قد تلحق بالجامعة نتيجة استنكافه ويحرم من لمشاركة في عطاءات الجامعة لمدة عام.
11. اذا تخلف المناقص الفائز عن تنفيذ العطاء الذي احيل عليه او خالف شرطا من شروط العقد يحق للجامعة مصادرة كفالة دخول العطاء أو حسن التنفيذ أو جزء منها وتنفيذ العطاء مباشرة من الجامعة أو اية جهة تراها مناسبة بالاسعار والشروط والطريقة المناسبة ويتحمل المناقص أي فروقات بالاسعار مضاف اليها 15% من اجمالي قيمة العطاء.
12. يتحمل المناقص المتخلف دفع تعويض بدل اي عطل او ضرر قد يلحق بالجامعة نتيجة لذلك.

13. تعاد كفالة حسن التنفيذ بعد استكمال التوريد وجميع شروط العقد أو أوامر الشراء وبموجب الوثائق الأصولية اللازمة للاستلام.
14. على المشاركين في العطاء ارفاق كتالوجات عن المنتج.
15. يلتزم من يرسو عليه العطاء بدفع غرامة تأخير بواقع (0.1%) عن كل يوم تأخير من قيمة الأعمال المنجزة عن الوقت المحدد في الاتفاقية، ويتم احتساب هذه الغرامات من الدفعات المستحقة له أو من كفالة حسن التنفيذ.
16. يحق لـ (AAUP) إلغاء العطاء دون إبداء الأسباب كما أن (AAUP) غير ملزمة بإحالة العطاء على أقل العروض سعراً دون إبداء الأسباب. ولها أن ترفض كل أو بعض العروض المقدمة لها دون أن يكون لأي من المشاركين الحق في الرجوع إليها بأي خسارة أو ضرر ناجم عن تقديم عرضه ولا يترتب على (AAUP) أي التزامات مادية أو غير مادية مقابل ذلك، كما يحق ل (AAUP) تجزئة العطاء بما تراه مناسبا ودون ابداء أسباب.
17. يلتزم من يرسو عليه العطاء بتقديم كفالة بنكية (صيانة) بقيمة (5%) من قيمة الأعمال المنجزة صالحة لمدة عام من تاريخ تسليم الأعمال.
18. على المشارك في العطاء تقديم عرضه على أساس المواصفات الفنية االمبينة في وثائق العطاء وبموجب الكميات المحددة في جدول الكميات المرفق.
19. لا يجوز للمشارك في العطاء أن يتنازل لأي طرف آخر عن كل أو جزء من أمر الشراء دون الحصول على إذن خطي من (AAUP) مع الاحتفاظ بكامل حقوق (AAUP) وفقاً لشروط أمر الشراء.
20. عند دراسة العروض يؤخذ بعين الاعتبار كفاءة المناقص من الناحيتين المالية والفنية وقدرته على الوفاء بالتزامات العطاء وخبرته في تقديم اللوازم المطلوبة والسمعة التجارية والتسهيلات التي يقدمها ويجوز استبعاد عرضه لنقص كل أو بعض هذه المتطلبات.
21. لا تقبل العروض أو التعديلات التي ترد بعد التاريخ والموعد المحدد كآخر موعد لتقديم العروض.
22. يجب تعبئة جداول المواصفات المرفقة و لن ينظر بأي عرض لا يلتزم بتعبئة الجداول.

ملاحظات

- **يسمح بتقديم عرضين اثنين فقط كحد اقصى لكل بند.**
- **يجب تقديم عرضي الاسعار الفني والمالي بنسختين: الأولى ورقية، والأخرى الكترونية (محوسبة).**
- **تقديم العرضين المالي والفني الورقيين بالظرف المختوم، مع ضرورة وضع ختم الشركة والتوقيع على كل الصفحات (للعرض المالي بالذات).**
- **قد تكون المواصفات مأخوذة من منتجات وعلامات تجارية معروفة ولكنها ليست إلزامية.**

(3)

طريقـــة الدفـــــع

خلال (90) يوماً من التوريد والقبول والاستلام النهائي، مقابل تقديم الكفالات المطلوبة.

الجـزء الثانـــي

1. جـــــدول الكميـــــات والمواصفات الفنية
Logging and Reporting Solution

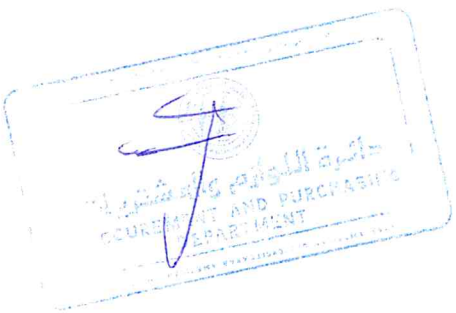
No.	Product	Qty	Unit Price USD	Total Price USD
	Logging and Reporting Solutions	1		
Total				

في حالة وجود استفسار يرجى تزويدنا بها من خلال البريد الالكتروني للرد عليها **pnp@aaup.edu**

1 Logging and Reporting Solution

Contents

Logging and Reporting Solution 7
Introduction 9
General Requirements 9
Objectives 10
Scope of Work 10
Technical Specifications 12
Submission Requirements 13
Support and Training 13
Total Cost 14
Evaluation Criteria 14



General Requirements and Technical Specifications

1-1 Introduction

AAUP is currently utilizing FortiAnalyzer **to collect and manage up to** 15 GB of logs per day **from** FortiGate **and** FortiWeb **devices only. This existing solution is limited in scope, as it only supports** Fortinet devices, **restricting our ability to integrate with other security solutions and technologies.**

As part of our ongoing commitment to improving IT security infrastructure, we aim to replace the current FortiAnalyzer **implementation with a more robust** Logging and Reporting Solution**. The new solution should be capable of supporting a broader range of devices, security solutions, and network environments, offering a scalable and flexible platform for future growth. Our objective is to deploy a** Logging and Reporting Solution **that is** upgradable, scalable**, and** flexible**, allowing seamless integration with other security tools such as** EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response)**, and more.**

This solution will ensure enhanced visibility, comprehensive reporting, improved threat detection, and a more versatile security monitoring framework that supports compliance requirements and helps mitigate risks across our entire IT ecosystem.

1-2 General Requirements

1. The proposed solution must meet all specifications outlined in the 'Mandatory Requirements' section.
2. The solution should support both hardware-based and virtualized deployment options.
3. The vendor must not be currently blacklisted by any government agency or public sector organization.
4. The solution should be recognized by industry-standard benchmarks such as Gartner Magic Quadrant, Forrester Wave, or equivalent certifications.
5. The solution provider should have been listed in the Gartner Magic Quadrant, Forrester Wave, or equivalent for "Logging and Reporting Solutions" for the past three years.
6. The vendor should have implemented similar solutions in the past two years in comparable environments.
7. The vendor must have a local support presence or an established partner network.
8. The solution must should be able to incorporate artificial intelligence (AI) and machine learning (ML) techniques for enhanced security.
9. Vendors must be prepared to provide a product demonstration and proof-of-concept (PoC) upon request.
10. Official in-person overseas training should be offered and included.

1-2-1

1-2-2 Objectives

The primary objective of this Tender is to solicit proposals for a Logging and Reporting Solution **that will:**

- **Collect, aggregate, and analyze logs from various devices, applications, and systems across the organization's network.**
- **Dashboards Templates, Ready and Scheduled Reports and Custom Searching and reporting capabilities.**
- **Enable real-time detection of security incidents and anomalies.**
- **Provide robust reporting and alerting capabilities.**
- **Ensure compliance with** ISO 27001 **and other relevant industry standards.**
- **Offer scalability for future growth and integration with other security solutions.**

1-2-3 Scope of Work

The Logging and Reporting Solution **must meet the following key requirements:**

1. Log Collection and Management:
   - **The solution must support the aggregation, processing, and storage of logs from a wide range of devices beyond just** Fortinet **solutions, including firewalls, routers, servers, endpoints, and cloud-based solutions.**
   - **It should be capable of handling log data from diverse sources such as network devices, servers, applications, and security tools (e.g., EDR, SIEM, SOAR).**
   - **The system must be able to process and store logs from systems generating at least** 15 GB of logs per day **at the outset, with the ability to scale as our log volumes grow over time.**
2. Real-Time Event Correlation and Analysis:
   - **The solution should provide** real-time log aggregation and correlation **to detect security incidents as they happen, with support for both** predefined rules **and** customizable correlation rules.
   - **It should offer the ability to leverage** AI, ML Machine Learning **and/or** Behavioral Analytics **to detect anomalies and potential threats proactively.**
3. Integration with Third-Party Security Solutions:
   - **The new** Logging and Reporting Solution **must offer 2 way** integration capabilities **with other security tools and solutions, including but not limited to** EDR systems, SIEM **platforms, and** SOAR solutions.
   - **It should enable seamless data exchange, such as importing event logs, telemetry, and security incident information for holistic threat analysis.**
   - **The solution should also provide APIs or other mechanisms for custom integration with additional security tools and technologies as needed.**
4. Scalable Architecture:
   - **The solution must be capable of handling increasing amounts of log data, with the ability to scale to support more devices, endpoints, and higher event processing rates as needed.**

- **It should allow the addition of** new devices **or solutions over time without requiring a complete overhaul of the system, ensuring that our security infrastructure can grow seamlessly.**
- **Scalability should extend to both data storage and event processing capabilities, ensuring that the solution can accommodate future expansions without performance degradation.**

5. Upgrade and Flexibility:
   - **The solution should be** upgradable **to accommodate future enhancements, additional features, and new integrations with emerging technologies.**
   - **It must offer flexibility in terms of deployment options (on-premises, hybrid, or cloud-based), with support for future technological shifts and evolving security requirements.**
6. Alerting and Notifications:
   - **The solution should provide customizable** alerting mechanisms**, capable of notifying security teams in real-time of critical security events or incidents, with automatic escalation workflows.**
   - **Alerts should be context-rich, providing actionable insights that aid in the response and resolution of potential security issues.**
7. Reporting and Dashboards:
   - **The solution should offer easy to use, clean UI/UX, comprehensive and customizable** reporting capabilities **that meet various internal and external reporting requirements.**
   - **Interactive** dashboards **should allow for the visualization of security metrics, trends, and threat intelligence in a user-friendly format.**
   - **Reports must be easily exportable in multiple formats (HTML, Word, PDF, CSV, XML, JSON, … etc.) for analysis and presentation.**
8. Compliance and Auditing:
   - **The solution must help maintain compliance with relevant regulations, including** ISO 27001**, and provide robust auditing features for logs, security events, and user activity.**
   - **The system should support long-term** log retention **policies, ensuring compliance with internal and external data retention requirements.**
9. Security and Data Integrity:
   - **The solution must ensure the** integrity and confidentiality of log data**, with built-in security features such as** role-based access control (RBAC), data encryption**, and** audit logging**.**
   - **It should support secure transmission of logs and other sensitive data to prevent unauthorized access and tampering.**
10. Deployment and Maintenance:

- **The solution should be deployable in various environments (on-premises, hybrid, cloud) with minimal disruption to existing operations.**
- **Ongoing support, software updates, and patches should be available to ensure the solution remains secure, up-to-date, and capable of adapting to emerging security threats.**

11. High Availability and Redundancy:

- **The** Logging and Reporting Solution **should be able to offer** high availability (HA) **and** redundancy **features to ensure continuous operation in case of hardware failure or other issues.**
- **Capabilities such as failover configurations should be supported to minimize downtime.**

12. Vendor Support:

- **The vendor must provide robust support, including troubleshooting, system monitoring, and product enhancements, along with adequate training for staff to effectively operate and manage the solution.**

1-2-4 Technical Specifications

The proposed solution must meet the following technical specifications for 50+ devices **and** 500+ Events Per Second (EPS) **with a** perpetual license or Open-Source Modules with Implementation:

1. Device Capacity:
   - **Support for at least** 50 devices **(e.g., servers, firewalls, routers, workstations, etc.).**
   - **Support for both physical and virtualized environments.**
   - **Scalability for adding additional devices as needed.**
2. Event Per Second (EPS):
   - **The solution should support the ability to handle at least** 500 Events Per Second (EPS).
   - **Capable of processing high-volume event logs without performance degradation.**
   - **Should be able to scale to higher EPS if needed, with minimal downtime.**
3. All-in-One Deployment:
   - **The solution must be an** all-in-one **configuration, integrating collection, processing, and storage in a single appliance.**
   - **The appliance should include built-in components for dashboards, reports, log aggregation, analysis, correlation, and storage.**
   - **Capable of handling high data throughput and concurrent processing for real-time event detection.**
4. Perpetual License or Open-Source:
   - **The license should be** perpetual or Open-Source, **with no recurring fees for the core functionality.**
   - **All core features, including log collection, analysis, and reporting, should be included in the perpetual license.**
   - **The solution should come with a** one-time licensing fee **for the initial deployment of 50 devices and 500 EPS.**
5. Data Retention and Storage:
   - **The solution must include sufficient storage for retaining logs according to organizational or regulatory requirements (e.g., 1 year, 5 years, etc.).**
   - **The storage should be scalable based on the organization's needs.**

- **The system should allow for the retention of logs with proper data integrity and compression for storage efficiency.**

6. Support and Maintenance:
   - **The vendor must be able to offer paid** premium support **for the perpetual license** or Open-Source**, which includes software updates, patches, and troubleshooting.**
   - Support plans **should include access to expert-level assistance, and support should be available 24/7.**
   - **The support plan should offer the ability to receive future product enhancements as they are released.**
7. High Availability and Redundancy:
   - **The solution should be able to support** high availability **configurations to ensure redundancy and minimize downtime.**
   - **Capabilities for failover in case of appliance failure must be included.**
8. Security and Compliance:
   - **The solution should meet** ISO 27001 **standards for** data security.
   - **The solution should include features such as role-based access control (RBAC), encryption of data at rest and in transit, and comprehensive auditing capabilities.**
   - **Compliance with** ISO 27001 **must be supported, including features for implementing security controls, evidence collection for audits, and reporting.**

1-2-5 Submission Requirements

Vendors are required to submit the following documentation with their proposals:

1. Company Profile**: A brief description of the company, its history, and its experience in the security solutions industry.**
2. Team Profiles**: A detailed information about the implementation and support experts involved in this project.**
3. Proposed Solution Plan**: A detailed description of the proposed** Logging and Reporting Solution**, including product specifications, architecture, and deployment options.**
4. Pricing**: A breakdown of the total cost of ownership, including licensing fees (free open-source, perpetual or subscription annually or monthly), implementation costs, and ongoing support and maintenance fees.**
5. Support and Maintenance Plan**: A description of the proposed support structure, including available service levels, response times, and maintenance plans.**
6. Case Studies/References**: Examples of similar** Logging and Reporting Solutions **provided to other organizations, including customer references.**
7. Compliance Certifications**: Explain how and Proof that the proposed solution complies with** ISO 27001 **and any other relevant certifications.**

1-2-6 Support and Training

Support:

A. Vendors should provide details on their professional service offerings and support structure.
B. Clear SLA should be provided.
C. Support should be available 24/7/365.

D. Local partner of the vendor must have trained personnel and an available stock of hardware / software in order to provide an immediate response.

Training:

E. **POC and Knowledge Transfer:** The bidder must conduct POC upon request, and mandatory knowledge transfer sessions for the IT team covering storage administration, expansion, and troubleshooting. This should be considered part of the implementation service and not as formal training.
F. **Training Option:** The bidder should provide an official vendor certifiable training program with a per-seat pricing model. The training must be:

o In-person and conducted outside the country (offshore).
o Exclusive of accommodation, travel, or per diem expenses.
o Online Courses (Including Instructor Led) is not acceptable.

Other capabilities

G. Knowledge transfer for any new products and updates in regular bases
H. Please set out any additional capabilities or other services you provide beyond the scope of those contained in this request which may be of interest to AAUP.

1-2-7 Total Cost

- All pricing must be inclusive of VAT and clearly itemized.
- The Financial proposals should differentiate between the costs (One-Time payments / Subscriptions) of hardware, software, services, training, and optional add-ons.

1-2-8 Evaluation Criteria

Proposals will be evaluated based on the following criteria:

- Functionality and Technical Capabilities**: Ability of the solution to meet the requirements outlined in this Tender.**
- Cost**: Total cost of ownership, including initial licensing, ongoing support, and potential for scalability.**
- Vendor Experience and Reputation**: Proven experience in deploying** Logging and Reporting Solutions **in similar environments.**
- Support and Maintenance**: The quality and responsiveness of support services offered by the vendor.**
- POC results**.**
- Proposed Training**.**
- Compliance with ISO 27001**: Ability of the solution to help meet the** ISO 27001 **certification and compliance requirements.**