Evrak Tarih ve Sayısı: 01.07.2024-E.445407

T.C.
GAZİOSMANPAŞA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilgi İşlem Daire Başkanlığı

Konu : Teklife Davet

Üniversitemiz bünyesinde kullanılmak üzere ihtiyaç duyulan "Wazuh Log Yönetim Sistemi İşletilmesi hizmeti alımı işi, 4734 Sayılı Kamu İhale Kanunu'nun 22. maddesinin (d) fıkrası uyarınca (**DOĞRUDAN TEMİN USULÜ**) satın alınacaktır. İlgilendiğiniz takdirde **K.D.V. hariç** fiyat teklifi göndermenizi, teklifinizde teslimat süresinin de bildirilmesini rica ederim.

Rafet DAYAN
Daire Başkanı

Ek: Teknik Şartname

Son Başvuru Tarih ve Saati : **03.07.2024 – 12:00**

Teklif Başvuru Yeri : Rektörlük Binası İdari ve Mali İşler Daire Başkanlığı
1.zemin kat 110 nolu oda - Taşlıçiftlik Kampüsü TOKAT

Teslimat Yeri : TOGOÜ Bilgi İşlem D.B. Taşlıçiftlik Kampüsü /TOKAT
Teklif Türü : İşin tamamı

İHTİYAÇ LİSTESİ

S.N.	Malzemenin Adı	MİKTARI	KDV HARİÇ BİRİM FİYAT	KDV HARİÇ TOPLAM FİYAT
1	WAZUH LOG YÖNETİM SİSTEMİ İŞLETİLMESİ HİZMETİ ALIMI	1 adet		
			KDV HARİÇ TOPLAM	

Yukarıda cinsi ve miktarı yazılı malzemelerin TAMAMI KDV HARİÇ (RAKAMLA).....(YAZI İLE)..... TL karşılığında vermeyi / yapmayı taahhüt ederim.

Teslimat Süresi : .....
KDV Oranı : .....
Diğer Açıklamalar:

FİRMA KAŞE
ADI SOYADI İMZA

NOT:

1- Talep Edilen mallara ilişkin ödeme, Maliye Bakanlığı'nın ödenekleri serbest bırakma oran ve ilkeleri doğrultusunda yapılacaktır.
2- Teklifler kapalı zarf içerisinde elden teslim edilebilir veya posta, kargo, faks yoluyla da gönderilebilir.
3- Teklif isteme yazımızda mal/malzeme/iş verilecek TOPLAM FİYAT üzerinden değerlendirmeye alınacaktır.
4- Şartlı teklifler ve Türk Lirası haricinde verilen fiyat teklifleri değerlendirilmeye alınmayacaktır.
5- Teslimat süresi değerlendirmede tercih nedeni olabilecektir.
6- Ulaşım, nakliye, kargo vb. giderler yüklenici firmaya aittir.

Taşlıçiftlik Kampüsü – TOKAT
Telefon (0 356) 252 15 80 Faks: (0 356) 252 16 05
e- posta: idarimali@gop.edu.tr
web: www.gop.edu.tr

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

WAZUH LOG YÖNETİM SİSTEMİ İŞLETİLMESİ

HİZMET ALIMI İŞİ

LOG YÖNETİM SİSTEMİ İŞLETİLMESİ HİZMET ALIMI İŞİ TEKNİK ŞARTNAMESİ-2024

1. İŞİN TANIMI

1.1. Genel Tanımlar

1.2. İDARE: Tokat Gaziosmanpaşa Üniversitesi

1.3. İŞ GÜNÜ: Resmî tatiller haricinde haftanın pazartesi, salı, çarşamba, perşembe, cuma günleridir.

1.4. SİSTEM: Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından işletilen donanım ve uygulamalarıdır.

1.5. TARAFLAR: İDARE ve YÜKLENİCİ 'yi belirtir.

1.6. YÜKLENİCİ: İhaleyi kazanan, İDARE ile sözleşme yaptıktan sonra ihale konusu işi yapmaya yetkili ve aynı zamanda idari ve teknik açıdan sorumlu firma.

1.7. İşin Konusu ve Kapsamı

Tokat Gaziosmanpaşa Üniversitesi Bilgi İşlem Daire Başkanlığı'nın kendi bünyesinde sağlamış olduğu bilişim tabanlı cihazlardan üretilen log.ların değerlendirilmesi için Wazuh SIEM konfigürasyonu yapılması, kural/korelasyonların yazılması, saldırı tespiti ve alarm üretilmesi, false positive alarm düzenleme, zafiyet yönetimi ve tespiti, güvenlik yapılandırma denetimi, regülasyon uyumluluğu, personele eğitim, yıllık bakım ve desteği kapsamaktadır.

2. GENEL ŞARTLAR

2.1. YÜKLENİCİ ve İDARE hizmet başlangıcında bu hizmete özel bir gizlilik sözleşmesi imzalayacaktır.

2.2. YÜKLENİCİ, sözleşmenin imzalanmasından itibaren en geç 10 (on) iş günü içerisinde, şartname kapsamında verilecek hizmetler ile ilgili detaylı proje planı hazırlayarak İDARE'ye sunacaktır.

2.3. YÜKLENİCİ, bu şartname kapsamında verilecek tüm hizmetleri koordine etmek ve projenin planlandığı gibi ilerlemesini kontrol etmek üzere bir proje yöneticisi görevlendirecektir.

2.4. YÜKLENİCİ, proje başlangıcında sunacağı iş planı, projenin planlama aşamasında İDARE ile birlikte detaylandıracak ve İDARE onayına sunacaktır.

2.5. YÜKLENİCİ personeli, sistem üzerinde yapacağı her türlü iş, işlem ve müdahaleyi İDARE personeli eşliğinde/izniyle yapacaktır.

2.6. YÜKLENİCİ, çalıştıracağı her personelin, İDARE yetkililerinin kontak noktası personelin kimler olduğunu, mesai içi ve mesai dışı saatlerde bu kişilere ulaşılabilecek telefon numaraları konusunda bilgilenmesini sağlamaktan sorumlu olacaktır.

2.7. Proje kapsamında hazırlayacağı ve İDARE'ye sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır. Teknik detaylar için İngilizce terimler kullanıldığı durumlarda parantez içinde Türkçe 'si yazılacaktır.

2.8. Proje kapsamında tüm hizmet, eğitim ve danışmanlıklar, uzaktan veya yerinde verilebilecektir.

2.9. Yüklenicinin Sanayi ve Teknoloji Bakanlığı Milli Teknoloji Genel Müdürlüğü Kamu Bilişim Yetki Belgesine sahip olmalıdır.

3. İŞİN YAPIMI

3.1. Wazuh SIEM Kurulum ve Konfigürasyonu

Wazuh SIEM sistemi, belirtilen sunuculara kurulacak ve temel konfigürasyonlar gerçekleştirilecektir. Kurulum sürecinde işletim sistemi gereksinimleri ve bağımlılıklar sağlanacak, gerekli yazılım paketleri yüklenerek yapılandırma dosyaları düzenlenecektir. Kurulum sonrası sistemin stabil çalışması test edilecektir.

3.2. Log Kaynakları Entegrasyonu

Log kaynakları (sunucular, ağ cihazları, uygulamalar vb.) Wazuh SIEM sistemine entegre edilecek ve logların doğru bir şekilde toplanması sağlanacaktır. Bu entegrasyon sırasında, her kaynağın özel gereksinimlerine uygun konfigürasyonlar yapılacak ve veri akışının sürekli ve kesintisiz olması temin edilecektir.

3.3. Kural/Korelasyon Yazılması

Güvenlik olaylarını tespit etmek amacıyla özel kurallar ve korelasyonlar yazılacaktır. Bu kurallar, belirlenen güvenlik politikalarına ve tehdit modellerine uygun olarak tasarlanacak ve sistem üzerinde etkin bir şekilde çalışması sağlanacaktır. Kuralların doğruluğu ve etkinliği test edilecektir.

3.4. Saldırı Tespiti ve Alarm Üretilmesi

Olası saldırı girişimlerini tespit etmek için sistem üzerinde alarm mekanizmaları yapılandırılacaktır. Tespit edilen saldırılar için ilgili alarmlar oluşturulacak ve bu alarmların doğru çalıştığı, yetkili personeli anında bilgilendirdiği doğrulanacaktır.

3.5. F/P Alarm Düzeltme

False Positive alarmların sayısını azaltmak ve True Positive alarmların etkinliğini artırmak amacıyla alarm düzenlemeleri yapılacaktır. Alarmların hassasiyeti ve eşiği ayarlanarak güvenlik ekibinin gereksiz alarmlarla meşgul edilmesi engellenecektir.

3.6. Zafiyet Yönetimi ve Tespiti

Sistemler üzerinde mevcut olan zafiyetlerin tespit edilmesi ve yönetilmesi sağlanacaktır. Wazuh üzerinden zafiyet taramaları düzenli olarak gerçekleştirilecek ve bulunan zafiyetler raporlanacaktır. Bu raporlar, zafiyetlerin giderilmesi için gerekli adımları içerecektir.

3.7. Dosya Değişiklik İzleme (FIM)

Kritik sistem dosyalarının değişikliklerinin izlenmesi amacıyla Dosya Bütünlük İzleme (FIM) konfigürasyonu yapılacaktır. Dosya değişiklikleri anlık olarak izlenecek ve yetkisiz değişikliklerde alarm üretilerek ilgili kişilere bildirilecektir.

3.8. Güvenlik Yapılandırma Denetimi (SCA)

Sistemlerin güvenlik yapılandırmalarının uygunluğunu denetlemek için Güvenlik Yapılandırma Denetimi (SCA) yapılacaktır. Sistem yapılandırmaları belirlenen güvenlik standartlarına göre düzenli olarak kontrol edilecek ve uyumsuzluklar raporlanacaktır.

3.9. Regülasyon Uyumluluğu

Mevcut regülasyonlara (KVKK, ISO 27001 vb.) uyumluluğun sağlanması amacıyla gerekli adımlar atılacaktır. Log yönetimi ve güvenlik olaylarının raporlanması, regülasyonların gerektirdiği şekilde yapılandırılacaktır.

3.10. Sistem Envanter Bilgisi Toplama

Agent kurulu cihazların envanter bilgisi toplanacak ve merkezi bir veri tabanında tutulacaktır. Bu envanter bilgileri, cihazların donanım ve yazılım detaylarını içerecek ve düzenli olarak güncellenecektir.

3.11. Eğitim

Wazuh SIEM sisteminin etkin bir şekilde kullanımı ve yönetimi konusunda yetkili personele eğitim verilecektir. Eğitimler, sistemin temel kullanımını, log analizi ve alarm yönetimini kapsayacak şekilde düzenlenecektir.

3.12. Periyodik Sağlık Kontrolü (yılda 4 kez)

Sistemlerin sağlığının ve performansının düzenli olarak kontrol edilmesi amacıyla yılda dört kez periyodik sağlık kontrolleri yapılacaktır. Bu kontrollerde, sistemin performansı, log akışı ve alarm mekanizmalarının doğru çalışıp çalışmadığı denetlenecektir.

3.13. Yıllık Bakım Destek (8x5)

Yıllık bakım ve destek hizmetleri kapsamında, haftada 5 gün, günde 8 saat boyunca destek sağlanacaktır. Bu hizmet, sistemde oluşabilecek herhangi bir sorun veya aksaklık durumunda hızlı müdahale ve çözüm sunmayı hedeflemektedir.

Mustafa KAPLAN
Mühendis

Engin TÜRK
Öğretim Görevlisi

Sakine YÜCE
Teknik