MERKEZİ LOGLAMA (SIEM) VE SİBER GÜVENLİK OPERASYON MERKEZİ (SOC) YAZILIMLARI TEKNİK ŞARTNAMESİ

1. İşin Adı ve Tanımı

Merkezli Loglama (SIEM) ve Siber Güvenlik Operasyon Merkezi (SOC) Yazılımları.

ŞİRKET'İN Merkezi Loglama Sistemi üzerinde oluşabilecek siber ataklara ve güvenlik ihlal olaylarına ilişkin alarmların 7x24 izlenmesi, alınması gereken aksiyonlar için yönlendirilmelerin yapılması, ileri seviye uzmanlık gerektiren olaylarda analiz ve raporlama çalışmalarının yapılması, siber atakları tespit etmek için kuralların yazılması, test edilmesi, mevcut kuralların iyileştirilmesi ve iyileştirme süreçlerinin devamlılığının sağlanması amacıyla Güvenlik Operasyon Merkezi hizmetinin genel esaslarını tespit etmektir.

2. Amaç

ŞİRKET Bilgi Teknolojileri altyapısı üzerinden verilmekte olan servis ve hizmetlerin güvenli biçimde (gizlilik, bütünlük, erişilebilirlik özelliklerini koruyarak) işletiminin sağlanması için gerekli hizmetlerin alınması amaçlanmaktadır.

Bilgi Güvenliği ihlal girişimlerinin/olaylarının zamanında tespit edilmesi, önceliklendirilmesi ve müdahale edilmesi amacıyla Bilgi Güvenliği Operasyon Merkezi (SOC) faaliyetleri gerçekleştirilmesi için aşağıdaki kapsam üzerinden hizmet sağlanacaktır;

- SIEM sistemi üzerinde oluşabilecek siber ataklara ve güvenlik ihlal olaylarına ilişkin alarmların Merkezi SOAR yapısı üzerinden izlenmesi,
- Alınması gereken aksiyonlara ilişkin yönlendirmelerin yapılması,
- İleri seviye ve uzmanlık gerektiren olaylarda analiz çalışmalarının yapılması,
- Siber atakları tespit etmek için kuralların yazılması ve test edilmesi,
- Mevcut kuralların iyileştirilmesi ve iyileştirme süreçlerinin devamlılığının sağlanması

için Güvenlik Analiz hizmetleri ile ilgili alınan tedbirleri test edilmesi, siber güvenliğin sağlanması ve bu süreçte ihtiyaç duyulan raporlamaların yapılması çalışmalarını kapsamaktadır.

7 Gün 24 saat esasına göre güvenlik izleme ile sistemlerinin ürettiği alarmların, raporların ve izleme ara yüzlerinin "tehdit ve olayların" tespitine yönelik takip edilmesi, incelenmesi sağlanacaktır. Bununla beraber, Güvenlik cihazları üzerinde kapatılması ve/veya iyileştirilmesi gereken bulguların kapatılması ve/veya iyileştirilmesi için gerekli olan çalışmalar ŞİRKET tarafından sağlanacaktır.

Güvenlik izleme süreçleri; Yüklenici Siber Güvenlik Operasyon Merkezi (SGOM) üzerinden gerçekleştirilecektir. Gerçekleşecek olaylarda Seviye-1, Seviye-2 ve Seviye 3 desteği YÜKLENİCİ bünyesinde yer alan kaynakların kullanımı ile sürdürülecektir.

Yapılacak Sürekli Güvenlik İzleme faaliyetleri esnasında bildirimi yapılan ve Aksiyon alınması gereken Olaylar kapsamında gerçekleştirilecek müdahale hizmeti ŞİRKET'İN hali hazırda çalıştığı "Servis Sağlayıcı"lar üzerinden gerçekleştirilecek olup "Servis Sağlayıcı" ile koordinasyon ŞİRKET tarafından gerçekleştirilecektir.

3. İşin Kapsamı

SOC/SGOM Hizmetinin sağlanması çerçevesinde aşağıdaki çalışmaların gerçekleştirilmesi hedeflenmektedir.

1. SIEM ürün Temini: İnsan-Süreç ve Teknoloji ekseninde yapılan olgunluk analizleri ile ŞİRKET bünyesindeki eksikliklerin belirlenmesi,
2. Kurulum Yapılandırma: SIEM/SOAR bileşenlerinin temel konfigürasyonlar ile belirlenen mimariye göre kurulumlarının tamamlanması.
3. Devreye Alma Analiz: Kurulu bileşenlerin siber güvenlik bakış açısı ile eksiklerinin belirlenmesi ve çalışmanın yol haritasının çıkartılması.
4. SOC/SGOM Devreye Alma: Tespit edilen ve bildirimi yapılan eksikliklerin tamamlanması için ŞİRKET'İN gerekli aksiyonları alması.
5. SOC/SGOM İzleme Hizmeti:
   - SOC Merkezi İzleme ve Analiz: SIEM/SOAR altyapısının Bilgi Güvenliği kayıtlarının anlık izlenmesi, Tehdit İstihbaratı hizmetinin gerçekleştirilmesi ve olası tehditlere karşı önlem alınması amacıyla gerekli yönlendirmenin yapılması sağlanacaktır.
   - SOC Raporlama
6. Sürekli İyileştirme: SOC/SGOM hizmeti kapsamında güncel güvenlik tehditlerine karşı gerekli iyileştirmelerin yapılması ve gürültülü kuralların temizlenmesi.

4. Tanımlar

Teknik Şartname içerisinde bahsi geçen aşağıdaki kelime ve deyimler bu bölümde belirtilen anlamları taşıyacaktır.

ŞİRKET: SAKARYA ELEKTRİK DAĞITIM A.Ş. Orhangazi Caddesi Trafo Tesisleri PK:160 54100 / SAKARYA

YÜKLENİCİ: Şartname kapsamındaki işleri yürütmekle görevli firmadır.

HİZMET: Bu Teknik Şartname kapsamında Yüklenicinin gerçekleştireceği bütün faaliyetlerdir.

KURULUM: Bu teknik şartname kapsamında olan ürün ve yazılımların belirtilen şekilde, proje planında belirtilen sürelerde, belirlenen Veri Merkezinde çalışır duruma getirilmesi.

EPS (Event Per Second): Saniyede üretilen olay sayısı

BAĞLANTI SAĞLAYICI (COLLECTOR): Her bir log ve veri kaynağında üretilen log ve verileri toplamak için kullanılan donanımsal ya da yazılımsal araç.

EKLENTİ (PLUGIN): Sistemler tarafından üretilen logların merkezi sisteme tanıtılması ve entegre edilmesini sağlayan yazılım parçası.

KORELASYON: Farklı veri kaynaklarından ŞİRKET' in belirlediği kurallara uygun olarak verilerin derlenmesi ve raporlandırılmasıdır.

GERÇEK ZAMANLI LOG VEYA VERİ: Bilişim Sisteminde çekilebilir hale gelen kaydın Log Yönetimi yazılımı tarafından maksimum 30 dakika gecikme ile Merkezi Log Yönetimi yazılımına aktarılacak olan log ya da veridir.

LOG: Bilgi sistemi içerisinde bulunan donanım ve yazılımların üzerinde yapılan işlemlere ait detay ve zaman bilgisi içeren kayıtlardır.

SIEM (Security Information and Event Management) Bilgi Güvenliği Tehdit ve Olay Yönetimi

SOC – (Security Operation Center) Güvenlik Operasyon Merkezi

MTTD: SOAR üzerinde açılan olayın analist tarafından üzerine alınana kadar geçen süre.

MTTI: SOAR üzerinde açılan olayın analist tarafından üzerine alındıktan sonra alarm üzerinde analizin gerçekleştirilip müşteriye bildirim yapılana veya Seviye-2 analiste aktarılana kadar geçen süre.

MTTR: Müşteriye bildirim yapıldıktan sonra e-posta üzerinde yapılan bildirime müşteri yanıt verene kadar geçen süre. (72 saat içinde dönüş yapılmayan çağrıların otomatik olarak kapatılması süreci işletilmektedir.)

5. **İş Yeri:** Sakarya Elektrik Dağıtım A.Ş.

6. **İşin süresi:** İşin süresi sözleşmenin imzalanması itibariyle 3 yıldır.

7. **Bildirimler ve Kalite Parametreleri**

YÜKLENİCİ, ŞİRKET tarafından iletilen tüm bildirimlerin çözümlenmesi, sınıflandırılması, çözümlenmek üzere yönlendirilmesi ve çözümün takip edilmesi için YÜKLENİCİ'NİN ya da ŞİRKET'İN yardım masası uygulamasını kullanır. Hangisinin kullanılacağı ŞİRKET tarafından belirlenir ve değiştirilebilir.

Söz konusu Yardım Masası Uygulaması sayesinde ŞİRKET sorunları kaydedilir, tekrarlayan hatalar belirlenerek bunlar için kalıcı çözümler geliştirilir veya daha önce çıkan sorunlar taranarak daha hızlı çözümlenir. Böylece sistemlerin ve sunulan hizmetlerin tarihçesi de kaydedilerek problem yönetimi ve değişiklik yönetimi süreci altyapısı oluşturulur.

7.1. Hizmet Kalitesi beklentisi aşağıdaki tablolar ile özetlenmiştir.

Hizmet Detayları	Açıklama	Çözüm süresi
Yıllık Bildirim Sayısı	Talep ve arıza bildirimleri	Sınırsız
7x24 Uzaktan Destek	Telefon, E-Posta, Uzak Masaüstü Bağlantısı vb.	Sınırsız
7x24 Yerinde Destek	İhtiyaç halinde yerinde destek	Sınırsız
Bildirim Önceliği	Açıklama	Çözüm Süresi
Acil Seviye Arıza	Sistemin bütünüyle hizmet dışı kalmasına sebep olan problemler.	4 Saat
Yüksek Seviye Arıza	Sistemin bir kısmının hizmet dışı kalması veya bütünün normal hizmetini vermesine engel olan problem (bütünün normal hizmet vermesine engel performans problemleri acil öncelikli olarak değerlendirilir).	8 Saat
Orta Seviye Arıza	Sistemin bütününün normal işleyişini engellemeyen ancak gerek performans gerekse az önemli alt servislerin hizmet vermesini engelleyen problem.	2 Gün
Düşük Seviye Arıza	Sistemin bütününün veya alt hizmetlerin normal işleyişini engellemeyen ancak ileride olabilecek bir problemi işaret eden sistem hataları.	5 Gün
Acil Seviye Talep	Kritik düzeyde sorunlara yol açabilecek risklerle ilgili iletilen talepler	1 Gün
Yüksek Seviye Talep	İleride problem oluşturabilecek riskler taşıyan ve yüksek düzeyde etkisi olan talepler.	3 Gün

Orta Seviye Talep	Alternatif bir çözüm uygulanabilecek durumlar ve hizmetin ana özelliklerini etkilemeyen talepler.	5 Gün
Düşük Seviye Talep	Sistem fonksiyonlarına herhangi bir etki olmadığı durum veya bilgilendirme soruları.	10 İş günü veya karşılıklı mutabakat

7.2. SOC İZLEME HİZMETİ KAPSAMINDA SLA SÜRELERİ

Vakalar aşağıdaki cetvele göre kategorize edilip önceliklendirilecektir.

Öncelik	Etkisi
Acil	Acil Aksiyon gerektiren durumlar. Sistem downtime vb. gibi alarmlar
Yüksek	Aksiyon alınmadığı takdirde sorun zarar verme ihtimali olan alarmlar. Ani trafik artışları vb.
Orta	Düşük etkili olabilecek alarmlar. Kullanıcının parola yenilemesi.
Düşük	Bilgilendirici ya da bakıma ilişkin alarmlar.

Vakalar SOC analistleri tarafından analiz edilecek ve İş sahibi vakanın oluştuğuna dair telefon, MSS Portal üzerinden ya da e-posta yolu ile aşağıdaki yer alan süreler dâhilinde ŞİRKET'E bilgilendirilecektir ve/veya aksiyonu alınacaktır.

Kritik Alarmlar için ŞİRKET yetkilisi önce aranacak, daha sonra e-posta ile bildirim yapılacaktır.
Yüksek alarmlar birden fazla kez tetiklendiğinde ŞİRKET yetkilisine telefon ile de bilgi verilecektir.
Geri kalan kritiklik seviyeleri için bildirim e-posta yolu ile yapılır.

Seviye-1 Analist Vaka Bildirimi veya Aksiyon Öncelik Seviyesi	MTTD	MTTI
Öncelik1: Acil	25 dk	10 dk
Öncelik2: Yüksek	25 dk	10 dk
Öncelik3: Orta	60 dk	10 dk
Öncelik4: Düşük	60 dk	10 dk

MTTI süresi içerisinde çözümlenemeyen vakaların Seviye-2 analistlere aktarımı sağlanır. Seviye-2 analist tarafından kayıt üstlenene kadar geçen süre MTTD olarak değerlendirilir. Seviye-2 analist, vakayı üstlendikten çözümleyene kadar geçen süre MTTI olarak ölçümlenir.

Seviye-2 Analist Vaka Bildirimi veya Aksiyon Öncelik Seviyesi	MTTD	MTTI
Öncelik1: Acil	10 dk	30 dk
Öncelik2: Yüksek	10 dk	30 dk
Öncelik3: Orta	10 dk	60 dk
Öncelik4: Düşük	10 dk	60 dk

SOC Hizmet Seviyesi Koşulları

Acil	10 dk.	20 dk.	• ŞİRKET Bilgi Güvenliği Yetkilileri telefonla aranır ve bilgilendirme yapılır. • İletişim planı çerçevesinde diğer yöntemler ile de bilgilendirme yapılır. • Olay ortadan kalktıktan sonra kök sebebi ile ilgili incelemeler yapılır ve çözüm önerileri oluşturulur.
Yüksek	20 dk.	40 dk.	• ŞİRKET Bilgi Güvenliği Yetkilileri telefonla aranır ve bilgilendirme yapılır. • İletişim planı çerçevesinde diğer yöntemler ile de bilgilendirme yapılır. • Olay ortadan kalktıktan sonra kök sebebi ile ilgili incelemeler yapılır ve çözüm önerileri oluşturulur.
Orta	45 dk.	2 saat	• İletişim planı çerçevesinde bilgilendirme yapılır.
Düşük	1 saat	Haftalık Rapor	• Haftalık raporlama yapılır

8. Teknik Özellikler

Hizmet ve ürün kapsamında alınan lisanslar ŞİRKET adına alınacaktır. Özelleştirilmiş kurulum gerektiren yazılımlar ŞİRKET bünyesinde bulunan sunuculara kurulacaktır.

SIEM ve SOC yazılımları özellikleri en az aşağıda belirtildiği gibi olmalıdır.

8.1. YÜKLENİCİ servislerin durumları ile ilgili olarak sistemi 7 gün 24 saat uzaktan izlemeli ve servislerde oluşan hatalara, olayın oluşma zamanından hemen sonra müdahale ederek düzeltmelidir.

8.2. SIEM ürünü yedekli bir şekilde çalışacak olup bir sunucuda herhangi bir sebepten kesinti olması durumunda log akışında bir kesinti yaşanmadan sistemin devam edebilecek yapıda olması gerekmektedir.

8.3. YÜKLENİCİ servis kalitesini ve hızını artırmak için sistem üzerinde var olan rolleri ve servisleri gerekli görülen durumlarda yedekleyebilmelidir.

8.4. YÜKLENİCİ, donanım değişikliği gibi durumlarda veri kaybı yaşanmaması için veri yedekliliği kontrolleri ve tüm sistem ayarlarının yedeklenmesi ile ilgili olarak prosedürleri uygulayarak geçiş, esnasında veri kaybına neden olmayacak şekilde sistemi faal duruma geçirebilmelidir.

8.5. YÜKLENİCİ, donanım yetersizliği durumlarında, sanal ortamdan fiziksel ortama taşıma ya da fiziksel ortamdan sanal ortama tasıma durumları için veri yedeklenmesi prosedürleri uygulamalıdır. Taşıma işlemleri hizmet kapsamı süresi içerisinde ücretsiz yapılmalıdır.

8.6. Yeni entegrasyonlar, plugin sorunlarının düzeltilmesi ve ek SIEM özelliklerinin kullanılabilmesi için sistem YÜKLENİCİ tarafından sürekli olarak güncel tutulmalıdır. Güncelleme sürece yeni versiyon testleri bittikten 48 saat sonra yapılmalıdır.

8.7. Geçmişe dönük log analizleri yapılabilmesi için re-index süreçleri YÜKLENİCİ tarafından yapılmalıdır. Re-index sürece tamamlandıktan sonra ŞİRKET' e özel olarak rapor ve görsel panolar hazırlanmalıdır.

8.8. ŞİRKET özelinde yapılmış, korelasyonlara ilişkin özel rapor ve görsel panellerin oluşturulması YÜKLENİCİ tarafından sağlanmalıdır.

8.9. Sisteme eklenecek özel uygulamaların ve donanımların verileri için plugin ve parsing hizmetleri YÜKLENİCİ tarafından sunulmalıdır. Genel olarak eklenmiş kaynaklar ya da ŞİRKET'e özel geliştirilen uygulamalar için plugin sorunları tespit edilmeli ve yazılım ekibinin çalışması için olay bildirimi yapılmalıdır.

8.10. 5651 sayılı kanun gereği toplanan logların imzalanma durumları YÜKLENİCİ tarafından kontrol edilmelidir. Gün sonu Log İmzalama Takibi, imzalama kontrolleri YÜKLENİCİ tarafından yapılmalı ve imzalama gecikme durumlarında elle tetikleme işlemi yine YÜKLENİCİ tarafından gerçekleştirilmelidir. Logların imzalanmaları ile ilgili imza doğrulama prosedürü YÜKLENİCİ tarafından uygulanmalıdır.

8.11. Konfigürasyon değişikliklerinde log kayıpları yaşanması halinde YÜKLENİCİ olay bildirimi yapmalıdır. Log bilgisinin akışının kesilmesi halinde YÜKLENİCİ tarafından olay anında tespit edilip bildirimde bulunulmalıdır.

8.12. Sistemde yapılan değişikliklere ilişkin haftalık raporlar YÜKLENİCİ tarafından hazırlanmalı ve iyileştirme durumları ile ilgili ayrıntılar paylaşılmalıdır.

8.13. Sistemin, saldırı zamanlarında normal değerinden çok yüksek log oluşturması halinde YÜKLENİCİ, olay anındaki artışları gözlemleyip bildirimde bulunmalıdır.

8.14. CPU, RAM ve Disk durumları YÜKLENİCİ tarafından gözlemlenmelidir. Kapasite yetersizliği durumları, herhangi bir soruna neden olmadan önce YÜKLENİCİ tarafından takip edilmeli ve bildirim yapılmalıdır.

8.15. Kaynaklardan gelen veriler için veri toplama anında ya da indexleme sırasında istenilen kriterlere göre veri politikası YÜKLENİCİ tarafından uygulanmalıdır. YÜKLENİCİ ŞİRKET'e özel DPM'ler oluşturmalı ve tanımlamalar yapmalıdır.

8.16. ŞİRKET tarafından iletilmiş olan log kaynaklarının SIEM platformuna entegrasyonu ve plugin hizmeti ücretsiz verilmelidir.

8.17. Korelasyon kurallarının yazılması ve devreye alınması hizmet süresi boyunca YÜKLENİCİ tarafından sağlanmalı ve raporlanmalıdır.

8.18. Mevcut korelasyon kuralları ve eklenen korelasyon kurallarına ek olarak ŞİRKET' in tabi olduğu uyumluluklara bağlı olarak yeni korelasyonların çıkartılması ve SIEM ortamına aktarılması YÜKLENİCİ tarafından sağlanmalıdır.

8.19. Talep edilmesi halinde ŞİRKET tarafından devreye alınmış olan korelasyon kurallarının iyileştirmelerinin yapılması YÜKLENİCİ tarafından sağlanmalıdır.

8.20. ŞİRKET bilgi güvenliği olaylarının, vardiyalı ekibimizce 7/24 izlenmesi ve aksiyon planının sunulması sağlanmalıdır.

8.21. YÜKLENCİ güvenlik analistlerinin vardiya değişimlerini takip edebilmeli ve raporlayabilmelidir.

8.22. YÜKLENCİ güvenlik analistlerinin ilgilendiği vaka ile ilgili anlık bilgi sağlamalıdır.

8.23. YÜKLENCİ olay yönetim platformu oluşan anomali durumlar için açıklama sunmalıdır.

8.24. ŞİRKET SIEM platformunda oluşan tüm olayların SLA süreleri dahilinde incelenip, sonuçlarıyla birlikte SIEM üzerinde takibi devam etmeli ve YÜKLENİCİ olay yönetimi platformu üzerinde incident ve case çözülerek kapatılması sağlanmalıdır.

8.25. Olay Yönetimi faaliyetleri için olayın kritiklik seviyesine göre iş akış diyagramlarının oluşturulması ve Siber Güvenlik Yardım Masası'na bu adımların eklenmesi ve takibinin yapılması sağlanmalıdır.

8.26. ŞİRKET' in tabi olduğu uyumluluklara bağlı olarak belirli periyotlarda oluşturulması gereken raporların hazırlanması ve SIEM ortamında otomatize edilmesi sağlanmalıdır.

8.27. SIEM platformuna uygun olarak yazılan eklentilerin uyumluluk kontrollerinin yapılmasının ardından ŞİRKET ortamına eklenmesi sağlanmalıdır.

8.28. ŞİRKETİ'İN sistemlerinde atak nedeni ile yaşanabilecek bir çökme ya da kapanma durumunda YÜKLENİCİ sistemlerin ayağa kaldırılması sürecinde aktif olarak yer alacaktır.

9. İşin İfası ile İlgili Şartlar (YÜKLENİCİ Sorumlulukları)

İşin ifası aşamalarında hiçbir işlem adedi sınırı bulunmadan hizmet sürdürülecektir. YÜKLENİCİ desteğiyle beraber ŞİRKET'İN talep etmesi durumunda hiçbir bedel talep edilmeden Üretici desteği sağlanacaktır.

9.1. SIEM & SOC Yazılım Devreye Alma Analizi

9.1.1. YÜKLENİCİ, güvenlik olaylarının etkin sınıflandırılması ve müdahale edilmesinin sağlanması amacıyla belirlenecek kurallara temel olmak üzere; ŞİRKET personeli ile ŞİRKET kritik envanterinin ve tehditlerin belirlenmesini sağlayacaktır.

9.1.2. Log toplama işlemleri standart araçlar ile gerçekleşmemesi ya da alınan verilerin yetersiz görüldüğü durumlarda yazılıma ait ajan yazılımlar ile gerçekleştirebilir olmalıdır

9.1.3. YÜKLENİCİ, SIEM/SOAR altyapısının mimari analizini gerçekleştirecek ve iyileştirme önerilerini oluşturacaktır. Bu kapsamda asgari aşağıdaki çalışmalar gerçekleştirilecektir

9.1.3.1. ŞİRKET kritik envanteri ve tehditlerinin belirlenmesi

9.1.3.2. Log kaynaklarının belirlenmesi

9.1.3.3. Use case'lerin belirlenmesi

9.1.3.4. Use case'lere göre kaynak log detaylarının belirlenmesi

9.1.3.5. Business case'lerin belirlenmesi

9.1.3.6. Business case'lere göre log kaynaklarının ve gerekli operasyonların belirlenmesi

9.1.3.7. Network ve varlık modelinin incelenmesi

9.1.3.8. İyileştirilecek kuralların belirlenmesi

9.1.3.9. Log toplayıcı ya da bileşen eksiklerinin belirlenmesi

9.1.3.10. Log imzalama konusunda ŞİRKET ile anlaşılması

9.1.3.11. Yazılacak use case'lerin kritiklik seviyelerinin belirlenmesi ve ŞİRKET ile bu konuda anlaşılması

9.1.3.12. ŞİRKET iş alanına özel use case'lerin belirlenmesi

9.1.3.13. SOAR Entegre edilecek kaynakların belirlenmesi

9.2. SIEM & SOC Yazılım Devreye Alma

9.2.1. YÜKLENİCİ Devreye Alma Analizi çıktılarına göre

9.2.1.1. Log toplayıcı ya da eksik bileşenlerin kurulması

9.2.1.2. Eksik log kaynaklarının alınması

9.2.1.3. Parsing hatalarının ve eksiklerinin giderilmesi

9.2.1.4. Log imzalama işlerinin yapılması

9.2.1.5. Hatalı kurallar üzerinde gerekli iyileştirmelerin yapılması

9.2.1.6. Yeni kuralların yazılması

9.2.1.7. Yeni kuralların tuning işlemlerinin yapılması

9.2.1.8. Framework mapping çalışmalarının yapılması (NIST, MITRE vs.)

9.2.1.9. Alarm ve kritikliklerin belirlenip tamamlanması

9.2.1.10. İzleme için SOAR'ın kurulması ve entegrasyonlarının tamamlanması işlemlerini yapacaktır.

9.2.2. YÜKLENİCİ, her <use-case>'i adresleyecek şekilde, iletişim kurulacak ŞİRKET personeli ve iletişim yöntemini içerecek iletişim planları oluşturacaktır.

9.2.3. YÜKLENİCİ, SIEM sistemi üzerinde tanımlı kuralların ve SOAR sistemi üzerinde tanımlı aksiyonların etkinlik kontrolünü gerçekleştirecek ve ilgili tanımların sağlıklı çalışması için gerekli iyileştirmeleri belirleyecek ve gerçekleştirilecektir.

9.2.4. YÜKLENİCİ, Olay yönetimi kapsamında iletişim planlarının içinde bulunduğu bir İletişim Kitabı hazırlayacak ve ŞİRKET'E sunacaktır.

9.2.5. YÜKLENİCİ, Hizmet süresi boyunca ŞİRKET'İN tabi olduğu uyum ve yükümlülüklere bağlı olarak ortaya çıkacak ihtiyaçlarda, yeni korelasyon kurallarını belirleyecek ve SIEM ortamına aktarılmasını sağlayacaktır.

9.2.6. YÜKLENİCİ, hizmet süresi boyunca ihtiyaç duyulacak yeni korelasyon kurallarının yazılmasını ve filtreleme, iyileştirme çalışmalarının sürekli olarak yürütülmesini sağlayacaktır.

9.3. SIEM & SOC Yazılım İzleme ve Müdahale

9.3.1. YÜKLENİCİ, 7 (yedi) gün x 24 (yirmi dört) saat vardiya sistemi ile İzleme yapacaktır.

9.3.2. YÜKLENİCİ, hali hazırda loglanan ve hizmet süresince loglanması planlanan tüm log kaynaklarından 7/24 kesintisiz log geldiğinden emin olunmasını sağlayacak kontrolleri gerçekleştirecektir.

9.3.3. Yüklenicinin ana izleme merkezinde kullanılan izleme sistemlerinde ve ağ bağlantısında bir sorun olması durumunda izleme faaliyetini gerçekleştirmeye devam edebileceği sistemlerin kurulu olduğu yedek bir veri merkezine sahip olacaktır.

9.3.4. Hizmet süresince izleme sistemlerinin kapsamlarında olan değişiklikler de YÜKLENİCİ 'ye bildirilerek izleme kapsamının güncel tutulması sağlanacaktır.

9.3.5. YÜKLENİCİ, alarmın oluşma sebebinin; sunucu, güvenlik ürünleri veya ağ ayarlarındaki bir eksiklikten olduğunu tespit ederse, durumu ŞİRKET'E hemen raporlayacaktır.

9.3.6. YÜKLENİCİ, siber olayın seviyesi KRİTİK ise ŞİRKET'E telefonla, diğer seviyeler için ise e-posta ile en kısa sürede bilgi verecektir.

9.3.7. İzleme faaliyetleri sadece 1. seviye ile sınırlı olmamalıdır. 1. seviyede çözülemeyen alarmlar daha uzmanlık ve detay bilgi gerektiren 2. ve/veya 3. seviye ekiplere eskale edebilecek ekiplere aktarılmalıdır.

9.3.8. Belirlenen güvenlik olayları için detaylı inceleme gerekmesi halinde 2. seviyede Analiz çalışmaları gerçekleştirilecektir. Bu kapsamda;

9.3.9. Değişik zaman aralıkları ve log kaynakları için sorgulama yapılabilecektir.

9.3.10. Olay etkisi ve alınması gereken önlemler belirlenecektir.

9.3.11. YÜKLENİCİ tespit edilen güvenlik olayları için olay bazında ŞİRKET'İN ilgili sorumlularına Olay Bildirim raporu düzenleyerek bildirim sağlayacaktır. Alınması gereken aksiyonlar için ŞİRKET tarafından sağlanan "Servis Sağlayıcı" bilgilerine göre; "SOC temsilcisi" gerekli koordinasyonu sağlayarak alınacak aksiyonların takibini gerçekleştirecektir. Alınmayan aksiyonlar için gerekli raporlama ŞİRKET yetkililerine yapılacaktır. Alınması gereken aksiyon seviyesi kritik ise bilgilendirme acil olarak telefon ile de yapılacaktır.

9.3.12. YÜKLENİCİ, ŞİRKET'E yaptığı olay bildirimleri için ŞİRKET tarafından ilgili bildirimin işleme alındığının teyidinin gelmemesi halinde, iletişim planı çerçevesinde düzenli hatırlatma ve gerekirse eskalasyon sağlayacaktır.

9.3.13. YÜKLENİCİ, SIEM/SOAR platformunda oluşan tüm olayların SLA süreleri dâhilinde incelenmesini, gerekli aksiyonların (bildirim, vs.) alınmasını, sonuçlarıyla birlikte ilgili platform üzerinde kapatılmasını sağlayacaktır.

9.3.14. YÜKLENİCİ izleme sırasında çok fazla gürültü üreten kuralları ŞİRKET ile koordine olarak Seviye-2 analistler ile düzenleyecektir.

9.3.15. YÜKLENİCİ, Olay Yönetimi faaliyetlerini, SOC Devreye Alma Analizi aşamasında hazırlanacak iş akış diyagramlarına uygun olarak gerçekleştirecektir.

9.3.16. Sisteme eklenecek özel uygulamaların ve donanımların verileri için plugin ve parsing hizmetleri YÜKLENİCİ tarafından sunulmalıdır. Genel olarak eklenmiş kaynaklar ya da ŞİRKET'e özel geliştirilen uygulamalar için plugin sorunları tespit edilmeli ve yazılım ekibinin çalışması için olay bildirimi yapılmalıdır.

9.3.17. 5651 sayılı kanun gereği toplanan logların imzalanma durumları YÜKLENİCİ tarafından kontrol edilmelidir. Gün sonu Log İmzalama Takibi, imzalama kontrolleri YÜKLENİCİ tarafından yapılmalı ve imzalama gecikme durumlarında elle tetikleme işlemi yine YÜKLENİCİ tarafından gerçekleştirilmelidir. Logların imzalanmaları ile ilgili imza doğrulama prosedürü YÜKLENİCİ tarafından uygulanmalıdır.

9.3.18. Konfigürasyon değişikliklerinde log kayıpları yaşanması halinde YÜKLENİCİ olay bildirimi yapmalıdır. Log bilgisinin akısının kesilmesi halinde YÜKLENİCİ tarafından olay anında tespit edilip bildirimde bulunulmalıdır.

9.3.19. CPU, RAM ve Disk durumları YÜKLENİCİ tarafından gözlemlenmelidir. Kapasite yetersizliği durumları, herhangi bir soruna neden olmadan önce YÜKLENİCİ tarafından takip edilmeli ve bildirim yapılmalıdır.

9.3.20. ŞİRKET tarafından iletilmiş olan log kaynaklarının SIEM platformuna entegrasyonu ve plugin hizmeti ücretsiz verilmelidir.

9.3.21. Korelasyon kurallarının yazılması ve devreye alınması hizmet süresi boyunca YÜKLENİCİ tarafından sağlanmalı ve raporlanmalıdır.

9.3.22. Mevcut korelasyon kuralları ve eklenen korelasyon kurallarına ek olarak ŞİRKET' in tabi olduğu uyumluluklara bağlı olarak yeni korelasyonların çıkartılması ve SIEM ortamına aktarılması YÜKLENİCİ tarafından sağlanmalıdır.

9.3.23. ŞİRKET' in tabi olduğu uyumluluklara bağlı olarak belirli periyotlarda oluşturulması gereken raporların hazırlanması ve SIEM ortamında otomatize edilmesi sağlanmalıdır.

9.3.24. ŞİRKETİ'İN sistemlerinde atak nedeni ile yaşanabilecek bir çökme ya da kapanma durumunda YÜKLENİCİ sistemlerin ayağa kaldırılması sürecinde aktif olarak yer alacaktır.

9.3.25. YÜKLENİCİ mevcutta kullanılan EPP çözümü için EDR özelliği olmaması durumlarında Windows sunucular için Poor EDR olarak Sysmon kurulumlarını ücretsiz olarak yapmalıdır.

9.3.26. YÜKLENİCİ, Sysmon konfigürasyonlarını ŞİRKET ile paylaşmalı ve güncel atak vektörlerine göre konfigürasyonları güncel tutmalıdır.

9.3.27. YÜKLENİCİ, Sysmon kurallarına göre alarm ve korelasyon kütüphanesini ŞİRKET özelinde güncellemelidir.

9.3.28. ŞİRKET envanterinde bulunan cihazlar üzerinde açık olan portlar internal ve external olarak tespit edilecek ve eş zamanlı olarak ŞİRKET ile paylaşılacaktır.

9.3.29. İnternet üzerinde sürekli olarak Domain ve Subdomain tespiti ve haritalandırması yapılarak, ŞİRKET ile paylaşılacaktır.

9.4. SIEM & SOC Yazılım Sürekli İyileştirme

SIEM/SOAR ürünü üzerinde yapılacak kurulum/devreye alma ve sürekli iyileştirme çalışmaları, belirtilen metodolojik yaklaşımlar ve aşamalara göre yapılmalıdır. Saldırganların bir sisteme sızarken gerçekleştirdikleri faaliyetlerin izlerini tespit etmeye yönelik indikatörler (ifşa, Atak, Zafiyet) tanımlanmalı ve bu indikatörlerin belirli bir dizgiye göre sıralanması sonucu oluşan Atak Senaryoları geliştirilerek etkin şekilde kullanılması hedeflenmelidir.

9.4.1. YÜKLENİCİ, işbu sözleşmede tarif edilen hizmeti bizzat kendisinin istihdam ettiği Seviye-1, Seviye-2 mühendisler ile gerçekleştirecektir.

9.4.2. YÜKLENİCİ'NİN Seviye-1/Seviye-2 mühendisleri bu sözleşme ile satın alımı yapılan SIEM ürününe destek verecek yetkinlikte olmalıdır.

9.4.3. YÜKLENİCİ en az 20 farklı ŞİRKET'te (en az 3 adet enerji sektöründe olması zorunludur) SIEM/SOAR konusunda destek vermiş olmalıdır.

9.4.4. YÜKLENİCİ, ŞİRKET'İN sahip olduğu/olacağı SIEM ürünü üzerinde en az 15K EPS ölçeğinde proje gerçekleştirmiş olmalıdır.

9.4.5. Sürekli iyileştirme kapsamında aşağıdaki çalışmalar yapılacaktır;

9.4.5.1. Periyodik takım lideri görüşmesi

9.4.5.2. Periyodik mühendis kontrolü

9.4.5.3. İzleme hizmetleri kapsamında Seviye-2 analistler tarafında alarm gürültü temizleme operasyonları

9.4.5.4. Teknik destek kapsamında çağrı bazlı operasyonlar

9.4.5.5. Teknik destek kapsamında hizmet boyunca oluşabilecek kural ihtiyaçlarının karşılanması

9.5. SIEM & SOC Aktif Müdahale

Aktif müdahale kapsamında;

9.5.1. YÜKLENİCİ tarafından analiz çalışmaları kapsamında çıkan use case'leri kategorilere ayırılması

9.5.2. ŞİRKET mevcut altyapısında entegrasyona dahil olabilecek teknolojilerin belirlenmesi

9.5.3. Belirlenen teknolojilere göre alınabilecek aksiyonların belirlenmesi

9.5.4. Aksiyonların ilgili kategoriler ile eşleştirilmesi

9.5.5. Alınacak aksiyonların çalışacağı SOAR platformu YÜKLENİCİ tarafından ŞİRKET'İN tahsis edeceği kaynak üzerine kurulacaktır ve YÜKLENİCİ'NİN operasyon merkezinde kullanılan SOAR ile entegre olacaktır.

9.5.6. Aksiyonlar için gerekli otomasyonların Seviye-1/Seviye-2 mühendisler tarafından YÜKLENİCİ tarafından SOAR üzerinde gerçeklenmesi ve test edilmesi

9.5.7. Aktif müdahale hizmetinin devreye alınması işlemleri gerçekleştirilecektir.

9.6. SIEM & SOC Olay Müdahale

9.6.1. YÜKLENİCİ bildirim işleminden itibaren en geç 6 saat içerisinde olaya müdahale edecektir.

9.6.2. YÜKLENİCİ Müdahale/Olay Yönetimi Sürecini detaylı olarak ŞİRKET'E sunar. ŞİRKET gerek görmesi durumunda değişiklik talep edebilir.

9.6.3. YÜKLENİCİ koordinasyon planını ŞİRKET'E sunar. ŞİRKET gerek görmesi durumunda değişiklik talep edebilir.

9.6.4. Olay müdahale koordinasyon planı çerçevesinde müdahale edecek ekip bilgileri (iletişim bilgisi, yetki alanı, vb) müdahale öncesi ŞİRKET yetkililerine bildirilecektir.

9.6.5. YÜKLENİCİ olay müdahale aşamalarında kullanacağı donanım ve yazılımı sağlamalıdır.

9.6.6. Olay müdahale hizmeti başlangıcında YÜKLENİCİ tarafından ŞİRKET'İN SOME personeli ile birlikte bir günlük bir olay müdahale tatbikatı (masa başı ve uygulamalı) gerçekleştirilecektir.

9.6.7. Olay müdahale sonrası etkilenen sistemlerde APT taraması yapılması ve raporlanması yapılacaktır.

9.6.8. Olay müdahale ekibindeki personellerden en az 1 (bir) personel SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling eğitimini almış olmalıdır.

9.6.9. Olay müdahale ekibi içerisinde en az 1'er adet Sistem Uzmanı, Güvenlik Danışmanı ve Sızma Testi uzmanı olmalıdır.

9.6.10. YÜKLENİCİ, olaya müdahaleden sonra 3 (üç) gün içerisinde olaya nasıl müdahale edildiği, neler yapıldığı, bulguların neler olduğu ve olayın etkisi ile ilgili değerlendirmelerin yer aldığı Olay Müdahale Sonuç Raporu'nu ŞİRKET'E teslim edecektir.

9.7. İstila Analizi Yazılımı

9.7.1. Yüklenici işi yürütmek için kullanacağı teknolojiyi ve lisanslamasını sağlayacaktır. Kullanılacak teknoloji;

9.7.1.1. WEB arayüzünden yönetilebilir konsola sahip olacaktır. WEB arayüzünden tüm ajanlar ve kurulan sistem yönetilebilir olacaktır.

9.7.1.2. Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10 ve Windows 11 işletim sistemlerinde çalışabilecektir.

9.7.1.3. Windows Server 2003 ve sonrasında çıkan Windows Server versiyonlarını destekleyecektir.

9.7.1.4. Sistem bir cihazda 120 adet delili toplama işlemini 10 dakikada bitirebilecek ve sonucu gösterebilecektir.

9.7.1.5. Topladığı delilleri zaman damgasıyla damgalayacaktır. Kullandığı zaman damgası RFC 3161 standardına uygun olacaktır.

9.7.1.6. Topladığı delilleri askeri düzeyde kabul gören AES 256 bit şifreleme yöntemi ile şifreleyebilecektir.

9.7.1.7. Topladığı delilleri sıkıştırma yeteneğine sahip olacaktır.

9.7.1.8. Kurulan sistem çalışırken delillerin CryptoLocker zararlılarından etkilenmemesi için kripto kalkan özelliğine sahip olacaktır.

9.7.1.9. Ajan mimarisi ile çalışacak ve ajan paketleri .MSI uzantılı olarak sağlanabilecektir.

9.7.1.10. Topladığı delilleri SFTP protokolü ile farklı bir lokasyona gönderebilecektir.

9.7.1.11. Ajan kurulu olan bir makinenin tüm RAM imajını eksiksiz olarak alabilme yeteneğine sahip olacaktır.

9.7.1.12. Kendi üzerinde YARA kuralları oluşturmaya ve eklemeye olanak sağlayacaktır. Yazılan kurallar eklenmeden önce üzerinden doğrulanabilecektir.

9.7.1.13. ŞİRKET'in etki alanı LDAP entegrasyonu ile etki alanına dahil olan cihazlardan olay bilgisi toplayabilecektir. LDAP bilgileri ayarlara girilerek bağlantıyı test etme özelliği olacaktır.

9.7.1.14. Delil toplanmak istenen istemci ve/veya sunucunun üstüne yeterli disk alanı olması halinde deliller toplanabilecektir.

9.7.1.15. Kapalı ağlarda da kurulabilecek ve çalışabilecektir.

9.7.1.16. ŞİRKET'İN idaresinde bulunan Merkezi Olay Bilgisi Toplama ve Korelasyon Sistemi (SIEM) üne iz kayıt bilgisini TCP veya UDP olarak gönderebilecektir. Ek olarak, alarm sonrası aksiyon (Post-Action) alabilen bir SIEM'de oluşan bir alarm ile tetiklenerek 30 saniye içerisinde, elle müdahale gerekmeden, delil toplama yeteneğine sahip olacaktır.

9.7.1.17. İstemcilerde, ajan üzerinden olay bilgisi toplama işlemi zamanlanmış görev olarak çalışabilecektir.

9.7.1.18. İstenilen sunucu ve/veya istemcilerden belirli aralıklar ile delil toplanmasını mümkün kılacaktır.

9.7.1.19. Toplanacak deliller özelleştirilebilir ve bir profile atanarak ileriki zamanlarda da kullanılabilir olacaktır.

9.7.1.20. Delil toplanan makinede arayüz var ise, ekran görüntüsü alarak toplanılan delilin içerisine koyma özelliği olacaktır.

9.7.1.21. Toplanılan delillerde istemci veya sunucunun kaç bitlik mimari yapısında olduğu bilgisi mevcut olacaktır.

9.7.1.22. Delil toplanan makinenin kullandığı işletim sisteminin detayları delil içerisinde yer alacaktır.

9.7.1.23. Delil toplanan makinenin IP adres ve MAC adres bilgileri toplanan delilde yer alacaktır.

9.7.1.24. Ajan kurulan sistemlerde, ajanın kaç gün önce sisteme kurulduğu bilgisi yer alacaktır.

9.7.1.25. Toplanan deliller yetkili kullanıcı tarafından silinebilecektir. Delillerin silindiği bilgisi iz kayıt olarak saklanarak silinemez veya değiştirilemez olacaktır.

9.7.1.26. Ajan bulunan makineler WEB arayüz üzerinden kapatılabilecek ve/veya yeniden başlatılabilecektir.

9.7.1.27. Ajan yüklü makine üzerinde YARA kuralları ile triaj yaparken CPU limitleme özelliği olacaktır. CPU limiti istenen yüzdesel değerde verilebilecektir.

9.7.1.28. Ajan yüklü makinelerin CPU, RAM ve disk değerleri WEB arayüz üzerinden görülebilir olacaktır.

9.7.1.29. Arayüzünden deliller incelenirken, şüpheli olduğu düşünülen deliller işaretlenebilecek, işaretlenen delillerin hepsi tek bir ekran üzerinde gösterilebilecektir.

9.7.1.30. Toplanan delillerin raporu HTML olarak kaydedilebilecektir.

9.7.1.31. Toplanan delillerden PDF rapor üretilebilecektir. Üretilen rapora sadece istenilen içeriklerin dahil edilmesi mümkün olacaktır.

9.7.1.32. Windows sistemlerde Clipboard, Crash Dump bilgileri, Çöp Kutusu bilgileri, Sistem Geri Yükleme Noktaları, Sürücüler, Süreç ve İşlemler, DNS Cache bilgisi, Proxy Listesi, Disk ve Volume bilgileri, Page File, Swap File, Hibernation File, MFT tablosu, LogFile dosyası, USN Journal dosyası, Registry Hive dosyaları, Network bilgisi (DNS, TCP, UDP cache verileri), Event Log dosyaları, WMI Fonksiyon girdileri, Prefetch dosyaları, Activities DB dosyası, AmCache.hve dosyası, RecentFileCache.bcf dosyalarını toplayabilme ve web arayüzünde okunabilir halde gösterme yeteneğine sahip olacaktır.

9.7.1.33. İstenilmesi durumunda Windows sistemlerden MongoDB iz kayıt bilgilerini, IIS iz kayıt bilgilerini, MSSQL iz kayıt bilgilerini, Microsoft Exchange iz kayıt bilgilerini, DHCP sunucu iz kayıt bilgilerini, DNS sunucu iz kayıt bilgilerini, Aktif dizin iz kayıt bilgilerini, Zoom veritabanını, Teamviewer iz kayıt bilgilerini, Microsoft Outlook e-postalarını, Whatsapp masaüstü cache bilgilerini ve çerezlerini, Skype veri tabanını ve medyalarını, Discord masaüstü cache bilgilerini toplayabilme yeteneğine sahip olacaktır.

9.7.1.34. Linux sistemlerde System kontrol dosyasını, Cron Job dosyasını, AppArmor profilini, ULimit bilgilerini, Kernel modüllerini, Lock dosyalarını, Block Devices bilgilerini, Fstab konfigürasyon bilgilerini, Mount bilgilerini, NFS bilgilerini, Process ve Process open files bilgilerini, Shared memory bilgilerini, Memory map bilgilerini, Kullanıcı gruplarını, kullanıcı listesi bilgilerini, son erişim bilgilerini, bağlı kullanıcı bilgilerini, Sudoers kullanıcı bilgilerini, Başarısız oturum denemeleri bilgilerini, SSH known host bilgilerini, SSH authorized key bilgilerini, SSH config bilgilerini, SSHD config bilgilerini, ICMP tablo bilgilerini, IP route ve table bilgilerini, network interface bilgilerini, ARP tablosu bilgilerini, DNS çözme bilgilerini ve log dosyalarını toplayabilme yeteneğine sahip olacaktır.

9.7.1.35. Dosya yolu verildiğinde altındaki dosya yapılarını delil olarak toplayabilme yeteneğine sahip olacaktır.

9.7.1.36. Şüpheli emare incelemesi yapılacak alanlar Windows işletim sistemleri için tarayıcı geçmişi alanı, Autoruns alanı, Service Analyzer alanı, iz kayıtların tutulduğu Event Recorder alanı, MFT alanı, Prefetch alanı, kullanıc dosya alanı, Shellbas alanı, Events of Interest alanı, Uygulama analiz alanı,

zamanlanmış görevler alanı, DNS bellek alanı, Host dosya alanı, Process alanı, Driver alanı, AMCache alanında incelemeler yapabilecektir.

9.7.1.37. Çalıştığı sistemlerde WebShell taraması ve tespiti yapabilmeli, bulgularını da WEB üzerinden raporda görüntülenebilecektir.

9.7.1.38. Raporda gösterilecek emarelerin kritiklik değeri tarama başlamadan WEB arayüz üzerinden ayarlanabilir olacaktır.

9.7.1.39. Bulunan emarelere kritiklik seviyesi atanarak kullanıcıya rapor olarak sunulabilecektir.

9.7.1.40. Üzerinde toplanan delillerin hepsi üstünden harici bir belleğe toplanabilecektir.

9.7.1.41. Söz konusu teknoloji ŞİRKET'İN belirlediği sayıda, yine ŞİRKET'İN belirttiği uç noktalar üzerine kurulacaktır.

9.7.1.42. Söz konusu teknolojinin kurulumu, kullanıma hazır hale getirilmesi ve işletilmesi YÜKLENİCİ tarafından yapılacaktır.

9.7.1.43. İstila analizi kapsamında YÜKLENİCİ aylık olarak bu çalışmayı gerçekleştirecek ve raporunu ŞİRKET'E sunacaktır

9.7.1.44. İstila analizi kapsamında güncel istila emareleri kural setleri ile uç noktalar üzerinde aramalar yapılacak, bu aramalarda istilaya dair bir emareye rastlanırsa, bununla ilgili saldırı tipini, saldırının hangi aşamada olduğu, yayılımının olup olmadığı ve sonlandırmak için nelere ihtiyaç olduğunu belirten ek raporu ŞİRKET'E sunacaktır.

9.8. Siber Tehdit İstihbaratı Yazılımı

9.8.1.Tehdit Avcılığı

9.8.1.1. YÜKLENİCİ, proje süresince ŞİRKET sistemleri üzerinde güncel atak ve senaryolara göre 6 aylık periyotlarda senaryo bazlı tehdit avcılığı hizmeti verecektir.

9.8.1.2. YÜKLENİCİ tehdit avcılığı hizmetini siber güvenlik alanında en az 5 yıl tecrübeli 3.seviye personel ile sunacaktır.

9.8.1.3. YÜKLENİCİ'NİN hipotez kütüphanesinde en az 10 adet tehdit avcılığı senaryosu olacak, ŞİRKET bunların arasından seçtiği senaryolar ile ilgili sistemler üzerinde araştırma talep edecektir.

9.8.1.4. YÜKLENİCİ'NİN sunduğu hipotez kütüphanesinde olmayan en fazla 2 adet senaryo ŞİRKET tarafından talep edilebilir olacaktır.

9.8.1.5. YÜKLENİCİ, tehdit avcılığı çalışmasından sonra 3 (üç) gün içerisinde detaylı raporu,

9.8.1.6. Hipotezin detaylı açıklaması

9.8.1.7. Hipoteze ait vektörün çalışma biçimi

9.8.1.8. Hipotez ile ilgili hangi sistemler üzerinde hangi yöntemlerle araştırma yapıldığı

9.8.1.9. Çıkan sonuçları

9.8.1.10. Düzeltici önerilerini

9.8.1.11. İçeren bir raporu ŞİRKET'E sunacaktır.

9.8.2.Tehdit İstihbaratı

Yazılım aşağıdaki ana özellikleri sağlamalıdır:

9.8.2.1. Web tabanlı grafik arayüzü (WEB GUI) üzerinden yönetilebilecek ve arayüz aşağıdaki özelliklere sahip olarak olacaktır:

9.8.2.2. Erişim şifreli bir şekilde (HTTPS) sağlanabilecektir.
9.8.2.3. 2FA desteklemelidir.
9.8.2.3.1. Web paneli içerisinde gösterge paneli bulunmalı ve yazılıma yönelik istatistiksel bilgiler sunulmalıdır.
9.8.2.4. Sistem üzerindeki kritik alarmlar, ŞİRKET'E e-posta aracılığıyla da iletilebilecektir.
9.8.2.5. E-posta bildirimlerinin aktiflik pasiflik durumları seviyelere ve alt modüllere göre ayrı ayrı yetkilendirme için düzenlenebilmelidir.
9.8.2.6. Bildirimlere otomatik olarak kritiklik seviyesi atayacaktır.
9.8.2.7. ŞİRKET risk skorunu hesaplayacak ve bu risk skorunu düşürebilmesi için ayrı bir sayfada yol haritası çıkaracaktır ve raporlanacaktır.
9.8.2.8. Yol haritası ilgili ekiplere düzenli şekilde dağıtılabilmesi için Excel formatında indirilebilmelidir.
9.8.2.9. Ticket ID ye göre arama özelliği sunacak ve hızlı erişim için kullanıcılara kolaylık sağlayacaktır.
9.8.2.10. Yazılım ile ilgili gelişmeler veya diğer bildirimler için yazılım içerisinde bir Kullanıcı Bildirimleri alanı olmalıdır ve yazılım kullanan kişilerin gelişmeleri takip etmesi bu yolla sağlanmalıdır.
9.8.2.11. Yazılım izin grupları oluşturabilmelidir ve yazılım kullanıcı bazında yetkilendirme/izin ayarlamaları yapabilmelidir.
9.8.2.12. Yazılım kullanıcılara haftalık olarak risk skoru, kritik bulgular ve açılan bildirimlerin özetini içeren E-posta gönderimi yapmalıdır.
9.8.2.13. Yazılım üzerinde detaylandırılmış sıkılaştırma dokümanları ve raporlar düzenli olarak sunulabilir ve Türkçe olarak dışarı aktarılabilir olmalıdır.
9.8.2.14. Malware, phishing mail gibi zararlı aktivite analiz işlemleri adet gözetilmeden ŞİRKET talebi ile inceleme yapılacaktır.
9.8.2.15. ŞİRKET zararlı bir siber aktiviteyle karşılaşması durumunda bu konuyla ilgili araştırma talebi oluşturmak ve detaylı bilgi almak için bir Ticket sistemi bulunmalıdır.
9.8.2.16. Yazılım aşağıdaki entegrasyon özelliklerine sahip olmalıdır:
9.8.2.16.1. API desteği sunacaktır.
9.8.2.16.2. Ürünün API dokümantasyonuna web üzerinden erişim olmalıdır.
9.8.2.17. ŞİRKET internet üzerindeki siber saldırı olaylarından düzenli olarak haberdar edilmesi için Güvenlik Haberlerini Türkçe içerik ile Yazılım üzerinden bildirmelidir.

9.8.2.18. Ulusal ve küresel siber güvenlik gelişmeleri hakkında genel ve sektörel istihbarat bildirimlerini sistem üzerinden düzenli olarak ŞİRKET'E bildirmelidir.

9.8.2.19. Yazılım içerisinde teknik belge paylaşımları, APT raporları, güvenlik analizleri ayrı bir alanda paylaşılmalı ve kullanıcıların indirmesine açık olmalıdır.

9.8.2.19.1. İçerisinde detaylı rapor alma imkanı bulunmalıdır.

9.8.2.19.2. Tarih aralığına göre filtreleme olmalıdır.

9.8.2.19.3. Varsa alt modüllere göre filtreleme olmalıdır.

9.8.2.19.4. İlgili bulgular seçildikten sonra otomatik olarak minimum CSV ve PDF formatında rapor hazırlanmalıdır.

9.8.2.20. Yazılım içerisinde tespit edilen bulguların sayısı, haftalık olarak e-posta yolu ile bildirimi sağlanmalıdır.

9.8.3. Tehdit İstihbarat Verisi

Yazılım aşağıdaki tehdit istihbaratı paylaşımı özelliklerini sağlamalıdır:

9.8.3.1. Yazılım tespit ettiği zararlı IP adreslerini sürekli güncellemeli ve paylaşmalıdır.

9.8.3.2. Yazılım tespit ettiği zararlı domain adreslerini paylaşmalıdır.

9.8.3.3. Yazılım tespit ettiği zararlı SSL sertifikalarını paylaşmalıdır.

9.8.3.4. Yazılım tespit ettiği zararlı yazılım özetlerini paylaşmalıdır.

9.8.3.5. Yazılım tespit ettiği zararlı mobil uygulama özetlerini paylaşmalıdır.

9.8.3.6. Yazılım sahip olduğu bir honeypot ağından beslenmeli ve honeypot ağı aracılığıyla keşfettiği verileri paylaşmalıdır.

9.8.3.7. Yazılım tespit ettiği zararlı urlleri ve aktiflik pasiflik durumlarını paylaşmalıdır.

9.8.3.8. Yazılım küresel alanda zararlı siber aktivitelerin takibini açık (open source) ve lisanslı olmak üzere çeşitli kaynaklardan yapabilecek ve kendi bal küplerinden (honeypot) gelen veriler ile bu aktivite verilerini zenginleştirerek gösterebilecektir.

9.8.3.9. Yazılım açık kaynaklardan gelen istihbarat verileri içerisinde false-positive ayıklaması yapabilecek ve false-positive alarmlar gösterilmeyecektir.

9.8.3.10. Dış Dünya'da tespit edilmiş zararlı Domain, IP ve zararlı yazılım hash bilgileri txt,csv formatlarında dışarıya aktarılabilir olmalıdır.

9.8.3.11. Yazılım üzerinde gelişmiş sürekli tehditler(APT) için inceleme raporları olacaktır.

9.8.3.12. APT grupları ile ilgili özel bir sayfada, IoC bilgileri, yara kuralları ve grup profillemesi bilgileri yer almalıdır.

9.8.3.13. Küresel ölçekte ŞİRKET'İ ilgilendirebilecek veriler sürekli olarak takip edilip şüpheli olarak tespit edilen aktivitelerin ŞİRKET kritik alarm bilgilendirmesi yapılmalıdır.

9.8.3.14. Küresel ölçekte tespit edilmiş zararlı Domain, IP ve zararlı yazılım hash bilgileri günlük periyotlarda sunulmalıdır.

9.8.4. Marka Koruması

Yazılım aşağıdaki marka koruma özelliklerini 1 (bir) adet ŞİRKET ana domaini için sağlamalıdır:

9.8.4.1. Yazılımda ŞİRKET marka değerini zedeleyecek haber veya içeriklerin takibi sağlanacaktır.

9.8.4.2. Marka değerine yönelik oluşabilecek risklerin bildirimleri sağlanacaktır.

9.8.4.3. ŞİRKET'İN alan adlarına benzer alınan yeni alan adları takip edilmeli ve olası sosyal mühendislik saldırılarına karşı alarm üretilmelidir.

9.8.4.4. ŞİRKET mobil uygulamalarını (Android ve IOS) taklit eden sahte mobil uygulamalar tespit edilecektir.

9.8.4.5. ŞİRKET'İN ve çalışanlarının deep web, dark web, sosyal medya ve siber istihbarat toplanabilecek ortamlarda verileri analiz edilecek ve sızıntı durumlarında alarm üretilecektir.

9.8.4.6. ŞİRKET envanterini ve marka değerini zedeleyebilecek bu durumlar platform üzerinden bildirilecektir.

9.8.4.7. Bildirimler toplu olarak bir ekranda görüntülenebilmeli ve filtrelenebilmelidir.

9.8.4.8. Filtrelemeler daha sonra kullanılabilmek üzere kaydedilebilmelidir.

9.8.4.9. Bildirimlere platform üzerinden yorum yapılabilmeli ve analistiler ile iletişime geçilebilmelidir.

9.8.4.10. Bildirimlerin durumları değiştirilebilmelidir.

9.8.4.11. Bildirimlere ait loglar yine ekran üzerinden görüntülenebilmelidir.

9.8.5. VIP Security

Yazılım aşağıdaki vip koruma özelliklerini en az 10 (on) kişi için lisanslama sağlamalıdır:

9.8.5.1. Yazılımda vip marka değerini zedeleyecek haber veya içeriklerin takibi sağlanacaktır.

9.8.5.2. Marka değerine yönelik oluşabilecek risklerin bildirimleri sağlanacaktır.

9.8.5.3. ŞİRKET'İN belirlediği anahtar kelimeler kullanılarak, sosyal medya üzerinde VIP'ye yönelik oluşabilecek siber tehditler takip edilmeli ve bunlarla ilgili alarm üretilmelidir.

9.8.5.4. VIP kişinin deep web, dark web, sosyal medya ve siber istihbarat toplanabilecek ortamlarda verileri analiz edilecek ve sızıntı durumlarında alarm üretilecektir.

9.8.5.5. Yöneticilere özel dolandırıcılık faaliyetlerinde kullanılan ve tespit edilen TTP paylaşımları platform içerisinden yapılabilmelidir.

9.8.5.6. Bildirimler toplu olarak bir ekranda görüntülenebilmeli ve filtrelenebilmelidir.

9.8.5.7. Filtrelemeler daha sonra kullanılabilmek üzere kaydedilebilmelidir.

9.8.5.8. Bildirimlere platform üzerinden yorum yapılabilmeli ve analistiler ile iletişime geçilebilmelidir.

9.8.5.9. Bildirimlerin durumları değiştirilebilmelidir.

9.8.5.10. Bildirimlere ait loglar yine ekran üzerinden görüntülenebilmelidir.

9.8.6. Periyodik Zafiyet Analizi

Yazılım aşağıdaki sürekli zafiyet analizi özelliklerini ŞİRKET domaini, alt domainler ve alt domain kapsamında DNS kaydı olmayan IP ler için sözleşme süresi boyunca sağlamalıdır:

9.8.6.1. Yazılım zafiyet yönetimini ve raporlamasını sunacaktır.

9.8.6.2. Yazılım içerisinde sağlanan verilere tek bir web paneli üzerinden erişilebilir olmalıdır.

9.8.6.3. ŞİRKET'İN tanımladığı envantere yönelik periyodik güvenlik taramaları gerçekleştirilmelidir.

9.8.6.4. ŞİRKET tarafından belirtilecek olan envanterler özelinde potansiyel zafiyet durumları ve yama bildirimleri yapılmalıdır.

9.8.6.5. Bildirimler minimumda aşağıdaki verileri içermelidir:

9.8.6.5.1. Tespit edilen envanter bilgisi

9.8.6.5.2. Kritiklik seviyesi

9.8.6.5.3. Tespit edilme tarihi

9.8.6.5.4. Zafiyet tipi

9.8.6.5.5. Zafiyet tanımı

9.8.6.5.6. Zafiyet etkisi

9.8.6.5.7. Zafiyet detayları

9.8.6.5.8. Etkilenen port veya parametre

9.8.6.5.9. Payload bilgisi

9.8.6.5.10. Atak araçları

9.8.6.5.11. Varsa ekran görüntüleri veya ekler

9.8.6.5.12. Erişim envanteri

9.8.6.5.13. Kullanıcı profili

9.8.6.5.14. Çözüm önerisi

9.8.6.5.15. Referanslar

9.8.6.6. Bildirimler toplu olarak bir ekranda görüntülenebilmeli ve filtrelenebilmelidir.

9.8.6.7. Filtrelemeler daha sonra kullanılabilmek üzere kaydedilebilmelidir.

9.8.6.8. Bildirimlere platform üzerinden yorum yapılabilmeli ve analistiler ile iletişime geçilebilmelidir.

9.8.6.9. Bildirimlerin durumları değiştirilebilmelidir.

9.8.6.10. Bildirimlere ait loglar yine ekran üzerinden görüntülenebilmelidir.

9.8.7. Sektörel ve Stratejik İstihbarat

9.8.7.1. Enerji sektörüne yönelik Türkiye özelinde ve global çapta güncel tehditler araştırılarak söz konusu tehditler ortaya çıktığı anda ŞİRKET'E bildirilecektir.

9.8.7.2. Enerji sektörü dışında kalmasına rağmen yankı uyandırmış güncel tehditler Türkiye özelinde ve global çapta araştırılarak ŞİRKET'E aylık olarak bildirilecektir. Aylık istihbarat raporunda bu detay hakkında bilgi verilecektir.

9.8.7.3. Sistem ve bilgi güvenlik altyapısında yer alan ürünler (donanım ve yazılım) hakkında yeni bir zafiyet ya da risk ortaya çıktığında ŞİRKET'E bildirimde bulunacaktır. İlgili ürünlerin bilgisi YÜKLENİCİ ile paylaşılacaktır.

9.8.7.4. Sistem ve bilgi güvenlik altyapısında yer alan ürünlere (donanım ve yazılım) yönelik atak vektörleri dünya genelinde araştırılarak ŞİRKET'E düzenli aralıklarla bildirilecektir.

9.8.7.5. Tespit edilen atak vektörleri ile ilgili ŞİRKET'E çözüm önerileri sunulacak, gelebilecek olası ataklara karşı nasıl davranılması gerektiği belirtilecektir.

9.8.7.6. IP/domain/hash sorgulaması API üzerinden yapılabilmelidir.

9.8.8. Dijital Varlık Takibi (VINT) ve Hack Ekosistemi

9.8.8.1. Sektör içerisinde hacklenen web sitesileri, RSS, GDPR ve KVKK bildirimleri için yazılım üzerinden teknoloji kabiliyeti sağlayacaktır.

9.8.8.2. Yazılım kendi üzerinde Tweet Wall, Vulnerability DB, Exploit DB ve teknoloji envanteri ile ilgili alarm mekanizması yazılım üzerinden sağlayacaktır.

9.8.8.3. YÜKLENİCİ, ŞİRKET'E ait ana alan adı, alt alan adları ve ŞİRKET'İN sahip olduğu ilişkisel alan adlarını ve bunların DNS kayıtlarını günlük olarak kontrol edecek, DNS kayıtlarında gerçekleşecek değişiklikleri yazılım üzerinden ve talep edildiğinde API üzerinden bu bilgileri sunacaktır.

9.8.8.4. YÜKLENİCİ, ŞİRKET'E ait ana alan adı ve ŞİRKET'İN sahip olduğu ilişkisel alan adlarının whois kayıtlarını günlük izleyecek ve olası bir değişiklik durumunda yazılım üzerinden ve talep edildiğinde API üzerinden bu bilgileri sunacaktır.

9.8.8.5. YÜKLENİCİ, ŞİRKET'E ait tüm IP adresleri ve ilişkili domainlere ait IP adreslerini düzenli olarak takip edecek ve herhangi bir kara listeye girme durumunda haber verecektir.

9.8.8.6. YÜKLENİCİ, ŞİRKET'E ait tüm IP adresleri ve ilişkili domainlere ait IP adresleri üzerindeki açık servis/portları düzenli olarak takip edecek ve herhangi bir değişiklik (Yeni port açılma, port üzerinde çalışan servisin değişmesi) durumunda haber verecektir.

9.8.8.7. YÜKLENİCİ, ŞİRKET'E ait tüm alan adı, alt alan adı ve ilişkisel alan adlarının web sitelerini günlük olarak kontrol edecek ve web sayfaları içerisinde görülen şüpheli değişiklikleri haber verecektir.

9.8.8.8. YÜKLENİCİ, ŞİRKET'E ait tüm alan adı, alt alan adı ve ilişkisel alan adlarının SSL sertifikalarını, SSL sertifikalarının "expire" sürelerini ve SSL sertifikalarında çıkabilecek zafiyetleri saatlik takip edecek ve görülen şüpheli değişiklikleri haber verecektir.

9.8.8.9. YÜKLENİCİ, ŞİRKET'E ait web siteleri önünde yer alan IPS/WAF gibi cihazların çalıştığını sistemi zora sokmayacak şekilde izleyecek ve olası bir devre dışı kalma durumunda ŞİRKET'E haber verecektir.

9.8.8.10. YÜKLENİCİ, ŞİRKET'E ait tüm ilişkisel alan adlarını, ip adreslerini, ssl sertifikalarını ve aktif portları otomatik olarak tespit edip birbirleri arasındaki ilişkiyi çıkarabilmelidir. ŞİRKET tarafından herhangi bir ek bilgi istenmeksizin bunları otomatik hazır sunabilmelidir.

9.9. Platform Analiz ve Destek

9.9.1.1. İnternet ortamında ŞİRKET'İN markasını zedeleyici bir olay olduğunda olayın araştırılmasına yönelik ücretsiz ve sınırsız analist desteği sağlıyoruz.

9.9.1.2. Tehdit aktörlerinin elinde ŞİRKET ile ilgili fakat henüz paylaşılmayan bir veri tespit edilmesi durumunda ilgili tehdit aktörleriyle iletişime geçilecek ve konuyu detaylandırmaya, elindeki veriyi elde etme çalışması yapılacaktır.

9.9.1.3. Sürekli olarak bilişim sektörü takip edilecek ve önemli görülen istihbaratı ve güvenlik haberlerini Türkçeleştirip yazılım üzerinden ŞİRKET ile paylaşılacak.

9.9.1.4. ŞİRKET'TEN gelecek olan talepler doğrultusunda zararlı yazılım analizi, eğitim, sıkılaştırma gibi siber güvenlik konulu dokümanlar hazırlanacak ve yazılım üzerinden paylaşılacaktır.

10. Eğitim

Şartname kapsamında alınmış olan ürünlere yönelik gerekli eğitimler ŞİRKET'İN talep ettiği zamanlarda katılımcı sınırı olmadan YÜKLENİCİ tarafından ŞİRKET faaliyet alanında bulunan lokasyonlarda veya ŞİRKET 'in uygun bulması durumunda online olarak sağlanacaktır. Ayrıca SIEM&SOC temel eğitimi de YÜKLENİCİ tarafından verilecektir.

11. Lisanslar

SIEM yazılımı en az 7500 EPS olmalıdır. Etik lisanslama olmalıdır ve aktif lisans adedini geçmiş olsa dahi hizmet kesintiye uğramadan devam etmelidir ve ek maliyet çıkmamalıdır.

12. Raporlama

12.1. YÜKLENİCİ 3 aylık periyotlar halinde SIEM olgunluk seviyesi ölçümü yapmalı ve ŞİRKET ile rapor paylaşılmalıdır.

12.2. YÜKLENİCİ 3 aylık periyotlar halinde SOC olgunluk seviyesi ölçümü yapmalı ve ŞİRKET ile rapor paylaşılmalıdır.

12.3. SOC Raporlama

12.3.1. YÜKLENİCİ, haftalık olarak; SIEM/SOC altyapısının sağlık durumu, tespit edilen alarmlar ve alınan aksiyonlar ile ilgili rapor hazırlayacak ve ŞİRKET'E gönderecektir.

12.3.2. YÜKLENİCİ, aylık olarak asgari aşağıdaki bilgileri içerecek şekilde raporlama yapacaktır:

12.3.2.1. Tespit edilen güvenlik olayları ve alınan aksiyonlar,

12.3.2.2. False Positive alarm oranı ve söz konusu oranın aylar bazında karşılaştırması,

12.3.2.3. Güvenlik olayı bazında SLA sürelerine uyum,

12.3.2.4. SOC süreçlerinin işletimi ile ilgili trend analizi (geçmiş dönemler ile ilgili ay içindeki güvenlik olaylarının ve alınan aksiyonların karşılaştırması, vb.)

12.3.2.5. SOC altyapısı ve süreçleri ile ilgili durum analizi ve iyileştirme önerileri

12.4. İstila Analizi Yazılımı

12.4.1.1. İstila analizi kapsamında YÜKLENİCİ aylık olarak çalışmayı gerçekleştirecek ve raporunu ŞİRKET'E sunacaktır.

12.4.1.2. İstila analizi kapsamında güncel istila emareleri kural setleri ile uç noktalar üzerinde aramalar yapılacak, bu aramalarda istilaya dair bir emareye rastlanırsa, bununla ilgili saldırı tipini, saldırının hangi aşamada olduğu, yayılımının olup olmadığı ve sonlandırmak için nelere ihtiyaç olduğunu belirten ek raporu ŞİRKET'E sunacaktır.

12.5. Tehdit İstihbaratı

12.5.1. YÜKLENİCİ periyodik olarak ŞİRKET varlıklarının botnet ağına dahil olup olmadığını ŞİRKET'E raporlayacaktır.

12.5.2. Çözüm üzerinde asgari olarak aşağıdaki raporlar bulunacak, bu raporlar her ay düzenli olarak ŞİRKET'E sunulacaktır.

· Zararlı IP adresi, hash, e-posta ve URL bilgileri

. Marka, üst yönetim ve çalışanlarına ya da müşterilerine yönelik aktif veri sızıntıları

· Sahte alan adları listesi

. ŞİRKET'e ait güvenlik (yazılım, donanım) envanteri zafiyetleri

· Çalıntı hesap ve kart bilgileri

· Enerji sektörü zararlı incelemeleri

· Dünya geneli güncel zararlı incelemeleri

13. Garanti, Bakım ve Kabul

Garanti süresince YÜKLENİCİ ŞİRKET'ten hiçbir ücret talep edemez. Garanti kapsamında bakım, onarım, parça değişimi ve nakliye de dahil olmak üzere tüm masraflar YÜKLENİCİ tarafından karşılanır.

Garanti süresince ürüne müdahale yapılması gerektiğinde, mümkün ise ürünün kullanım yerinde gerekli müdahale yapılır.

13.1. Garanti Şartları ve Süresi

Ürün sözleşme süresi boyunca YÜKLENİCİ garantisi altında olup tüm talepler herhangi bir ek maliyet talep edilmeden YÜKLENİCİ tarafından karşılanacaktır.

13.2. Bakım

Ürünün güncellenmesi, yama geçilmesi vb. işlemler ŞİRKET talepleri doğrultusunda YÜKLENİCİ tarafından sözleşme kapsamında yapılacaktır.

13.3. Kesin kabul

Ürünün tüm entegrasyonları birlikte kurulması ve aktif olarak çalışır hale getirilmesi sonrasında ŞİRKET'in yazılı onayıyla kesin kabul yapılacaktır. Yaygınlaştırma işlemleri kesin kabul sonrasında devam edecektir.

14. Birim Fiyatlar ve Birim Fiyat Tarifeleri

-

15. İşin Yürütülmesi için Gerekli Personel ve Araç, Gereç ve Malzemeler

15.1. SOC/SGOM Personel Yetkinlikleri

15.1.1. YÜKLENİCİ'nin çalıştıracağı Seviye-1 analist (izleme yapan personel) personel yetkinlikleri aşağıdaki şekilde olacaktır.

15.1.1.1. Minimum 2 yıllık bir üniversitenin teknik bölümlerinden mezun olmak.

15.1.1.2. İyi derecede İngilizce bilmeli.

15.1.1.3. Problem çözme yetkinliğinin gelişmiş olması.

15.1.1.4. İnsanlarla iletişim ve takım çalışmasına uyum yetkinliklerinin gelişmiş olması.

15.1.1.5. Temel güvenlik protokolleri hakkında bilgi sahibi olması.

15.1.1.6. Firewall, IPS, Loadbalancer, DDOS koruma, Antivirüs gibi güvenlik cihazlarına hakim ve bu cihazlardan gelen log ve alarmları anlaması.

15.1.1.7. Tercihen SIEM deneyimi olması ve çalışma mantığına hakim olması.
15.1.1.8. Tercihen bir SIEM ürünü sertifikasına sahip olması.
15.1.1.9. Tercihen CEH sertifikasyonuna sahip olması.

15.2. YÜKLENİCİ'nin sağlayacağı Seviye-2 analist personellerin yetkinlikleri aşağıdaki şekilde olacaktır

15.2.1. Minimum 2 yıllık bir üniversitenin teknik bölümlerinden mezun olmak.
15.2.2. Minimum 2 yıl IT Güvenliği konusunda deneyimi olması.
15.2.3. İyi derecede İngilizce bilmeli.
15.2.4. Problem çözme yetkinliğinin gelişmiş olması.
15.2.5. İnsanlarla iletişim ve takım çalışmasına uyum yetkinliklerinin gelişmiş olması.
15.2.6. Temel güvenlik protokolleri hakkında iyi derecede bilgi sahibi olması.
15.2.7. Firewall, IPS, Loadbalancer, DDOS koruma, Antivirüs gibi güvenlik cihazlarına hakim ve bu cihazlarda operasyonel deneyimi olması.
15.2.8. Sunucu ve Sistem güvenliğine hakim olması, atak olduğunda sistemlerde araştırma yapabilecek ve güvenlik olay loglarını anlamlandırabilmesi.
15.2.9. Mevcut atak ve tehditleri analiz edebilmesi.
15.2.10. Seviye-1 analistlerin değerlendiremediği karmaşıklıkta problemlere destek vermeli ve kök sorun analizi yapabilmelidir.
15.2.11. Atak analizi yapabilmeli, olay korelasyon ve analiz konularında ileri seviyede deneyim sahibi olmalı.
15.2.12. SIEM deneyimi olmalı ve çalışma mantığına hakim olmalı.
15.2.13. Bir SIEM ürünü sertifikasına sahip olmalı.
15.2.14. Tercihen CEH sertifikasyonuna sahip olmalı

15.3. YÜKLENİCİ'NİN sağlayacağı Seviye-3 analist personellerin yetkinlikleri aşağıdaki şekilde olacaktır

15.3.1. Minimum 4 yıllık bir üniversitenin teknik bölümlerinden mezun olmak.
15.3.2. Minimum 5 yıl IT Güvenliği konusunda deneyimi olması.
15.3.3. İyi derecede İngilizce bilmeli.
15.3.4. Problem çözme yetkinliğinin gelişmiş olması.
15.3.5. İnsanlarla iletişim ve takım çalışmasına uyum yetkinliklerinin gelişmiş olması.
15.3.6. Temel güvenlik protokolleri hakkında iyi derecede bilgi sahibi olması.
15.3.7. Olay Müdahale konusunda bilgi ve tecrübe sahibi olması.
15.3.8. Firewall, IPS, Loadbalancer, DDOS koruma, Antivirüs gibi güvenlik cihazlarına

hakim ve bu cihazlarda operasyonel deneyimi olması.

15.3.9. Ofansif güvenlik metodolojileri konusunda bilgi ve tecrübe sahibi olması

15.3.10. Seviye-2 analistlerin değerlendiremediği karmaşıklıkta problemlere destek vermeli ve kök sorun analizi yapabilmelidir.

15.3.11. Atak analizi yapabilmeli, olay korelasyon ve analiz konularında ileri seviyede deneyim sahibi olmalı.

15.3.12. Tercihen CISSP veya SANS EITCA/IS sertifikasyonuna sahip olmalı

16. Teklif Fiyatına Dahil Olan/Olmayan Hususlar

Sözleşmenin amir hükümleri geçerlidir.

17. Teslimat

Sözleşmenin amir hükümleri geçerlidir.

18. Fiyat Farkları ile İlgili Hususlar

Sözleşmenin amir hükümleri geçerlidir.

19. Yüklenicinin Çalıştırdığı Personel

19.1. Çevre sağlığı

Yüklenici ŞİRKET lokasyonlarda gerçekleştireceği işler esnasında tüm çevre kanun ve yönetmeliklerine uyarak, çevreyi koruyacak şekilde işlerini yürütmekle yükümlüdür.

19.2. İş Sağlığı ve Güvenliği

YÜKLENİCİ,

- Kanun ve yönetmeliklerde öngörülen her türlü önlemin yanında, o işyerinde iş güvenliğini sağlamak için gerekli olan ve bilimin, tecrübenin, teknolojinin imkân verdiği her türlü önlemi mevzuatta hükme bağlanmamış olsa da almakla,
- İşyerinde iş sağlığı ve güvenliği organizasyonu kurmak iş kazası ve meslek hastalığı risklerini tespit etmek ve bunlara karşı tedbir alınmasını sağlamak,
- İşyerinde güvenli bir şekilde çalışılmasını sağlamak üzere gerekli kontrollerin yapılmasını koordine etmek,
- Hizmete konu olan işle ilgili çalışanlarına mevzuatın zorunlu kıldığı süre ve nitelikte İSG eğitimi ve mesleki eğitimleri vermek,
- İşin yürütülmesi esnasında gerekli her türlü sağlık ve güvenlik önlemlerini (ortam güvenliğini sağlamak, uygun kişisel koruyucu donanımları temin etmek vb.) almak,
- Periyodik kontrol ve muayene gerekliliği olan malzeme, ekipman, KKD bulunması durumunda, gerekli kontrollerin periyodik olarak yapılmasını sağlamak ve kayıt altına almak,
- Çalışanların sahada tanımlanmış İSG kurallarını uygulamalarını güvence altına almak için gözetim ve denetimler yapmak ve istendiğinde gösterilmek üzere bu gözetim ve denetimleri kayıt altına almış olmak,
- SEDAŞ taşınmazları içerisinde görev yapan çalışanlarının SEDAŞ Ziyaretçi Aydınlatma Metnini imzalamasını sağlamak,
- İSG mevzuatı gereği tüm kayıtları muhafaza etmek,
- Sözleşmeye uygunluğu takip etmek ile yükümlüdür.

19.3. Ayrım

YÜKLENİCİ, elemanları kişilik özelikleri veya inançları temelinde değil, işi yapabilme becerilerini esas alarak; din, dil, ırk, renk, cinsiyet, uyruk, yaş, hamilelik veya medeni durum ayırımı yapmaksızın istihdam edecektir.

Aynı zamanda tüm çalışanlarına ücret ve sosyal haklar sağlarken; din, dil, ırk, renk, cinsiyet, uyruk, yaş, hamilelik veya medeni durum ayırımı yapmayacaktır.

19.4. Zorla Çalıştırma

YÜKLENİCİ, herhangi bir şekilde insan ticaretine iştirak edemez, zorla, gönülsüz ve köle işçi çalıştıramaz ve bu tür eleman çalıştıran şirketlerden malzeme veya hizmet satın alamaz.

19.5. Çocukların Çalıştırılması

YÜKLENİCİ, 18 yaşını doldurmamış çalışanı kesinlikle istihdam etmeyecektir.

19.6. Birlik Kurma Özgürlüğü

YÜKLENİCİ çalışanları; yasalara uygun şekilde birlik kurma veya kurulmuş olanlara katılma özgürlüğüne sahiptirler.

20. Yönetim Sistemi

YÜKLENİCİ, yürürlükte bulunan yasalara, düzenlemelere ve SEDAŞ'ın ilkelerine uygun bir yönetim sistemine sahip olmalı, bu sistemin sürekli bir şekilde geliştirilmesi ve değişen yasalara ve düzenlemelere uyacak şekilde uyumluluğu sağlamaları gerekmektedir.

SEDAŞ hizmet sağlayan Yüklenicilerine, Kalite (ISO9001), Çevre (ISO14001), İş Sağlığı ve Güvenliği (ISO 45001) vb. sistemleri sağlamalarını tavsiye etmektedir.