Privia SECURITY

SOC Olgunlaştırma Hizmeti

Profesyonel Defensive Security Hizmetleri

"Operasyon Merkezinizi Güçlendirin!"

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

"Güçlü bir SOC, tehditleri hızla tespit etme ve bunlara anında yanıt verme kabiliyetiyle organizasyonun siber güvenliğine katma değer sağlar."

SOC (Security Operations Center) Olgunlaştırma Hizmeti, organizasyonların siber güvenlik operasyonlarını daha etkin ve verimli hale getirmek amacıyla tasarlanmıştır. SOC'un mevcut yeteneklerini değerlendirerek, süreçlerin, teknolojilerin ve insan kaynaklarının optimize edilmesi hedeflenir. SOC-CMM (Security Operations Center Capability Maturity Model) gibi uluslararası kabul görmüş çerçeveler kullanılarak, SOC'un olgunluk seviyesi belirlenir ve geliştirilmesi gereken alanlar tespit edilir.

Hizmet kapsamında öncelikle SOC'un mevcut durumu detaylı bir şekilde analiz edilir. Analizler süreçlerin etkinliği, kullanılan teknolojilerin yeterliliği ve personelin yetkinlik düzeyini kapsar. Değerlendirmeler SOC-CMM gibi modellerin kriterlerine göre yapılır ve uluslararası standartlarla uyumlu bir yol haritası oluşturulur. Analiz sonrasında belirlenen geliştirme alanlarına yönelik stratejik bir plan oluşturulur. Oluşturulan plan, süreçlerin iyileştirilmesi, teknolojik altyapının güçlendirilmesi ve personelin eğitim ihtiyaçlarını içerir.

Süreçlerin standardizasyonu, otomasyonun artırılması ve en iyi uygulamaların entegrasyonu sağlanır. Ayrıca personelin yetkinliklerini artırmak için düzenli eğitim programları ve tatbikatlar düzenlenir. Teknolojik altyapı, güncel tehditlere karşı korunacak şekilde güncellenir ve optimize edilir. SOC'un performansı düzenli olarak ölçülür ve elde edilen veriler ışığında gerekli iyileştirmeler yapılır.

Hizmete Ait Bileşenler

Mevcut Durum Değerlendirmesi

Mevcut durum değerlendirmesi, SOC'un genel operasyonel seviyesini ve yeteneklerini anlamaya yönelik ilk adımdır. Değerlendirme süreci SOC'un mevcut güvenlik altyapısını, kullanılan teknolojileri ve işleyişini analiz ederek başlar. SOC'un ne kadar etkili çalıştığını görmek için kullanılan araçlar, tehdit istihbaratı altyapısı ve olay yönetimi gibi unsurlar ayrıntılı bir incelemeden geçirilir. Ayrıca SOC personelinin teknik yetkinliği, bilgi düzeyi ve görevlerdeki etkinliği bu değerlendirme kapsamında ele alınır. Mevcut güvenlik tehditlerine karşı SOC'un ne kadar hazırlıklı olduğu ve yanıt verebilme kapasitesi gözlemlenir. SOC'un işlevselliğini artırmak için gerekli iyileştirme alanları belirlenerek somut veriler elde edilir. Ekiplerin kriz anındaki performansı ve iş birliği yetenekleri de değerlendirilir.

Boşluk (GAP) Analizi

Boşluk analizi, SOC'nin mevcut durumu ile hedeflenen olgunluk seviyesi arasındaki farkları belirlemek için yapılır. Analiz sırasında SOC'nin operasyonel süreçleri, teknoloji kullanımı, insan kaynağı ve tehdit yönetim yetkinlikleri detaylı olarak incelenir. SOC-CMM çerçevesine göre yapılan analizler sayesinde SOC'nin hangi seviyede olduğu ve hangi seviyeye ulaşması gerektiği konusunda bir yol haritası oluşturulur. Boşluk analizi, güvenlik zafiyeti tespitinden olay müdahaleye kadar SOC'nin tüm işleyişini kapsayan bir analiz çalışmasıdır. Mevcut ile hedeflenen olgunluk seviyesi arasındaki farkların belirlenmesi, hangi alanlarda öncelikli iyileştirme yapılması gerektiğini netleştirir. Analiz sonucunda, güvenlik süreçlerinde hangi geliştirmelerin yapılması gerektiği tespit edilir.

Yol Haritası Oluşturma

Yol haritası, SOC'nin hedeflenen olgunluk seviyesine ulaşması için stratejik bir plan oluşturarak başlar. Yol haritası süreç iyileştirmeleri, teknoloji güncellemeleri, eğitim gereksinimleri ve diğer operasyonel gelişimleri kapsayan adımları içerir. Yol haritası kısa, orta ve uzun vadeli hedefler belirleyerek SOC'nin olgunlaşma sürecindeki ilerlemesini yapılandırır. Olaylara hızlı müdahale süreçlerinin oluşturulması ve verimliliği artıran yeni teknolojilerin SOC'ye entegre edilmesi planlanır. Her bir geliştirme adımı için belirli bir zaman çizelgesi oluşturulur ve bu süreçler net hedeflerle desteklenir.

Süreç ve Prosedür Geliştirme

Süreç ve prosedür geliştirme, SOC'nin tüm operasyonlarını daha verimli ve hızlı hale getirmek için yapılan iyileştirmeleri içerir. Mevcut güvenlik süreçleri detaylı olarak incelenir ve iyileştirilmesi gereken alanlar belirlenir. Tehdit tespitinden olay müdahaleye kadar olan tüm süreçler uluslararası standartlara uygun olarak optimize edilir. Güvenlik olaylarına hızlı müdahale sağlamak için süreçlerde sadeleştirme ve standartlaştırma yapılır. Yapılan iyileştirmeler SOC personelinin rollerini daha iyi

anlamasını ve kriz anında doğru görev dağılımını yapmasını kolaylaştırır. Otomasyon araçlarının entegrasyonu ile süreçler daha hızlı ve verimli hale getirilir.

Teknoloji ve Araçların Değerlendirilmesi

Teknoloji ve araçların değerlendirilmesi, SOC'nin mevcut güvenlik altyapısının etkinliğini artırmaya yönelik bir analiz sürecidir. SOC'nin tehdit istihbaratı, olay müdahale, SIEM ve EDR gibi temel güvenlik araçlarının yetkinliği incelenir. SOC'nin siber tehditlerle etkin mücadele edebilmesi için güncel teknolojilere ihtiyaç duyulur, bu nedenle mevcut araçlar iyileştirilir veya gerekli yenilikler yapılır. Güvenlik araçlarının uyumluluğu ve performansı, SOC operasyonlarının hız ve doğruluğunu etkileyen önemli bir unsurdur. SOC'nin tehdit algılama, müdahale ve izleme kapasitesi gerçekleştirilen değerlendirmeler ışığında optimize edilir.

Eğitim ve Farkındalık Programları

SOC personelinin yetkinliklerini artırmak amacıyla düzenlenen eğitim ve farkındalık programları, SOC olgunlaştırma sürecinin önemli bir parçasıdır. Eğitimler, personelin siber tehditler karşısında daha bilinçli ve donanımlı olmasını sağlar. Eğitim programları, personelin teknik yeteneklerini geliştirmenin yanı sıra kriz anında iş birliği içinde hareket etme becerilerini de güçlendirir. Farkındalık programları ise sadece SOC personelini değil, tüm organizasyon çalışanlarını siber tehditler konusunda bilinçlendirmeyi amaçlar. Eğitimlerde tehdit tespiti, olay müdahale ve güvenlik araçlarının etkin kullanımı gibi temel konular ele alınır.

Performans İzleme ve Sürekli İyileştirme

SOC'nin performansının düzenli olarak izlenmesi ve iyileştirilmesi, dinamik tehdit ortamına uyum sağlamak için önemli bir adımdır. Performans izleme, SOC'nin tehdit tespiti, olay yanıt ve genel operasyonel verimliliğini değerlendirmeyi amaçlar. Çeşitli performans göstergeleri (KPI) kullanılarak SOC'nin mevcut durumu ölçülür ve veriler sürekli analiz edilir. Elde edilen sonuçlara göre SOC'nin operasyonel eksiklikleri belirlenir ve iyileştirme adımları planlanır. Sürekli iyileştirme, SOC'nin esnek ve uyarlanabilir bir yapıya kavuşmasını sağlar. Performans izleme sayesinde, SOC'nin zaman içinde nasıl geliştiği ve hangi alanlarda iyileştirme gerektiği tespit edilir.

Sık Sorulan Sorular

SOC olgunlaştırma hizmeti nedir ve organizasyonlara nasıl bir katkı sağlar?

SOC olgunlaştırma hizmeti, bir organizasyonun Güvenlik Operasyon Merkezi'nin (SOC) etkinliğini artırmayı hedefleyen kapsamlı bir süreçtir. SOC'nin tehdit tespit etme, yanıt verme ve güvenlik olaylarını önleme kapasitesini geliştirmeyi amaçlar. Olgun bir SOC, organizasyonun güvenlik risklerini daha hızlı ve doğru bir şekilde yönetmesini sağlar. Ayrıca operasyonel verimliliği artırarak kaynakların daha etkin kullanılmasına katkıda bulunur. Organizasyonlar, SOC olgunlaştırma süreci ile uluslararası güvenlik standartlarına daha kolay uyum sağlar.

SOC olgunluk seviyeleri nelerdir ve nasıl belirlenir?

SOC olgunluk seviyeleri genellikle beş ana aşamada değerlendirilir. Başlangıç, gelişmekte olan, tanımlanmış, yönetilen ve optimize edilmiş. Başlangıç seviyesinde SOC temel işlevleri yerine getirirken, optimize edilmiş seviyede süreçler sürekli iyileştirilir ve en iyi uygulamalar benimsenir. Olgunluk seviyeleri, SOC'nin süreçleri, teknolojileri ve insan kaynakları gibi bileşenlerinin derinlemesine incelenmesiyle belirlenir. SOC olgunluğunun değerlendirilmesinde SOC-CMM gibi çerçeveler sıklıkla kullanılır. Çerçeveler her bir seviyeyi tanımlayan kriterler sunarak SOC'nin mevcut durumu hakkında net bir tablo oluşturulmasına yardımcı olur. Olgunluk seviyesinin belirlenmesi, SOC'nin hangi alanlarda iyileştirme yapılması gerektiğini saptamaya yardımcı olur.

SOC olgunlaştırma sürecinde hangi adımlar izlenir?

SOC olgunlaştırma süreci, bir dizi stratejik adımla yapılandırılır. İlk olarak organizasyonun mevcut SOC yapısı değerlendirilir ve bu yapının olgunluk seviyesi belirlenir. Ardından SOC'nin güçlü ve zayıf yönleri tespit edilerek boşluk analizi yapılır. Gerçekleştirilen analizlere dayanarak, kısa ve uzun vadeli hedefler içeren bir yol haritası oluşturulur. Süreç ve prosedürler yeniden yapılandırılarak operasyonel etkinlik artırılır. Eğitim ve farkındalık programları ile SOC personelinin yetkinlikleri geliştirilir. Teknolojik altyapı güçlendirilerek tehditlere karşı daha dayanıklı bir yapı oluşturulur. Performans izleme ve sürekli iyileştirme adımları ile SOC'un etkinliği artırılır.

SOC olgunlaştırma sürecinde hangi çerçeveler ve standartlar kullanılır?

SOC olgunlaştırma sürecinde SOC-CMM gibi olgunluk modelleri önemli bir rehber olarak kullanılır. NIST SP 800-53 ve ISO/IEC 27001 gibi uluslararası standartlar da süreci yön verir. Çerçeveler SOC'nin süreçlerini, teknolojilerini ve personel becerilerini yapılandırmada yol gösterir. SOC-CMM, SOC'nin mevcut kapasitesini ve olgunluk seviyesini belirlemek için detaylı bir model sunar. Kullanılan standartlar, SOC'nin uluslararası en iyi uygulamaları benimsemesini sağlar. Aynı zamanda düzenleyici gerekliliklerin karşılanmasına da yardımcı olur.

SOC olgunlaştırma sürecinin organizasyonlara sağladığı faydalar nelerdir?

SOC olgunlaştırma süreci, organizasyonlara operasyonel verimlilik ve siber güvenlik açısından önemli faydalar sağlar. Tehdit tespiti ve yanıt süreçlerinin hızlanması, organizasyonun riskleri daha etkin bir şekilde yönetmesine olanak tanır. Operasyonel verimlilik artışı, kaynakların etkin kullanılmasını sağlar ve maliyetleri azaltır. Güvenlik olaylarına hızlı müdahale, iş sürekliliği açısından önemli bir avantajdır. Personelin teknik becerileri geliştirilir ve güvenlik farkındalığı artırılır. Uluslararası standartlara uyum sağlanması, yasal gerekliliklerin karşılanmasına yardımcı olur.

SOC olgunlaştırma sürecinde karşılaşılan zorluklar nelerdir?

SOC olgunlaştırma sürecinde, organizasyonlar çeşitli zorluklarla karşılaşabilir. Bütçe kısıtlamaları, yeterli kaynak sağlama konusunda engeller oluşturabilir. Eğitim ihtiyacı, personelin mevcut bilgi seviyesine uygun olarak planlanmalıdır. Teknolojik entegrasyon sorunları, yeni sistemlerin mevcut altyapıyla uyumlu olmasını gerektirir. Süreçlerin standardizasyonu, bazı organizasyonlarda dirençle karşılanabilmektedir. Ayrıca üst yönetim desteği olmadan SOC olgunlaştırma süreci zor ilerleyebilir. İletişim eksiklikleri ve geri bildirim süreçleri de gelişime açık alanlar olarak öne çıkar.

SOC olgunlaştırma süreci ne kadar sürer?

SOC olgunlaştırma süreci, organizasyonun mevcut durumuna ve hedeflenen olgunluk seviyesine bağlı olarak değişiklik gösterebilir. Genel olarak kapsamlı bir olgunlaştırma süreci birkaç ay ila bir yıl arasında sürebilir. Başlangıç aşamasındaki bir SOC için süreç daha uzun sürebilirken, olgun seviyeye yakın bir SOC için daha kısa bir süre yeterli olabilir. Süreç mevcut teknolojilerin ve politikaların değerlendirilmesi, boşluk analizinin yapılması ve yol haritasının oluşturulması ile başlar. Süreçte performans izleme ve sürekli iyileştirme adımlarıyla SOC'nin geliştirilmesi sağlanır. Teknoloji entegrasyonları ve süreç standardizasyonları da süreyi etkileyen unsurlar arasındadır.

SOC olgunlaştırma sürecinde hangi metrikler kullanılır?

SOC olgunlaştırma sürecinin başarısını ölçmek için çeşitli metrikler kullanılır. Tehdit tespit süresi, yanıt süresi ve müdahale süresi gibi operasyonel metrikler bu süreçte önemli yer tutar. Ayrıca yanlış alarm oranı (F/P), olay başına harcanan süre ve olay başına maliyet gibi metrikler de izlenir. Eğitim ve farkındalık seviyeleri, personelin yetkinlik düzeylerini ölçmek için kullanılır. Performans göstergeleri (KPI'lar) ile SOC'nin süreç etkinliği ve işlevselliği analiz edilir. Teknoloji etkinliği ve araçların kullanılabilirliği gibi metrikler de değerlendirme kapsamına alınır.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

Privia
SECURITY