Privia SECURITY

Defensive as a Service

Profesyonel Defensive Security Hizmetleri

"Operasyon Merkezleri için Tamamlayıcı Güç!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Siber saldırıları, güvenlik zafiyetlerini hızla tespit etmek ve vakalara anında müdahale etmek için siber güvenlik operasyon merkezlerinin tamamlayıcı unsuru."

Profesyonel Defensive Hizmetlerimiz (Defensive as a Service), organizasyonların siber güvenlik altyapılarını güçlendirmesi ve olası siber tehditlere karşı savunma becerilerini artırması amacıyla tasarlanmış kapsamlı bir hizmettir. SOC (Siber güvenlik operasyon merkezi, SGOM) altyapılarının güvenliği sağlanarak, siber güvenlik tehditlerinin tespit edilmesi ve müdahale edilmesi sağlanır. Profesyonel Defensive Hizmetlerimiz, tüm güvenlik operasyonlarını bir araya getirerek kurumların siber güvenlik durumunu sürekli olarak değerlendirmelerini ve iyileştirmelerini mümkün kılar.

SOC olgunlaştırma, tehdit istihbaratının entegrasyonu, EDR, SIEM, SOAR yönetimi gibi hizmetler, organizasyonun savunma sisteminin tüm bileşenlerini kapsar. Organizasyonlar, olası tehditleri analiz ederek proaktif bir koruma sağlayabilir ve olay yönetim süreçlerini olgunlaştırabilir. Hizmetin sağladığı bir diğer önemli özellik ise tehdit istihbaratının kurumsal yapıya entegre edilmesidir. Global tehdit istihbaratı ağlarından elde edilen veriler analiz edilerek organizasyon özelinde uygulanabilir hale getirilir. Tehdit istihbaratı entegrasyonu, karar alma süreçlerini hızlandırarak, saldırılara daha kısa sürelerde yanıt verilmesini sağlar.

Defensive as a Service ayrıca SIEM yönetiminde optimizasyon sunarak güvenlik verilerinin düzenli ve anlamlı bir şekilde analiz edilmesini sağlar. SIEM sistemleri, güvenlik ekiplerinin gerçek zamanlı tehditleri belirlemesine yardımcı olur. Aynı zamanda geçmiş verilere dayanarak gelecekteki tehditleri öngörebilmeyi sağlar. Defensive as a Service, kurumların elektronik/dijital varlıklarını koruma altına alarak, güvenlik operasyonlarını daha verimli hale getirmeyi amaçlar. Güvenlik zafiyetlerini tespit eden, anlık olarak tehditlere karşılık veren ve riskleri minimize eden bu hizmetimiz, organizasyonlara siber saldırılara karşı uzun vadeli bir perspektif ile sürdürülebilir bir koruma sağlar.

Hizmete Ait Bileşenler

L1-L2 ve L3 Seviye Analiz Hizmeti

Siber güvenlik operasyon merkezinde (SOC) tespit edilen tehditlerin farklı uzmanlık seviyelerinde analiz edilmesini sağlayan bir süreçtir. L1, temel seviye güvenlik izleme ve hızlı yanıt sürecini kapsarken; L2, tehditlerin daha ayrıntılı incelenmesini ve karmaşık olayların çözümünü içerir. L3 ise, ileri düzeyde adli analiz ve kök neden analizleriyle karmaşık saldırılara karşı stratejik çözümler sunar.

L1 Seviye Analiz Hizmeti

L1 seviye analiz hizmeti, siber güvenlik izleme sürecinin ilk aşamasını oluşturarak olayların hızlıca tespit edilmesi ve ön analiz yapılmasını sağlar. L1 Analistler temel siber güvenlik olaylarını değerlendirme ve gerekirse olayları bir üst seviyeye (L2) eskale etme sorumluluğuna sahiptir. L1 analistler, düşük riskli olayları inceleyerek false/positive alarmları ve bazı daha karmaşık olayları inceleyerek, ilgili üst analizlere yönlendirir.

L2 Seviye Analiz Hizmeti

L2 seviye analiz hizmeti, daha ayrıntılı bir olay incelemesi gerektiren güvenlik olayları için analiz sürecini derinleştirir. L2 seviye analist, L1 seviyesinden gelen olayları detaylı bir şekilde değerlendirerek risk analizlerini gerçekleştirir ve gerektiğinde yanıt prosedürlerini başlatır. L2 analistler, olayların kök nedenini araştırarak tekrarlayan tehditler için kalıcı çözümler geliştirmeye çalışır. Ayrıca, daha karmaşık saldırıların analiz edilmesi ve tehditlerin kaynaklarının belirlenmesi gibi görevleri üstlenir.

L3 Seviye Analiz Hizmeti

L3 seviye analiz hizmeti, ileri düzey analiz ve kök neden incelemelerini içeren en üst seviye güvenlik analizidir. L3 analistler, karmaşık saldırı senaryolarını değerlendirerek sofistike tehditlere karşı stratejik çözümler sunar. L3 seviye analiz, adli analiz ve tehdit istihbaratı kullanarak saldırganların yöntemlerini ve motivasyonlarını detaylı bir şekilde analiz etmeye odaklanır.

Ürün ve Teknoloji İşletme (MDR)

Ürün ve Teknoloji İşletme, organizasyonların siber güvenlik altyapısını destekleyen çeşitli güvenlik ürünlerinin yönetimini ve işletilmesini kapsar. Siber güvenlik operasyonlarının sürdürülebilir ve kesintisiz bir şekilde yürütülmesini sağlayarak tehditlere karşı sürekli koruma sunar. MDR (Managed Detection and Response) yaklaşımına uygun olarak, Tenable, Picus, ThreatMon, Trellix (McAfee ve FireEye), Wazuh, PaloAlto, DarkTrace, BurpSuite gibi güvenlik çözümlerinin etkin işletilmesi sağlanır. Hizmet, siber güvenlik ekiplerinin bu teknolojilerden en yüksek verimi almasını sağlar.

SOC Olgunlaştırma

SOC olgunlaştırma, siber güvenlik operasyon merkezi (SOC-SGOM) altyapısının güçlendirilmesi ve yeteneklerinin uluslararası standartlar çerçevesinde geliştirilmesini amaçlar. Süreç boyunca SOC ekiplerinin kapasitesi, teknolojik araçlar ve süreçlerin etkinliği değerlendirilerek, iyileştirme ihtiyacı tespit edilen alanlar belirlenir. SOC Olgunlaştırma Hizmeti organizasyonun, güvenlik olaylarına karşı hızlı ve doğru tepki verebilme kaslarını geliştirir. Organizasyonun ihtiyaçlarına göre özelleştirilen SOC yapısı, saldırı tespit ve müdahale süreçlerinin başarısını yükseltir.

SIEM Yönetimi ve Optimizasyonu

SIEM yönetimi, güvenlik olaylarını izleyip analiz ederek tehditleri tespit etmek için kullanılır. SIEM sistemin etkin işletilmesi ve yönetimi kurumsal güvenlik için kritik öneme sahiptir. SIEM optimizasyonu sayesinde verilerin daha doğru analiz edilmesi ve hatalı (F/P) alarmların en aza indirilmesi sağlanır. SIEM yönetim sistemi, gerçek zamanlı analizlerle anlık tehditleri algılayarak hızlı müdahale imkânı sunar.

Tehdit İstihbaratı Entegrasyonu

Tehdit istihbaratı entegrasyonu, iç-dış tehditlerin analiz edilmesi ve güvenlik operasyonlarına entegre edilmesini sağlar. Global tehdit ağlarından elde edilen veriler işlenerek kurumlara özgü bir savunma stratejisi geliştirilir. Tehdit istihbaratı, SOC ekiplerine saldırıların doğasını anlamada yardımcı olur ve önleyici tedbirlerin alınmasına katkıda bulunur.

Ağ Güvenliği İzleme

Ağ güvenliği izleme, kurumların ağ altyapısındaki tehditleri anında tespit etmelerini sağlar. Gerçek zamanlı izleme araçları kullanılarak, saldırı girişimlerinin anında belirlenmesi ve müdahale edilmesi sağlanır. Ağ güvenliği yönetimi, trafiğin düzenli analiz edilmesini ve saldırı paternlerinin tespit edilmesini kolaylaştırır. Bu süreç, özellikle DDoS saldırıları ve veri sızıntısı gibi tehditlerin erken tespit edilmesinde etkilidir. Güçlü bir ağ güvenliği altyapısı, kurumların güvenlik açıklarını kapatarak güvenliğini artırır.

Olay Müdahalesi (Incident Response)

Güvenlik olaylarına müdahale, saldırı veya güvenlik ihlalleri durumunda hızlı ve etkili bir şekilde karşılık vermek amacıyla planlanır. Hizmet, güvenlik ihlalinin etkisini en aza indirmek için olayın analiz edilmesini ve müdahale süreçlerinin hızla uygulanmasını içerir. Güvenlik olaylarına müdahale, olay sonrası adli analizlerin yapılmasını da kapsayabilmektedir. Güvenlik ekipleri, bu süreçte tehditleri analiz ederek organizasyona yönelik riskleri minimize eder.

Eğitim ve Farkındalık

Güvenlik ekiplerinin yeteneklerini artırmak ve organizasyon içinde güvenlik farkındalığı oluşturmak amacıyla kapsamlı eğitim programları düzenlenir. Çalışanlar olası tehditlere karşı bilinçlendirilerek, güvenlik ihlallerine karşı daha hazırlıklı hale gelmeleri

sağlanır. Farkındalık eğitimleri sosyal mühendislik saldırıları gibi insan kaynaklı güvenlik risklerini en aza indirmeyi amaçlar. Eğitim programları ayrıca güvenlik ekiplerinin en son tehditler ve saldırı yöntemleri hakkında güncel teknik bilgilere sahip olmalarını sağlar.

SIEM Lokal Bakım Destek Danışmanlığı

SIEM Ürünü Lokal Bakım Destek Danışmanlığı, SIEM sistemlerinin kesintisiz çalışması ve maksimum performans sunması için gereken bakım ve destek hizmetlerini sağlar. SIEM ürünlerinde meydana gelebilecek sorunlar yerinde çözülerek, güvenlik operasyonlarının aksamadan devam etmesi sağlanır. Lokal destek, SIEM sistemlerinde oluşabilecek hata veya performans sorunlarına hızlıca müdahale eder. Bakım süreçleri boyunca sistem güncellemeleri, yamalar ve performans optimizasyonları gerçekleştirilir.

SIEM Olgunlaştırma Danışmanlığı

SIEM Ürünü Olgunlaştırma Danışmanlığı, SIEM çözümlerinin güvenlik operasyon merkezinde (SOC) daha etkin kullanılabilmesi için optimize edilmesini hedefler. Olgunlaştırma sürecinde, SIEM sisteminin veri toplama, analiz ve korelasyon yetenekleri analiz edilir. Organizasyonun ihtiyaçlarına göre özelleştirilmiş korelasyon kuralları ve güvenlik alarmlarının geliştirilmesini sağlanır.

Korelasyon Kurallarının Çalışırlığının Denetlenmesi

Korelasyon Kurallarının Çalışırlığının Denetlenmesi, SIEM sistemi üzerinde tanımlı korelasyon politikaların çalışırlığını test eden bir hizmettir. Gerçekleştirilen denetim, politikaların doğru alarm ürettiğinden emin olmak için periyodik olarak gerçekleştirilir. Yanlış veya eksik yapılandırılmış politikaların düzeltilmesiyle, tehdit tespiti artırılır ve F/P (false-positive) alarmların önüne geçilir. Korelasyon kurallarının çalışırlığı düzenli olarak izlenir ve ihtiyaç halinde iyileştirmeler yapılır. Gerçekleştirilen denetimler, güvenlik olaylarının zamanında ve doğru şekilde tespit edilmesine yardımcı olur.

Log Toplama Mimarisi ve Log Olgunlaştırma Danışmanlığı

Log Toplama Mimarisi ve Log Olgunlaştırma Danışmanlığı, kurumsal güvenlik altyapısının etkin bir şekilde izlenmesi için gerekli log toplama yapılandırmasını sağlar. Hizmet, sunucular, ağlar, uygulamalar ve diğer tüm elektronik cihazlardan toplanan logların adli bilişim ekseninde, herhangi bir vakayı aydınlatabilecek doğru loglamanın yapılmasını hedefler. Olgunlaştırma sürecinde log verileri de ayrıca optimize edilerek depolama maliyetleri azaltılarak analiz süreçleri hızlandırılır. Güvenlik ekiplerinin vakaları analiz etme süresini kısaltarak tehditlere hızlı yanıt verilmesini sağlar.

Yama Analizi

Yama Analizi, kurumların dijital varlıklarına yönelik güncelleme ve yama gereksinimlerini belirleyen bir güvenlik sürecidir. Gerçekleştirilen analizler, sistemlerin en güncel güvenlik yamalarıyla korunmasını sağlamak için periyodik olarak yapılır. Eksik veya hatalı yamalar güvenlik risklerine yol açabileceği için analiz sonuçlarına göre doğru yamaların uygulanması temin edilir. Yama analizi, tehditlerin ve siber saldırıların en güncel güvenlik önlemleriyle önlenmesini sağlar.

Varlık Görünürlük Analizi

Varlık Görünürlük Analizi, kurumun tüm dijital varlıklarının haritasını çıkararak görünürlüğünü artıran bir güvenlik sürecidir. Gerçekleştirilen analizler sayesinde güvenlik ekipleri, hangi varlıkların korunması gerektiğini ve bu varlıklara yönelik tehditleri daha net bir şekilde görme imkânı elde ederler. Varlık görünürlüğünün artırılması, saldırganların zafiyetlerden yararlanma ihtimalini azaltır. Analiz, aynı zamanda varlıkların güvenlik politikalarına uygun çalışıp çalışmadığını da değerlendirir.

Segmentasyon Analizi

Segmentasyon Analizi, ağ altyapısındaki güvenlik segmentlerinin doğru yapılandırılıp yapılandırılmadığını kontrol eden bir güvenlik sürecidir. Gerçekleştirilen analizler, farklı ağ segmentleri arasında erişim sınırlamalarını denetleyerek güvenlik risklerini minimize eder. Ağdaki her segmentin güvenlik gereksinimleri doğrultusunda izole edilebilmesi sağlanarak saldırı yüzeyi azaltılır. Segmentasyon, tehditlerin bir bölümden diğerine yayılmasını engeller ve ağ güvenliğini sağlamada en önemli süreçlerden biridir. Hizmet ayrıca, segmentasyon politikalarının güncel tehdit ortamına göre optimize edilmesini de sağlar.

Uzaktan Erişim Analizi

Uzaktan Erişim Analizi, kurumların dış erişim noktalarını değerlendirerek güvenli bir erişim altyapısı sağlar. Gerçekleştirilen analizler, VPN, uzaktan masaüstü bağlantıları ve diğer dış erişim yöntemlerinin güvenliğini denetler. Özellikle COVID-19 sonrası artan uzaktan çalışma talepleri için Uzaktan Erişim Analizi siber güvenlik risklerinin önlenmesinde kritik önem taşır. Güvenli olmayan erişim noktaları belirlenerek, yetkisiz girişler tespit edilir. Ayrıca, uzaktan erişim politikalarının güncellenmesi ve güçlü kimlik doğrulama yöntemlerinin uygulanması için öneriler sunulur.

Kimlik Doğrulama Altyapısı Analizi

Kimlik Doğrulama Altyapısı Analizi, organizasyonların kullanıcı kimlik doğrulama mekanizmalarını değerlendirerek güvenlik seviyelerini analiz eder. Analizler, çok faktörlü kimlik doğrulama (MFA) ve güçlü parola politikaları gibi güvenlik önlemlerinin etkinliğini ölçer. Kimlik doğrulama altyapısı, kullanıcı erişimlerinin kontrol altına alınmasını ve yetkisiz erişimlerin önlenmesini sağlar. Analiz sırasında, kimlik doğrulama sistemlerinde eksiklikler tespit edilir ve güncel güvenlik politikalarına uyumlu hale getirilir.

Kurumsal SOME Danışmanlığı

Kurumsal SOME (Siber Olaylara Müdahale Ekibi) Danışmanlığı, kurumların siber olaylara hızlı ve etkili müdahale edebilmeleri için profesyonel danışmanlık hizmetleri sunar. SOME, güvenlik ihlallerine karşı stratejik bir plan oluşturup anında müdahale sağlar. Kurumun iç dinamiklerine uygun olarak, siber olaylara yanıt verme yetkinlikleri olgunlaştırılır ve ekipler ilgili konularda eğitilir. Danışmanlık kapsamında, güvenlik olaylarına müdahale prosedürleri ve iletişim planları oluşturulur. SOME ekibinin etkinliği artırılarak, olay sonrası iyileştirme süreçleriyle ilgili politikalar da oluşturulur.

Regülasyon Uyumlu Veri İmha Etme Danışmanlığı

Regülasyon Uyumlu Veri İmha Etme Danışmanlığı, kurumların hassas verileri yasal gerekliliklere uygun şekilde yok etmesini sağlar. Ulusal ve uluslararası regülasyonlara uyumlu veri imha politikaları oluşturarak, veri güvenliğini sağlar. Hassas bilgilerin güvenli bir şekilde imha edilmesi, veri ihlali risklerini minimize eder. İmha süreci sırasında güvenilir yazılımlar ve fiziksel imha yöntemleri kullanılarak verilerin geri döndürülemez şekilde yok edilmesi sağlanır. Veri imha işlemi sonrası veri imha raporları sunularak sürecin tamamlandığı belgelenerek, kayıt altına alınır.

Zafiyet Yönetimi Danışmanlığı

Zafiyet Yönetimi Danışmanlığı, organizasyonların elektronik varlıklarındaki güvenlik zafiyetlerini belirlemek ve bu zafiyetleri kapatmak için kapsamlı bir çözüm sunar. Hizmet boyunca güvenlik zafiyetleri düzenli olarak tespit edilerek, saldırganların yararlanabileceği zayıf noktalar ortadan kaldırır. Güvenlik taramaları ve analizler gerçekleştirilerek organizasyonun risk durumu sürekli olarak izlenir. Tespit edilen zafiyetlerin giderilmesi için gerekli yamalar ve güncellemelerin uygulanması temin edilir. Zafiyet yönetimi sürecinde, tehdit önceliklendirmesi yapılarak kritik açıkların öncelikli olarak ele alınması sağlanır.

Siber Güvenlik Politika ve Prosedürlerinin Geliştirilmesi Danışmanlığı

Siber Güvenlik Politika ve Prosedürlerinin Geliştirilmesi Danışmanlığı, organizasyonlara özel güvenlik politikaları ve prosedürleri oluşturarak, organizasyonun güvenlik stratejisini sağlamlaştırır. Güvenlik süreçlerinin sistematik bir yapıya kavuşturulması ve organizasyonel uyumluluğun sağlanması siber güvenlik açısından önemli bir süreçtir. Politika ve prosedürlerin oluşturulması, tüm çalışanların güvenlik standartlarına uygun davranmasını destekler. Geliştirilen güvenlik politikaları erişim kontrolü, veri koruma ve güvenlik olaylarına müdahale gibi konuları kapsar. Prosedürlerin düzenli olarak güncellenmesi ile değişen tehdit ortamına uyum sağlanır. Güvenlik politikaları, çalışanların bilinçlendirilmesi ve kurum içinde güvenlik kültürünün oluşturulması için önem arz eder.

Sık Sorulan Sorular

MDR hizmeti, güvenlik operasyonlarında nasıl bir avantaj sağlar?

MDR (Managed Detection and Response), tehditlerin tespit edilip hızlı müdahale edilmesini sağlayan kapsamlı bir güvenlik hizmetidir. SIEM, SOAR, DLP, EPP, SANDBOX EDR ve NDR gibi sistemlerle bütünleşik çalışan MDR Hizmetimiz, güvenlik olaylarının anında tanımlanması ve önlenmesi için önemli bir rol oynar. Tehditlerin sürekli izlenmesi, anında müdahale edilmesi ve güvenlik teknolojilerinin organizasyon içerisinde işletilmesi MDR Hizmetinin en büyük avantajlarından biridir. MDR Hizmeti güvenlik operasyonlarında kesintisiz koruma sağlar ve tehdit istihbaratı ile güncellenen sistemler sayesinde güvenlik zafiyetleri hızlıca giderilir. MDR Hizmeti iş yükünü azaltarak güvenlik ekiplerinin kritik olaylara odaklanmasına yardımcı olur.

Olay müdahalesi sürecinde hangi adımlar izlenir ve bu sürecin faydaları nelerdir?

Olay müdahalesi, olayların tespiti ile başlayan, analiz, izolasyon, yok etme ve iyileştirme adımlarıyla tamamlanan bir hizmettir. İlk adımda, SIEM ve diğer güvenlik teknolojileriyle tehditler tespit edilir. Analiz aşamasında siber güvenlik uzmanlarımız tarafından tehdidin kaynağı ve potansiyel etkisi detaylı şekilde incelenir. Ardından, izole etme ve yok etme evreleriyle tehdit unsurları sistemlerden temizlenir. Müdahale süreci boyunca güvenlik ekipleri iş birliği içinde çalışarak tehdidin yayılmasını önlenir. İyileştirme aşaması, gelecekte benzer olayların yaşanmaması için gerekli düzenlemeleri içerir.

SIEM optimizasyonu, güvenlik operasyonlarında nasıl bir rol oynar?

SIEM optimizasyonu, güvenlik olaylarının analizini hızlandırarak tehditlere etkili yanıt verilmesini sağlar. Sistem performansını artırmak ve yanlış alarmları (F/P) azaltmak için optimize edilen SIEM teknolojileri, güvenlik ekiplerinin verimliliğini artırır. Verilerin düzenli ve anlamlı bir şekilde analiz edilmesi, güvenlik açıklarının daha hızlı fark edilmesine yardımcı olur. Gerçekleştirilen optimizasyonlar, tehditlerin geçmişe dönük incelenmesi ve gelecekteki tehditlerin öngörülmesi açısından önemlidir. SIEM'in düzenli güncellenmesi ve uyumlu çalışması, güvenlik operasyonlarının sürdürülebilirliği açısından hayati önem taşır.

Tehdit istihbaratı entegrasyonunun güvenlik operasyonlarına katkısı nedir?

Tehdit istihbaratı entegrasyonu, güvenlik operasyonlarının etkin yönetilmesi için kritik bir rol oynar. Güncel tehdit bilgilerini güvenlik teknolojilerine entegre ederek tehditlere karşı güçlü bir savunma sağlar. SOC ekipleri, entegre edilen istihbarat verileri ile tehditlerin kökenini ve yöntemlerini daha iyi analiz eder. Organizasyon, dış kaynaklı tehditlere karşı koruma sağlarken iç tehditleri de öngörme şansına sahip olur. Süreç, güvenlik ekiplerinin karar alma hızını artırarak olaylara daha çabuk yanıt verilmesini sağlar. Tehdit istihbaratı verileri ile yapılan değerlendirmeler, organizasyonun uzun

vadeli güvenlik stratejileri geliştirmesine olanak tanır. Karar süreçlerinin hızlanması güvenlik zafiyetlerinin hızla kapanmasını sağlar.

SOC olgunlaştırma süreci nasıl işler ve organizasyonlara faydası nedir?

SOC olgunlaştırma süreci, güvenlik operasyon merkezinin tehditlere karşı daha etkin çalışmasını sağlayan düzenlemeler içerir. Güvenlik olaylarına yanıt verme kapasiteleri artırılarak SOC'un verimliliği yükseltilir. Olgunlaştırma süreci, SOC-CMM veya NIST çerçevesine göre yönetilerek uluslararası standartlara uyum sağlanır. Olgunlaştırma süreci boyunca, SOC ekiplerinin yetenekleri geliştirilir ve hızlı müdahale kasları güçlendirilir. Olayların tespit süresi hızlanırken müdahale süreleri kısaltılır. Güçlü bir SOC yapısı, saldırılara karşı daha güçlü bir savunma yapısı kurarken ve tehditlere karşı daha hazırlıklı olunmasını sağlar. SOC olgunlaştırma süreci, uzun vadede organizasyonun güvenlik seviyesini optimize eder. Sürekli iyileştirme ve değerlendirme ile SOC'un yetkinlikleri artırılır.

L1, L2 ve L3 seviye analiz hizmetleri nasıl farklılaşır ve her seviyenin katkısı nedir?

L1, L2 ve L3 seviye analiz hizmetleri, tehditlerin farklı seviyelerde detaylı incelenmesi için oluşturulmuş bir hizmettir. L1 seviye analiz temel izleme ve hızlı yanıt hizmeti sunarken düşük riskli olayları değerlendirir ve gerektiğinde L2'ye yönlendirir. L2 seviyesi, olayların detaylı analizini yaparak kök neden araştırması yapar ve tekrarlayan tehditler için çözümler geliştirir. L3 seviyesinde ise karmaşık saldırılar için stratejik çözümler sunarken adli analiz süreçlerini de yürütür. İleri analiz, saldırıların kaynağını ve saldırganın izini sürerek güvenlik zafiyetlerini kapatmaya ve kök problemi gidermeye yardımcı olur.

Ürün ve teknoloji işletme süreçlerinde MDR çözümlerinin avantajları nelerdir?

MDR çözümleri, ürün ve teknoloji işletme süreçlerinde tehdit algılama ve yanıt verme kapasitesini yükseltir. Güvenlik ürünlerinin yönetimi, MDR ile birlikte otomatik hale getirilerek tehditlerin tespiti daha etkin hale gelir. MDR Hizmeti, tehditlerin büyümesini önlerken organizasyonun genel güvenlik seviyesini artırır. MDR ayrıca, sürekli güncellenen tehdit bilgileri ile güvenlik politikalarını iyileştirir. Güvenlik ekipleri için iş yükünü azaltarak operasyonel verimliliği yükseltir. Tehditlerin hızlıca tespit edilip yanıtlanması sayesinde güvenlik riskleri en aza indirilir.

SIEM ve SOAR entegrasyonu neden önemlidir?

SIEM ve SOAR entegrasyonu, güvenlik olaylarının analiz edilmesi ve otomatik yanıt mekanizmalarının devreye alınması için önemlidir. SIEM olayları analiz ederken SOAR, önceden tanımlanmış kurallara göre otomatik yanıt süreçlerini başlatır. Entegrasyon sayesinde güvenlik olaylarına daha hızlı ve etkili bir yanıt verilir. Güvenlik ekiplerinin iş yükü azalırken önemli olaylara odaklanmaları sağlanır. SOAR'ın sunduğu otomatik süreçler, olaylara anında müdahale etmeyi ve hatalı alarm (F/P) sayısını azaltmayı mümkün kılar. SIEM ve SOAR çözümleri, tehditlerin hızlı tespit edilmesine ve etkisiz hale getirilmesine katkı sunar.

Olay sonrası adli analiz, güvenlik operasyonlarına nasıl katkı sağlar?

Olay sonrası adli analiz, saldırının kaynağını ve izlerini belirlemek için yapılan kapsamlı bir inceleme sürecidir. Güvenlik zafiyetlerinin nereden kaynaklandığını belirleyerek olayın tam kapsamını değerlendirir. Adli analiz, saldırganların izini sürerek güvenlik zafiyetlerinden faydalanan yöntemleri de tespit eder. Analiz süresince toplanan bulgular, gelecek olası saldırılara karşı önlem alınmasına yardımcı olur. Ayrıca adli analiz sonrası düzenlenen raporlar, organizasyonun güvenlik politikalarının olgunlaştırılmasına katkıda bulunur.

Ağ güvenliği izleme (NDR) nasıl çalışır ve hangi faydaları sağlar?

Ağ güvenliği izleme (NDR), organizasyonların ağ trafiğini gerçek zamanlı analiz ederek anormal aktiviteleri tespit etmeyi amaçlar. Veri sızıntıları, arka kapı ve DDoS saldırıları gibi tehditlerin erken tespit edilmesine ve yanıt verilmesine olanak tanır. Gerçek zamanlı izleme, güvenlik ekiplerinin tehditleri anında algılayarak müdahale etmesini mümkün kılar. Ağ trafiğinin sürekli analiz edilmesi, saldırı tekniklerini ve güvenlik zafiyetlerini tespit etmek için kullanılır. İzleme araçları sayesinde güvenlik ekipleri olası tehditleri daha iyi yönetebilir. Düzenli ağ güvenliği izleme, tehditlerin kontrol altında tutulmasına ve diğer ağ segmentlerine bulaşmasını engeller.

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