Privia SECURITY

OT Sızma Testi Hizmeti

Profesyonel Offensive Security Hizmetleri

"Endüstriyel Siber Riskleri Görünür Hale Getirin!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Endüstriyel altyapılarınızda görünmeyen siber tehditleri tespit etmek, gelecekteki olası saldırılara karşı hazırlıklı olmanızı sağlar."

OT (Operational Technology) Güvenlik Testi Hizmeti, endüstriyel kontrol sistemlerinin (EKS/SCADA) ve altyapılarının siber tehditlere karşı korunmasını sağlamak amacıyla tasarlanmış kapsamlı bir test sürecidir. Endüstriyel tesislerde kullanılan donanımlar, artan siber saldırı risklerinden etkilenmekte ve bu durum, üretim süreçlerinin kesintisiz bir şekilde devam etmesini tehlikeye atmaktadır. OT Güvenlik Testi Hizmetimiz, kritik altyapıların güvenliğini geliştirmek ve siber tehditlere karşı güvenlik olgunluğunu artırmayı hedefler.

Gerçekleştirdiğimiz testler, OT (EKS/SCADA) sistemlerinin zayıf noktalarını tespit etmek için bir dizi kontrol ve test yöntemi içerir. Saldırı simülasyonları, zafiyet taramaları, boşluk analizi ve yapılandırma testleri gibi farklı teknikler kullanarak, sistemlerin mevcut güvenlik durumu detaylı bir şekilde test edilerek raporlanır. Test sürecinde, ulusal/uluslararası güvenlik standartlarına uygun hareket edilmesi, testlerin kalitesini ve güvenilirliğini artırır.

OT Güvenlik Testi Hizmetimiz, yalnızca mevcut tehditlerin tespit edilmesiyle sınırlı kalmaz, aynı zamanda gelecekteki risklere karşı hazırlıklı olmanız için ek çözümler sunar. Testler esnasında elde edilen bilgi, belge ve bulgular doğrultusunda, donanımların ve sistemlerin güvenlik seviyesini olgunlaştırmaya yönelik stratejik öneriler sunulur. Testler sonucunda endüstriyel tesislerdeki operasyonların güvenliği geliştirilir ve olası güvenlik kaynaklı kesintiler önlenir.

OT Güvenlik Testi Hizmeti, endüstriyel kontrol sistemlerinin siber güvenliğini artırarak, iş sürekliliğini koruma amacına hizmet eder. Testler sonucunda hazırlanan detaylı raporlar, güvenlik açığının tespit edilmesi ve giderilmesi için gerekli tüm adımları ve yönlendirmeleri içerir. Organizasyonlara özel hazırlanan aksiyon planları ile birlikte, sistemlerinin her zaman güvenli ve güncel kalmasına yardımcı olur.

Hizmete Ait Bileşenler

Güvenlik Değerlendirmesi

OT sistemlerinin donanım ve yazılım bileşenleri testler sırasında incelenir. Test sürecinde, olası güvenlik zafiyetleri belirlenir ve her bir bileşenin güvenlik durumu analiz edilir. Elde edilen bilgi, belge ve bulgular, zayıf noktaların nasıl giderileceğine dair stratejik öneriler sunar. Gerçekleştirilen testler sayesinde sistemin güvenliğini artırılarak, siber saldırılara karşı altyapının olgunluk seviyesi yükseltilir.

Ağ Güvenliği Testleri

OT (EKS/SCADA) sistemlerinde bulunan olası güvenlik zafiyetleri detaylı bir şekilde incelenir. Gerçekleştirilen testler, OT sistemlerde tespit edilen zafiyetlerin risk seviyeleri organizasyon güvenlik ekibiyle birlikte değerlendirilmektedir. Yapılan çalışma güvenlik zafiyetlerinin önceliklendirilmesi, kritik zafiyetlerin öncelikle ele alınması için fayda sağlar.

Zafiyet Analizi

Zafiyet testleri çerçevesinde organizasyonun endüstriyel kontrol sistemleri, PLC, SCADA, RTU, DSS gibi çevre birimleri ve çevre birimlerinden oluşan sensör verilerinden beslenen IT varlıklarına yönelik güvenlik testleri gerçekleştirilir. Testler sırasında tesislerdeki fiziksel erişim kontrol sistemleri, güvenlik kameraları ve diğer güvenlik önlemleri de ayrıca test edilir. Fiziksel güvenlik zafiyetlerinin tespit edilmesi, yetkisiz girişlerin önlenmesi için kritik bir adımdır. Zafiyet testleri gerçekleştirilirken fiziksel güvenlik denetimleri de gerçekleştirilir.

Fiziksel Güvenlik

OT sistemlerinin fiziksel güvenliği, önemli bir denetim evresidir. Gerçekleştirilen testler, tesislerdeki fiziksel erişim kontrol sistemlerini, güvenlik kameralarını ve diğer güvenlik önlemlerini denetler. Fiziksel güvenlik zafiyetlerinin belirlenmesi, yetkisiz girişlerin önlenmesi için en kritik adımların başında gelir. Fiziksel güvenlik denetimleri, tüm sistemlerin bütünlüğünü koruyarak, operasyonların kesintisiz devam etmesini sağlar.

Siber Tehdit Simülasyonları

Siber tehdit simülasyonları, OT sistemlerinin güvenlik zafiyetlerini tespit etmek ve gerçek saldırı senaryoları kullanarak, siber güvenlik altyapısını olgunlaştırır. Simülasyonlar ile saldırganların kullanabileceği teknik, taktik ve yöntemler organizasyona özel olarak geliştirilir. Testler sırasında, sistemlerin ağ yapısı, donanım ve yazılım bileşenleri, birtakım saldırılarla test edilerek zafiyetler ortaya çıkarılır.

Sık Sorulan Sorular

OT Sızma Testi Nedir?

OT (SCADA) sızma testi, endüstriyel kontrol sistemlerinin (EKS/ICS), PLC, SCADA ve çevre birimlerinin siber güvenlik durumunu inceleyen bir test biçimidir. Testler, kritik altyapıların zayıf noktalarını belirleyerek siber tehditlere karşı önlem almayı hedefler. Testler sırasında, saldırganların kullanabileceği yöntemler kullanılarak sistemlerin güvenlik zafiyetleri keşfedilir. SCADA altyapısının güncel siber tehditlere karşı periyodik olarak test edilmesi, iş sürekliliği ve üretim açısından kritik öneme sahiptir. Testler sonucunda elde edilen tüm bilgi, belge ve bulgular doğrultusunda kritik altyapıların güvenliği olgunlaştırılır.

OT Sızma Testi Neden Gereklidir?

OT (SCADA) sistemleri genellikle kapalı devre prensibiyle çalıştığından dolayı, siber güvenlik önlemleri konusunda da zayıf kalır. EKS/SCADA Sızma testleri sayesinde kritik altyapıların zafiyetleri tespit edilerek giderici çözümler sunulur. Testlerin amacı, operasyonel süreçlerin güvenliğini sağlamak, iş kesintilerini önlemek ve veri ihlallerini engellemektir. Özellikle üretim tesislerine yönelik gerçekleşen siber saldırılar büyük finansal zararlara, mali kayıplara ve üretimin azalmasına yol açabilir. Periyodik SCADA testleri hem güvenlik seviyesini artırır hem de gelecekteki olası siber saldırılara karşı hazırlıklı olmayı sağlar.

Hangi Sistemler ve Cihazlar OT Sızma Testine Dahil Edilir?

OT sızma testleri, endüstriyel kontrol sistemleri, PLC, SCADA, RTU, HMI, DSS, MES, Engineering Workstation gibi kritik cihazları kapsar. Sistemlerin bağlı olduğu sensörler ve çevre birimleri de teste dahil edilir. Ağ güvenlik duvarları ve erişim kontrol sistemleri de incelenerek tam kapsamlı bir test gerçekleştirilir. Hem donanım hem de yazılım katmanlarındaki zafiyetler tespit edilerek giderilir.

OT Sızma Testi Süresi Ne Kadardır?

SCADA Sızma Testinin süresi, sistemin büyüklüğüne ve karmaşıklığına bağlı olarak değişir. Küçük ölçekli altyapılarda birkaç gün süren testler, büyük ve karmaşık sistemlerde birkaç ay sürebilir. Testler operasyonları kesintiye uğratmadan gerçekleştirilecek şekilde planlanır. Kritik süreçlerin test edilmesi sırasında alternatif iş akışları planlanarak iş sürekliliği sağlanır.

OT Sızma Testi Sonucunda Neler Raporlanır?

OT Sızma testi sonunda, tespit edilen zafiyetler ve risk seviyeleri ayrıntılı bir şekilde raporlanır. Her zafiyet için çözüm önerileri geliştirilir ve uygulanabilir aksiyon planları önerilir. Rapor, hem teknik ekipler için detaylı bilgiler hem de yöneticiler için özet bir değerlendirme içerir. Test sonuçları, sistemlerin iyileştirilmesi ve uzun vadeli siber güvenlik stratejilerinin belirlenmesi için en önemli kaynaklardan biridir.

OT Sızma Testi Sırasında Sistem Kesintisi Yaşanır mı?

EKS Sızma Testlerinin amacı, operasyonları aksatmadan güvenlik zafiyetlerini tespit etmektir. Kritik sistemlerin test edilmesi sırasında önceden planlama yapılarak iş sürekliliği sağlanır. Bazı durumlarda, testler gece vardiyalarında veya düşük yoğunluklu zaman dilimlerinde gerçekleştirilir. Proje Yönetim Ekipleriyle birlikte koordine edilen testler, süreçlerin aksamaması için gerekli önlemlerin alınmasını sağlar. Tüm testler, organizasyonun operasyonel ihtiyaçları göz önünde bulundurularak planlanır.

OT Sızma Testlerinin Risk Yönetimine Katkısı Nedir?

OT Sızma testleri, risk yönetim sürecinin temel bir parçasıdır. Tespit edilen zafiyetlerin önceliklendirilmesi, kritik risklerin hızlıca ele alınmasını sağlar. Testler sonucunda oluşturulan risk raporları, işletmelerin güvenlik açıklarını gidermek için stratejik planlar geliştirmesine yardımcı olur.

OT Sızma Testleri Ne Sıklıkla Yapılmalıdır?

OT sistemlerde sızma testlerinin yılda en az iki kez yapılması önerilir. Ancak yeni bir sistem kurulumu veya önemli bir güncelleme sonrasında da testlerin tekrarlanmasının gerektiği unutulmamalıdır. Periyodik olarak yapılan OT Sızma Testleri, sistemlerin her zaman güncel tehditlere karşı korunmasını sağlar. Gerçekleştirilen testler sayesinde yeni ortaya çıkan zafiyetlere karşı erken önlem almak ve müdahale etmek mümkün hale gelir. Sık periyotlarda gerçekleştirilen testler, işletmelerin siber güvenlik olgunluğunu artırır.

OT Sızma Testi Hangi Standartlara Uygundur?

OT sızma testleri, ISO 27001, IEC 62443, EPDK gibi ulusal/uluslararası standartlara uygun olarak gerçekleştirilir. Standartlar ve regülasyonlar, testlerin kapsamını belirleyerek, siber güvenlik süreçlerinin iyileştirilmesini sağlar. Mevzuata uyum sağlamak, işletmelerin yasal gereklilikleri karşılaması ve itibar kazanması açısından çok önemlidir.

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