Privia SECURITY

Siber Tatbikat Hizmeti

Profesyonel Defensive Security Hizmetleri

"Hazırlıksız Cephede Başarı Olmaz!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Siber Güvenlik Tatbikatları, ekiplerin gerçekçi senaryolarla deneyim kazanarak, kriz anında hızlı ve etkili yanıt verebilmesini sağlar."

Günümüzde siber uzay, kara, hava, deniz ve uzay alanlarından sonra ilan edilen beşinci savaş alanı olarak literatürde yer almıştır. Devletlerin ve organizasyonların siber uzayda gerçekleşebilecek tehditlerin yaratacağı sonuçlar hakkındaki farkındalıkları her geçen gün artmakta ve riskleri etkin bir şekilde tespit edilip yok edilmesi amaçlanmaktadır. Siber uzaydaki tespit edilmesine yönelik gerçekleştirilen en etkin eylemler, gerçeğe dayalı ve günün şartlarına uygun değişkenler ile üretilen siber tatbikat süreçleridir.

Siber Güvenlik tatbikatları, bir organizasyonun siber güvenlik tedbirlerini ve kriz yönetimini test etmek amacıyla düzenlediği senaryoya dayalı aktif/pasif simülasyonlardır. Gerçek bir siber saldırı gibi tasarlanmış bu tatbikatlar, organizasyonun zayıf noktalarını belirlemesine, müdahale planlarını test etmesine ve personelinin siber güvenlik bilincini geliştirmesine yardımcı olur. Siber Güvenlik Tatbikatları, organizasyon altyapısında alınabilecek önlemler konusunda karar vericilere ve teknik ekiplere geliştirilebilecek araçlar, teknikler ve prosedürler konusunda fikirler verir.

Siber Güvenlik tatbikat senaryoları ile gerçeğe en yakın şekilde yapılan aktiviteler, organizasyonun ilgili siber savunma ekipleri, senaryo bağlamında etkilenmesi beklenen departmanlar ve paydaşlarının stres altında olaya müdahale etmeye ve engellemeye yönelik karar süreçlerinin iyileştirilmesini sağlamaktadır. Tatbikatın gerçekleştirilmesi esnasında ve sonrasında organizasyonun siber güvenlik ekibi ile senaryodan etkilenecek diğer departmanların arasındaki iletişimin geliştirilip güçlenmesini de sağlayabilmektedir.

Hizmete Ait Bileşenler

Masaüstü (Table-Top) Tatbikatlar

Table-Top tatbikatlar, olası bir siber saldırı sırasında ekiplerin alması gereken aksiyonların tanımlanmasını içen bir tatbikat türüdür. Organizasyonun siber güvenlik uzmanlarıyla birlikte ekiplerimiz bir araya gelerek, saldırıyı nasıl tespit edeceklerini, nasıl yanıt vereceklerini ve vakadan sonra sistemlerin nasıl iyileşeceklerini tartışırlar. Masaüstü tatbikatları herhangi bir saldırıyı canlı ortamda simüle etmeye gerek duymadan karmaşık saldırılara karşı yanıt verme süreçlerinin planlanmasını amaçlar.

Red Team (Tam Canlı-Full Live) Tatbikatlar

Bir siber saldırıyı en gerçekçi şekilde simüle eden bir siber güvenlik tatbikat türüdür. Tatbikatlarda saldırganların kullandığı teknik ve taktikler kullanılarak gerçek sistemlere ve verilere erişebilmeyi amaçlar. Bu tatbikat türünde organizasyon siber güvenlik ekiplerinin gerçek bir saldırıya karşı nasıl tepki vereceklerini öğrenmelerine yardımcı olur. Siber saldırıyı simüle edecek kırmızı takım, yapılacak olan zararlı aktivitelere ait ana başlıkları organizasyon ile paylaşırken aktivitelerin detaylarını mavi takım ile paylaşmaz. Tatbikat süreci boyunca gerçekleştirilen saldırılar ve organizasyonun aldığı önlemler sonucunda kırmızı takım yeni saldırı vektörleri üreterek son noktaya kadar ilerlemeye devam eder.

Karma (Hibrit) Tatbikatlar

Gerçekleştirilecek senaryoların teknik detayları ve saldırı yapacak ekibin bilgisi tatbikat öncesinde kuruma bildirilir. Siber saldırıları gerçekleştiren ekip, senaryoda belirlenen tekniklerin haricinde herhangi bir yeni saldırı gerçekleştirmez. Kuruma bildirilen aşamalara bağlı kalarak tatbikat süreçleri gerçekleştirir. Tatbikat süreci boyunca kurumun siber güvenlik ekibi ve saldırı gerçekleştiren ekip koordineli bir şekilde çalışmaktadır. Bu tatbikatlar masaüstü tatbikatların, kontrollü ortamı ile tam canlı tatbikatların gerçekçiliği arasında bir denge kurmayı amaçlar. Siber tatbikat senaryoları kurumun sahip olduğu envanter ve personelin yetkinliğine göre özenle kurgulanmalıdır. Kurumun ihtiyacına yönelik kurgulanamayan siber tatbikat senaryolarının gerçekleştirilmesi hali hazırda olan risklerin kesin tespitinin yapılamamasına ve gelecekte ortaya çıkabilecek potansiyel tehdit unsurlarının doğurabileceği sonuçların ön görülememesine sebep olacaktır.

Senaryonun Kurgulanması

Senaryonun kurgulanması, siber tatbikatın en önemli aşamasını oluşturur ve tatbikatın etkinliği açısından kritik bir öneme sahiptir. Organizasyonun güvenlik ihtiyaçlarına ve olası tehdit ortamına uygun olarak tatbikat senaryoları oluşturulur. Senaryolar organizasyonun karşılaşabileceği gerçekçi siber saldırı türlerini, tehdit vektörlerini ve saldırgan davranışlarını içerecek şekilde uygulanır.

Ekiplerin kriz anında nasıl tepki vereceğini değerlendirmek amacıyla senaryo, hedef alınacak sistemler, kullanılacak saldırı yöntemleri ve müdahale süreçlerini kapsar. Ayrıca senaryonun organizasyonun mevcut güvenlik altyapısına uygun olması sağlanarak, personelin yetkinlik düzeyi ve altyapının olgunluk seviyesi göz önünde bulundurulur.

Senaryonun Uygulanması

Tatbikat senaryosunun uygulanması, kurgulanan senaryonun pratik olarak devreye alındığı aşamadır. Bu aşamada, ekipler belirlenen senaryo doğrultusunda hareket ederek olayları tespit etme, izleme, yanıt verme ve müdahale süreçlerini deneyimler. Senaryonun uygulanması sırasında ekipler, koordinasyon içinde çalışarak hızlı karar alabilme ve krize yanıt verebilme kabiliyetlerini geliştirme fırsatı bulur. Tatbikat sırasında ekiplerin izlediği adımlar, kriz anında organizasyonun operasyonel süreçlerini nasıl yönettiğini gözlemlememizi sağlar. Tatbikatın uygulanması, ekiplerin senaryo doğrultusunda aksiyon alabilmesi, iş birliği içinde hareket etmesi ve güvenlik zafiyetlerini kontrol altına alması açısından önemlidir.

Analiz ve Değerlendirme

Analiz ve değerlendirme aşaması, tatbikat sonrası süreçte elde edilen verilerin detaylı olarak incelenmesi ve tatbikatın etkinliğinin değerlendirilmesini kapsar. Güvenlik ekiplerinin müdahale süreçlerinde karşılaştıkları zorluklar, alınan aksiyonların başarısı ve eksiklikler analiz edilir. Tatbikat sırasında kaydedilen veriler, ekiplerin yetkinlik seviyelerini ve güvenlik altyapısının dayanıklılığını ölçme imkânı sunar. Değerlendirme sürecinde, senaryo sırasında tespit edilen güvenlik zafiyetleri ve iyileştirme ihtiyaçları belirlenir.

Sık Sorulan Sorular

Siber Tatbikat Hizmeti nedir ve neden önemlidir?

Siber Tatbikat Hizmeti, organizasyonların siber tehditlere karşı hazırlık düzeylerini artırmak ve kriz anında nasıl hareket etmeleri gerektiğini deneyimlemelerini sağlamak amacıyla yapılan uygulamalı eğitimler ve simülasyonlardan oluşur. Tatbikatlar, organizasyonların güvenlik ekiplerinin yanı sıra üst yönetim ve diğer çalışanların da dahil olduğu senaryolarla siber olaylara nasıl yanıt vereceklerini öğretir. Siber tehditlerin giderek arttığı günümüzde iş sürekliliği sağlamak ve olası zararlardan korunmak için kritik öneme sahiptir. Tatbikatlar sırasında ekipler, gerçekçi senaryolarla müdahale yeteneklerini geliştirir ve ekip koordinasyonunu güçlendirir.

Siber Tatbikat Hizmeti hangi tür tatbikatları içerir?

Siber Tatbikat Hizmeti; Masaüstü (Table-Top), Tam Canlı (Full Live) ve Karma (Hibrit) Tatbikatlar gibi farklı türleri içerir. Masaüstü tatbikatlarda, saldırı senaryoları tartışma ortamında ele alınır ve ekipler herhangi bir canlı saldırı olmadan teorik yanıt süreçlerini tartışır. Tam canlı tatbikatlar, gerçekçi bir siber saldırıyı simüle ederek güvenlik ekiplerinin kriz anında nasıl hareket edeceğini gözlemleme imkânı sağlar. Karma tatbikatlarda ise masaüstü ve tam canlı tatbikatların unsurları birleştirilerek kontrollü bir ortamda gerçeklik sağlanır. Her tatbikat türü, organizasyonun ihtiyaçlarına ve çalışanların deneyim seviyelerine göre belirlenir.

Siber tatbikatlar sırasında hangi senaryolar uygulanır?

Siber tatbikat senaryoları, organizasyonun karşılaşabileceği potansiyel siber tehditlere dayalı olarak özenle kurgulanır. Tatbikatlarda hak-yetki yükseltme, veri sızıntıları, kimlik doğrulama ihlalleri, fidye yazılımları, phishing gibi çeşitli saldırı türleri ele alınır. Senaryoların gerçekçi olması, ekiplerin bu tür saldırılara nasıl yanıt vereceklerini ve hangi adımları atmaları gerektiğini öğrenmeleri açısından önemlidir. Ayrıca iç tehdit senaryoları gibi organizasyon içinden gelebilecek riskler de değerlendirilebilir.

Tatbikatlar neden düzenli olarak yapılmalıdır?

Siber tehditlerin sürekli değişen doğası, organizasyonların güvenlik protokollerini düzenli olarak test etmelerini zorunlu kılar. Düzenli tatbikatlar, organizasyonun güvenlik durumunu güncel tehditlere karşı sürekli olarak hazır tutar. Her tatbikat, farklı senaryolar ve tehdit türleri içerecek şekilde yapılandırılarak güvenlik ekiplerinin çeşitli tehditlere karşı hazırlıklı olmasını sağlar. Tatbikatlar, güvenlik zafiyetlerinin hızlı bir şekilde belirlenmesine ve iyileştirilmesine olanak tanır. Güvenlik ekipleri, tatbikatlar yoluyla deneyim kazanarak kriz durumunda daha etkin ve hızlı yanıt verebilir.

Hangi departmanlar siber tatbikatlara katılmalıdır?

Siber tatbikatlar, yalnızca güvenlik ekiplerinin değil, aynı zamanda üst yönetim, IT departmanı, hukuk ve iletişim gibi diğer kritik departmanların da katılımını gerektirir. Üst yönetim, tatbikatlarda alınacak kararların organizasyonel etkisini görebilir ve kriz

anında hangi adımları atması gerektiğini deneyimler. IT departmanı, teknik altyapıyı yönetirken güvenlik protokollerini uygulama yetkinliğini kazanır. Hukuk ve iletişim departmanları ise kriz anında organizasyonun yasal gereksinimlere ve kamuoyuna nasıl yanıt vereceği konusunda hazırlıklı hale gelmesi sağlanır. Tüm bu departmanların katılımı, organizasyonun iş birliği içinde çalışarak krize uyum sağlayabilmesini sağlar.

Siber tatbikatlar hangi sıklıkla yapılmalıdır?

Siber tatbikatlar, tehditlerin karmaşıklığı ve organizasyonun ihtiyaçlarına göre genellikle yılda birkaç kez yapılması tavsiye edilmektedir. Özellikle yüksek riskli ve kritik sektörlerde faaliyet gösteren organizasyonlar için daha sık tatbikat yapmak, güvenlik durumunu güncel tutmak açısından önemlidir. Düzenli olarak yapılan tatbikatlar, ekiplerin siber tehditlere karşı hazırlıklı olmasını sağlar ve güvenlik politikalarının etkinliğini test eder. Tatbikat sıklığı, organizasyonun büyüklüğüne, sektörüne ve güvenlik ihtiyaçlarına göre değişiklik gösterebilir. Bazı organizasyonlar, çeyrek dönemlerde kapsamlı tatbikatlar yaparak güvenlik kapasitelerini sürekli değerlendirmeyi tercih eder.

Siber Tatbikat Hizmeti çalışanların güvenlik bilincini nasıl artırır?

Tatbikatlar, çalışanların siber güvenlik tehditlerine karşı nasıl yanıt vermesi gerektiğini uygulamalı olarak öğretir. Tatbikatlarda farklı senaryoların deneyimlenmesi, çalışanların olası tehditlere karşı daha bilinçli hareket etmelerini sağlar. Sosyal mühendislik ve phishing gibi saldırılara karşı farkındalık kazanarak, bilgi güvenliği politikalarına uyum düzeylerini artırırlar. Tatbikat sürecinde, çalışanlar kendi görev alanlarına düşen sorumlulukları öğrenir ve bir kriz durumunda nasıl hareket etmeleri gerektiğini bilir.

Siber Tatbikat Hizmeti, Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi'nin BİG (Bilgi ve İletişim Güvenliği) Rehberi'ndeki siber güvenlik tatbikatı gereksinimlerine uygun mudur?

Evet, Siber Tatbikat Hizmeti, Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi'nin yayımladığı BİG Rehberi'nde belirtilen siber güvenlik tatbikatı gereksinimlerini karşılayacak şekilde yapılandırılmıştır. BIG Rehberi, kamu kurumlarının bilgi güvenliği seviyesini yükseltmek amacıyla siber güvenlik tatbikatlarının düzenli olarak yapılmasını tavsiye eder. Hizmetimiz, bu rehberdeki ilkelere uygun olarak farklı tatbikat türleri (Masaüstü, Tam Canlı ve Karma Tatbikatlar) sunar. Tatbikat sürecinde organizasyonun siber güvenlik ekiplerinin yanı sıra, yöneticiler ve diğer ilgili personelin katılımı sağlanır. Rehberin belirttiği gibi, tatbikat sonrası analiz ve değerlendirme yapılır ve güvenlik zafiyetleri ile iyileştirme gereksinimleri raporlanır. Ayrıca tatbikat senaryoları BIG Rehberi'ndeki kılavuzlara uygun olarak, organizasyonun ihtiyaçlarına ve olası tehdit profiline göre özelleştirilir. Siber Tatbikat Hizmeti sayesinde organizasyonlar, BİG Rehberi ile uyumluluk sergileyerek kamu güvenliğini ve bilgi bütünlüğünü güçlendirme yolunda önemli adımlar atabilir.

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