EMA SECURITY

Red Teaming Hizmeti

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Hizmet Tanımı

Red Team hizmeti, organizasyonların siber güvenlik dayanıklılığını gerçek dünya saldırı senaryoları ile test eden, proaktif bir güvenlik değerlendirme hizmetidir. Geleneksel güvenlik testlerinden farklı olarak, yalnızca belirli zafiyetleri tespit etmek yerine, saldırgan bakış açısıyla hareket ederek organizasyonun güvenlik önlemlerini aşmaya, algılama mekanizmalarını atlatmaya ve olay müdahale süreçlerini değerlendirmeye odaklanır. Red Team çalışmaları, organizasyonun savunma mekanizmalarının, tehdit algılama yeteneklerinin ve müdahale süreçlerinin ne kadar etkili olduğunu belirlemek amacıyla yürütülür.

Bu hizmet kapsamında, iç ve dış saldırı vektörleri analiz edilerek saldırganların kullanabileceği teknikler ve yöntemler simüle edilir. MITRE ATT&CK çerçevesine uygun olarak gerçekleştirilen saldırı modellemeleri, kimlik bilgisi ele geçirme, ağ ihlalleri, ayrıcalık yükseltme, yanlamasına hareket (lateral movement), veri sızdırma (data exfiltration) gibi aşamaları içerir. Red Team uzmanları, sosyal mühendislik saldırıları, fiziksel güvenlik testleri, ağ ve uygulama güvenliği ihlalleri gibi çeşitli saldırı yöntemleri kullanarak organizasyonun güvenlik açıklarını ortaya çıkarır ve kritik varlıklarına yetkisiz erişim sağlamayı hedefler.

Red Team hizmeti, Mavi Takım (Blue Team) ve Güvenlik Operasyon Merkezi (SOC) ile entegre çalışarak, olay tespit ve müdahale süreçlerinin etkinliğini test eder. Tehdit istihbaratı destekli siber saldırı simülasyonları, organizasyonun saldırılara karşı ne kadar hazırlıklı olduğunu değerlendirmek ve geliştirilmesi gereken güvenlik kontrollerini belirlemek için kritik bir rol oynar. Ayrıca, Red Team çalışmaları sonucunda elde edilen bulgular, savunma mekanizmalarının güçlendirilmesi, güvenlik politikalarının iyileştirilmesi ve çalışan farkındalığının artırılması için detaylı raporlar ve öneriler sunar.

Günümüzün gelişen tehdit ortamında, saldırganların giderek daha sofistike yöntemler kullanması nedeniyle, organizasyonların güvenlik sistemlerini düzenli olarak test etmeleri büyük önem taşımaktadır. Red Team hizmeti, güvenlik açıklarının saldırganlardan önce tespit edilmesini ve organizasyonun güvenlik stratejilerini sürekli olarak iyileştirmesini sağlayarak, daha dirençli bir siber güvenlik altyapısı oluşturulmasına katkı sunar.

Hizmete Ait Bileşenler

Tehdit Simülasyonu ve Saldırı Modelleme

Red Team hizmeti, gerçek dünya saldırı senaryolarını simüle ederek organizasyonun güvenlik kontrollerini ve tehdit algılama mekanizmalarını test eder. MITRE ATT&CK çerçevesi kullanılarak saldırganların taktik, teknik ve prosedürleri (TTP) modellenir ve kurum özelinde özelleştirilmiş saldırı senaryoları oluşturulur.

Sosyal Mühendislik Testleri

Çalışan farkındalığını ölçmek ve organizasyonun insan odaklı güvenlik açıklarını değerlendirmek için oltalama (phishing), telefonla dolandırıcılık (vishing) ve fiziksel güvenlik testleri gerçekleştirilir. Yetkisiz erişim girişimleri ile organizasyonun güvenlik politikaları ve erişim kontrolleri sınanır.

Ağ ve Sistem Güvenliği Testleri

Dış ve iç ağ penetrasyon testleri gerçekleştirilerek güvenlik açıkları tespit edilir. Yetkisiz erişim, ayrıcalık yükseltme, yanlamasına hareket (lateral movement) ve veri sızdırma (data exfiltration) gibi saldırı senaryoları uygulanarak savunma mekanizmalarının etkinliği ölçülür.

Uygulama Güvenliği Değerlendirmesi

Web ve mobil uygulamalarda, kurumsal yazılımlarda ve API'lerde güvenlik açıkları belirlenir. OWASP Top 10 ve SANS 25 gibi çerçeveler doğrultusunda yapılan testler ile güvenlik zafiyetleri tespit edilir ve saldırganların kullanabileceği giriş noktaları analiz edilir.

Tehdit Algılama ve Olay Müdahale Testleri

SOC ve Mavi Takım (Blue Team) ile entegre çalışarak olay tespit ve müdahale süreçlerinin etkinliği test edilir. Saldırıların güvenlik ekipleri tarafından ne kadar hızlı tespit edildiği ve nasıl yanıt verildiği değerlendirilerek geliştirilmesi gereken noktalar belirlenir.

Fiziksel Güvenlik Testleri

Yetkisiz erişim, kart kopyalama, güvenlik kameraları ve fiziksel bariyerlerin aşılması gibi testler ile organizasyonun fiziksel güvenliği değerlendirilir. Güvenlik açıkları raporlanarak organizasyonun fiziksel varlıklarını koruma stratejileri güçlendirilir.

Bulguların Raporlanması ve Güvenlik Güçlendirme Önerileri

Gerçekleştirilen testler sonucunda elde edilen bulgular detaylı bir şekilde raporlanır ve organizasyonun güvenlik önlemlerini geliştirmesi için öneriler sunulur. Bulgular, teknik detaylar ve yöneticiler için özet raporlar halinde sunularak güvenlik açıklarının giderilmesi için aksiyon planları oluşturulur.

Mevcut Durum Analizi

Red Team hizmeti uygulanmadan önce, organizasyonun mevcut siber güvenlik durumu detaylı bir şekilde incelenir. Ağ altyapısı, güvenlik duvarları, kimlik doğrulama mekanizmaları, erişim kontrolleri, uç nokta güvenlik çözümleri ve olay müdahale süreçleri analiz edilerek güvenlik açıkları belirlenir. Organizasyonun güvenlik politikaları, çalışan farkındalığı ve tehdit algılama yetenekleri değerlendirilerek, Red Team çalışmalarının odaklanacağı alanlar tespit edilir. Bu analiz sonucunda, en kritik zafiyetlerin önceliklendirildiği bir saldırı senaryosu ve yol haritası oluşturulur.

Strateji ve Yol Haritası Belirleme

Red Team çalışmalarının kapsamı, organizasyonun büyüklüğü, sektörü ve karşılaşabileceği tehdit vektörlerine göre özelleştirilir. Hedef varlıklar, potansiyel saldırı yüzeyi ve uygulanacak test yöntemleri belirlenir. MITRE ATT&CK çerçevesi baz alınarak saldırganların kullanabileceği taktikler, teknikler ve prosedürler (TTPs) belirlenir ve saldırı simülasyonları hazırlanır. Gerçek dünya tehditlerine uygun senaryolar geliştirilerek ağ ihlalleri, sosyal mühendislik, uygulama güvenliği testleri ve fiziksel güvenlik değerlendirmeleri gibi farklı vektörler dahil edilir.

Red Team Hizmeti Uygulama Aşamaları

Red Team hizmeti kapsamında ilk olarak organizasyonun güvenlik durumu analiz edilerek, potansiyel saldırı yüzeyi ve güvenlik açıkları belirlenir. Gerçek dünya saldırı senaryolarına dayanarak sosyal mühendislik testleri, ağ ve sistem penetrasyon testleri, uygulama güvenliği değerlendirmeleri ve fiziksel güvenlik testleri gibi farklı saldırı teknikleri planlanır. Simülasyon aşamasında, yetki yükseltme, yanlamasına hareket (lateral movement), veri sızdırma (data exfiltration) ve güvenlik kontrollerini atlatma gibi saldırı yöntemleri kullanılarak, organizasyonun savunma mekanizmaları test edilir.

Elde edilen bulgular detaylı olarak analiz edilerek, organizasyonun güvenlik açıklarını kapatmasına yardımcı olacak düzeltici önlemler ve güvenlik iyileştirme önerileri sunulur. Red Team operasyonları, SOC ve Mavi Takım (Blue Team) ile entegre şekilde yürütülerek, tehdit algılama ve olay müdahale süreçlerinin ne kadar etkin olduğu ölçülür. Sürecin sonunda, saldırı tespit ve yanıt yeteneklerini geliştirmek için Purple Team tatbikatları gerçekleştirilir ve organizasyonun güvenlik farkındalığı artırılır. Red Team hizmetinin düzenli olarak tekrarlanmasıyla, organizasyonun siber tehditlere karşı dayanıklılığı sürekli olarak güçlendirilir.

MDR ve SOC Uygulama Metodolojisi

Red Team hizmetlerinin etkin bir şekilde uygulanabilmesi için MITRE ATT&CK, NIST 800-115 Teknik Güvenlik Testi ve OSSTMM (Open Source Security Testing Methodology Manual) gibi uluslararası güvenlik çerçeveleri temel alınarak kapsamlı bir metodoloji izlenir. İlk aşamada, organizasyonun mevcut güvenlik durumu analiz edilerek potansiyel saldırı yüzeyi, güvenlik açıkları ve kritik varlıklar belirlenir. Bu süreçte, ağ topolojisi, kimlik doğrulama mekanizmaları, uç nokta güvenliği, güvenlik politikaları ve çalışan farkındalığı gibi unsurlar değerlendirilir.

Saldırı simülasyonları gerçekleştirilirken, ağ penetrasyon testleri, sosyal mühendislik saldırıları, kimlik doğrulama bypass teknikleri, ayrıcalık yükseltme (privilege escalation), yanlamasına hareket (lateral movement) ve veri sızdırma (data exfiltration) gibi saldırganların kullandığı yöntemler uygulanır. Gerçekleştirilen saldırılar, SOC ve Mavi Takım (Blue Team) ile koordineli olarak değerlendirilerek, organizasyonun saldırıları tespit etme ve bunlara yanıt verme yetenekleri test edilir.

Tespit edilen güvenlik açıkları ve eksiklikler teknik ve yönetsel detaylarla raporlanarak, organizasyonun güvenlik kontrollerini geliştirmek için öneriler sunulur. Purple Team tatbikatları ile saldırı tespit süreçleri iyileştirilir ve organizasyonun güvenlik duruşu güçlendirilir. Red Team çalışmaları, yeni tehdit tekniklerine karşı sürekli olarak güncellenerek, organizasyonun siber saldırılara karşı adaptasyon yeteneğini artırır ve proaktif güvenlik önlemleri geliştirmesine katkı sağlar.

Raporlama ve İyileştirme

Red Team hizmetleri kapsamında gerçekleştirilen saldırı simülasyonları, test edilen güvenlik kontrolleri ve tespit edilen zafiyetler detaylı olarak raporlanır. Elde edilen bulgular, saldırı vektörleri, istismar edilen güvenlik açıkları ve organizasyonun olaylara karşı tepkisi teknik ve yönetsel bakış açısıyla analiz edilir. Red Team operasyonlarının etkinliği ölçülerek, organizasyonun güvenlik açıklarını kapatması için düzeltici ve önleyici aksiyon planları oluşturulur.

Olay sonrası analiz çalışmaları ile, organizasyonun savunma mekanizmalarının saldırılara nasıl tepki verdiği değerlendirilir ve güvenlik politikaları güçlendirilerek benzer saldırıların tekrarlanmasının önüne geçilir.

Sıkça Sorulan Sorular (SSS)

Red Team ile Penetrasyon Testi (Pentest) arasındaki fark nedir?

Penetrasyon testleri belirli bir süre içinde hedef sistemleri ve uygulamaları güvenlik açıkları açısından test ederken, Red Team çalışmaları daha geniş kapsamlıdır ve uzun vadeli, gerçekçi saldırı simülasyonlarını içerir. Red Team çalışmaları, organizasyonun tespit ve müdahale yeteneklerini de değerlendirir.

Red Team hizmeti kimler için uygundur?

Büyük ölçekli şirketler, finans kuruluşları, devlet kurumları, sağlık sektörü ve kritik altyapıya sahip organizasyonlar için uygundur. Özellikle siber tehditlere karşı dayanıklılığını test etmek ve gelişmiş saldırganların tekniklerini anlamak isteyen organizasyonlar için önemlidir.

Red Team çalışmaları sırasında sistemlerimize zarar gelir mi?

Hayır. Red Team çalışmaları kontrollü bir şekilde gerçekleştirilir ve kritik sistemlere zarar vermeden, operasyonları aksatmadan güvenlik değerlendirmeleri yapılır. Ancak, organizasyon ile mutabık kalınan çerçevede bazı saldırı simülasyonları uygulanabilir.

Red Team testi sırasında Mavi Takım (Blue Team) bilgilendirilir mi?

Genellikle hayır. Red Team testleri, Mavi Takım'ın tehdit algılama ve müdahale yeteneklerini gerçekçi bir şekilde değerlendirmek için habersiz gerçekleştirilir. Ancak, organizasyona bağlı olarak Purple Team çalışmaları kapsamında iş birliği yapılabilir.

Red Team çalışmaları neden düzenli olarak yapılmalıdır?

Siber tehditler sürekli geliştiğinden, organizasyonların güvenlik açıklarını düzenli olarak test etmesi ve savunma mekanizmalarını güçlendirmesi gerekir. Red Team çalışmaları, güvenlik açıklarını erkenden tespit etmek ve organizasyonun tehditlere karşı dayanıklılığını artırmak için düzenli olarak yapılmalıdır.

Red Team hizmetinden sonra organizasyonumuz nasıl iyileştirilebilir?

Red Team çalışmaları sonucunda sunulan rapor doğrultusunda güvenlik açıkları kapatılır, çalışanlara güvenlik farkındalık eğitimleri verilir, algılama ve müdahale süreçleri geliştirilir ve güvenlik politikaları güçlendirilerek organizasyonun siber dayanıklılığı artırılır.