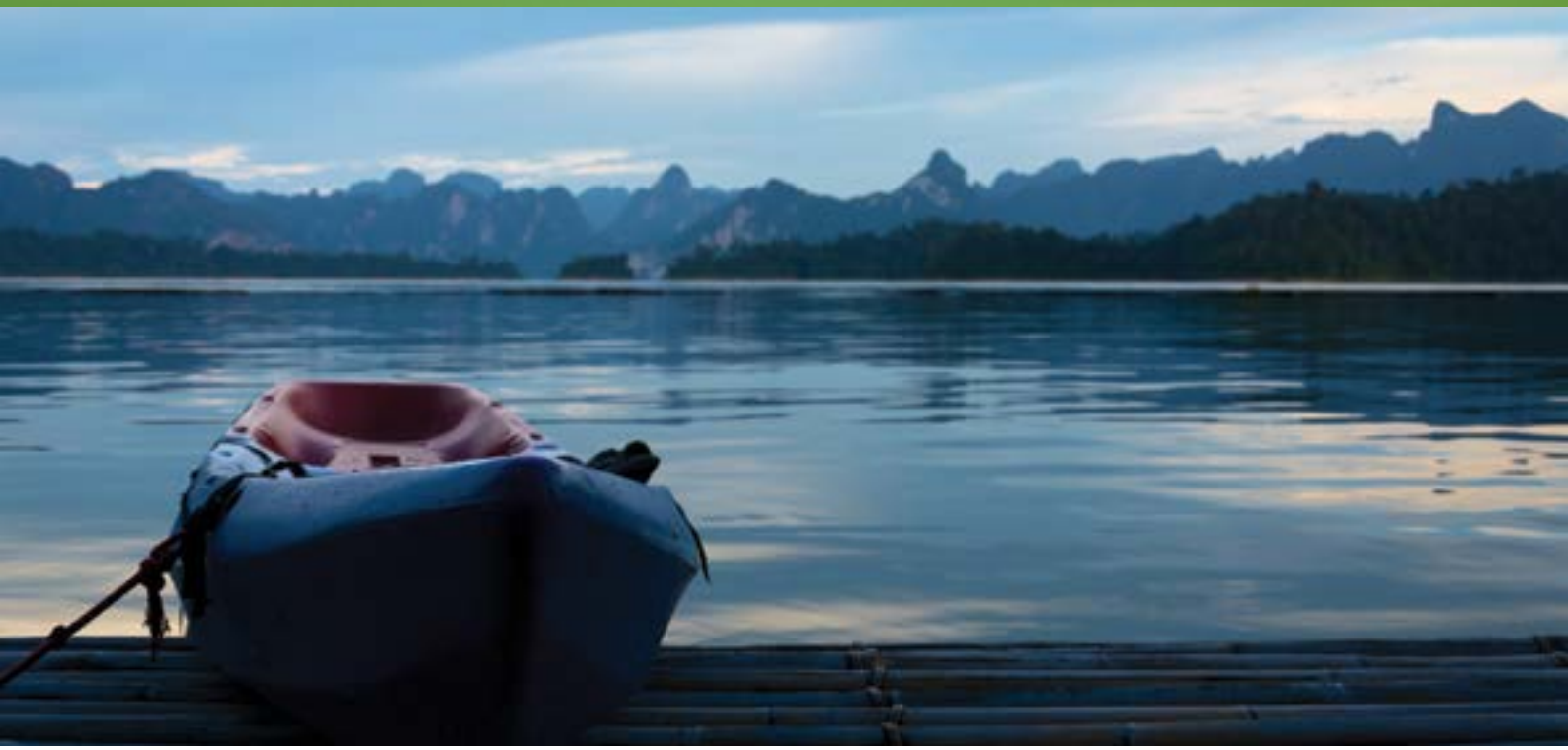
SİBER GÜVENLİK ÇÖZÜMLERİ

Stratejik Siber Güvenlik Danışmanlığı Hizmetleri



www.bgasecurity.com

BGA SECURITY

Hakkımızda

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile faaliyetlerini Ankara, İstanbul, Azerbaycan ve USA'da sürdüren BGA Bilgi Güvenliği A.Ş.'nin ilgi alanlarını "Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

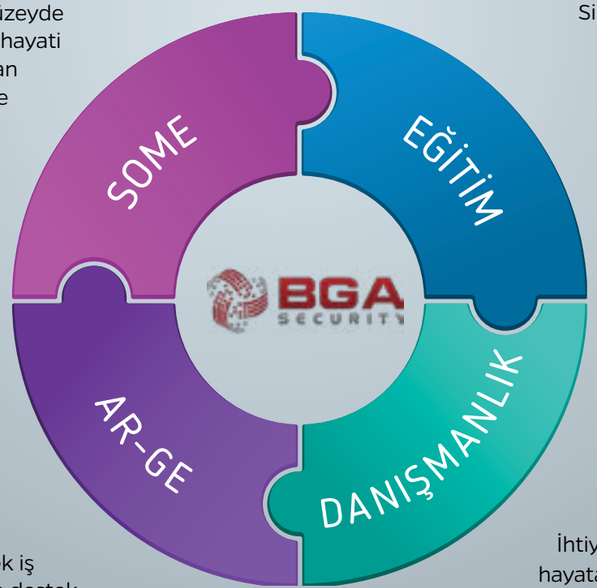
BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi gibi sosyal sorumluluk projeleri ile birçok konuda gönüllü faaliyetlerde bulunmuştur.

SOME

Siber olayların ulusal düzeyde yönetimini sağlayan ve hayati yapılardan bir tanesi olan Siber Olaylara Müdahale Ekibi ile siber saldırılar ve tehditlere karşı önleme, tespit ve müdahale görevlerini üstlenmektedir.

AR-GE

Siber Güvenlik konusunda bilgi birikimini paylaşmayı amaçlayan BGA sektörün gelişmesine yönelik uygun olabilecek iş modellerini sunmaya ve destek vermeye devam etmektedir.



EĞİTİM

Siber güvenlikte başarıya ulaşmak için gerekli olan bilgi güvenliği eğitimleri, uzman eğitmenlerimiz tarafından Türkçe hazırlanan dokümanlarla sunulmaktadır.

DANIŞMANLIK

Şirketlere ve kamu kurumlarına siber güvenlik konularında hizmetler sunuyoruz. İhtiyaca yönelik çözümlerin hayata geçirilmesinde destek sağlıyoruz.

Akreditasyon ve Yetkinliklerimiz

Rakamlarla Son 5 Yılın Özeti

Son beş yılda binden fazla kuruma, siber güvenlik danışmanlığı ve eğitim hizmetleri verilmiştir. Danışmanlık ve eğitim hizmetlerinin yanı sıra, siber güvenlik kampları ile yüzlerce öğrenci yetiştirilerek siber güvenlik sektörüne insan kaynağı sağlanmıştır.

Uzman ekip ve eğitmenlerimiz tarafından hazırlanan binlerce sayfalık teknik dokümanlar sektörün gelişimi için BGA Security'nin tüm kanallarından ücretsiz olarak paylaşılmaktadır.

Türkiye ve dünyadaki gelişmeleri paylaşmak, gündemin yakından takip edilmesini sağlamak amacıyla sektörün önde gelen uzmanları, bilgi güvenliği alanına meraklı kişiler ve birçok kurumun üst düzey yöneticilerinin de yer aldığı 8.500 kişilik e-posta gurubu oluşturulmuştur.

Oluşturulan e-posta gruplarında bilgi aktarımının daha hızlı gerçekleşmesi sağlanmış, güncel bilgiye erişme imkanı arttırılmıştır.

Siber güvenlik konularında ilgilileri aydınlatmaya, eğitmeye ve sektör gelişimini desteklemeye yönelik hazırlanan yayınlar, yabancı dil bilmeyenlerin de faydalanabilmesi için Türkçe içerikli olarak hazırlanmıştır.

Bilgi güvenliği alanında çalışan ve bu alana merak duyan kişiler arasında etkileşim yaratmayı amaçlayarak her yıl düzenlenen İstSec (İstanbul Bilgi Güvenliği Konferansı) ve Siber Güvenlik Konferansları ile binlerce katılım talebi almaktadır.

BGA, kış ve yaz dönemleri olmak üzere sosyal sorumluluk projesi kapsamında senede iki defa düzenlediği siber güvenlik kampları ile 250'den fazla öğrenciyi eğitmiş, öğrencilerin kariyer yollarına bir adım önde başlamalarına vesile olmuştur.

Üniversitelerle işbirliği yaparak mevcut olanaklarını öğrencilere sunan ve onlara faydalı platformlar yaratan BGA Security uzman kadrosu, farklı üniversitelerde eğitimler de vermektedir.

Siber Güvenlik Danışmanlık Hizmetleri

Ürün Bağımsız Tehdit Odaklı Siber Güvenlik Danışmanlığı

BGA Security, gelişen teknoloji ve yaygınlaşan internet kullanımı ile birlikte güçlü bir silah haline gelen siber saldırılara karşı kurum ve kuruluşlara ihtiyaç duydukları konularda destek vermektedir. Ürün bağımsız güvenlik yaklaşımı sayesinde **"güvenlik satan değil, güvenlik sağlayan"** bir şirket olma özelliğini korumaktadır.

BGA Security, genel danışmanlık çatısı altında kurumlara yönelik saldırıları ve güvenlik ihtiyaçlarını tespit ederek siber güvenlik konusunda doğru alana yatırım yapmalarını sağlamaktadır.

Yapılan görüşmeler sonucu verilecek olan danışmanlık hizmetinin genel çerçevesi ile çizilerek BGA Security danışman kadrosu tarafından kurumun envanteri, internet ortamındaki varlığının haritası çıkartılır ve bir sızma testi yapılır.

Bu test sonuçları kurumun siber güvenlik risk haritasının çıkartılmasını ve yapılması gereken güvenlik yatırımlarının en doğru şekilde yönlendirilmesini sağlar.

Bu sayede kurum kendisine karşı yapılabilecek siber saldırılara karşı doğrudan önlem alabilmekte ve geri dönüşü zayıf harcamaların kurum bütçesini olumsuz yönde etkilemesini önleyebilmektedir.

Dokuz adımdan oluşan BGA Security Danışmanlık hizmetlerinin detayları için **bilgi@bga.com.tr** e-posta adresimizden bilgi alabilirsiniz.

Siber Güvenlik Danışmanlık Hizmetleri

- Penetrasyon (Sızma) Testleri
- DoS / DDoS, Performans ve Yük Testleri
- Kaynak Kod Güvenlik Denetimi Hizmeti
- Linux / UNIX Sistem Güvenliği Sıkılaştırma Hizmeti
- Windows Sistem Güvenliği Sıkılaştırma Hizmeti
- ISO 27001 (BGYS) Kurulum ve Yönetimi
- Web ve Mobil Uygulama Güvenlik Testleri
- Zararlı Yazılım (Malware) Analizi
- PCI DSS Danışmanlığı
- Bilgi Güvenliği İhlal ve Olay Yönetimi Hizmeti
- SOC Danışmanlık Hizmeti
- Siber Suç ve Adli Bilişim Analizi
- Siber Tatbikat ve Güvenlik Verimlilik Ölçümü
- Açık Kaynak Kod Güvenlik Çözümleri
- APT Testi ve Analizi Hizmeti
- Log Yönetimi ve Korelasyonu Hizmeti
- Bilgi Güvenliği Proje Yönetimi Hizmeti
- Kurumsal Bilgi Güvenliği Eğitimleri
- Sızma Testi Sonuçları Kapama ve Destek Hizmeti
- Siber Tehdit İstihbaratı Hizmeti
- Normshield Güvenlik Zafiyeti Yönetim Sistemi
- Outsource Bilgi Güvenliği Uzman Temini
- SCADA Kurulumu
- ICS / SCADA Güvenlik Testleri ve Güvenliği
- Sürdürülebilir Bilgi Güvenliği Farkındalık Programı
- Kurumlara Yönelik Bilgi Güvenliği Karnesi Oluşturma
- SIEM Korelasyon ve SOME Tatbikat Hizmeti

Sızma testleri ve zafiyet tarama birbirine benzeyen ancak farklılıkları olan iki ayrı kavramdır.

Sızma Testleri

Bilişim sistemlerindeki güvenlik zafiyetlerinin üçüncü bir göz tarafından kontrol edilmesi ve raporlanması güvenliğin ilk basamağıdır.

Sistemlerdeki potansiyel zafiyetler, sistem yöneticileri tarafından kolaylıkla fark edilemez.

Bu durum kurum güvenliği adına istenmeyen sonuçlara yol açabilir. Bu noktada savunmacı güvenlik olan defansif güvenlik (defensive security) ve proaktif olarak tabir edebileceğimiz ofansif güvenlik (offensive security) devreye girer.

Sızma testleri (Pentest), müşteri tarafından belirlenen bilişim sistemlerine mümkün olabilecek ve onay verilen her yolun denenerek sızılmaya çalışma işlemlerinin tamamına verilen hizmetleri kapsamaktadır. Sızma testlerinde amaç güvenlik açıklığını bulmaktan öte bulunan açıklığın değerlendirip yetkili erişimler elde edilmesidir. Whitebox, blackbox ve graybox olmak üzere genel kabul görmüş üç türde sızma testi yapılır.

Pentest çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıkları kullanarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin belirlenmesidir.

Pentest Metodolojisi

Sızma testlerini gerçekleştiren uzmanlar çalışmalarının doğrulanabilir, yorumlanabilir ve tekrar edilebilir olmasını sağlamak için önceden hazırlanmış olan metodolojileri kullanır ve edindiği tecrübelere göre bu metodolojileri geliştirir.

Metodoloji kullanımı sızma test ekipleri için hayati önem taşımaktadır. Sızma testlerinde daha önce denenmiş ve standart haline getirilmiş kurallar uygulandığında daha başarılı sonuçlar elde edilir.

İnternet üzerinden ücretsiz olarak edinilen bazı metodolojiler incelenerek yapılacak güvenlik denetim testlerinin daha sağlıklı ve tekrar edilebilir sonuçlar üretmesi sağlanır.

› OWASP › OSSTMM › ISSAF › NIST SP800-155

OWASP

OWASP, web/mobil uygulamalar için detaylı güvenlik testlerinin nasıl yapılacağını anlatan kontrol listesidir.

ISSAF

ISSAF, bilgi güvenliği uzmanları tarafından sızma testlerinde kullanılmak üzere geliştirilmiş güvenlik testi kontrol listesidir.

OSSTMM

OSSTM, sızma testlerinin teknik, idari ve yönetimsel yönlerini bir bütün olarak ele alan ve bu konularda yapılması gerekenleri aktaran tavsiye dökümanıdır.

NIST SP800-115

Amerika Birleşik Devletleri tarafından kamu kurumlarına verilecek güvenlik denetimi hizmetlerini düzenleme amaçlı geliştirilmiş standart dökümandır..

BGA Security tarafından sızma testlerinde kullanılan kontrol listesi, 400 farklı madde içermektedir ve bilinen tüm sızma testi standartlarını desteklemektedir.

Neden BGA Sızma Testleri

BGA Security Pentest hizmetini tercih etmeniz için bazı önemli nedenler.

- BGA Security Türkiye ve dünyada sızma testleri konusunda 100'ün üzerinde kurumsal referansa sahiptir.
- Pentest ekibimiz uluslararası geçerliliğe sahip CEH, CISSP, LPT, OSCP sertifikalarına sahiptir.
- Uygulama testleri 10 yıllık tecrübesi olan kıdemli üyeler tarafından gerçekleştirmektedir.
- Sızma testleri konusunda tecrübelerimizi BGA Security Blog adresimizde paylaşmaktayız.
- BGA Security 15 kişilik teknik ekip ve 100'ün üzerinde kurumsal referans ile hizmet vermektedir.

Referanslar

BGA Security kuruluşundan bu yana 100'ün üzerinde farklı kuruma sızma testi gerçekleştirmiştir. Hizmet verilen firmalar arasında ülkemizin en büyük finans kurumları, telekom şirketleri, enerji firmaları, savunma sanayi firmaları ve kamu kurumları yer almaktadır. Referanslar **Non Disclosure Aggrement (NDA)** kapsamında korunmaktadır. Detaylı bilgi için **bilgi@bga.com.tr** adresimiz ile iletişime geçebilirsiniz.

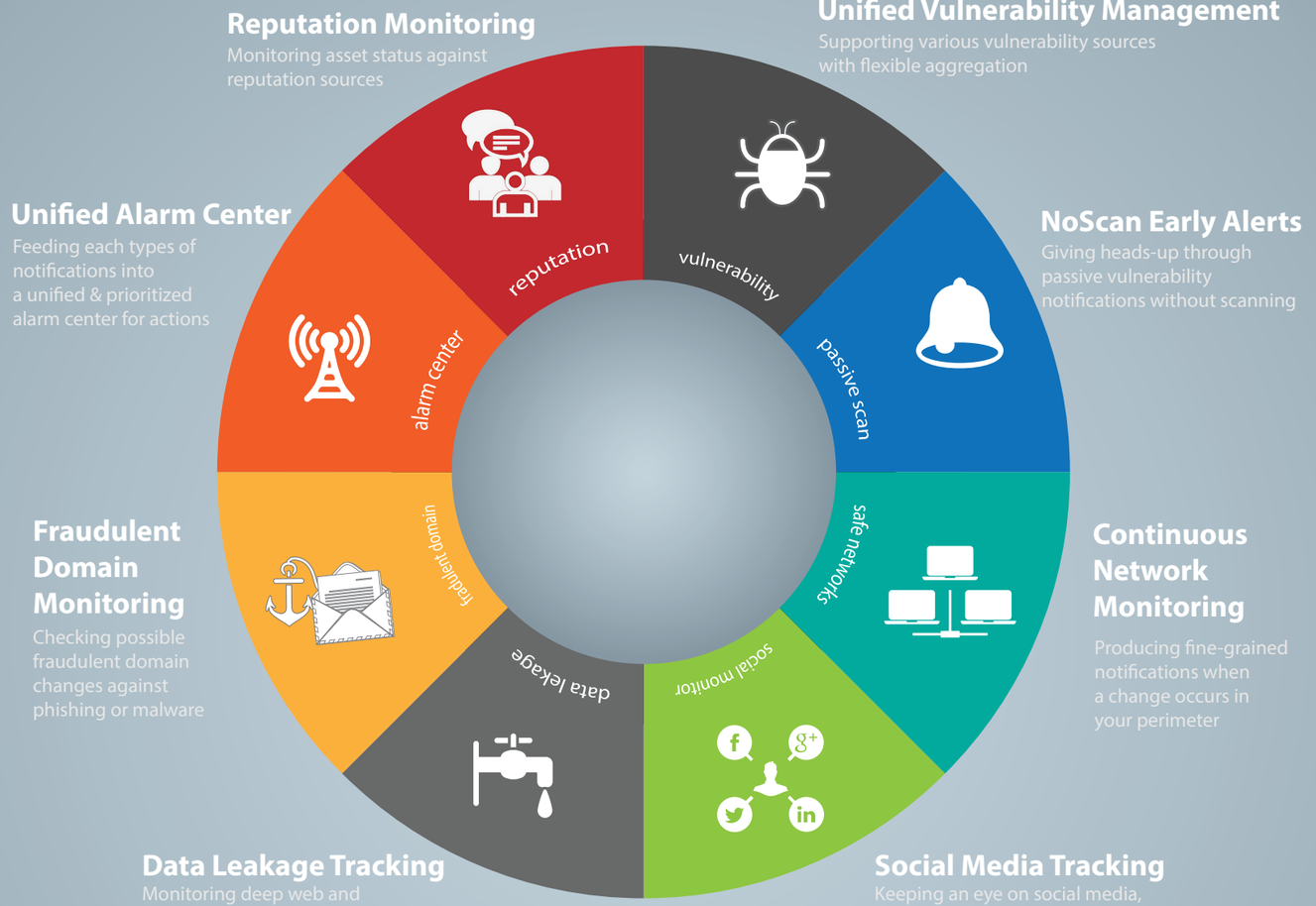
Düzenli Zafiyet Tarama ve Yönetim Hizmeti

Zafiyet Yönetimi

Kullanılan tarama yazılımları ve sızma testleri sonuçlarında ortaya çıkan güvenlik zafiyetlerinin siber istihbarat bilgileriyle önceliklendirmesi, sistem, ağ, uygulama ve veritabanı yöneticilerine atanması, Active Directory üzerinden takibi ve korelasyon amaçlı SIEM sistemine gönderilmesi bu hizmetin en önemli özelliklerindendir.

Tehdit Gözetleme

PTM modülü, sadece yerel ağ üzerindeki trafiği pasif olarak dinleyip kurum içi ağının siber hijyen durumunu anlık olarak gözetler ve olası tehditler konusunda anlık uyarılar üretir. PTM modülü kullanıldığında kurum yerel ağında güvenliği ihlal edecek tüm olaylar seviyelendirilerek tanıtılmış ve sisteme öğretilmiştir. PTM modülü aynı zamanda yerel ağdan İnternete doğru oluşacak kirli trafiği de düzenli olarak takip eder ve bilgilendirme yapar.



Reputation Monitoring
Monitoring asset status against reputation sources

Unified Vulnerability Management
Supporting various vulnerability sources with flexible aggregation

Unified Alarm Center
Feeding each types of notifications into a unified & prioritized alarm center for actions

NoScan Early Alerts
Giving heads-up through passive vulnerability notifications without scanning

Fraudulent Domain Monitoring
Checking possible fraudulent domain changes against phishing or malware

Continuous Network Monitoring
Producing fine-grained notifications when a change occurs in your perimeter

Data Leakage Tracking
Monitoring deep web and paste portals seeking valuables

Social Media Tracking
Keeping an eye on social media, harvesting security related big data

Siber İstihbarat

Siber Tehdit İstihbaratı, kurumlar hakkında İnternet'te açık ve yarı açık kaynaklarda dolaşan bilgilerin siber güvenlik bakış açısı ile değerlendirilmesi ve aksiyon üretecek şekilde çıktı üretmesidir. NormShield CTI modülü, kurumunuzla ilgili İnternet üzerindeki her türlü bilgiyi düzenli olarak arşivler ve kurumunuzla ilgili olası tehdit durumlarında erken uyarı sistemi olarak çalışır. Sizi hedef alacak bir sosyal mühendislik veya veri sızıntısı saldırısını ortalama bir hafta öncesinden haber vermektedir.

Soc Radar

SOC yöneticilerinin ihtiyaç duyabileceği tüm izleme araçlarının merkezi olarak sunulduğu bir modüldür. Kurumların İnternet'e açık Asset'leri üzerinde çıkabilecek güvenlik açıklarının takibi, kurum ip adreslerinin kara liste kontrolü, kontrolsüz açılacak yeni host veya uygulama kontrolü ile güvenlik cihazlarının işlevsellik kontrolü temel özelliklerindendir. SOC Radar modülü aktif olduktan hemen sonra kurumun dış sistemlerini dakikalık kontrollerle izlemeye başlar ve kurumun siber güvenliğini ihlal edecek herhangi bir durum gerçekleşmesi halinde alarm üretir.

IT sistemlerinde her hafta yüksek ve kritik öneme sahip güvenlik açıklıkları yayınlanmaktadır.

Düzenli Açıklık Tarama Aracı

Kurumların tercihine bağlı olarak proaktif güvenliğin temel bileşenlerinden olan sızma testi çalışmaları, (genellikle) maliyet faktöründen dolayı yılda bir kez yapılmaktadır. Oysa ki orta ve büyük ölçekli firmaların kullandığı IT sistemlerinde ortalama olarak her hafta kritik öneme sahip güvenlik açıklıkları ortaya çıkmaktadır.

Firmaların sızma testi yaptırmadığı zaman aralığında İnternet üzerinden otomatize bir şekilde düzenli olarak güvenlik taraması yapabilmesi için bu hizmet geliştirilmiştir.

Kullanımından önce kurumun varlıkları sisteme tanımlanır. Ardından da düzenli aralıklarla güvenlik tarama istekleri gönderilir. Güvenlik tarama istekleri sistem yöneticilerine gelir, talep ve varlığın tipine göre (Network, Sistem, Uygulama gibi) güvenlik taramaları gerçekleştirilir.

Güvenlik Seviyenizi Artırın!

Güvenlik Seviyesi İyileştirme Hizmeti

Kurumlardaki IT sistemlerinin zafiyetleri temelde üç ana maddeden kaynaklanmaktadır.

- **Güncelleme eksikliği**
- **Yazılım zafiyetleri**
- **Yapılandırma hataları ve ön tanımlı hesaplar**

Yazılım haricindeki diğer iki maddeye ait bulgular sistemler üzerinde gerçekleştirilecek güvenlik sıkılaştırma çalışmalarıyla büyük bir oranda çözülebilir. Sistem sıkılaştırma hizmeti Windows, UNIX, ağ cihazları ve güvenlik sistemlerinin, Amerika Standartları Enstitüsü (NIST) gibi kabul görmüş kurumlar tarafından yayınlanan ve standart olarak kabul edilen en iyi güvenlik ayarlarına getirilmesi için gerekli testleri ve iyileştirme çalışmalarını içermektedir.

- Gerekli sıkılaştırma ayarlarının raporlanması
- Kullanılan Wi-fi sistemlerinin yapılandırmalarının kontrol edilmesi
- Ağ altyapısının ve konumlandırılan güvenlik sistemlerinin incelenmesi
- Kullanılan ağ sistemlerinin (switch, router v.b) yapılandırma kontrolü
- Windows, Linux ve UNIX sistemlerin NIST'e göre kontrol edilmesi
- Güvenlik sistemlerinin (IPS/WAF/AV/VPN/AntiSpam v.b) kural ve yapılandırma kontrolü
- Güvenlik duvarı kurallarının analiz edilmesi ve güvenlik duvarı yapılandırmasının kontrol edilmesi
- Güvenlik sıkılaştırma hizmeti için hazırlanan kuruma özel betikler (script) hizmet verilen kurumla paylaşılmakta ve düzenli olarak sıkılaştırma testleri yapmaları konusunda destek sağlanmaktadır.

DoS / DDoS Test ve Koruma Hizmetleri

DOS ve DDOS saldırıları bilgi güvenliğinin erişilebilirlik bileşenini hedef alıyor. Hemen hemen her yıl kurumların altyapılarına yönelik DDOS saldırıları yapılmakta ve kesin bir engelleme yöntemi bulunmamaktadır.

DDOS saldırılarına hedef olmadan altyapınızı test ettirmek ve uzmanların gözetiminde ağ altyapısının düzenlenmesi bu noktada alınabilecek önlemlerin en başında gelir.

Hizmetlerimiz aşağıdaki ana başlıklardan oluşmaktadır.

DDOS testi ve engelleme konusunda en az beş yıllık deneyime sahip sertifikalı uzmanlarımız, kurumunuza gelebilecek tüm DDOS ataklarının gerçek ortamlarda BotNet gibi illegal sistemler kullanmadan özel olarak geliştirdiğimiz yazılımlar sayesinde test ettirmeniz mümkündür.

- Tüm DDOS tiplerine karşı 5 Mbps – 5 Gbps arası düzenli testler yapılır.
- Sistemlerinizi olası DDOS saldırıları durumlarına karşı raporlanması.
- DDOS testleri klasik performans testlerinden farklı olarak gerçekleştirilir.
- Saldırı anında ya da saldırı sonrasında DDOS ataklarının incelenmesi.
- Hukuki açıdan gerekli kanıtların toplanması ve sunulması.

Bu hizmete DDOS engelleme sistemleri dahil değildir. DdoS engelleme için yapılması gerekenler yapılan analizler sonrası ortaya çıkartırlır.

Siber Suç İnceleme Hizmeti

Hayatın her alanında olduğu gibi suç ve suçlu bilişim sistemlerinde de karşımıza çıkmaktadır. Gerçekleşen siber olayların aydınlatılmasında anahtar bileşen olarak konumlandırılan bilişim sistemleri; doğru ve tarafsız analiz edildiğinde suçluya ait normal yollarla tespit edilemeyen deliller sunabilir.

Adli bilişim analizi (Computer Forensics) suçlu psikolojisi ve teknolojinin gücü ile birleştirildiğinde inkar edilemez somut deliller ortaya çıkarmaktadır.

İşlenen suç veya yaşanan siber güvenlik ihlali sonrası delillerin profesyonel bir ekip tarafından toplanması suçlu hakkında önemli bilgiler sağlar. Bu tür olaylarda sıkça gözden kaçan "sisteme sızan başka ne yapmış?" sorusuna da en kapsamlı şekilde bu çalışmalar ile cevap bulunabilir.

Siber Suç Örnekleri

Zararlı yazılımların sistem üzerinden bilgi kaçırması, iç çalışan tehdidi, sahte e-posta gönderimi, Phishing (oltalama) saldırıları, DDOS saldırısına maruz kalmak, kurum web sayfasının hacklenmesi, kurum sistemleri üzerinden Spam gönderilmesi, IP spoofing yapılarak firmanın suçlu duruma düşürülmesi, Facebook, Twitter gibi sosyal medya hesaplarının ele geçirilmesi, şirket yöneticilerinin e-posta hesaplarının başkaları tarafından okunması, şirkete ait önemli verilerin şirket dışına yetkisiz bir şekilde çıkartılması.

Güvenlikte en zayıf halka, “insan davranışları” üzerine odaklanıyoruz.

sinara labs

Bilgi Güvenliği Farkındalık Programı

Dünyaca ünlü bilişim firmalarının son yıllarda yaşadığı bilgi güvenliği ihlal olayları detaylıca incelendiğinde, çalışanların bilgi güvenliği farkındalığı noktasındaki eksikliği karşımıza çıkmaktadır. Bilgi güvenliğini tehdit eden risklerin en başında çalışanların güvenlik konusundaki farkındalık eksikliği gelmektedir.

Bilgi Güvenliği Farkındalık Ölçümü ve İyileştirme

Siber güvenliğin sağlanmasında en önemli etken firma çalışanları için bilgi güvenliği farkındalığı oluşturmaktır. Yapılan araştırmalar çalışanların bilgi güvenliği farkındalık seviyesinin dünya genelinde oldukça düşük olduğunu ortaya çıkarmıştır. Çalışanların bilgi güvenliği farkındalığını yükseltmeden yapılacak olan teknik yatırımlar, sadece otomatize saldırılara karşı önlem sağlayabilir.

SİNARA LABS

Sinara Labs, çalışanlarınız için farklı senaryolarda oltalama testleri gerçekleştirmenize ve farkındalık düzeyini arttıracak kampanyalar oluşturmanıza olanak sağlar. Her test sonucunu kullanıcı ve gurup bazlı ayrıntılı olarak raporlar. Bu raporlar sayesinde aksiyon alarak, kullanıcı odaklı eğitimler geliştirmenize yardımcı olur.

Oltalama saldırıları, kurumlara en çok zarar veren ve sızma testlerinde zararlı yazılım bulaştırmak için kullanılan etkili saldırı yöntemlerinden biridir. Sinara Labs, bu tür saldırılara karşı şirket çalışanlarının bilgi güvenliği farkındalığını test ederek önlem alınmasını sağlar.

Kurum çalışanları için farklı senaryolarda oltalama testleri gerçekleştirerek farkındalık düzeyini arttıracak kampanyalar oluşturmanıza olanak sağlayan Sinara Labs ile detaylı durum raporları oluşturarak güvenlik seviyenizi artırabilirsiniz.

APT Testleri

Hedefin belli olması, kullanılan yöntemlerin farklılıkları ve saldırganların yüksek motivasyona sahip olması nedeniyle siber güvenlikte en çok zarar veren saldırı türü APT saldırılarıdır.

Karşı karşıya olduğumuz saldırgan profiline ve kullandıkları yöntemlere uygun olarak geliştirilen yöntem ve araçlarla yapılan APT değerlendirme testleri, kurumun gerçek güvenlik seviyesini bu saldırganların gözünden ortaya koyma imkanı sağlamaktadır.

BGA tarafından sunulan APT değerlendirme testleri, mevcut bilgi güvenliği seviyenizi sıradan sızma testlerinden çok daha etkili bir şekilde ölçebilmenize olanak sağlar.

Farkındalık Eğitimleri

Çalışanların farkındalık seviyelerinin arttırılmasında en önemli maddelerden biri düzenli olarak eğitim verilmesi ve eğitimler sonrası farkındalık senaryolarını içeren saldırı simülasyonlarının gerçekleştirilmesidir.

BGA Bilgi Güvenliği AKADEMİSİ farkındalık eğitimi, teorik ve pratiği bir araya getirerek katılımcıların sıkılmadan bir günü geçirmesini sağlayacak bir içeriğe ve işleyişe sahiptir. Güncel saldırı yöntemleri ve bunlara karşı alınabilecek önlemlerin senaryolar eşliğinde anlatıldığı eğitim sonrası gerçekleştirilecek farkındalık seviyesi ölçüm / değerlendirme sınavı katılımcıların farkındalık seviyesindeki artışı da somut olarak gösterecektir.

Verizon Veri Sızıntı Raporu 2014'e göre SIEM/LOG çözümleri günümüz saldırılarının %1'ini zamanında tespit edebiliyor.

SIEM / LOG Korelasyon Hizmetleri

Bilişim sistemlerinde yaşanabilecek her tür güvenlik problemi IT sistemlerinden alınacak düzenli LOG'larla tespit edilebilir. Bu bağlamda kurumsal firmalarda Merkezi LOG Yönetim Sistemleri kullanılır. Kurumların güvenlik olaylarına karşı hangi LOG'ları toplaması gerektiğini tespit edememesi ve birden fazla güvenlik probleminin bir araya gelerek nasıl bir tehdit oluşturabileceğini ön görememesi büyük bir risk taşır.

"BGA Security Log Korelasyon Hizmeti" kurumların hangi tip Log'lara ihtiyaç duyabileceğine ve bu Log'ların ilgili sistemlerden alınıp merkezde toplandıktan sonra anlamlı verilerin elde edilmesi için yorumlanmasına yönelik çalışmalardan oluşmaktadır. Bununla birlikte hizmet kapsamında aşağıdaki ana başlıklarla ilgili çalışmalar yapılmaktadır

- Örnek Log incelemesi
- Log Kaynaklarının Belirlenmesi
- Gelişmiş Korelasyon Kurallarının Oluşturulması
- Siber Saldırı Simülasyon ve SOME Tatbikat Çalışması
- Log Anlamlandırma, Etiketleme ve Seviyelendirme Çalışması
- Gereksinimlerin Tespiti, Kapsam Belirleme ve Proje Yönetimi
- Kaynaklardan Alınacak Log'lar için detay ve içeriğinin belirlenmesi
- Log toplanacak sistemlerin tespit edilerek korelasyon kurallarının hazırlanması
- Korelasyon kurallarının yazılımı sonrası pratikte test edilerek çalışıp çalışmadığının belirlenmesi
- Log yönetim sistemi tarafından tanınmayan veya özel olarak geliştirilmiş uygulamalara ait sarmal aracı yazılımların geliştirilmesi

SOME Tatbikatı ve Tehdit Simülasyon Hizmeti

Kurumların "güvenliğe yatırım yapıyoruz ve güvendeyiz" anlayışı ile gerçek manada güvenli olmaları birbirinden farklı ancak karıştırılan bir durumdur. BGA Security "Siber Güvenlik Tatbikat Hizmetimiz" ile kurumun dış ve iç güvenlik bileşenlerini (çalışanlar dahil) siber saldırgan gözüyle gerçek hayattakine benzer bir saldırı simülasyonu yapılarak ölçülebilir.

Siber Tatbikat Hizmeti, sızma testi veya güvenlik denetimi hizmetlerinden farklıdır. Hizmet boyunca kurum için yapılan tüm güvenlik yatırımlarının (Log'lama, Antivirüs, Ips, Firewall, bilgilendirme vb.) gerçek bir siber saldırı karşısında ne kadar işe yaradığını somut bulgularla ortaya çıkarmaktadır.

Bu hizmet sonrasında kurum, yatırım yapmış olduğu bilgi güvenliği alanlarının ne kadar efektif olduğunu, gerçek manada eksik noktalarını ve iyileştirme alanlarını görebilir. Hizmet sonrası ortaya çıkacak rapor kurumun karşısına çıkabilecek bir siber saldırı sonucunu net olarak ortaya koyacaktır.

SOME tatbikatlarının klasik sızma testlerinden en önemli farkı hedef sistemin sahip olduğu güvenlik önlemlerinin ve güvenlik birimi çalışanlarının efektif olarak ölçülmesi ve somut değerlerle raporlanmasıdır. Tatbikat hizmeti sonrası ilgili kurumun bünyesinde barındırdığı güvenlik cihazı, yazılım ve çalışanların İnternet üzerinden veya yerel ağdan gelebilecek bir siber saldırı sonrası nasıl davrandığı ölçülmüş ve varsa eksik noktaların iyileştirilmesiyle sonuçlanmış olacaktır.

Some Hizmetleri Tablosu

Hizmet Kapsamı / Açıklama	Basic	Pro	Enterprise	Custom
SOME Strateji Dökümanının yazılması	✓	✓	✓	✓
SOME için Gerekli Altyapı Kurulum Danışmanlığı	✓	✓	✓	✓
Olay Müdahale ve Analiz Hizmeti	✓	✓	✓	✓
Yönetilen Log/SIEM Hizmeti (Kiralama & Yönetim)				✓
Yönetilen Tehdit Gözetleme & IDS Hizmeti				✓
Siber Tehdit İstihbaratı ve SOC Radar			✓	✓
Düzenli Güvenlik Açıklığı Tarama Hizmeti (Aylık)		✓	✓	✓
SOME Eğitim Paketi		✓	✓	✓
Sızma Testi ve Sistem Sıkılaştırma Hizmeti			✓	✓
Olay Müdahele, Forensic Analizi, Zararlı Yazılım Analizi	✓	✓	✓	✓
SIEM/Log Korelasyon ve Doğrulama Hizmeti			✓	✓
APT Testi ve Analiz, Tespit Sistemi Kurulumu (DNS Tabanlı)				✓
SOME Tatbikat ve Tehdit Simülasyonu				✓
SOME Akreditasyon ve Sertifikasyon Süreci (TI)				✓
7/24 Güvenlik İzleme ve Bilgilendirme				✓
ICS/SCADA Güvenliği Analizi ve Denetimi				✓
Açık Kaynak Saldırı Tespit/Tehdit Gözetleme ve Loglama Altyapısı Hizmeti	✓	✓	✓	✓

Ölçemediğiniz şeyi yönetemezsiniz!
Güvenliğinizi ölçmek ve yönetmek ister misiniz?

Güvenlik Ölçüm Hizmeti Seviyeleri

Hizmet Adı ve Açıklama	Standart	Professional	Enterprise
Analiz Aşaması ve Durum Tespiti	✓	✓	✓
Teknik Altyapı Yeterliliği Ölçümü için Siber Tatbikat ve Simülasyon		✓	✓
Değerlendirme & Raporlama Çalışmaları (Siber Karne Hazırlama)		✓	✓
Siber Güvenlik İyileştirme Çalışmaları			✓
Düzenli Ölçüm ve Bilgilendirme			✓
Information Security Score Card Hazırlama			✓

Siber Güvenlik Seviye Tespit ve İyileştirme

BGA Security **“Siber Güvenlik Karne Çalışması”** ile kurumların güvenlik seviyeleri ve yaptıkları güvenlik yatırımlarının kurum güvenliğine sağladığı katkı ortaya çıkartılmaktadır. Kurumlar, verilerinin güvende olup olmadığını kullandıkları güvenlik teknolojilerini denetleyerek saptayabilirler.

“Siber Güvenlik Karne Çalışması” kapsamında gerçekleştirilen teknik analizler ile kurumun bilgi sistemlerine ait siber güvenlik olgunluk seviyesi somut parametrelerle ortaya koyulmakta ve sistemi güvenlik açısından etkileyebilecek bilgi teknolojileri risklerine karşı önlemler sunulmaktadır. Hizmet sonrasında sunulan raporla kurumlar, bilgi güvenliği alanındaki uygulamalarının ne kadar etkin olduğunu, bu alandaki eksik noktalarını ve iyileştirme alanlarını görebilmektedirler. Bu rapor ile olası bir siber saldırı karşısında kurumun durumunun ne olacağı net bir şekilde ortaya çıkmaktadır.

En önemlisi de **“Ne kadar güvendeyiz?”** sorusunun cevabı verilerle yanıtlanmaktadır. Diğer taraftan sunulan rapordaki her bir kontrol maddesi, yıllık plan içerisinde düzenli olarak takip edilmekte ve bu sayede ölçümlenen siber güvenlik durumu kontrol altında tutulabilmektedir.

Analiz

Analiz ve durum tespiti iki aşamalı olarak gerçekleştirilir. Farklı ekip ve birimlerdeki çalışanlardan bilgi toplandıktan sonra teknik sistem yapılandırmalarının denetimi sağlanır ve zafiyet durumu incelenir. Kurumun tercihine bağlı olarak ağın Siber Güvenlik Hijyen Durumu çalışması da yapılmaktadır. Böylece alınması gereken acil bir önlem varsa, çalışmanın sonlanması beklemeden hemen aksiyon alınabilir.

Tatbikat

Kurumun bilgi teknolojileri alt yapısının ve kurumdaki tüm güvenlik bileşenlerinin (çalışanlar da dahil) bir saldırı simülasyonu ile ölçümüdür. Siber Tatbikat ve Saldırı Simülasyon Hizmeti ile kuruma yöneltilebilecek tüm saldırılar sanal sistemler üzerinde gerçekleştirilmekte, süreç sırasında sistemlerin üretmesi gereken alarm tipi saptanmakta ve kurumun sistemleri üzerinde düzenlemeler yapılmaktadır.

Raporlama

Birinci ve ikinci adımlarda gerçekleştirilen çalışmaların sonucu raporlama yapılır. Bu kategoriler **“İnsan Odaklı”**, **“Teknoloji Yatırımları”** ve **“Süreç ve Yönetim”** şeklinde üç ana kategoride yapılır.

İyileştirme

Değerlendirme ve Raporlama çalışmaları sonucu ortaya çıkan rapor ve karne durumuna göre ilk adımdan başlayarak bir yol haritası hazırlanmakta ve iyileştirme çalışmalarına başlanmaktadır.

Secure 24 Yönetilen Güvenlik Hizmetleri

Günümüz bilişim güvenliği ürünlerinin sayısı, çeşitliliği ve kompleksitesi standart seviyedeki güvenlik uzmanlarının yönetmeyeceği kadar ileri seviye uzmanlık gerektirmektedir. Genellikle alınan ürünler ön tanımlı ayarlarıyla çalıştırılmakta ve siber dünyadaki tecrübeli saldırganlar tarafından rahatlıkla aşılabilmektedir.

BGA Security MSS (Managed Security Services) barındırdığı uluslararası geçerliliğe sahip sertifikalı uzmanlarıyla bilişim güvenliği cihazlarının yönetimini üstlenmekte ve size sahip olduğunuz güvenlik sistemlerinden en yüksek verimi almanızı ve en üst düzeyde korumayı sağlamaktadır.

Secure 24 MSS Özellikleri

- LOG yönetimi için korelasyon hizmeti
- Gerekli durumlarda yerinde eğitim imkanı
- Kompleks güvenlik ürünlerinin 7/24 yönetimi, ve izlemesi
- Yeni özelliklerin test edilerek var olan sistemlere eklenmesi
- Yeni güvenlik cihazlarının testleri ve seçimi konusunda destek
- Tüm sistemlerin düzenli olarak güvenlik taramasından geçirilmesi ve açıklıkların kapatılması
- Bilgi güvenliğini ihlal edebilecek olaylarda sürecin tamamını kapsayacak şekilde destek olunması
- Tüm cihazların yıllık Disk, Memory, Performans, Uptime, Audit gibi bileşenlerinin izlenerek raporlanması
- Düzenli olarak güvenlik cihazlarının yedeklenmesi, yapılandırmalarının güvenlik açısından denetlenmesi ve yamalarının kontrol edilmesi

BGA Security'nin konularında uzman, sertifikalı mühendisleriyle kurumlara sunduğu yönetilebilir güvenlik hizmetlerinden (Managed Security Services) faydalanmak için **bilgi@bga.com.tr** adresimizden bilgi alabilirsiniz.

Aşağıdaki Güvenlik Ürünleri İçin Secure 24 Hizmeti Sunulmaktadır

- Web Uygulama Güvenlik Duvarı
- Saldırı Tespit ve Engelleme Sistemi
- DLP Veri Sızıntısı Engelleme Sistemi
- DoS / DDoS Engelleme ve Tespit Sistemleri
- Güvenlik Duvarı / Yeni Nesil Güvenlik Duvarı
- Log Yönetimi, Analizi ve Korelasyon Sistemleri

"Siber güvenlik araştırmacılarına göre, kurumların
Siber saldırıları fark etme süresi ortalama 180 gündür"

Siber Olay Müdahale Hizmeti

Bilgi güvenliği ihlal olaylarına zamanında müdahale edilip gerekli önlemler alınmadığında sonuçları çok daha ciddi olabilir. BGA Security uzun yıllara dayanan tecrübesi ile bilgi güvenliği olay ve ihlal yönetimi konusunda deneyimli uzmanlarıyla kurum ve kuruluşlara bilgi güvenliği ihlali, olay yönetimi, bilgisayar olaylarına müdahale ekiplerinin (CSIRT) kurulumu, anlık olay müdahale ve delil toplama hizmetleri ile birlikte sertifikalı eğitim programı da sunmaktadır.

Siber saldırıdan sonra vereceğiniz ilk beş karar kurumunuz için en kritik olan kararlardır. Yanlış bir karar basit bir saldırının kurum itibarını zedeleyecek seviyeye gelmesine neden olabilir. Öte yandan yarı bilgili kişilerin sistemlere yapacakları müdahaleler çok önemli adli bilişim ipuçlarının kaybolmasına yol açabilir. Bu nedenle siber saldırı sonrası verebileceğiniz ilk ve en doğru karar BGA Security ile iletişime geçmektir. Dokuz yıl boyunca birçok kuruma profesyonel olarak hizmet veren BGA Security, her durumda size yardıma hazırdır.

"Siber hijyen, kurumları Siber saldırılara karşı korumakta önemli bir etkendir"

Ağ Siber Hijyen Ölçümü

Siber Hijyen Haritası ve APT Tespiti Hizmeti, kurum ağının bir ay süresince izlenerek siber güvenlik noktasında siber hijyen haritasının çıkarılması ve daha önce kuruma gerçekleştirilmiş ve başarılı olmuş siber saldırılar sonucunda sistemlere erişimlerin, yüklenmiş zararlı yazılımların ve olası APT saldırılarının tespit edilmesini amaçlamaktadır.

Ağınızın 360 Derece İncelenmesi ve Siber Hijyen Haritasının Çıkartılması

Bu hizmet kurum bünyesinde yer alan sistemlerin Botnet'lere dahil olanları, zombi hale getirilmiş sistemleri, veri sızıntısı için kullanılan araçları, uzaktan yetkisiz erişim programlarının kurulu olduğu sistemleri, arka kapıları, Trojan bulaşmış sistemleri, siber tehdit istihbaratı ağından gelen verilerden de faydalanılarak tespit edilmekte ve raporlanmaktadır.

Siber Hijyen Durumu ve APT tespiti için toplamda 30.000 anomali kuralından ve veritabanında 200.000.000 kategorize edilmiş alan adı (domain) bulunan özel sistemlerden faydalanılmaktadır. Talep edilen hizmet seviyesine bağlı olarak elde edilen trafik, altı farklı APT ve Antimalware sisteminde kontrol edilerek hata oranı (false positive - false negative) minimum seviyeye indirgenmektedir.

Siber Hijyen ve APT Tespit Hizmeti

- Zararlı yazılım bulaşmış sistemlerin tespiti
- Yerel ağa internet üzerinden bağlı potansiyel sistemlerin tespiti
- DNS tünelleme tespiti ve raporlaması
- Veri sızdırma programlarının tespiti
- Ağa bağlı işletim sistemleri ve güvenlik zafiyeti durumlarının raporlanması
- Farklı bağlantı noktalarında (port) çalışan ağ ile sistem servislerinin tespiti ve raporlanması
- İnternet üzerinden yapılan bağlantıların Siber Tehdit İstihbaratı ile karşılaştırılması
- Ağa bağlı izinsiz / yetkisiz sistemlerin tespit edilmesi
- Ağa bağlı mobil sistemler ve kurum politikalarına uygunlukları
- Kategorize edilmiş alan adları (domain) ile uygunsuz veya yasa dışı (illegal) içeriklere erişim taleplerinin tespiti
- Zombi olarak kullanılan (aktif / pasif) sistemlerin tespiti
- Tünelleme amacıyla kullanılan protokol ile programların tespiti
- Botnet'e üye bilgisayarların tespiti, takibi ve raporlanması
- Güvenlik zafiyeti barındıran sistemlerin tespiti ve raporlanması
- Ağa bağlı sistemlerin haberleştiği ülkelerin tespiti (gelen ve giden trafik için)
- Ağda şifresiz haberleşen protokollerin tespit edilerek raporlanması
- SSL bağlantılarının analizi ve anormallik gösteren bağlantıların raporlanması
- Cryptolocker ve benzeri zararlı fidye yazılımlarının bulaştığı sistemlerin tespiti
- Ön tanımlı parola kullanan hesapların tespiti
- Henüz saldırıya maruz kalınmamış sistemler için, olası bir APT saldırısına karşı altyapının mevcut direnç seviyesinin belirlenmesi

Hizmet Adımları

1-Gizlilik sözleşmesi imzalama
2-Kurum içi sensörlerin kurulum ve yapılandırılması
3-Trafik analiz sürecinin başlaması
4-Raporlama ve aksiyon listesi hazırlığı
5-Kapanış toplantısı ve öneriler

Referanslarımız

32 BANKA

31 KAMU

60 FİNANS

5 SAĞLIK

11 SAVUNMA

5 ENERJİ

5 SERVİS SAĞLAYICI

*İmzaladığımız gizlilik sözleşmeleri nedeniyle firma adı belirtemiyoruz.

Ekip Yetkinlikleri

EC-Council Accredited Training Center · CISSP · SSCP · CISCO CERTIFIED CCSP SECURITY · CISCO CERTIFIED CCNA

ECSP · CEH · ECIH · LPT · CHFI

LICENSED PENETRATION TESTER · CISA 30 · Security+ CERTIFIED · ISO 27001

OSCE · OSCP · OSWP · PMI PMP · OPST Professional Security Tester

Sosyal Sorumluluk

Siber Güvenlik Yaz ve Kış Kampları

Sosyal sorumluluk kapsamında düzenlemiş olduğumuz Siber Güvenlik Kampları'na öğrenciler tarafından yoğun ilgi gösterilmektedir. Bugüne kadar düzenlenen Yaz ve Kış kamplarına 20.000'den fazla başvuru gerçekleşmiştir. Bu başvurularda her dönem elliye yakın öğrenci kabul edilmiş olup, bugüne kadar iki yüz elliden fazla öğrenci BGA Bilgi Güvenliği AKADEMİSİ'nin siber güvenlik uzmanları tarafından yetiştirilmiştir. Kampta çeşitli siber saldırı yöntemleri ve bunlara karşı uygulanacak savunma yöntemleri detaylı olarak ele alınmaktadır. Siber Güvenlik Kampları'na katılım tamamen ücretsizdir ve üniversite öğrencilerine yöneliktir. Kamplara katılmaya hak kazanan öğrencilerin tüm masrafları BGA Security tarafından karşılanmaktadır.

Dernek ve Vakıflar'a Destek

BGA Security, 2014 yılı itibariyle güvenlik bütçesi olmayan dernek ve vakıflar için sosyal sorumluluk kapsamında ücretsiz olarak siber güvenlik desteği sunmaya başlamıştır. Dernek, vakıf gibi sivil toplum örgütlerine siber güvenlik konusunda destek vererek ihtiyaç duydukları güvenlik danışmanlığı hizmetini vermekle beraber ihtiyaç duyulduğunda NormShield ve Sinara güvenlik ürünlerini de ücretsiz olarak vakıf ve derneklerin kullanımlarına sunmaktadır.

Staj Okulu

Ülkemizde yüksek bir oranda siber güvenlik uzmanı açığı bulunmakla birlikte bu açığın kapatılması ülkemize yönelik düzenlenen siber saldırıların önüne geçilmesi ve zafiyetlerimizin tespit edilmesi gibi konular açısından büyük önem arz etmektedir. BGA Security bu konunun anlaşılması için sorumluluk üstlenmekte ve bu tarz çalışmalarına aralıksız olarak devam etmektedir. Siber güvenlik sektörüne istihdam kazandırma amacıyla bu alanda kariyer yapmak isteyen üniversite öğrencilerine kurum bünyesinde staj yapma imkanı tanıyan BGA Security, staj süresince öğrencilere deneyimli eğitmen kadrosu ile eğitim vermektedir.

E-Posta Listeleri

Ülkemizde bilgi güvenliği konusunda bilinçlenmenin artması adına e-posta listeleri oluşturan BGA Security, sektör uzmanlarını e-posta listeleri üzerinden paylaşım yapmaya davet ederek güncel bilgilerin daha kısa sürede daha çok kişiye ulaştırılmasına ön ayak olmaktadır. Kurulan e-posta listeleri ülkemizin önde gelen siber güvenlik uzmanları, kurumların ilgili departmanlardaki üst düzey yöneticileri ve siber güvenlik alanına ilgi duyan katılımcılardan oluşmaktadır.

Siber Kütüphane

Türkiye'de bir ilki gerçekleştirerek siber güvenlik ile ilgili tüm kurumsal bilgi hafızasını BGA Blog ve SlideShare üzerinden paylaşıma açan BGA Security, kurulduğu ilk günden bu yana siber güvenlik konusundaki bilgi dokümanlarını açıkça ve ücretsiz olarak paylaşmaktan gurur duymaktadır. **BGASecurity.com/blog** ve **Slideshare.com/BGASecurity** adreslerinden paylaşılan 10.000 sayfaya yakın Türkçe dokümana rahatça erişim sağlayabilirsiniz.

Kariyer Danışmanlığı

"Bilgi güvenliği uzmanları en iyisine layıktır" sloganıyla yola çıktığımız bu projede Bilgi Güvenliği AKADEMİSİ müşterilerine insan kaynağı danışmanlığı akademi öğrencileri için ise profesyonel kariyer desteği sağlıyor.

İSTANBUL

Adres: 19 Mayıs Mah. İnönü Cad.
Çetinkaya İş Merkezi No:92 Kat:4
KADIKÖY / İSTANBUL

Telefon: +90 (216) 474 0038
E-posta: bilgi@bga.com.tr

ANKARA

Adres: Ceyhun Atuf Kansu Caddesi
Gözde Plaza İş Merkezi Kat:5 No:72
Balgat ÇANKAYA / ANKARA

Telefon: +90 (312) 472 22 21
E-posta: bilgi@bga.com.tr

VIRGINIA

Address: 8201 Greensboro Drive,
Suite 300, McLean, VA / USA 22102

Phone: +1 (571) 335-0222
E-mail: bilgi@bga.com.tr

BAKÜ

Adres: Narimanov, Elesker Gayibov
Sokağı 10A AZ1029
BAKÜ / AZERBAYCAN

Telefon: +99 (450) 504 0003
E-posta: bilgi@bga.com.tr

BGASecurity BGASecurity BGASecurity BGASecurity

www.bgasecurity.com

BGA SECURITY