

**GamaAUDIT** Bilişim sistemleri altyapısı, süreç prosedürleri, yerel ağ altyapısı, ağ cihazları ile sunucuların verimlilik ve güvenlik denetimini kapsamaktadır. Bilişim cihazlarının analizi, prosedür ve politikaların analizi, kaynak kullanım verimliliğinin analizi, ağ cihazlarının analizi, ağ ve sunucu altyapısında olabilecek güvenlik açıklarının denetimi ile sunuculara yapılacak otomatize güvenlik açığı taramalarını içermekte olup, sonuçlar çözüm önerileri ile beraber raporlanmaktadır.

## Kazanımlarınız

- Zaafiyet ve eksiklikleri bilmek: Bilişim sistemleri altyapınızda ki politika, prosedür ve uygulamaların geçerliliklerini görmek, yönetsel veya uygulamalardan kaynaklanan zaafiyetleri belirlemek
- Mevcudu onaylamak: Hazırlanmış politika, prosedür ve uygulamaların geçerliliğini kontrol etmek, istenen devamlılık ve güvenlik seviyesinin sağlandığını doğrulamak
- Farkındalık: Organizasyonun tüm seviyelerinde farkındalık yaratarak şirket güvenlik politikasının gelişimine katkı sağlamak

## GamaAUDIT - Denetim Metodolojisi

- Erişilebilir Bilgi Taraması
- Güvenlik Politikası
- Örgütsel Güvenlik
- Varlık Sınıflandırması ve Denetimi
- İnsan Kaynakları Güvenliği
- Fiziksel ve Çevresel Güvenlik
- Haberleşme ve İşletim Yönetimi
- Erişim Denetimi
- İş Sürekliliği Yönetimi
- Yerel Alan Ağı Yapısı, Güvenliği ve Yönetimi
- Geniş Alan Ağı Yapısı, Güvenliği ve Yönetimi
- Sunucu Yapısı, Güvenliği ve Yönetimi
- İstemci Yapısı, Güvenliği ve Yönetimi
- Sistem Odası
- İnternet Erişim Denetimi
- Güvenlik Zaafiyeti Analizi

## Güvenlik Politikası

Kurumsal olarak kullanılan, yönetimin onayını almış ve kurumun güvenliğe yaklaşımını ifade eden bir bilgi güvenliği politikası varlığı denetlenmektedir.

## Örgütsel Güvenlik

Kurumun oluşturmuş olduğu bilgi güvenliği yönetim sistemi doğrultusunda çalışanların rol ve sorumluluk tanımları ile dış hizmet sağlayıcılar arasındaki ilişki denetlenmektedir.

## Varlık Sınıflandırması ve Denetimi

Kurum için önemli olan bilgi varlıklarının envanteri, sınıflandırmaları, sorumluları, zaafiyetleri ve risk değerlendirmesi raporları incelenmektedir.

## İnsan Kaynakları Güvenliği

Çalışanların işe alım ve son verme süreçleri, rol ve sorumluluk tanımları, yeterlilikleri, istihdam değişimi ve dış kaynaklı istihdam denetlenmektedir.

## Fiziksel ve Çevresel Güvenlik

Önemli ve hassas bilgilerin işlenmekte olduğu ortamlara erişim, giriş çıkış denetimi, güvenlik kontrolleri ve teçhizatların güvenliği için alınmış fiziksel önlemler denetlenmektedir.

## Haberleşme ve İşletim Yönetimi

Haberleşme ve bilgi aktarım süreçleri, aktarım yöntemleri ve uygulanmakta olan kontroller, organizasyonlar arası bilgi paylaşımı, yasal sorumluluklar ve yedekleme yöntemleri denetlenmektedir.

## Erişim Denetimi

Sistemler ve ağlar arası erişim haritaları, seçilen erişim denetim yöntemleri, mobil çalışma ve iletişim yöntemleri ile sistem içi erişim denetimi denetlenmektedir.

## İş Sürekliliği Yönetimi

Ticari süreklilik yönetimi için belirlenmiş yöntem ve süreçler, teçhizat arızaları için alınmış önlemler, felaket durumunda zarar azaltıcı önlemler ve kurtarma planları denetlenmektedir.

## GamaSEC Denetim Hizmetleri

- GamaNET İnternet Güvenlik Denetimi
- GamaAPP Web Uygulama Güvenlik Denetimi
- GamaLAN Yerel Ağ Güvenlik Denetimi
- GamaAUDIT Bilişim Sistemleri Denetimi
- GamaWIRELESS Kablosuz Ağ Güvenlik Denetimi
- GamaSCAN Otomatize Güvenlik Denetimi
- GamaVPN Sanal Özel Ağ Güvenlik Denetimi
- GamaDMZ DMZ Ağı Güvenlik Denetimi

## GamaSEC Danışmanlık Hizmetleri

- GamaPOLICY Güvenlik Politikası Danışmanlığı
- GamaCON Bilgi Güvenliği Danışmanlığı

## GamaSEC Tecrübesi

➤ **GamaSEC** danışmanları, kurumsal güvenlik ihtiyacınızın belirlenmesi, bilgi güvenliği yatırımınızın verimliliğinin ölçülmesi, bilgi varlıklarınıza yönelik güvenlik tehditlerinin belirlenmesi, kurumsal risk analizinizin yapılması hizmetlerini sunabilmek amacıyla en yeni teknolojileri, kendi geliştirmiş oldukları yöntemleri ve araçları kullanmaktadır.

➤ **GamaSEC** danışmanları, güvenlik denetimi ağı/sunucuya sızma sürecinde kullanmak üzere **GamaSEC** Exploit Framework yazılımını geliştirmiş, kendi geliştirmiş olduğu teknik ve araçları yazılıma entegre etmiştir. GamaSEC Exploit Framework yazılımı ile çok sayıda yayınlanmış veya ekibe geliştirilmiş exploit merkezi yapıya sokulmuş, ağı/sunucuya sızma süreci daha verimli hale getirilmiştir.

➤ **GamaSEC** danışmanlarınca geliştirilen bir diğer ortam olan **GamaSEC** Audit Framework ile de ticari yazılımlar, açık kaynaklı yazılımlar ve **GamaSEC** Exploit Framework arası entegrasyon sağlanmış, raporlama süreçleri iyileştirilmiş ve güvenlik denetim süreçleri yönetilebilir hale getirilmiştir.

## Yerel Alan Ağı Yapısı, Güvenliği ve Yönetimi

Yerel alan ağ altyapısı kaynakları, cihazlar, kablolu dağınıklık, verimliliği, uygulanan güvenlik kontrolleri ve yönetim yöntemleri incelenmektedir.

## Geniş Alan Ağı Yapısı, Güvenliği ve Yönetimi

Geniş alan ağ altyapısı kaynakları, cihazlar, bağlantı türleri, verimliliği, uygulanan güvenlik kontrolleri ve yönetim yöntemleri incelenmektedir.

## Sunucu Yapısı, Güvenliği ve Yönetimi

Sunucu altyapısı, yük dağılımı, donanım ve yazılım yeterlilikleri, uygulanan güvenlik kontrolleri ve yönetim yöntemleri incelenmektedir.

## İstemci Yapısı, Güvenliği ve Yönetimi

İstemcilerin yapısı, kullanılan cihaz türleri, kurumsal ağa bağlantı türleri, donanım ve yazılım yeterlilikleri, uygulanan güvenlik kontrolleri ve yönetim yöntemleri incelenmektedir.

## Sistem Odası

Sistem odası fiziksel yerleşimi, iş devamlılığı önlemleri, kullanılan teçhizatlar, fiziksel erişim denetim kontrolleri ve yönetim yöntemleri incelenmektedir.

## İnternet Erişim Denetimi

Kurum içi İnternet kullanım oranları, kullanılan servisler ve protokoller, tercih edilen yazılımlar, güvenlikleri ve yeterlilikleri incelenmektedir.

## Güvenlik Zaafiyeti Analizi

Kurum yerel ve uzak alan ağlarında yer alan sunucu, istemci ve ağ cihazlarının güvenlik zaafiyetlerine karşı zaafiyet analizinden geçirilmektedir. Zaafiyet analizi otomatize yazılımlar kullanılarak yapılmakta ve elde edilen çıktılar ile değerlendirmeler rapora eklenmektedir.