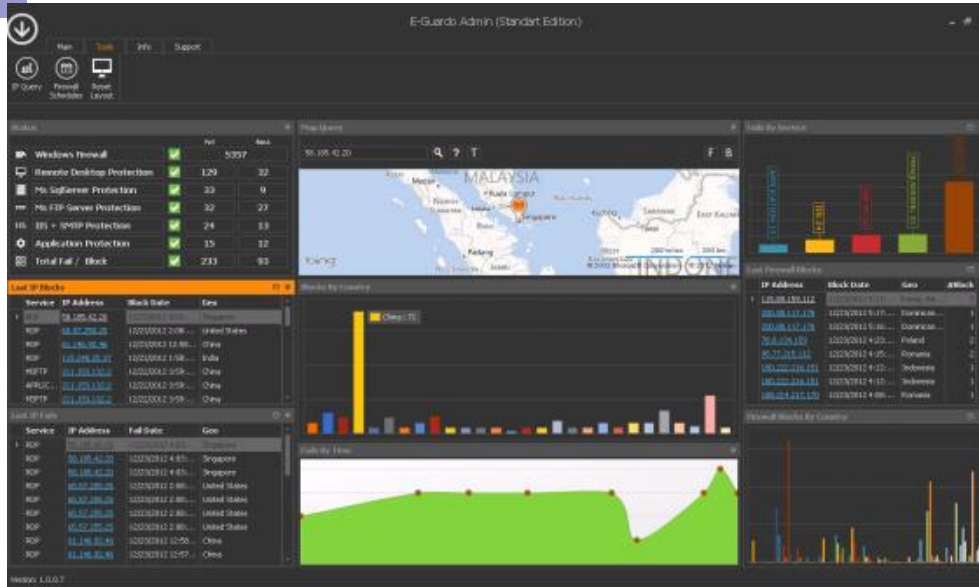


# INTEGRATED INFORMATION SECURITY MANAGEMENT SYSTEM COMPLIANCE TOOL

- Our "Artificial Intelligence Based Information Security Management System-SISMS" is integrated with a software eGuardo, which automatically detects the threats. The risks created by these threats are compared with the knowledge base included in the Information Security Management System. The system provides dynamic risk analysis and recommends rules to reduce risks.



- E-Guardo is a security and intrusion detection software developed to protect the security of many services on the network. The types of attacks detected by the software integrated with ABGYS are grouped and transferred to ABGYS. Dynamically incoming threats by the ISMS are matched to the asset categories and are assessed individually in the risk analysis phase. Thus, in addition to the default risks, dynamically determined risks are analyzed and measures can be taken to reduce these risks

**ISO/IEC 27001 AKILLI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ(ABGYS)**

**1010 CYM SOFT 0101 BİLİŞİM TEKNOLOJİLERİ** **CYMSOFT Bilişim Teknolojileri** 

**Son Giriş Tarihiniz :** 04.01.2017 - 11:40:43 [ Administrator ]

Anasayfa Genel Ayarlar Yönetim Mevcut Durum Analizci Risk Analizci Raporcu Korumacı Uyum İzleyici İç Denetim Güvenli Çıkış

**SALDIRI ve VARLIK GRUPLANDIR**

TEHDİT TÜRÜ	SALDIRI YAPILAN VARLIK	DURUM	
HEURISTIC	FIREWALL	<b>YENİ</b>	Tehditlere Ekle
MSSQLSERVER	MSSQL\$CRMSQL	<b>YENİ</b>	Tehditlere Ekle
RDP	Microsoft-Windows-Security-Auditing	<b>YENİ</b>	Tehditlere Ekle
IIS	URLScan	<b>YENİ</b>	Tehditlere Ekle
ABGYS	FIREWALL	Tehdit tablosuna kaydedilmiştir.	Tehditlere Ekle
ABGYS	FIREWALL	<b>YENİ</b>	Tehditlere Ekle

AKILLI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ(ABGYS)  
CYMSOFT Bilişim Teknolojileri


- The types of attacks identified by E-Guardo are grouped and transferred to SISMS.

**CYMSOFT** BİLİŞİM TEKNOLOJİLERİ **CYMSOFT Bilişim Teknolojileri** ?

Son Giriş Tarihiniz : 08.01.2017 - 15:08:41 [ Administrator ]

Anasayfa Genel Ayarlar Yönetim Mevcut Durum Analizci Risk Analizci Raporcu Korumacı Uyum İzleyici İç Denetim Güvenli Çıkış

### Kategori, Zafiyet ve Tehdit İlişkilendirme

DİL :  

VARLIK KATEGORİLERİ	Zafiyetler	Tehditler
<ul style="list-style-type: none"> <li>Bilgi Varlıkları                             <ul style="list-style-type: none"> <li>Kağıt doküman</li> <li>Elektronik doküman</li> <li>Elektronik veri</li> </ul> </li> <li>Yazılım Varlıkları                             <ul style="list-style-type: none"> <li>Uygulama yazılımları</li> <li>İşletim sistemi</li> <li>Kaynak kodları</li> <li>Ticari yazılımlar</li> <li>Sistem yazılımları</li> </ul> </li> <li>Donanım Varlıkları                             <ul style="list-style-type: none"> <li><b>Sunucu</b></li> <li>Depolama ünitesi</li> <li>Taşınabilir bilgisayar, PDA</li> <li>Network ünitesi</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Korumasız iletişim hatları</li> <li>Korumasız parola tabloları</li> <li>Korumasız saklama koşulları</li> <li>Kötü kullanıma açık olma</li> <li>Kullanıcı tanımlama ve silme için resmi prosedür eksikliği</li> <li>Kullanıcı tanımlama ve yetkilendirme eksikliği</li> <li><input checked="" type="checkbox"/> Kullanıma açık gereksiz servisler</li> <li>Kurum dışına çıkanlar varlıkların kontrol eksikliği</li> <li>Mekanik hasarlara açık olma</li> <li>Mesajlaşma ve iletişim ortamının doğru kullanımı için politika eksikliği</li> <li>Mobil cihaz kullanımı resmi prosesinin eksikliği</li> <li>Olgunlaşmamış veya yeni yazılım</li> </ul>	<ul style="list-style-type: none"> <li>Mesajların yanlış yönlendirilmesi (misrouting)</li> <li>Mesajların yeniden yönlendirilmesi (rerouting)</li> <li>Meteorolojik olgular</li> <li>Personelin erişilebilirliğinin ihlali</li> <li>Personelin görünüm ve davranışlarındaki uygunsuzluk</li> <li><input checked="" type="checkbox"/> RDP (E)</li> <li>Sabotaj</li> <li>Sahte veya kopyalanmış yazılımın kullanımı</li> <li>Sektör içerisinde zayıf imaj</li> <li>Silinme</li> <li>Su baskını</li> <li>Tahrifat veya sahtekarlık</li> <li>Tanınmama (repudiation)</li> <li>Tesisin kötü bir görünüme sahip olması</li> <li>Toz ve ucusan parçacıklar</li> </ul>

- The threats coming dynamically to SISMS side are matched with the asset categories.

## Kontrol Tehdit

DİL : Türkçe

- Kullanılmaz hale gelme
- Kullanım hatası
- Kurcalanma
- Lisanssız kullanım
- Malzeme veya ortamın imha olması
- Mesajların yanlış yönlendirilmesi (misrouting)
- Mesajların yeniden yönlendirilmesi (rerouting)
- Meteorolojik olgular
- Personelin erişilebilirliğinin ihlali
- Personelin görünüm ve davranışlarındaki uygunsuzluk
- RDP (E)
- Sabotaj
- Sahte veya kopyalanmış yazılımın kullanımı
- Sektör içerisinde zayıf imaj
- Silinme
- Su baskını
- Tahrifat veya sahtekarlık
- ...

- A.9.1 Erişim kontrolünün iş gereklilikleri
  - A.9.1.1 Erişim kontrol politikası
  - A.9.1.2 Ağlara ve ağ hizmetlerine erişim
- A.9.2 Kullanıcı erişim yönetimi
  - A.9.2.1 Kullanıcı kaydetme ve kayıt silme
  - A.9.2.2 Kullanıcı erişimine izin verme
  - A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
  - A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama
  - A.9.2.5 Kullanıcı erişim haklarının gözden geçirme
  - A.9.2.6 Erişim haklarının kaldırılması veya düzeltilmesi
- A.9.3 Kullanıcı sorumlulukları
  - A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanılması
- A.9.4 Sistem ve uygulama erişim kontrolü
  - A.9.4.1 Bilgiye erişimin kısıtlanması
  - A.9.4.2 Güvenli oturum açma prosedürleri
  - A.9.4.3 Parola yönetim sistemi
  - A.9.4.4 Ayrıcalıklı destek programlarının kullanılması

KAYDET

- What needs to be done in order to eliminate dynamic threats is achieved by matching them with the relevant control elements.

RDP (E) KAPAT

**A.9.1.1 Erişim kontrol politikası :** Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.

- İş güvenliğinin gerektirdiği, dokümente edilmiş ve yönetim tarafından gözden geçirilmiş bir erişim kontrol politikası bulunmalıdır.
- Kuruluş içerisinde ortak iş rollerine göre standart kullanıcı erişim profilleri bulunmalıdır.
- Erişim kontrolleri uygulanırken ticari uygulamaların gerektirdiği ayrı güvenlik ihtiyaçları göz önüne alınmalıdır.

**A.9.1.2 Ağlara ve ağ hizmetlerine erişim :** Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.

- Kullanıcılar network kolaylıklarından kendilerine verilen yetkilerine göre faydalanabilmelidirler.
- Network yönetim kontrolleri ve network bağlantıları ile hizmetleri korumak için yönetim tarafından onaylanan bir prosedür bulunmalıdır.

**A.9.2.2 Kullanıcı erişimine izin verme :** Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

- Tüm kullanıcılar şahsi kullanımları için kendine ait tek bir kullanıcı tanımına sahip olmalıdır.
- Kullanıcının kimliğini doğrulamak için uygun bir doğrulama tekniği seçilmelidir.
- Teknik destek personeli, operatörler, ağ yöneticileri, sistem programcıları ve veri tabanı yöneticileri dâhil her tür kullanıcıya kontroller uygulanmalıdır.
- Kullanıcı tanımları sorumlu personelin faaliyetlerini izlemek için kullanılmalıdır.
- Her zamanki (düzenli-rutin) kullanıcı faaliyetleri ayrıcalıklı hesaplar üzerinden yapılmamalıdır.
- İstisnai durumlarda açık bir iş çıkarı söz konusu olduğunda belli bir iş veya kullanıcı grubuna bir kullanıcı tanımının paylaşımlı kullanımı tahsis edilebilmeli ancak bu durum yönetim tarafından dokümente edilmelidir.
- Kullanıcıların faaliyetlerinin izlenmesinin gerekli olmadığı durumlarda (sadece okuma erişimi gibi) jenerik kullanıcı tanımları kullanılabilir.
- Kuvvetli yetkilendirme ve kimlik doğrulamasının gerektiği durumlarda sadece parola ile yetinilmeyip şifreleme, akıllı kartlar, tokenlar ve

- What to do to eliminate dynamic threats is automatically provided to the user.

# INTEGRATED INFORMATION SECURITY MANAGEMENT SYSTEM COMPLIANCE TOOL