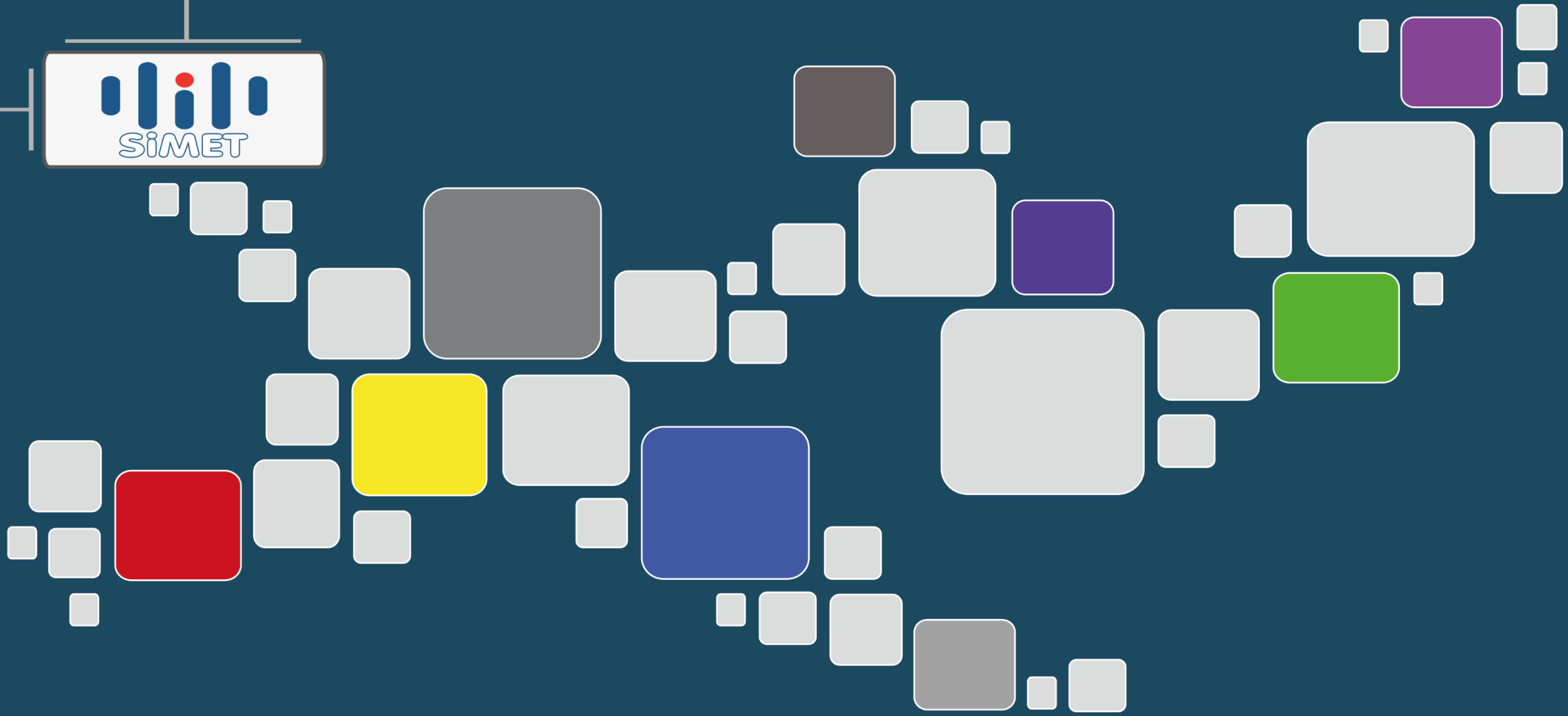


Integrate with the Universe

www.simet.com.tr

SECPOINT PENETRATOR TANITIMI

SİMET SSH TEKNİK DESTEK MÜDÜRLÜĞÜ

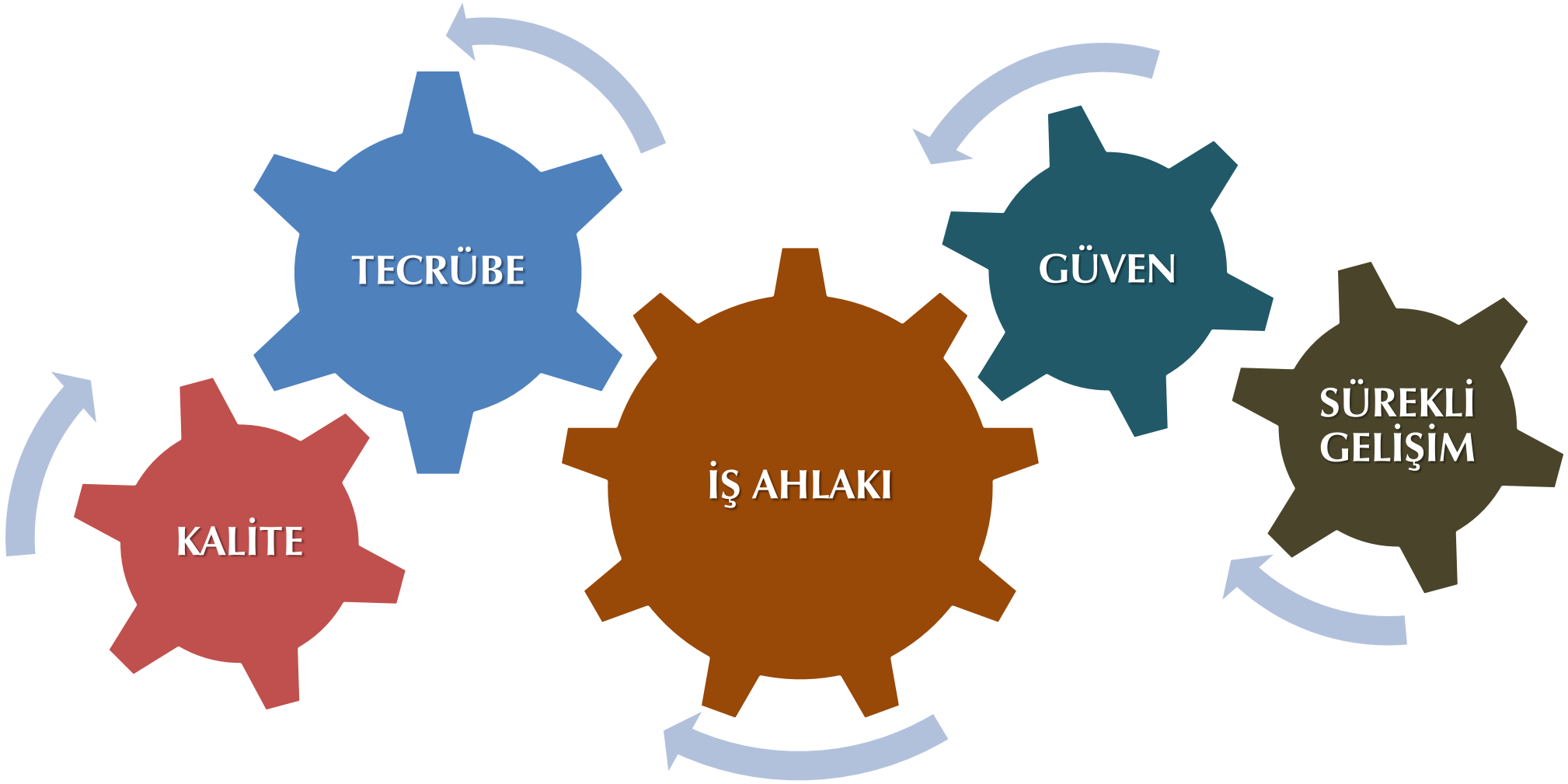
Bilgisayar ağları ve iletişim teknolojileri alanında
Yarım Asırlık katma değer ve tecrübe!"

Simet Hakkında

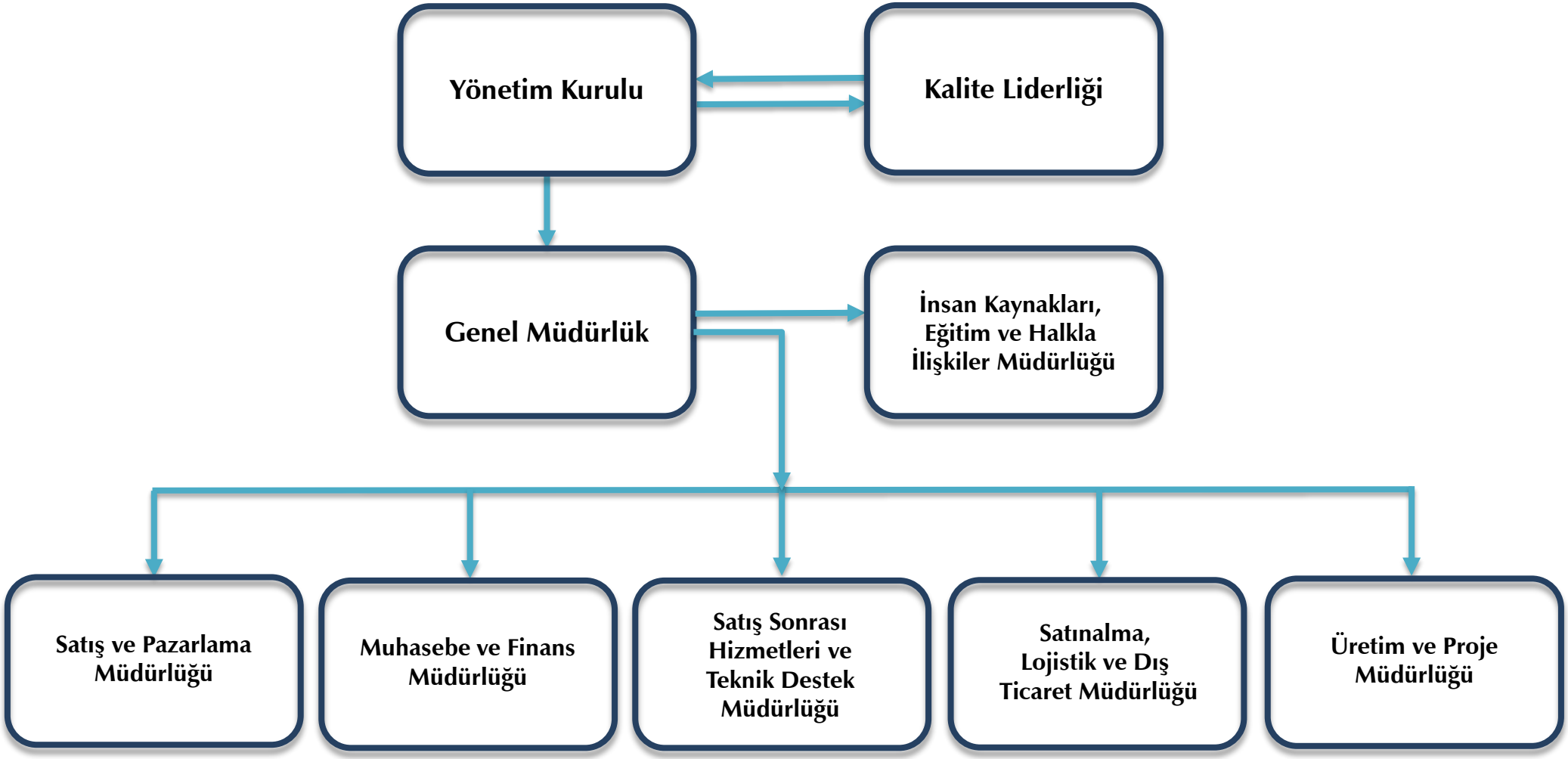
Simet, 90'lı yılların başından bu yana bilişim sektörüne yön vermiş, etki etmiş, bir çok profesyonelin yetişmesini sağlamış, yenilikçi ağ ve iletişim teknolojilerinde önder olmuş bir kadro ile kurulmuştur. Etik (ahlak) değerler bir numaralı şirket anayasamızdır. Hizmet verdiklerimiz, hizmet aldıklarımız ve çalışanlarımız en önemli değerlerimizdir. Dürüst, açık, net, sade, yaklaşımcı, çözüm odaklı çalışanlar seçmek için her tür çabayı göstermekteyiz. Kurucu çekirdek kadro olarak kaliteye ulaşmanın, çok çalışmak, dürüst ve samimi iş çıkartmaktan geçtiğini biliyor ve organizasyonumuzu bu temeller üzerine inşa ediyoruz.

Simet Katma Değerli Ağ ve İletişim Teknolojileri ürün ve çözümlerini portföyünde bulundurmaktadır. Özellikle ürün geliştirme, ürün özelleştirme, yerel özelliklerin ilavesi, trendler doğrultusunda yol haritası belirleme gibi faaliyetleri sayesinde en gelişmiş ve özel bilgisayar ağları ve iletişim ürünlerini bilişim profesyonellerinin kullanımına sunmaktadır.

Çalışma Değerlerimiz



Kurumsal Şirket Yapımız



Faaliyet Alanı ve Çalışma Modeli

Kuruluşumuz esnek, güvenilir, kullanılabilir, hayatı kolaylaştıran, Bilgisayar Ağları ve İletişim Teknolojileri ürün, çözüm ve hizmetleri konusunda faaliyet göstermektedir.

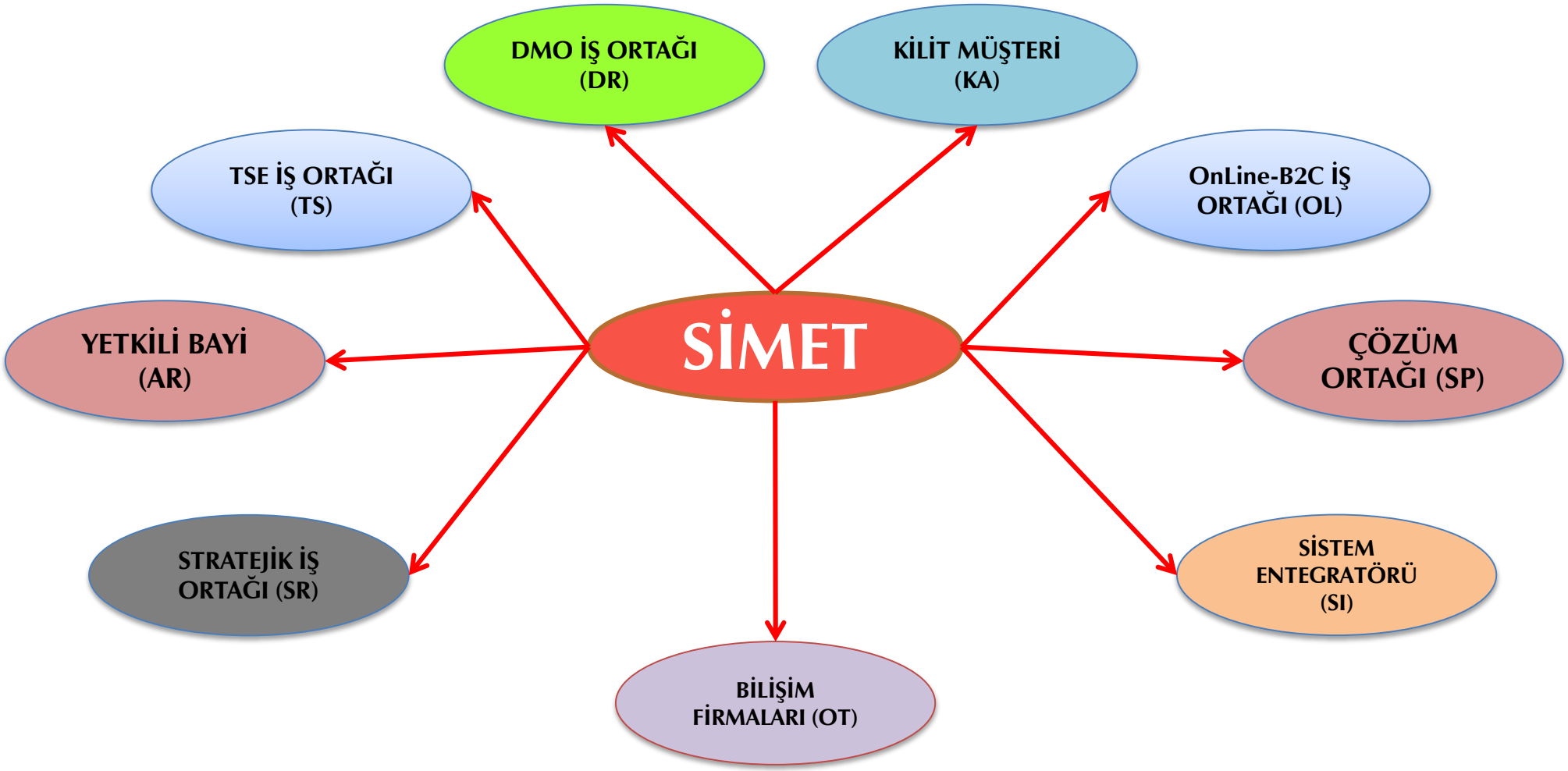
Ana faaliyet konularımız;

- ***Bilgisayar Ağları***
- ***İletişim Teknolojileri***

Tüm faaliyet alanlarımızda ürün, hizmet, teknoloji üretimi, temini, takibi, danışmanlık, projelendirme ve eğitim çalışmaları başta olmak üzere geniş bir yelpazeye sahip olan kuruluşumuz sektörel bir ayrım yapmamaktadır.

Kuruluşumuz **sadece kanal yapısı üzerinden** çalışma yapmaktadır. Bu nedenle **SON KULLANICI** satışı **bulunmamaktadır**. Fakat, kanal yapısına yardımcı olmak amacı ile proje ve iş geliştirme faaliyetlerinde doğrudan tüketici ile irtibat kurarak kanal iş ortaklarına yeni alanlar açmaktadır.

Kanal Yapısı



Kurumsal Özet Bilgiler

Firma Resmi Ünvanı	**: SİMET BİLİŞİM TEKNOLOJİLERİ A.Ş.**
Firma Resmi Adresi	**:** İlkbahar Mah. Medine Müdafii Cad. No:45 Çankaya/ANKARA/TÜRKİYE
Telefon/ Faks	**:** +90.312.4728787 / +90.312.4723131
Web – E-Mail	**:** www.simet.com.tr - satis@simet.com.tr
Vergi Dairesi ve No	**:** SEĞMENLER / 7700863632
Çalışma Modeli	**:** Kanal Yapısı ile Katma Değerli Teknoloji Ürün ve Çözümleri Dağıtımı
Uzmanlık Alanları	**:** Bilgisayar Ağları ve İletişim Teknolojileri

Gücümüz

1

BİLGİ

Tüm faaliyetlerimizde kendi bilgi kaynaklarımızı ve bilgi birikimimizi kullanırız. Sürekli geliştiririz.

2

MALİ YAPI

%100 yerli Sermayeye sahibiz. Tüm ürün ve çözümlerimizde kendi kaynaklarımızı kullanırız.

3

İNANÇ

Gelişim, ARGE ve dürüst ticarete inancımızı ilk gün gibi taze tutarız. Hep araştırırız. Zarar edecek olsak ta doğruyu söyleriz.

4

GÜVEN

Sektörün ve kullanıcının güvenini kaybetmemek için para kaybetmeyi her zaman göze alırız.

5

TECRÜBE

Türkiye ve Dünya pazarlarında elde edilmiş tecrübe ile yaklaşım farkına sahibiz.

Teknolojimiz ve Sunduklarımız

Kurumsal web sitemiz :

www.simet.com.tr

Tüm ürünlerimizin detaylarına, şirketimizden haberlere, teknik detaylara, duyurulara, eğitim ve etkinliklere kadar bir çok farklı konuda detaylı bilgilere ulaşabilirsiniz!

Hem İngilizce hem de Türkçe ara yüzü mevcuttur. ERP sistemimiz ile entegredir.

Teknolojimiz ve Sunduklarımız

B2B web sitemiz :

www.alodepo.com

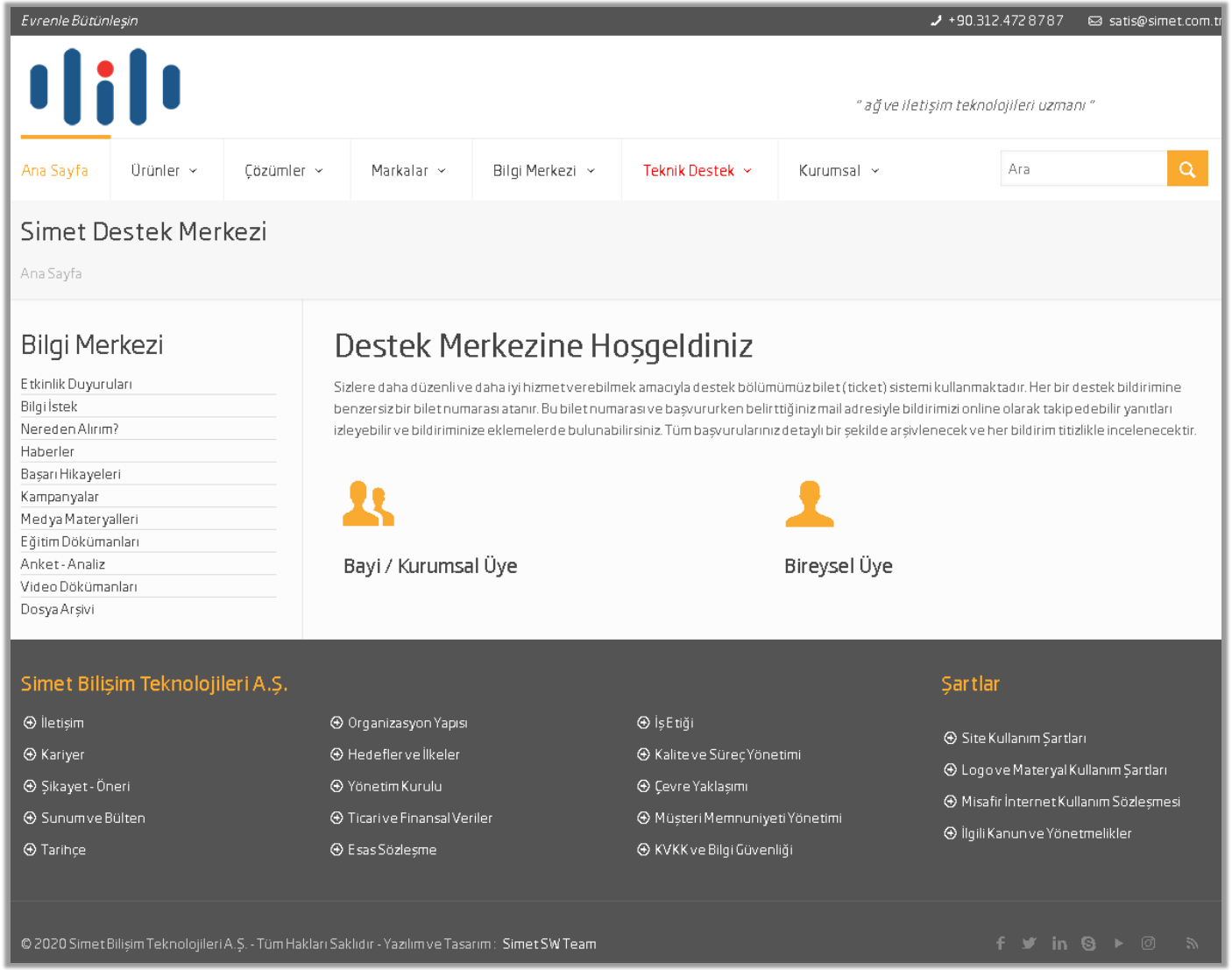
Sadece kanal yapımızdaki iş ortaklarımız için geliştirilmiş olan, tüm ürünlerimizin fiyatlarına, stoklarına, detaylarına, şirketimizden haberlere, teknik detaylara, duyurulara, eğitim ve etkinliklere kadar bir çok farklı konuda detaylı bilgilere ulaşabilen özel portaldir. ERP sistemimiz ile entegredir.

Teknolojimiz ve Sunduklarımız

Destek web sitemiz :

destek.simet.com.tr

Temsil etmiş olduğumuz tüm marka ürünlerinin teknik desteğini güçlü teknik ekibimiz ile merkezi olarak vermekteyiz. Bu amaçla geliştirmiş olduğumuz Teknik Destek Takip Sistemimiz doğrudan ERP sistemimiz içinde çalışmaktadır.



Tüm dinamik verilerimize ERP sistemimizle bağlantılı kurumsal web sitemizden erişebilirsiniz;

www.simet.com.tr

Tüm ürünlerimizin detaylarına, şirketimizden haberlere, teknik detaylara, duyurulara, eğitim ve etkinliklere kadar bir çok farklı konuda detaylı bilgilere ulaşabilirsiniz!

Hem İngilizce hem de Türkçe ara yüzü mevcuttur.

SecPoint ApS Hakkında

SecPoint, 1999 yılında **Danimarka** 'da kurulmuş innovatif network güvenliği ürün ve çözümleri üreten bir firmadır. Merkezi Kuzey Avrupa Danimarka 'da bulunan firmanın Hollanda, Yunanistan, İsveç ve Amerika 'da ofisleri mevcuttur. Özellikle, müşteri ihtiyaçları doğrultusunda **UTM Firewall** (Ağ Güvenlik Duvarı) ve **Network PenTest** (Ağ Güvenlik Testi) ürünlerine odaklanmıştır.

Dağıtıcı kanal yapısı ve son kullanıcı ile çok yakın çalışan firma, kullanıcı isteklerine hızla cevap verebilmektedir. Tüm hata ayıklama ve destek takımı ile yakından pazarı takip eden firmanın en önemli avantajlarından birisi de hızlı destek dönüşleridir. Müşteri memnuniyeti firmanın odağındadır. Firmanın iki ana ürün grubu mevcuttur;

1. Bilgisayar ağları için en iyi açıklık tespit ürünü olan **PENETRATOR**, hem donanım olarak hem de yazılım ve servis olarak sunulmaktadır.
2. Bilgisayar ağları için güvenlik ağ geçidi olan **PROTECTOR**, UTM(Unified Threat Management) ürünüdür.

SecPoint PENETRATOR

Bilgisayar ağları güvenlik zafiyetlerini tarayan ve açıklıkları tespit etmeye yarayan SecPoint **PENETRATOR**, hem donanım (cihaz ve yazılım birlikte), hem uygulama yazılımı ve hem de bulut servisi olarak sunulmaktadır.

1. **HARDWARE PENETRATOR**
2. **VIRTUAL PENETRATOR**
3. **PORTABLE PENETRATOR**
4. **CLOUD PENETRATOR**

2013 YILINDAKİ BT GÜVENLİĞİ MANŞETLERİ

- Cyber Weapon Of Mass Destruction - The Blackhole Exploit Kit
- Washington Hospital Hit By $1.03 Million Cyberheist
- Oracle Updates Java Versioning To Allow More Security Fixes
- US Data Breach Exposes 160,000 Social Security Numbers
- Microsoft Fixes 33 Issues Next Tuesday
- China Accounts For 41% Of Global Computer Attack Traffic
- The great $45m bank cyber-heist: Seven New Yorkers cuffed

Bazı web siteleri hacklendi

Ferrari 2013

chrome

Danger: Malware Ahead!

Google Chrome has blocked access to this page on www.nbc.com.

Content from walterjeffers.com, a known malware distributor, has been inserted into this web page. Visiting this page now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Go back Advanced

Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

Bazı web siteleri hacklendi

NBC 2013

Bazı web siteleri hacklendi

Vatican 2012

GENEL GÜVENLİK SORUN TÜRLERİ

Remote Code Execution	Saldırganların hedef sistemde kod yürütmesine ve tam bir erişime yol açmasına izin verebilir
SQL Injection	Eski saldırı formu ama yine de çok popüler. Saldırganın web sunucuları veritabanlarından hassas bilgileri almasına izin verir. Tam sistem erişimine neden olabilir.
Cross Site Scripting (XSS)	Saldırganlar, ilk bakışta meşru görünebilecek kötü niyetli URL'leri yürütmek için kurbanı kandırır.
Format String vulnerabilities	Bunun nedeni kötü programlamadır ve bir saldırganın bellekteki konumlardan veri yazdırmasına izin verebilir. Hedef sistemden ödün vermek için isteğe bağlı verilerin yazılmasına da izin verebilir.

GENEL GÜVENLİK SORUN TÜRLERİ

Username Enumeration	Saldırganın hedefteki gerçek kullanıcıları tahmin etmesine izin verir ve başka saldırılara yol açabilir.
Denial of Service DoS attacks	Saldırganın, bir web sunucusunun amaca hizmet etmesini engellemesine veya kapatmasına izin verir. Bu, örnek olarak bir sitenin sipariş almasını engelleyebilir.
Human mistakes	Bu, saldırganların insan hataları ve kötü yapılandırmalar nedeniyle hassas dosyaları veya dizinleri ortaya çıkarmasına izin verebilir.
Sensitive Information Leaking	Google ve Bing gibi arama motorlarına hassas bilgilerin sızdırılması.

CLOUD PENETRATOR

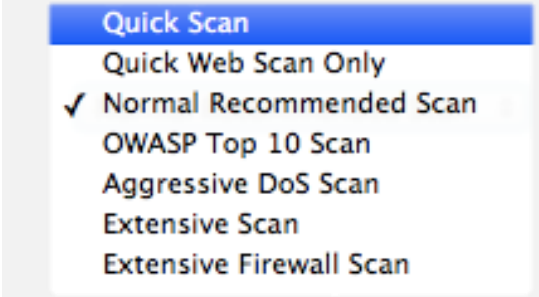
Aşağıdakiler için tarama yapabilir

- SQL Injection
- XSS Cross Site Scripting
- Format String Vulnerabilities
- Command Execution
- Joomla,Wordpress Security

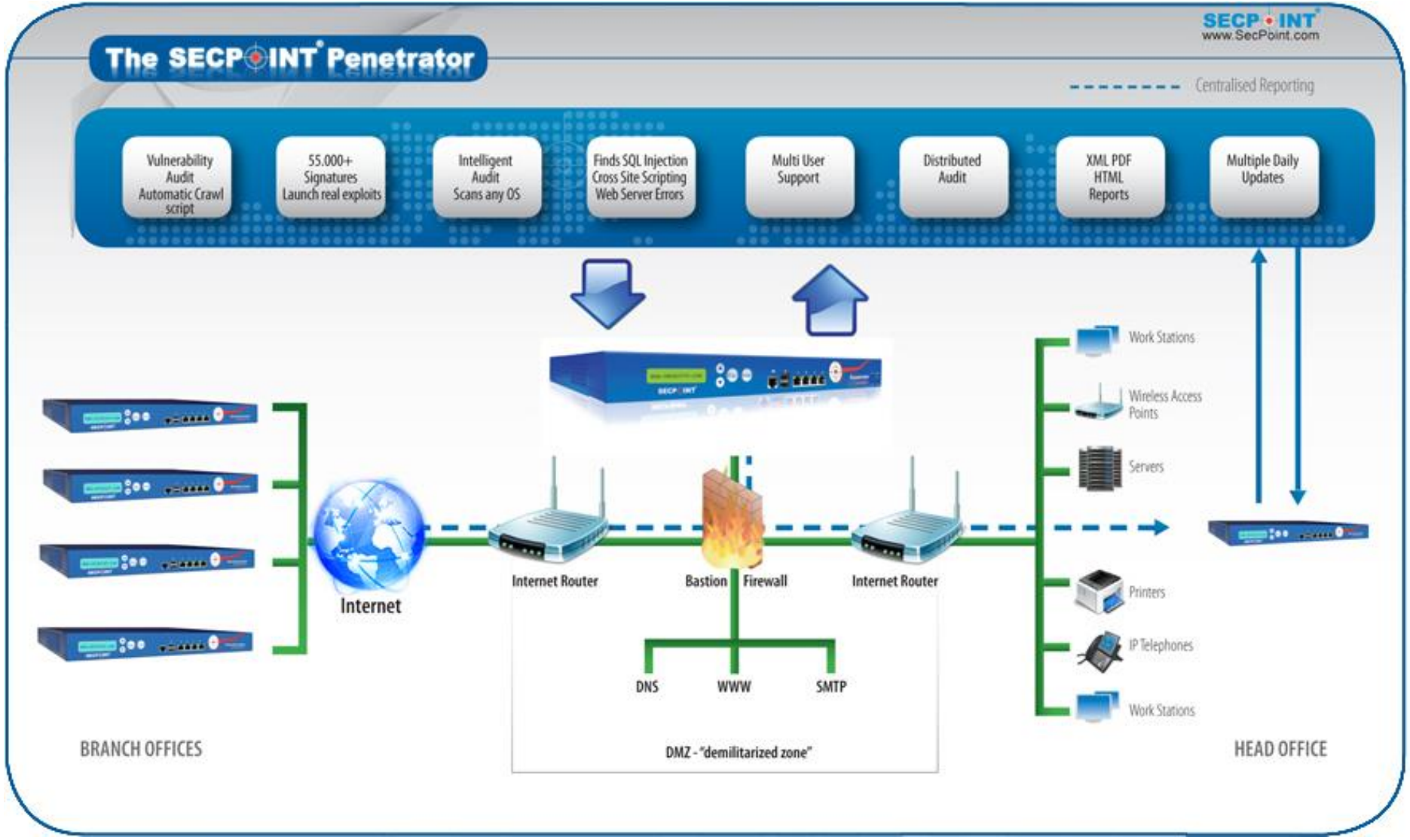
Scanner

- Google Security Scanner
- SEO Bblackhat Scanner
- Username Guessing
- Denial of Service DoS

- 60.000+ Security Checks.
- Profile Scanning
- Information Disclosure



PENETRATOR DIAGRAM (Donanım)



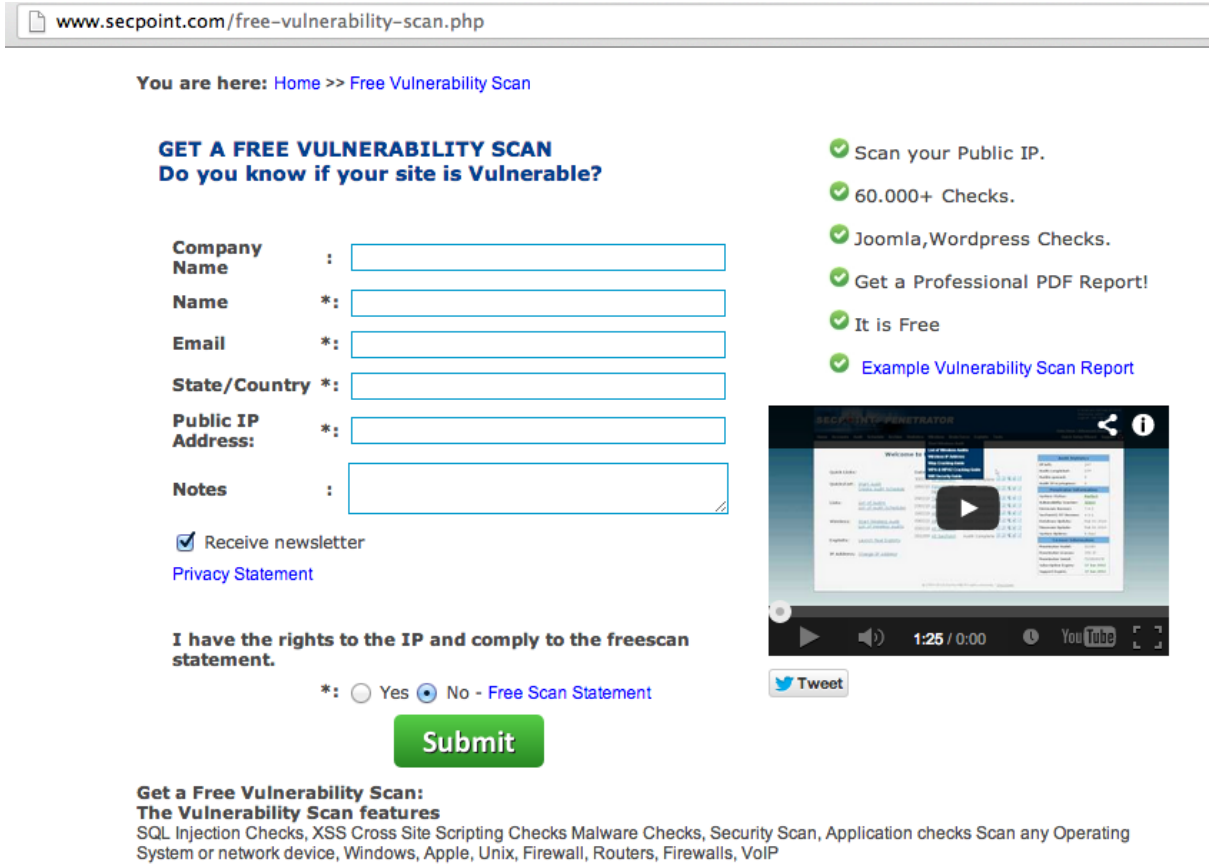
ÜCRETSİZ GÜVENLİK AÇIĞI TARAMASI

Yeni müşteriler bir sorunları yoksa satın almazlar

Yeni müşteri, siz onlara bir sorunları olduğunu gösterene kadar sizinle konuşmak istemiyor

Ağlarının durumunu görebilmeleri için onlara (ücretsiz) bir Güvenlik Denetimi sunun

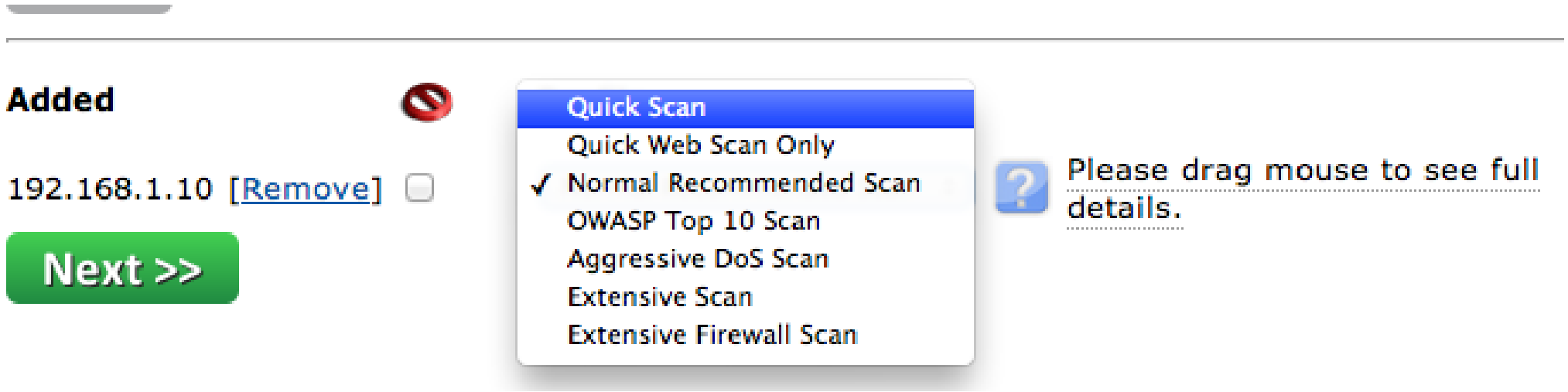
http://www.secpoint.com/free-vulnerability-scan.html



PROFİLLERLE DOĞRU TARAMA NASIL YAPILIR?

Doğru şekilde nasıl taranır

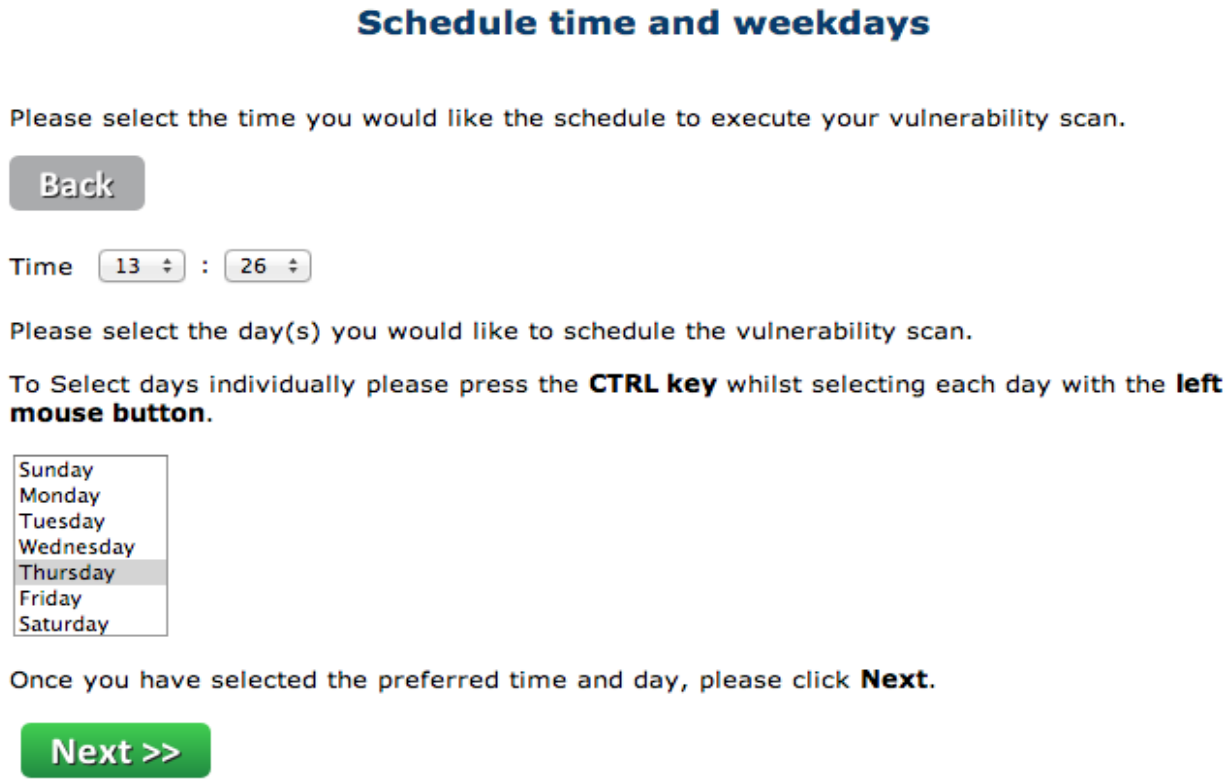
Tüm genel ve yerel otomatik Günlük veya Haftalık kapsamlı güvenlik taraması



Arayüzü gösterin https://penetrator.secpoint.com

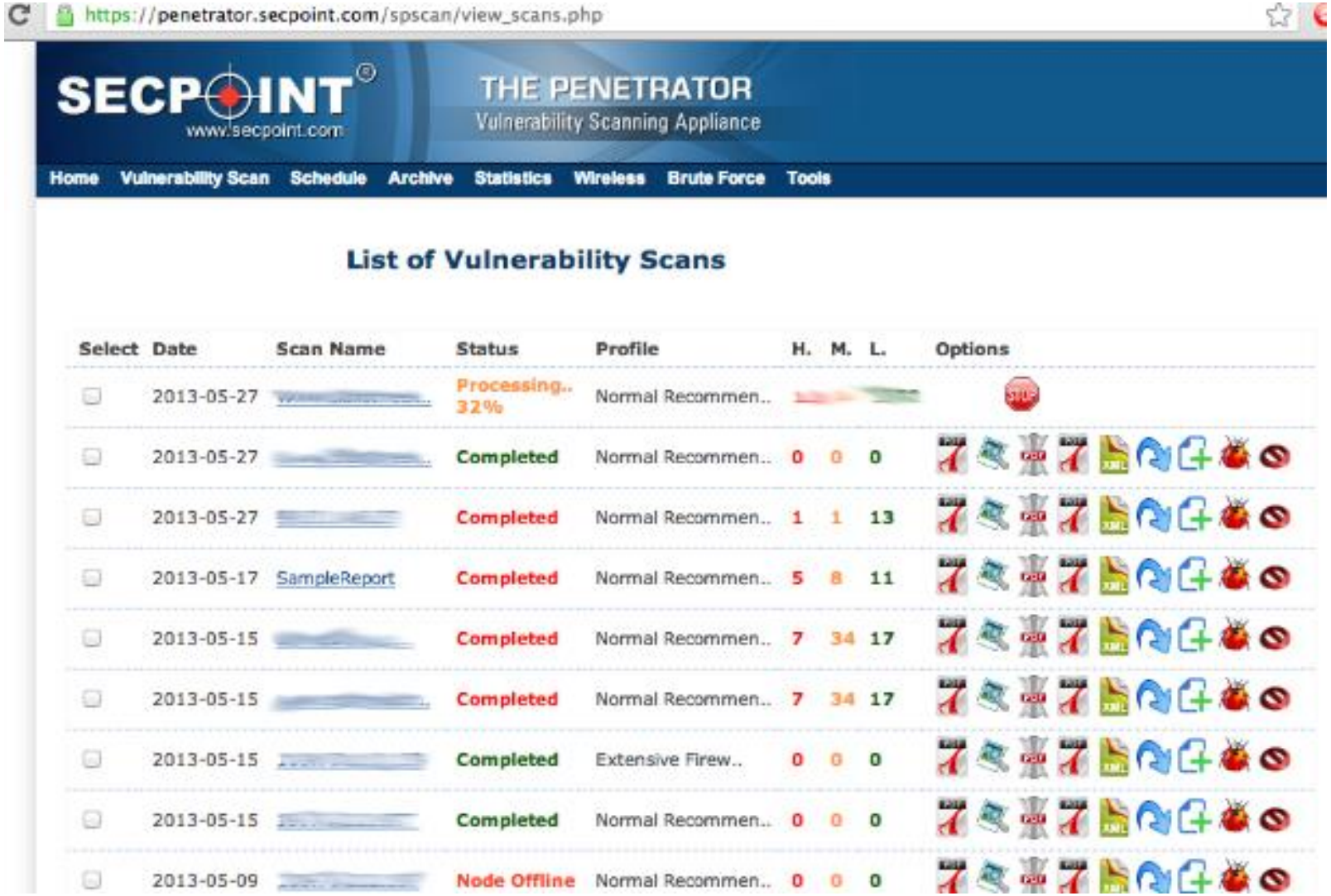
OTOMATİK PROGRAMLI TARAMAYI AYARLAMA

Automatic Daily or Weekly comprehensive security scanning of any Public or Local IP



Arayüzü gösterin https://penetrator.secpoint.com

CLOUD PENETRATOR ARAYÜZÜ

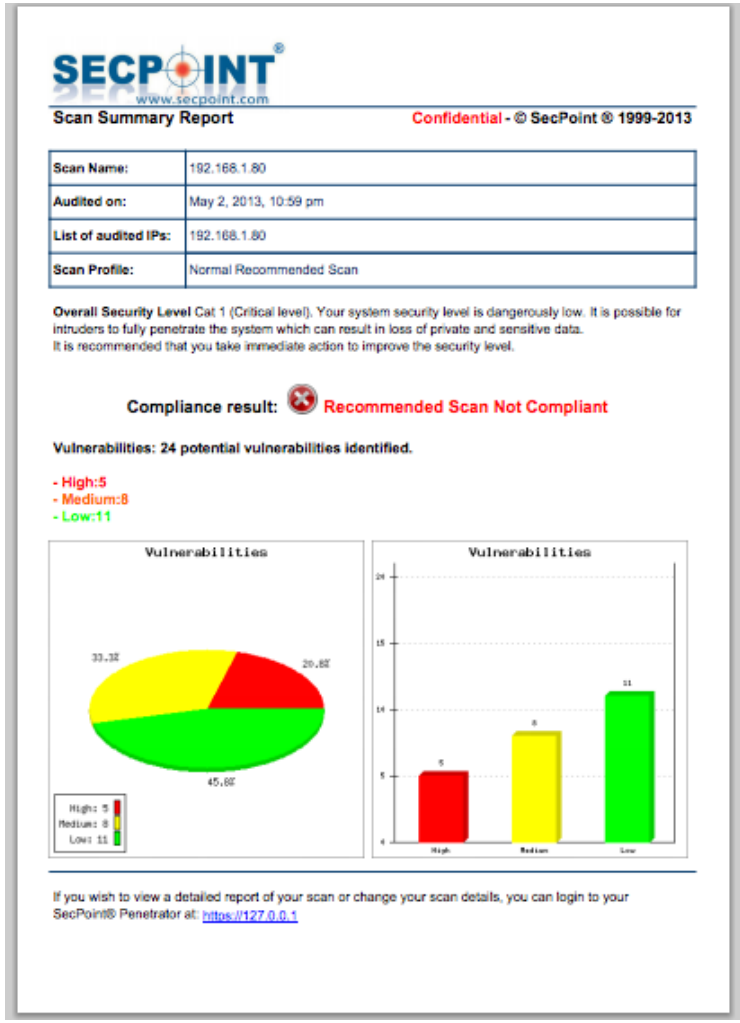


ÖRNEK RAPORLAMA

ÖRNEK AÇIKLIK TARAMA RAPORU

ÖZET RAPOR

http://www.secpoint.com/manual/Penetrator_Example_Audit_Summary.pdf



SECPOINT®
www.secpoint.com

Scan Summary Report Confidential - © SecPoint ® 1999-2013

Scan Name:	192.168.1.80
Audited on:	May 2, 2013, 10:59 pm
List of audited IPs:	192.168.1.80
Scan Profile:	Normal Recommended Scan

Overall Security Level Cat 1 (Critical level). Your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data.
It is recommended that you take immediate action to improve the security level.

Compliance result: Recommended Scan Not Compliant

Vulnerabilities: 24 potential vulnerabilities identified.

- High:5
- Medium:8
- Low:11

Vulnerabilities

Vulnerabilities

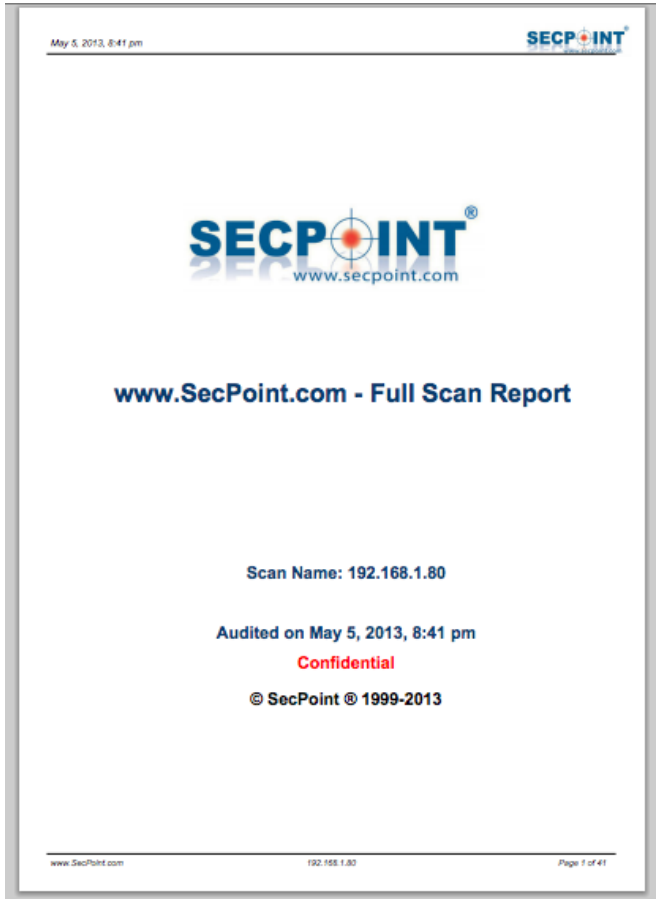
If you wish to view a detailed report of your scan or change your scan details, you can login to your SecPoint® Penetrator at: https://127.0.0.1

ÖRNEK RAPORLAMA

ÖRNEK AÇIKLIK TARAMA RAPORU

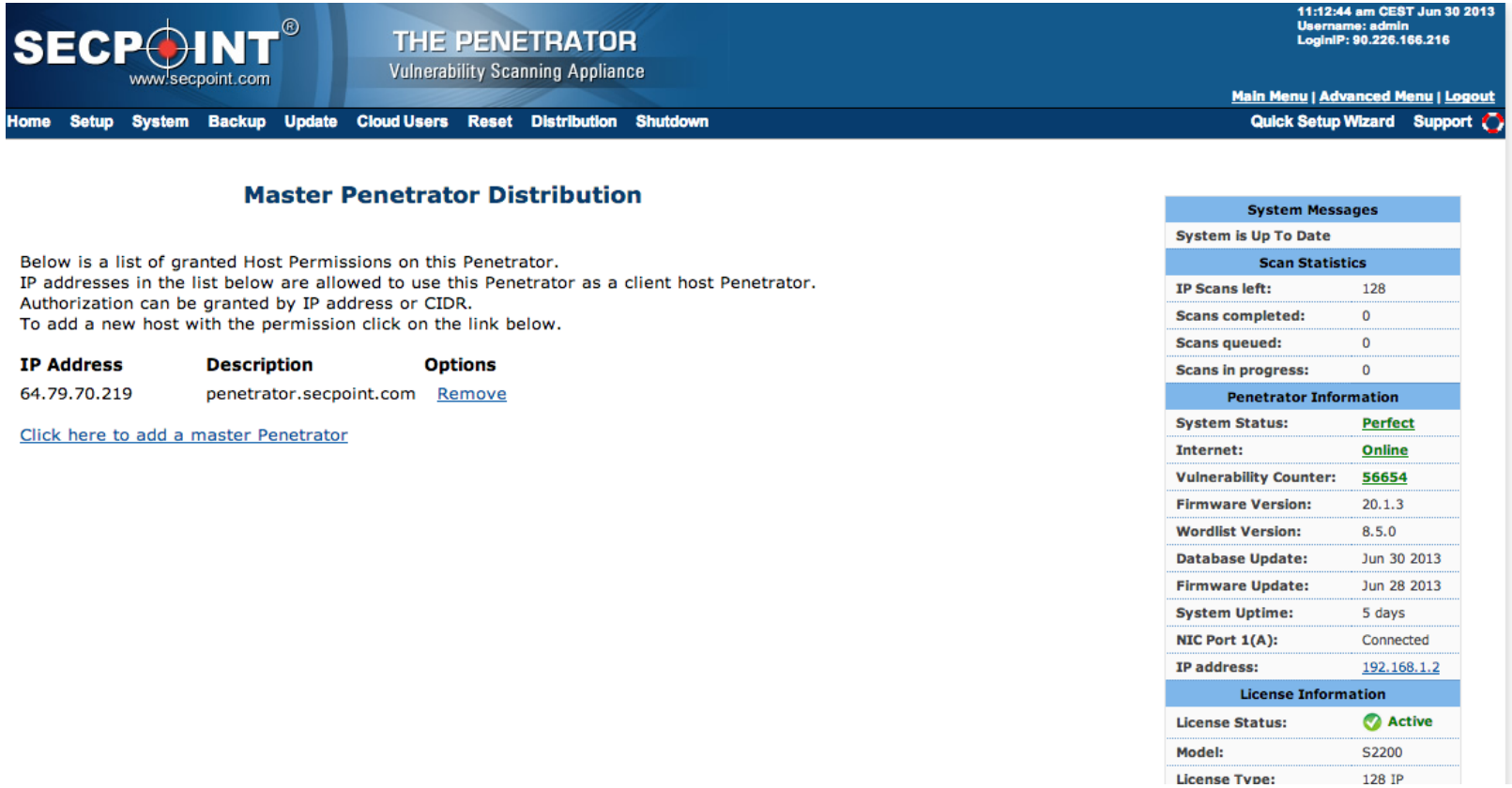
KOMPLE RAPOR

http://www.secpoint.com/manual/Penetrator_Example_Audit.pdf



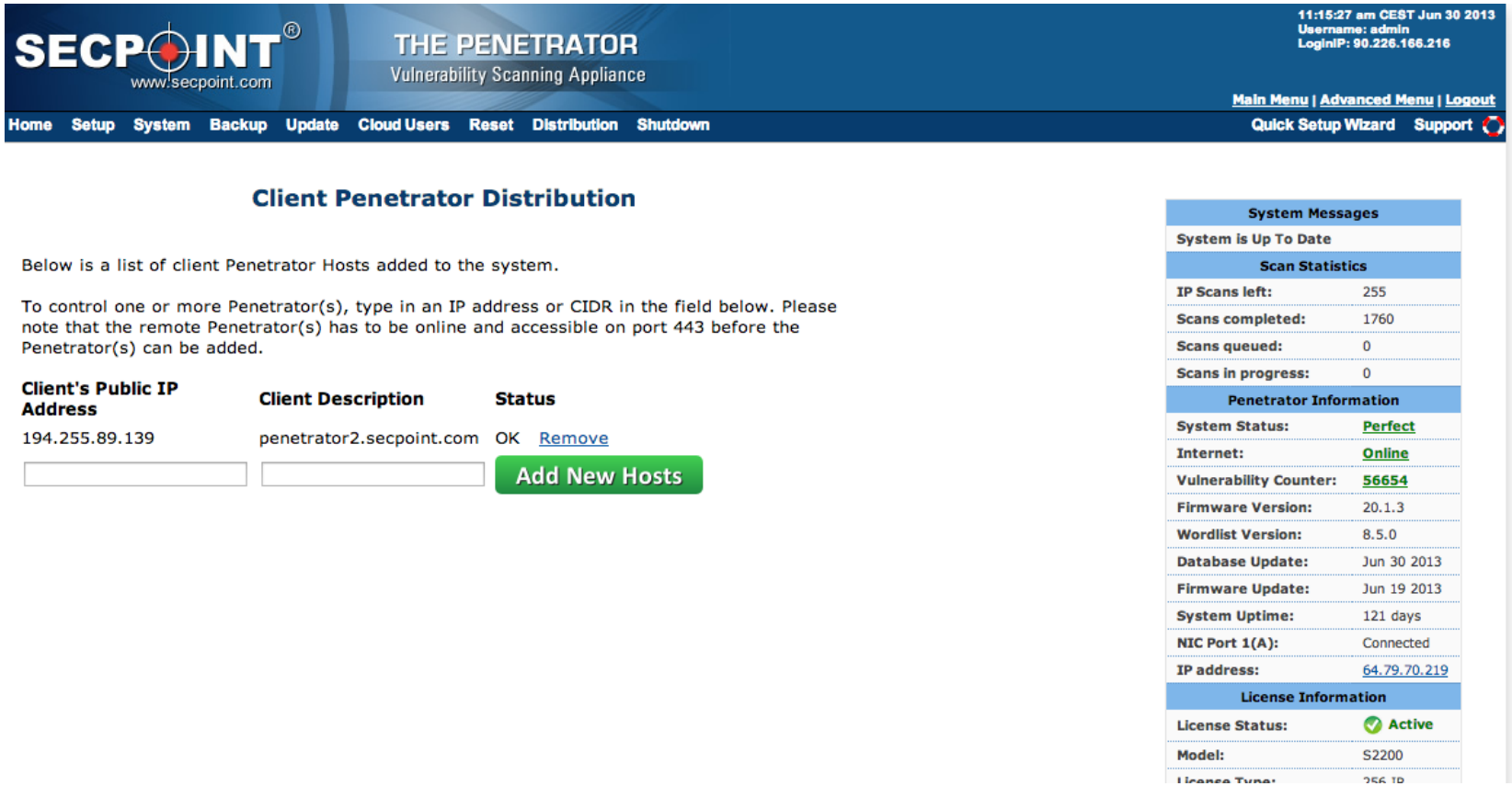
DAĞITIK TARAMA – MASTER OLANI BELİRLE

- Merkezi noktadan birden fazla konumu tarayın
- Merkezi raporlama alın
- Güvenli tasarım
- Birden fazla Peetrator'u birbirine kolayca bağlayın



DAĞITIK TARAMA – MASTERDAN İSTEMCİ EKLE

Master'a bağlanma yetkisi olan İstemcileri kolayca ekleyin



TEŞEKKÜRLER