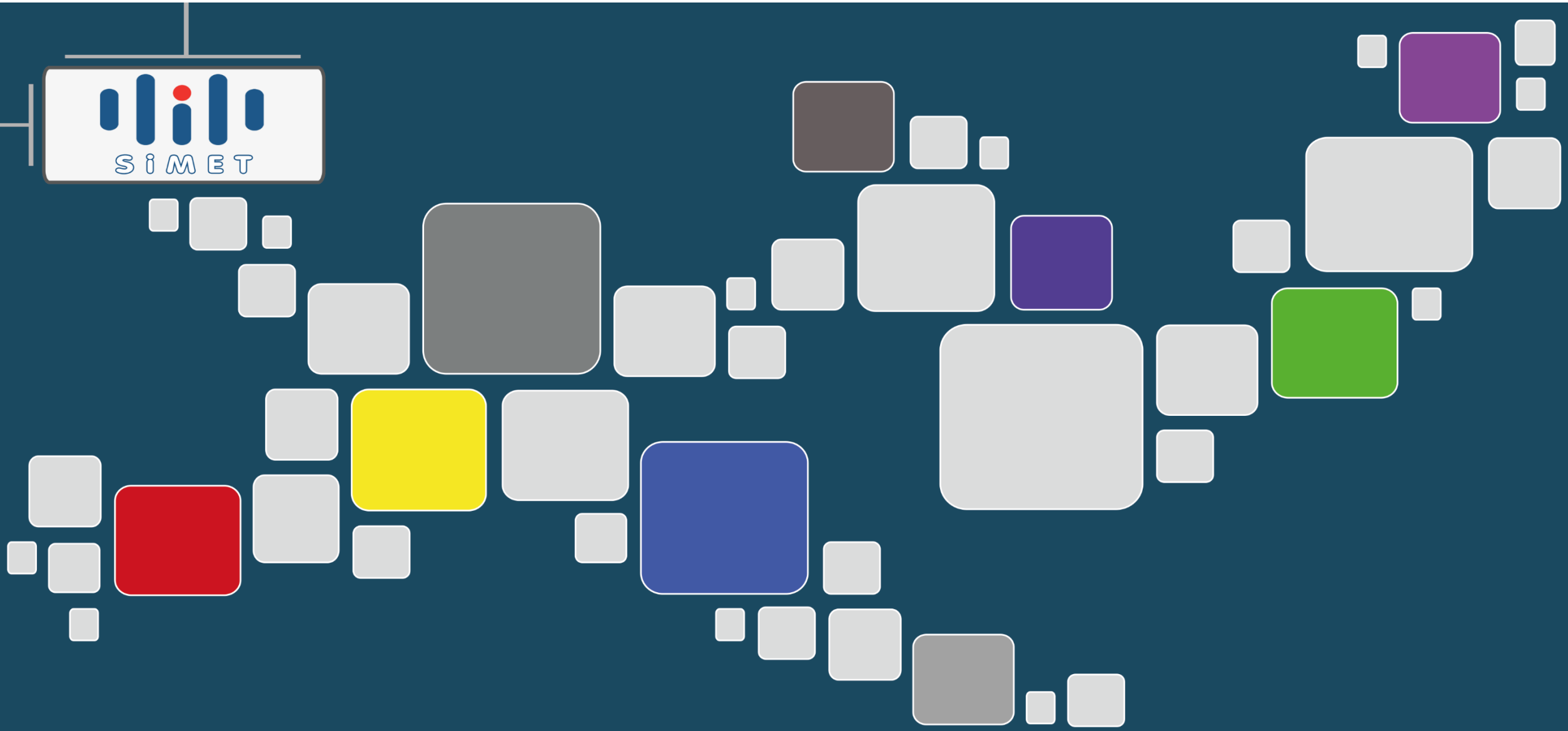


SİMET BİLİŞİM TEKNOLOJİLERİ A.Ş.
SECPOINT PENETRATOR SUNUMU

Penetrator

« Otonom Penetrasyon Test Aracı »

SecPoint Hakkında

- SecPoint, 1999 yılında Danimarka 'da kurulmuş, innovatif ağ güvenliği ürün ve çözümleri üreticisi bir firmadır. Merkezi Kuzey Avrupa Danimarka 'da bulunan firmanın Hollanda, Yunanistan'da ofisleri mevcuttur. Özellikle, müşteri ihtiyaçları doğrultusunda UTM Güvenlik duvarı ve Ağ güvenliği test ürünlerine odaklanmıştır.
- SecPoint güvenlik ürünleri ile ilgili; Secus, SC Magazine, Hacking Magazine, Network Security, HIPAA gibi dünyanın tanınmış kurumlarından almış olduğu onlarca ödülü mevcuttur.

Penetrator nedir?

- **Secpoint Penetrator**, bir güvenlik cihazı değildir ancak sistemin daha güvenli hale gelmesi için potansiyel açıkları tespit etmeyi ve bu açıklarla ortaya çıkan sorunları düzeltme konusunda yol gösteren anlaşılır raporlar sunabilen bir araçtır.

- Bilgisayar ağları için en iyi açıklık tespit ürünü olan Penetrator, hem donanım hem yazılım ve hem de servis olarak sunulmaktadır.

SECPOINT® PENETRATOR-MATRIX







	S9 - SFF	S9 - 128	S9 - 256	S9 - 512	S9 - 2048	S9 - Virtual Appliance	S9 – Cloud
Architecture	64 Bit	64 Bit	64 Bit	64 Bit	64 Bit	64 Bit	-
Maximum Concurrent Scans	4-8 IPs	64-128 IPs	64-128 IPs	256-512 IPS	No software limit	1- 1024 + IPS	1- 1024 IPS
Maximum Cloud Users	Max 10 users	Max 100 users	Max 500 users	Max 1000 users	No software limit	No software limit	-
Maximum Ip Reporting in interface	500+ IP Reports	1000+ IP Reports	5000+ IP Reports	10,000+ IP Reports	No software limit	10,000+ IP Reports	No software limit
All Data stored locally	✓	✓	✓	✓	✓	✓	EU, US
WiFi Pen Testing WPA WPA2 WPS	✓	✓	✓	✓	✓	✓	-
Helpdesk Ticket System	✓	✓	✓	✓	✓	✓	✓
Customize Report Branding	✓	✓	✓	✓	✓	✓	-
Customize Interface Branding	✓	✓	✓	✓	✓	✓	-
Interfaces	4x RJ45	6x GE RJ45	6x GE RJ45	6x GE RJ45	6x GE RJ45	-	-
Local Storage	320 Gb	320 Gb	500 Gb	750 Gb	1 Tb	500 Gb	-
RAM / CPU	4 Gb / Quad	4 Gb / 13	8 Gb / 15	8 Gb / 17 Quad	8 Gb / 17 Quad	Min 2 Gb / 13 Recom. 8 Gb / 17	-
Power Supply	Single AC PS	Single PS	Single PS	Single PS	Single PS	-	-
Form Factor	Small Form Factor	Rack Mount 1RU	Rack Mount 1RU	Rack Mount 1RU	Rack Mount 1RU	-	-
Support & Firmware included	✓	✓	✓	✓	✓	✓	✓
Schedule Scans Support	✓	✓	✓	✓	✓	✓	✓
9 Scan profiles	✓	✓	✓	✓	✓	✓	✓
DoS – Aggressive Scan	✓	✓	✓	✓	✓	✓	✓
All data stored locally	✓	✓	✓	✓	✓	✓	✓
Distributed node scanning	✓	✓	✓	✓	✓	✓	✓
Multi user support	✓	✓	✓	✓	✓	✓	✓
Vulnerability scanning	✓	✓	✓	✓	✓	✓	✓
Full Linux no reboot required	✓	✓	✓	✓	✓	✓	✓

Kuruluşunuzda bulunan IT sistemlerinin (sunucu, bilgisayar, veri depolama cihazı, kablosuz erişim cihazı, yazıcı ve benzeri tüm ağ cihazları) potansiyel birer zaafiyet açığı oluşturabileceğini biliyor musunuz?

Zaafiyet Taraması ve Zaafiyet Yönetimi

- **Zaafiyet Taraması**

Bilgisayar ağlarınızda mevcut ya da ortaya çıkması muhtemel olan zaafiyetlerin çeşitli araçlar yardımı ile tespit edilmesidir.

- **Zaafiyet Yönetimi**

Zaafiyetlerden doğabilecek risklerin azaltılması için yapılan çalışmaların tümü olarak tanımlanabilir.

Bilgisayar Ağları Zaafiyetleriniz Pahalıya Mal Olabilir!

Zaafiyet Taraması ve Zaafiyet Yönetimi NEDEN Önemlidir?

- Kritik güvenlik açıklıklarının sıklıkla ortaya çıkması,
- Saldırganların boş durmaması,
- Tehditlerin gün geçtikçe artması,
- Tehdit vektörlerinin çeşitlenmesi v.b nedenlerden dolayı zaafiyet taraması ve yönetimi gün geçtikçe önem kazanmaktadır.

Yaygın Saldırı Tipleri

Remote Code Execution	Saldırganların hedef sistemde kod çalıştırmasına ve güvenlik ihlaline yol açmasına izin verir.
SQL Injection	Eski bir saldırı şeklidir ama yine de oldukça popülerdir. Saldırganın bir web sunucu veri tabanından hassas bilgileri almasına izin vererek sistemi tehlikeye atmasını sağlayabilir.
Cross Site Scripting (XSS)	Saldırganlar, kurbanı ilk bakışta meşru görünebilecek kötü amaçlı URL'yi çalıştırması için kandırır.
Format String vulnerabilities	Bunun nedeni kötü programlamadır ve bir saldırganın bellekteki konumlardan veri yazdırmasına izin verebilir. Ayrıca, hedef sistemi tehlikeye atmak için rastgele verilerin yazılmasına da izin verebilir.

Yaygın Saldırı Tipleri

Username Enumeration	Saldırganın hedefteki gerçek kullanıcıları tahmin etmesine ve başka saldırılara yol açmasına izin verir.
Denial of Service DoS attacks	Saldırganın bir web sunucusunu kapatmasına veya bir amaca hizmet etmesini engellemesine izin verir. Buna örnek olarak bir sitenin sipariş alamaması verilebilir.
Human mistakes	Bu, saldırganların insan hataları veya kötü yapılandırmalardan kaynaklanan hassas dosyaları veya dizinleri ortaya çıkarmasına izin verebilir.
Sensitive Information Leaking	Hassas bilgilerin Google ve Bing gibi arama motorlarına sızdırılması…

2020'de en çok istismar edilen 5 Güvenlik Açığı

1. CVE-2020-12720: vBulletin SQL Enjeksiyonu

vBulletin, çevrimiçi topluluk web sitelerini oluşturmak ve yönetmek için kullanılan tescilli bir internet forumu yazılım paketidir. Bu modül, bir saldırganın yöneticinin parolasını sıfırlayarak bir **RCE (uzaktan kod/komut çalıştırma) saldırısı** başlatmasına olanak tanıyan bir **SQL enjeksiyon** güvenlik açığıdır. **CVSS Temel Puan: 9,8**

2. CVE-2020-5902: F5 BIG-IP RCE ve LFI

F5 BIG-IP üzerindeki Trafik Yönetimi Kullanıcı Arayüzü, rastgele komut çalıştırmaya ve yerel dosya okumaya karşı savunmasızdır. Bu açık, uç noktalara erişilmesine izin verir. Zafiyetin başarılı olması durumunda, bir saldırgan sistem üzerinde rastgele kod çalıştırabilir. **CVSS Taban Puanı: 9,8**

3. CVE-2020-15506: MobileIron Kimlik Doğrulaması Atlatma

MobileIron Core ve **Connector 10.6** ve önceki sürümlerinde, saldırganların kimlik doğrulama mekanizmasını atlatmasına olanak tanıyan bir zafiyeti bulunmaktadır. Bu, saldırganların hizmetlere ve yönetici paneline erişmesine izin verir. **CVSS Temel Puan: 9,8**

4. CVE-2020-14882: Oracle WebLogic RCE

Eklenmemiş **Oracle WebLogic** sunucuları, saldırganların dosyaları indirmek, tuş vuruşlarını günlüğe kaydetmek, hassas verileri çalmak ve bir ağ üzerinde yanal olarak hareket etmek için rastgele komutlar yürütmesine olanak tanır. Güvenlik açığından yalnızca sunucuya bir istek gönderilerek yararlanılabilir. **CVSS Taban Puanı: 9,8**

5. CVE-2020-14750: Oracle WebLogic RCE

Bu, **Oracle Fusion Middleware**'in **Oracle WebLogic Server** ürünündeki bir uzaktan kod çalıştırma (RCE) güvenlik açığıdır. Yukarıdaki CVE-2020-14882'ye benzer şekilde, güvenlik açığından yalnızca sunucuya bir istek gönderilerek yararlanılabilir. **CVSS Taban Puanı: 9.8**

Kaynak: https://h4cktimes.com/guvenlik-aciklari/2020de-listelere-eklenen-en-kritik-10-cve.html (Defecity)

Watcguard'ın 2020 yılı için hazırladığı rapora göre;

- Türkiye'de bir yılda 1,692,320 adet kötü amaçlı yazılım saldırısı düzenlendiği,
- Önceki yıla göre saldırılarda yaklaşık %81 oranda artış gerçekleştiği,
- Türkiye'de dakikada 3 adet kötü amaçlı yazılım saldırısı yapıldığı,
- Türkiye'de ağ güvenliği saldırıları 5 kat artış gösterdiği,
- Expolit, Web Brute Force Login, Truva atı ve Dolandırıcılık saldırılarının 2020'ye damga vurduğu görülmektedir.

Kaynak: https://www.watchguard.com/wgrd-resource-center/security-report-q1-2020

Tehditlerin sürekli arttığı,

siber korsanların boş durmadığı

internet ortamında yoksa siz hala

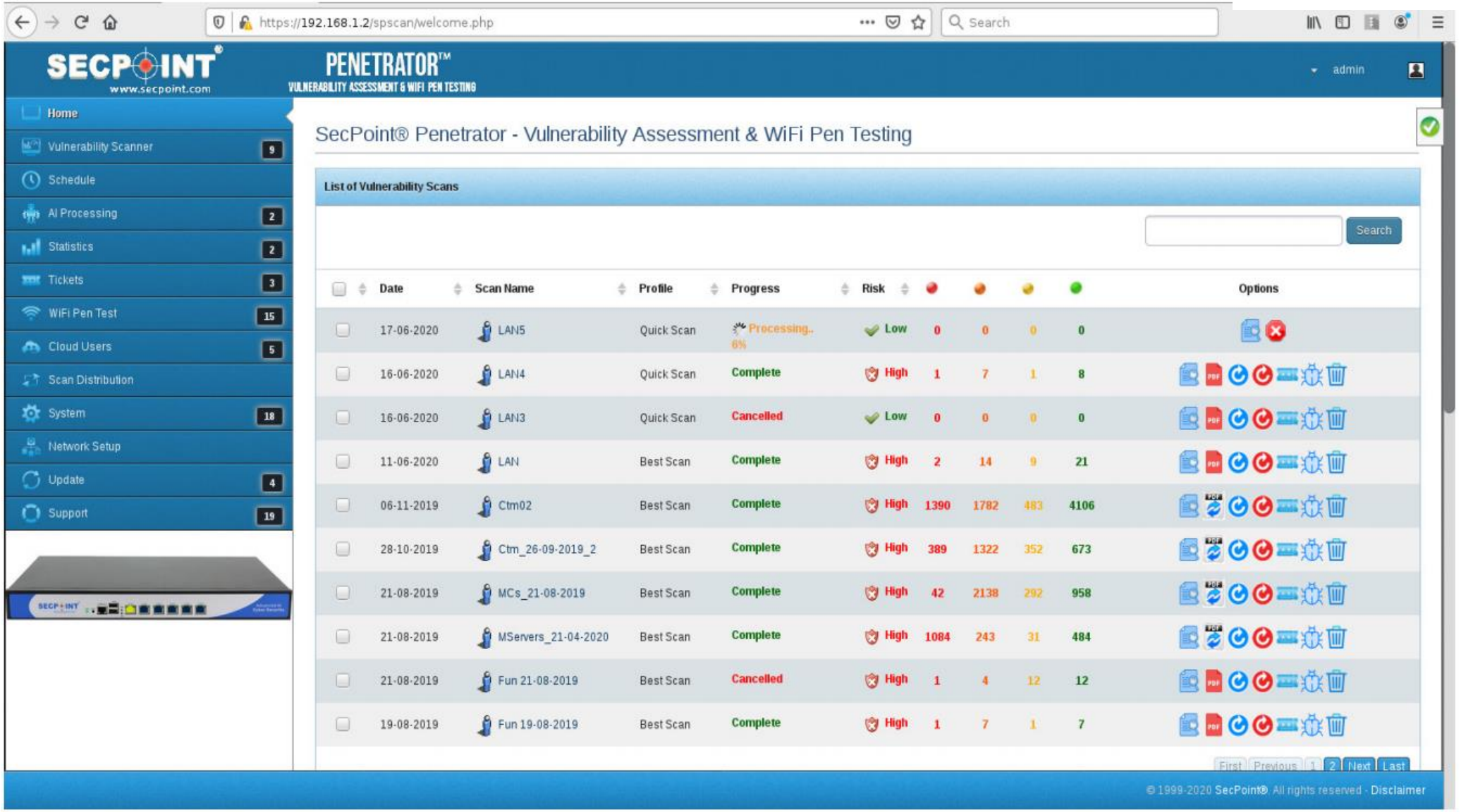
güvende olduğunuzu mu düşünüyorsunuz?

SecPoint Penetrator nasıl çalışır?

- Kullanılacak BT sistemine bağlı bulunan tüm sistemi tarar ve açık iletişim portlarını bulur ve nasıl erişilebileceğini tespit eder.
- Tespit ettiği portları kullanan uygulamaları bulur ve bu uygulamalara exploit ya da farklı yöntemlerle saldırmayı dener. Dışarıdan yapılan kötü amaçlı ataklardan farklı olarak dosya ve sisteme zarar vermeden sadece yolun açık olup olmadığı kontrolünü yapmaktadır.*
- Tek tık ile yapılan bu işlemlerin sonucunu rapor olarak alabilirsiniz.
- En belirgin özelliği; raporların ve sunulan çözümlerin uzmanlık gerektirmeyecek şekilde açık ve kolay anlaşılır olmasıdır.

*Buna rağmen yapılan test yapılması sırasında bazı ağ yazıcılarının bios kaybetme ve benzeri sorunlar yaşadığı rapor edilmiştir.

SecPoint PENETRATOR| SİMET



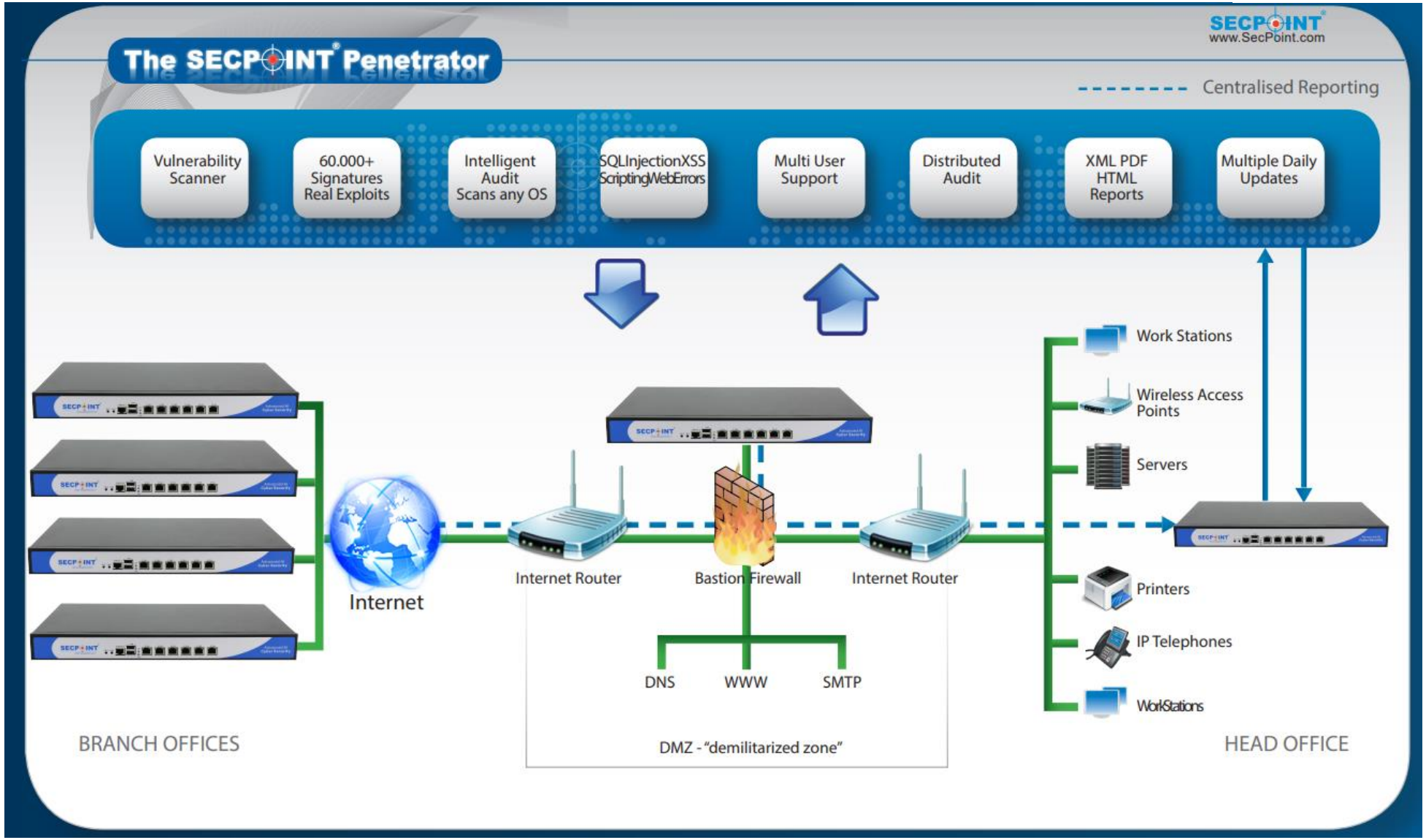
SecPoint Penetrator Özellikleri

- 60.000+ SQL injectionların kontrol edilmesi,
- %100 backdoor güvenliği (Firma hakkında bilgi paylaşımının yapılmaması),
- Tüm dataların müşteride tutulması, üretici firmaya bilgi gönderiminin yapılmaması,
- Kullanıcı dostu, anlaşılır arayüz ve raporlama,
- Kendi logo ve şirket adınızla raporlama imkanı,
- Raporlarda belirtilen açıkların tamamen teknik olarak delillendirilmesi,

SecPoint Penetrator Özellikleri

- Hızlı raporlama ve export etme kolaylığı,
- Vmware ESXI ve Hyper-V sanallaştırma desteği,
- Kablosuz cihazların bulunması (keşfedilmesi),
- Google veri tabanı atakları- SEO verilerinde hassas tarama,
- Scheduled (Planlanmış) task tarama desteği (günlük, haftalık, aylık, yılın istenen çeyreği),
- Yeni zaafiyetlerde otomatik bilgilendirme (E-Mail),
- DOS, DDoS atakları tarama…

SecPoint PENETRATOR| SİMET



Zaafiyet Tarama Profilleri

10 farklı profil arasından tarama seçiminizi yapabilirsiniz…

Profile 1 - Best Scan - Popular Ports
Profile 2 - CMS Web Scan
Profile 3 - Quick Scan
Profile 4 - Large Scan – All 65.535 Ports
Profile 5 - Firewall Scan - Stealth Scan
Profile 6 - Aggressive Scan - Full Scan, Exploits & DoS Attacks
Profile 7 - OWASP Top 10 Scan - OWASP Checks
Profile 8 - PCI-DSS Preparation for Web Applications
Profile 9 - HIPAA Policy Scan for Compliance
Profile 10 - SCADA ICS PLC

Özetle;

Günümüzde artan güvenlik açıklıklarına karşı zaafiyet taramasının yapılması ve zaafiyet yönetimi gittikçe önem kazanmaktadır. Dolayısıyla;

- Zaafiyet taramaları mümkün olduğunca daha sık yapılmalıdır.
- Zaafiyet taramalarınızı otomatik ve scheduled (planlanmış) olarak yapılabilmesi işinizi kolaylaştıracaktır.
- PDF, XML veya HTML formatında ve şirketinize uygun olarak (şirket ismi, logo vb.) rapor oluşturarak zaafiyetlerinizi teknik olarak delillendirebilirsiniz.
- KVKK, ISO 27001, PCI DSS, HIPAA uyumlulukları vardır…
- Kullanıcı farkındalığını artıracak çalışmalara (seminer, konferans v.b) ağırlık verilmelidir.

Ayrıca Penetrator'*un en belirgin özelliği raporların ve sunulan çözümlerin uzmanlık gerektirmeyecek şekilde açık ve kolay anlaşılır olmasıdır.*

Secpoint Penetrator demosuna nasıl sahip olabilirim?

SecPoint Penetrator Demo hesabı açtırmak veya teknik destek için

teknik@simet.com.tr adresine mail atabilirsiniz.

TEŞEKKÜRLER

Integrate with the Universe

www.simet.com.tr

SİMET