IBM'den Atak Önleme Sistemlerine Yeni Bakış

Hakan Turgut
Business Unit Executive
IBM Security Systems
CEE, Turkey, Russia, CIS Countries
hakant@tr.ibm.com

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

Ağ Tehdidi Yönetimi İş Senaryosu

- Bir imalat şirketi, 6 veri merkezi ile küresel çapta çok büyük bir varlığa sahiptir.
- Ağlarından akan trafiğin ne olduğunu ayrıntılı olarak bilmek ve yetkili olduğundan ve kötü niyetli içerik içermediğinden emin olmak istemişlerdir.
- Çok sayıda güvenlik açığının güncel yamasının bulunmadığını bilmektedirler ve bu sorunu çözecek bir çözüm aramaktadırlar.
- İş hacmi gereksinimlerini karşılamak için ölçeklenebilecek, yüksek performanslı bir çözüm istemektedirler.

IBM bu senaryoyu nasıl ele alıyor?

- **IBM Security Network Intrusion Prevention (NIPS) aygıtları**, tüm ağ trafiğini derinlemesine inceler.
- Bu aygıtlar, IBM X-Force tarafından sağlanan istihbarat aracılığıyla kendilerini otomatik olarak güncelleyebilir ve "Tehdidin Bir Adım Ötesinde" kalır.
- Şirketin Web sitelerinin IBM Security NIPS aygıtları tarafından korunması, şirkete sektördeki en iyi korumayı sağlar.
- Bu aygıtlar, ağda neler olduğuna ilişkin gerçek anlamda "durum farkındalığı" sağlar ve SiteProtector ile iyileştirme önceliklerinin belirlenmesi kolaydır.
- IBM Security “Virtual Patch”, satıcı firmaların güvenlik açıklarının giderilmesi için herhangi bir yama mevcut olmasa bile, altyapılarını korur.

Rakipsiz Güvenlik İstihbaratı

Çok miktarda veriye sahibiz...

IBM X-Force® Araştırma ve Geliştirme

- **Tehdit ve koruma sorunlarının araştırılması ve değerlendirilmesi**
- **Günümüzün güvenlik sorunları için güvenlik koruması sağlanması**
- **Yarının güvenlik zorlukları için yeni teknoloji geliştirilmesi**
- **Medya ve kullanıcı topluluklarının eğitilmesi**

X-Force Araştırmaları

14 milyar/ay analiz edilen Web sayfaları ve görüntüler

40 milyon/ay istenmeyen posta ve e-dolandırıcılık saldırıları

60.000 belgelenmiş güvenlik açığı

Milyarlarca her gün gerçekleşen izinsiz giriş teşebbüsü

Milyonlarca özgün kötü niyetli yazılım örneği

Aşağıdakiler için Belirli Analiz Sağlar:

- **Güvenlik açıkları** ve **istismarlar**
- **Botnet** komuta ve kontrolü
- **Kötü Niyetli**/İstenmeyen Web siteleri
- İstenmeyen posta ve e-dolandırıcılık
- **Kötü niyetli yazılım**
- **Yaygınlaşan eğilimler**

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

IBM X-Force İstihbarat Yaşam Çevrimi

Yeni koruma rehberliği

- Bilinen Kötü Niyetli Web Sitelerinin Derinlemesine Taranması
- Yeni İstismar Yöntemlerinin Analiz Edilmesi
- Yeni Koruma Rehberliği Sağlanması

Yeni IPS güncellemeleri

- Korumanın Geliştirilmesi
- Güncellemeler Sağlanması

Yeni kötü niyetli Web siteleri

- Yönetilen Güvenlik Hizmetleri Bağlantılarının Sınıflandırılması
- İlgili Web Sitelerinin Bulunması (Derin Tarama)
- Kötü Niyetli Yazılımların Aranması
- Yeni Kötü Niyetli Web Sitelerinin Bulunması
- Tüm Kötü Niyetli Etki Alanlarının Engellenmesi

Kötü niyetli URL adresleri

- Taramalarının İzlenmesi:
  - Milyonlarca Son Kullanıcı
  - Binlerce Müşteri
  - Yüzlerce Ülke
- Kötü Niyetli Bağlantıların Engellenmesi
- X-Force'a Bağlantılar Gönderilmesi

Entegre Servis Yönetimi ve Güvenlik Çözümleri

30 Mayıs 2012, Çarşamba

Grand Hyatt İstanbul

IBM IPS Sıfır Gün (Güvenlik Açığı/İstismar) Web Uygulaması Performansı

IBM IPS Enjeksiyon Mantığı Motoru, tüm büyük çaplı SQL enjeksiyonu veya XSS saldırılarını ilk defasında durdurmuştur.

- Asprox – bildirilme 11/12/2008 – durdurulma 7/6/2007
- Lizamoon – bildirilme 29/3/2011 – durdurulma 7/6/2007
- SONY (yayınlanmıştır) – bildirilme Mayıs/Haziran/2011 – durdurulma 7/6/200
- Apple Geliştirme Ağı – bildirilme Temmuz/2011 – durdurulma 7/6/2007

Yeni Güvenlik Açığı veya İstismar	Bildirim Tarihi	Hangi Tarihten İtibaren Tehdidin İlerisinde
Nagios genişleyen siteler arası komut dosyası çalıştırma	1/5/2011	7/6/2007
Easy Media komut dosyası başlatma parametresi XSS	26/5/2011	7/6/2007
N-13 News XSS	25/5/2011	7/6/2007
I GiveTest 2.1.0 SQL enjeksiyonu	21/6/2011	7/6/2007
RG Board SQL Enjeksiyonu Yayınlanmıştır:	28/6/2011	7/6/2007
BlogiT PHP Enjeksiyonu	28/6/2011	7/6/2007
IdevSpot SQL Enjeksiyonu (iSupport)	23.5.2011	07.06.2007
2Point Solutions SQL Enjeksiyonu	24.06.2011	07.06.2007
PHPFusion SQL Enjeksiyonu	17.01.2011	07.06.2007
ToursManager PhP Komut Dosyası Kör SQL enjeksiyonu	xx.7.2011	07.06.2007
Oracle Veritabanı SQL Enjeksiyonu	xx.7.2011	07.06.2007
LuxCal Web Takvimi	07.07.2011	07.06.2007
Apple Web Geliştirici Web Sitesi SQL	xx.7.2011	07.06.2007
MySQLDriverCS Siteler Arası Parametre SQL Enjeksiyonu	27.06.2011	07.06.2007

Tehdidin İlerisinde

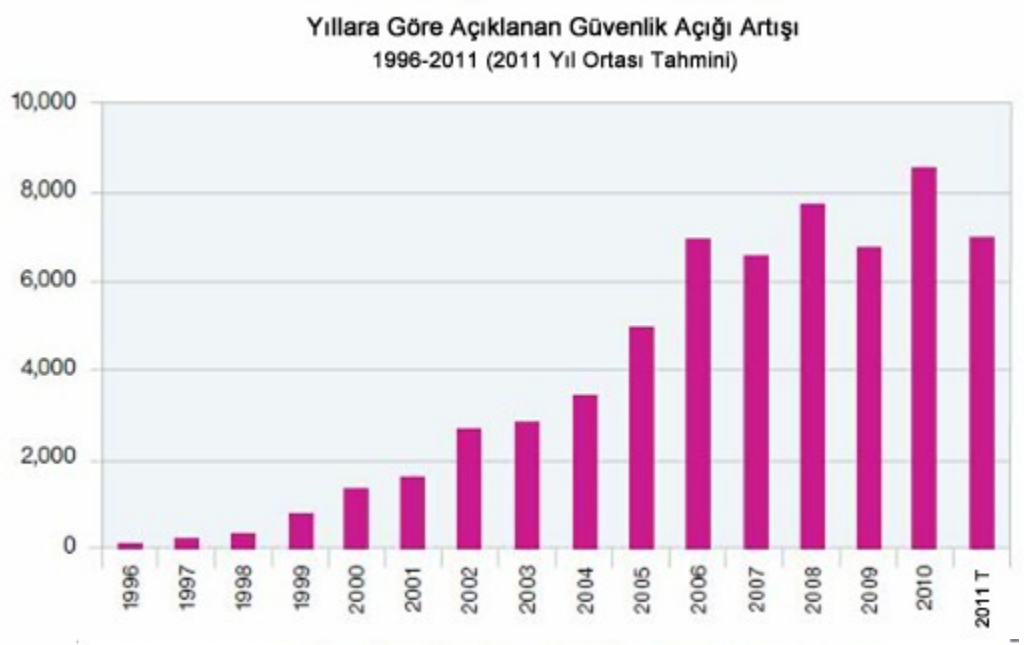
Açıklanan İlk 48 Güvenlik Açığı

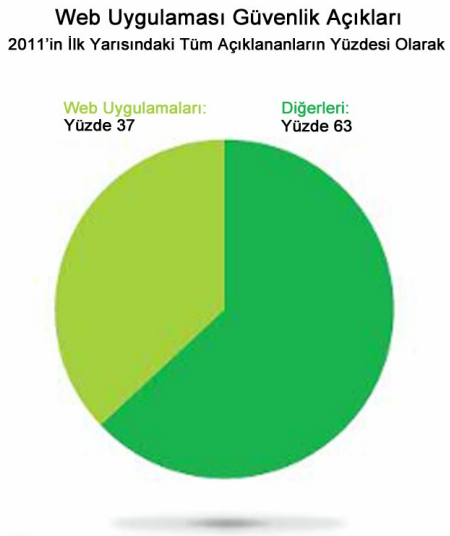
"Tehdidin İlerisinde" **%35** (Ortalama 1 yıldan uzun)
Aynı Gün **%54**
15 Gün İçinde **%11**

IBM Müşterileri, 2010 yılında %89 oranında saldırıdan önce veya 24 saat içinde korunmuştur

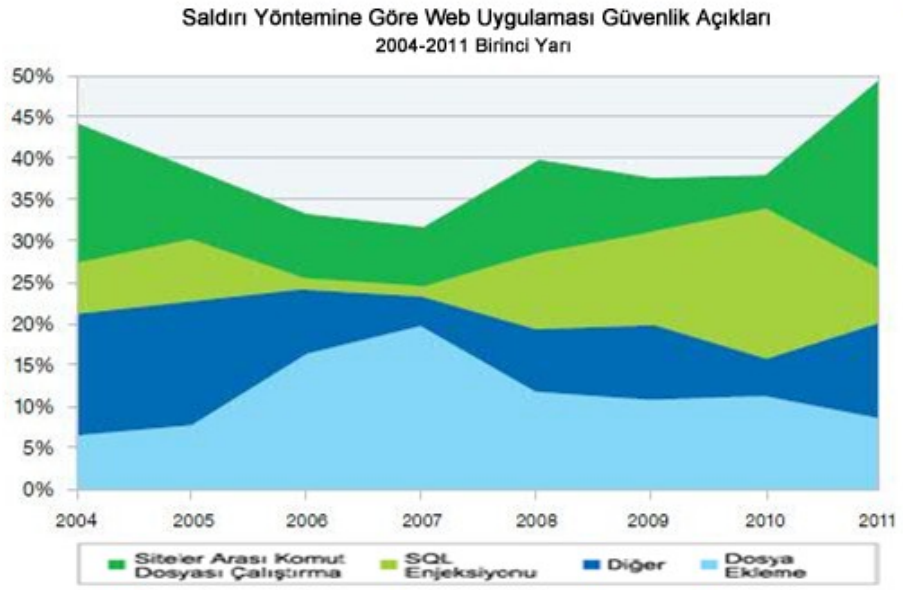
Güvenlik Açığı Açıklamaları

- Toplam güvenlik açığı sayısı azalmaktadır, ancak bu durum döngüseldir.
- Azalma Web uygulaması güvenlik açıklarındadır.





Şekil 28: 2011'in İlk Yarısındaki Tüm Açıklananların Yüzdesi Olarak Web Uygulaması Güvenlik Açıkları



Şekil 29: Saldırı Yöntemine Göre Web Uygulaması Güvenlik Açıkları - 2004-2011 Birinci Yarı

Entegre Servis Yönetimi ve Güvenlik Çözümleri

Ağlarımıza kim saldırıyor?

Saldırgan Tipleri ve Yöntemleri 2011 Birinci Yarı

Kullanıma Hazır araçlar ve yöntemler

- Fark gözetmez
- Gelişmiş teknik becerilere sahip değildir
- İstismar araç takımı ve kötü niyetli yazılım seti kullanır
- Botnet geliştiricileri
- Finansal amaçlı kötü niyetli yazılım etkinliği
- İstenmeyen posta ve DoS

- Finansal amaçlı hedefli saldırılar
- DDoS saldırıları
- LulzSec ve Anonymous (aktivist bilgisayar korsanları)

Gelişmiş

- Siber Savaş

Geniş Çaplı

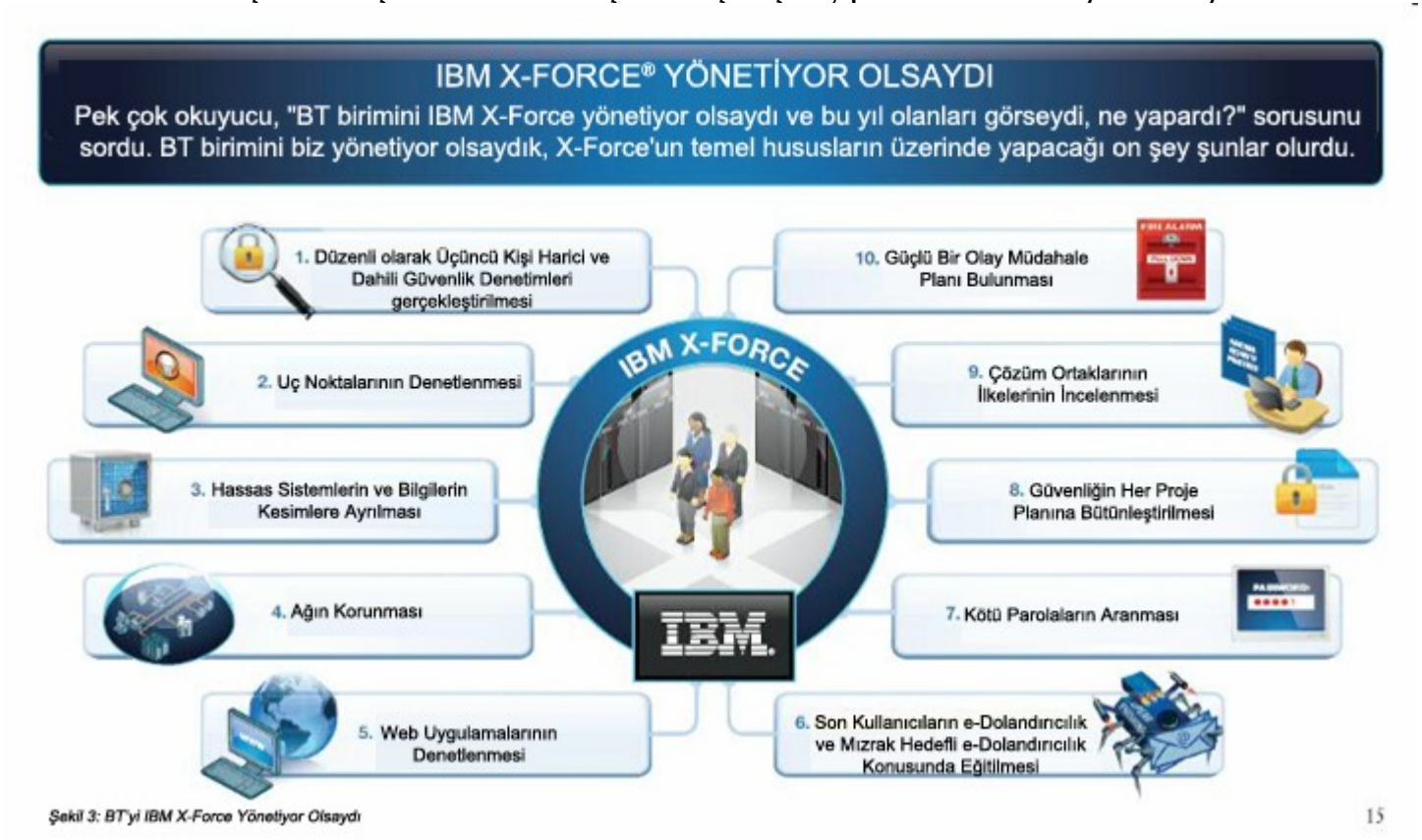
- Advanced Persistent Threat
- Organize, devlet destekli ekipler
- Yeni sıfır gün açıkları bulunması
- Benzeri görülmemiş saldırı yöntemleri

Hedefli

Kaynak: IBM X-Force® Araştırma ve Geliştirme

Teknik bir sorun değil, ancak bir iş zorluğu

- İhlallerin çoğu önlenebilirdi
- Ancak, her güvenlik açığının envanterinin oluşturulması, tanımlanması ve kapatılması önemli ölçüde çaba gerektirmektedir
- Her zaman finans ve işletim açısından dirençle karşılaşılır, peki ne kadar yatırım yeterlidir?



Network IPS

Müşterilerimizde gördüğümüz İş ile ilgili Yaşanan Sorunlar

- Güvenlik açıklarının düzeltilmesi için yama uygulanmasının mümkün olmaması
- Uygulamaların istismara ve kötü niyetli kullanıma karşı korunmasına gereksinim duyulması
- Bilinen tehditlerin ağ üzerinde yayılmasının önlenmesine gereksinim duyulması
- Sıfır gün saldırılarının önlenmesine gereksinim duyulması

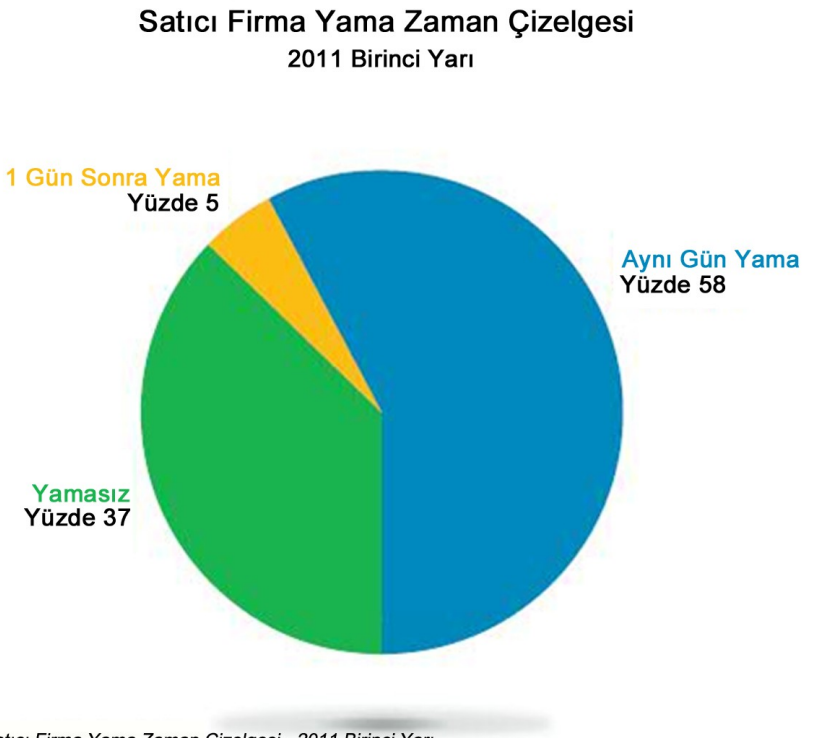
Etkileri

- Şirketin gizli bilgileri veya müşteri bilgileri dahil olmak üzere gizli bilgilerin kaybı
- Bir güvenlik ihlalinin ortalama maliyeti 7,2 milyon ABD dolarıdır*
- Ele geçirilen bir kaydın ortalama maliyeti 214 ABD dolarıdır*
- İş operasyonlarındaki kesintiden veya marka imajının zedelenmesinden kaynaklanan ek gelir kaybı
- İş açısından kritik altyapının kullanılabilirliğinin veya hizmet kalitesinin azalması nedeniyle verimliliğin düşmesi
- Değişen güvenlik risklerine ayak uydurmaya çalışmanın artan maliyeti ve karmaşıklığı

*Kaynak: Ponemon Institute

Yama Uygulama

- Yama uygulanmamış güvenlik açıklarında önemli ölçüde iyileşme
- Beş yılda %44'ün altına inmemiştir

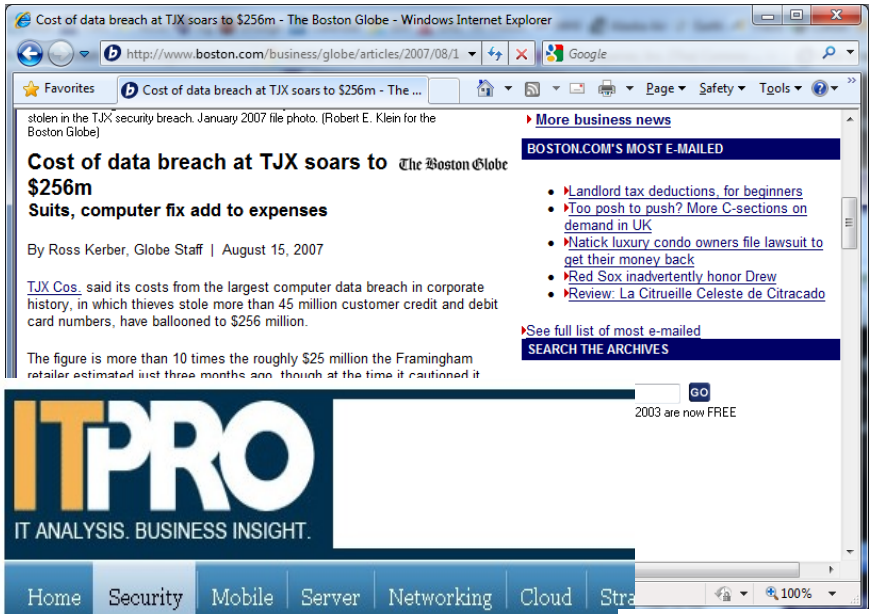


Şekil 33: Satıcı Firma Yama Zaman Çizelgesi - 2011 Birinci Yarı

	2011 1Y	2010	2009	2008	2007	2006
Toplam G.Açığı	3541	8562	6737	7671	6543	6924
Yamasız	1294	3774	3041	3989	2920	3229
Yamasız %	36.5%	44.1%	45.1%	52.0%	44.6%	46.6%

1 Temmuz 2011 itibariyle yaması olmayan güvenlik açıkları

Güvenlik uygulamanın maliyeti yüksek olabilir


Cost of data breach at TJX soars to $256m - The Boston Globe - Windows Internet Explorer

http://www.boston.com/business/globe/articles/2007/08/1

Favorites | Cost of data breach at TJX soars to $256m - The ...

stolen in the TJX security breach. January 2007 file photo. (Robert E. Klein for the Boston Globe)

Cost of data breach at TJX soars to $256m

The Boston Globe

Suits, computer fix add to expenses

By Ross Kerber, Globe Staff | August 15, 2007

TJX Cos. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

The figure is more than 10 times the roughly $25 million the Framingham

More business news

BOSTON.COM'S MOST E-MAILED

- Landlord tax deductions, for beginners
- Too posh to push? More C-sections on demand in UK
- Natick luxury condo owners file lawsuit to get their money back
- Red Sox inadvertently honor Drew
- Review: La Citrueille Celeste de Citracado

See full list of most e-mailed

SEARCH THE ARCHIVES

GO

2003 are now FREE

ITPRO

IT ANALYSIS. BUSINESS INSIGHT.

Home | Security | Mobile | Server | Networking | Cloud | Stra

News | Analysis & Insight | Reviews | Tutorials | Whitepapers

Windows Internet Explorer 9 a more

Home : Security : News

Data breach cost hits £1.9 million

Email | Share

The average cost for a data breach in the UK rises to £1.9 million in 2010, up 13 per cent from 2009.

By Tom Brewster, 21 Mar 2011 at 09:05


The Register®

Hardware | Software | Music & Media | Networks | Security | Cloud | Public Sector | Busin

Financial News | Small Biz | CIO | Tech Panel

Print | Tweet | Like 9 | Alert

PlayStation Network breach will cost Sony $171m

And counting

By **Dan Goodin in San Francisco** · **Get more from this author**

Posted in Financial News, 24th May 2011 05:00 GMT

Create, deploy and manage web apps in the cloud with Windows Azure - 3 Month free trial

The cost of a criminal intrusion that exposed sensitive data for more than 100 million Sony customers and resulted in a 23-day closure of the PlayStation Network will cost the company at least $171 million, executives said.

The estimated cost doesn't included expenses related to any lawsuits that may be filed in response to the security breach, which was discovered on April 19. The estimate includes


RSA SecurID Breach Cost $66 Million

EMC details second quarter 2011 cost to replace tokens, monitor customers, and handle fallout from RSA's SecurID breach.

By **Mathew J. Schwartz** InformationWeek

July 28, 2011 12:10 PM

Between April and June 2011, EMC spent $66 million dealing with the fallout from a March cyber attack against its systems, which resulted in the compromise of information relating to the SecurID two-factor authentication sold by EMC's security division, RSA.

t clean-up figure was disclosed last week during an EMC earnings call, David Goulden, the company's chief financial officer. It doesn't include post-breach expenses from the first quarter, when EMC began investigating the attack, hardening its systems, and working with customers to prevent their being exploited as a result of the attacks.

In spite of the breach, EMC reported strong second-quarter

More Security Insights

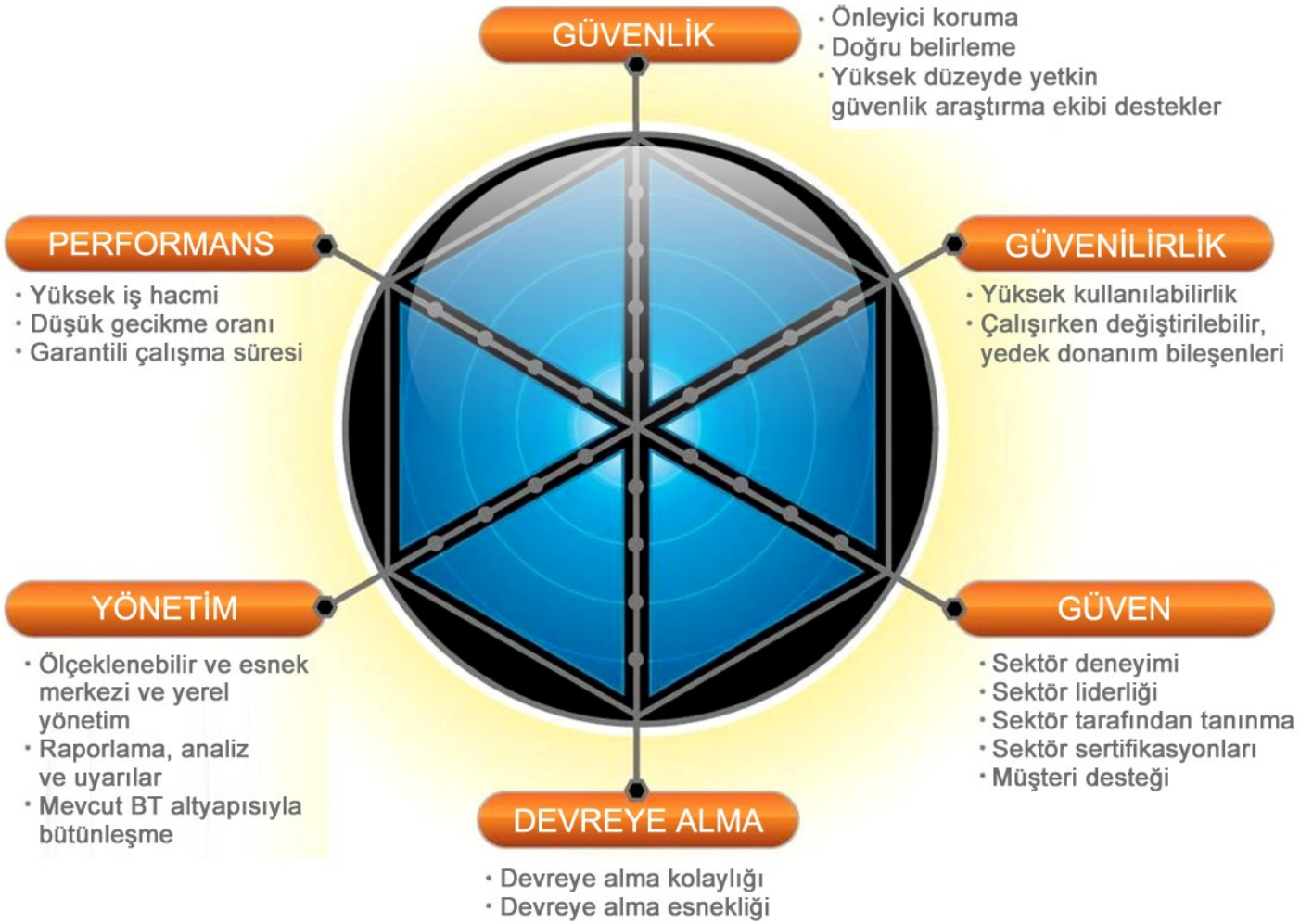
TJ-maxx Marshalls

(click image for larger view)

Slideshow: 10 Massive Security Breaches

Entegre Servis Yönetim Güvenlik Çözümleri

Etkin Ağ Güvenliği Gereksinimleri



IBM Security Network IPS Yazılımının Yetenekleri

Önemli Sorunlar

- Güvenlik ile iş açısından kritik uygulamaların performansının dengelenmesi
- Değişen tehditlerin sınırlı uzmanlık, kaynaklar ve bütçe ile çözülmesi
- Güvenlik altyapısı maliyetinin ve karmaşıklığının azaltılması
- Daha büyük kuruluşların, ağın merkezinde güvenliğe gereksinim duyması

Temel Yetenekler

Geleneksel ağa izinsiz girişi önleme sisteminin ötesinde, aşağıdakiler dahil olmak üzere kapsamlı güvenlik sağlanması:

•Web uygulaması koruması
•İstemci tarafı saldırılarından koruma
•Veri Kaybının Önlenmesi
•Uygulama denetimi
•Virtual Patch Teknolojisi

Güvenliğin kalitesinden ve çeşitliliğinden taviz verilmeksizin 20 Gb/sn'nin üzerinde veri çıkışı ve 10 GbE bağlanırlık sağlayan **rakipsiz performans**

"Tehdidin ilerisinde" kalınması için gücünü dünyaca ünlü X-Force araştırmalarından alan sürekli **gelişen koruma**

Nokta çözümlerinin birleştirilmesi ve diğer güvenlik araçlarıyla bütünleştirme aracılığıyla **daha düşük maliyet ve karmaşıklık**

IBM İletişim Kuralı Analizi Modüler Teknolojisi

İzinsiz Girişi Önleme Çözümleri

- Tehditleri kuruluşunuzu etkilemeden <u>önce</u> engelleyin
- X-Force® tarafından desteklenen tavizsiz güvenlik
- 200 Mb/sn'den 20 Gb/sn'nin üzerine kadar incelenen veri çıkışı
- 8 adet ağ kesimine kadar koruma
- Uzak ofislerden ağın merkezine kadar kapsayan ölçek

IBM Security Network IPS Modelleri									
	Remote	Perimeter			Core				
Model	GX4004-200	GX4004	GX5008	GX5108	GX5208	GX7412-5 YENİ	GX7412-10 YENİ	GX7412 YENİ	GX7800 YENİ
Denetlenmiş Veri Çıkışı	200 Mb/sn	800 Mb/sn	1,5 Gb/sn	2,5 Gb/sn	4 Gb/sn	5 Gb/sn	10 Gb/sn	15 Gb/sn	20 Gb/sn'den yüksek
Korunan Kesimler	2	2	4	4	4	8	8	8	4

YENİ !
IBM Security Network IPS v4.4 ve "Hibrid Koruma"

Security Intelligence Platform

- Log Manager
- SIEM
- Network Activity Monitor
- Risk Manager
- Future

Threat Intelligence and Research

- Vulnerability Data
- Malicious Websites
- Malware Information
- IP Reputation

Advanced Threat Protection Platform

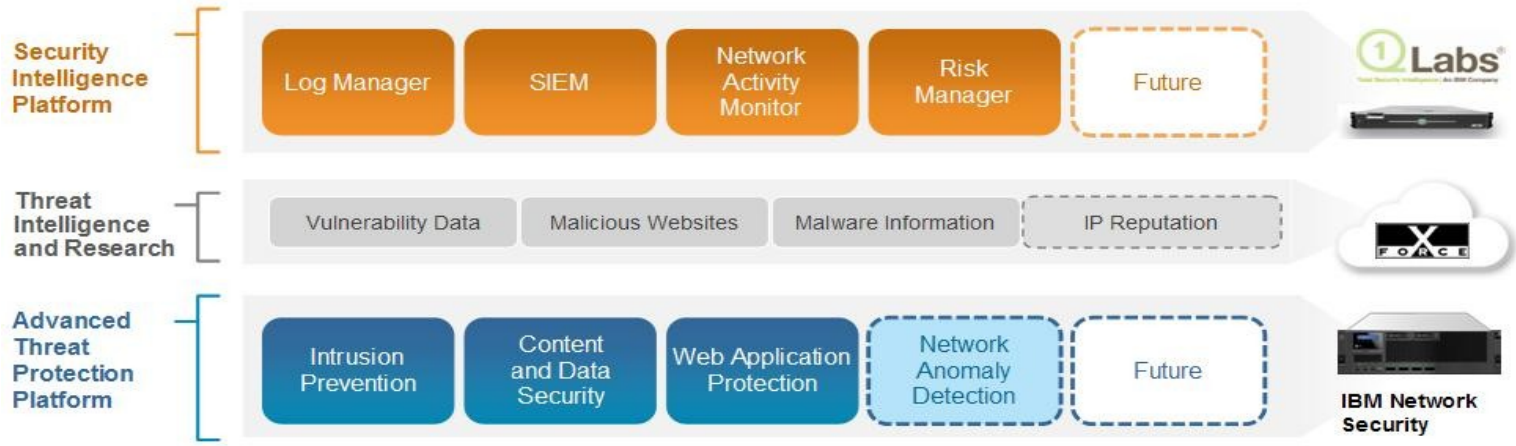
- Intrusion Prevention
- Content and Data Security
- Web Application Protection
- Network Anomaly Detection
- Future

IBM Network Security

Entegre Servis Yönetimi ve Güvenlik Çözümleri

IBM Security Network IPS v4.4 ve "Hibrid Koruma"- IBM Gelişmiş Tehdit Koruma Platformu

- Web uygulaması güvenlik açıklarından Advanced Persistent Threat (APT) türü tehditlere kadar pek çok tehdide yanıt veren kapsamlı portföy



- Gerçek zamanlı tehdit bilgileri ve Güvenlik Zekasıyla birlikte geniş çeşitlilikteki ağ güvenliği yeteneklerinden yararlanarak olağandışı ağ davranışını saptamakta ve kapsamlı tehditlerden koruma sağlamaktadır.

IBM Gelişmiş Koruma Platformu, IBM'in güvenlik alanındaki en yeni inovasyonlarını içerir:

- **IBM Security Network IPS v4.4** ve "Hibrid Koruma"
  - X-Force ile desteklenen, Zero Day saldırıları olarak bilinen tehditlere karşı koruma özelliği
  - SNORT tabanlı imza oluşturma ve içe aktarma yeteneği sunma
  - Üstün güvenlik ve esneklik özelliği
- **QRadar Network Anomaly Detection**, IBM'in ağ IPS platformuna güçlü güvenlik zekası ve öngörüsü katar ve şu avantajları sağlar:
  - Güvenlik ihlallerinin işe olan etkisini azaltma ve bu ihlalleri daha kısa sürede saptama
  - Güvenlik olaylarını daha hızlı ve kapsamlı bir şekilde araştırma ve çözme
  - Güvenlik operasyonlarına ve uyumluluk raporlarına ilişkin manuel süreçleri azaltma
- Güvenlik eğilimlerine ilişkin kapsamlı analiz için:

IBM X-Force 2011 Eğilim ve Risk Raporu sayfası

Müşterilerimize nasıl yardımcı olur

- Mevzuata ve yasalara uygunluğu destekler
- Veri ve Fikri Mülkiyet içeren şifrelenmemiş trafiği engeller
- Güvenlik ihlallerinden kaynaklanan kapalı kalma süresini azaltır
- Önleyici güvenlik sayesinde toplam sahip olma maliyetini düşürür
- Etkin, basit Web Uygulaması koruması, yeni iş kazanılmasını destekler
- Tehditleri anlamaya olan gereksinimi ortadan kaldırır: X-Force gerekeni yapar
- Güvenlik bir iş etkinleştiricisi haline gelir (örneğin, bulut)

- Erken iyileştirme için geliştirilmiş görünürlük ve uyarılar
- Daha yüksek ağ performansı
- İşle ilgili hizmet seviyesi sözleşmelerinin karşılanmasına yardımcı olur
- İstenmeyen uygulamalar için iletişim kurallarını devre dışı bırakır
- Yamalar devreye alınmadan önce koruma sağlar
- Basit, merkezileştirilmiş yönetim
- Aracısız Koruma (VSP)

Örnek başarı hikayeleri!

İhtiyaç

- Müşteri, işin büyümesini desteklemek için Asya Pasifik bölgesine yönelik yeni bir veri merkezini hızla kurmaya gereksinim duymaktaydı
- Aynı zamanda, maliyetleri düşürmek ve verimliliği artırmak için bazı lokasyonları birleştirmek istiyordu
- İki veri merkezinin gerektirdiği kurulum nedeniyle zaman çizelgesine uyulması zordu
- Müşteri, ortamda devreye alınacak çözümde ve ürünlerde kaliteye ve güvenilirliğe gereksinim duyuyordu

Çözüm

- İnternet tehditlerini işi etkilemeden önce durdurulması için IBM Security Network Intrusion Prevention System (IPS).
- Müşteri aynı zamanda, harici tehditleri daha da azaltacak önleyici koruma için bir IBM Altyapı Hizmetleri çözümü uygulamıştır.

İş Avantajları

- Müşteri, nokta çözümlerinin devreye alınması ve yönetilmesi ile bağlantılı maliyeti ve karmaşıklığı azaltırken, aynı zamanda da kapsamlı koruma elde etmiştir.
- Buna geleneksel ağa izinsiz girişin önlenmesinin ötesine geçilmesi dahildir:
  - Yüksek değerli varlıklara yönelik hedefli saldırıların önlenmesi için ileri düzey tehdit belirleme ve önleme sağlanması
  - Web uygulamalarının SQL enjeksiyonu ve siteler arası komut dosyası çalıştırma saldırıları gibi tehditlerden korunması
  - Ağın kötü niyetli kullanımdan ve anında ileti sistemi ve eşler arası dosya paylaşımı istismarından korunması
  - IBM Rational AppScan yazılımı gibi başka güvenlik çözümleri ile bütünleşme
  - Dünyaca ünlü IBM X-Force araştırmaları ile desteklenen "tehdidin ilerisinde" koruma sağlanması

AXA TECHNOLOGY SERVICES
redefining / service

Örnek başarı hikayeleri!

İhtiyaç

- Vietnam Merkez Bankası, bir finans kuruluşu olarak, iş operasyonlarını ve müşterilerinin varlıklarını korumak için çok yüksek düzeyde güvenliğe gereksinim duymaktadır.
- Kuruluş, beş bölgesel merkezi ve 17 şehirdeki ofisleri destekleyen karmaşık bir sistem olan ağ altyapısının güvenliğini, kararlılığını ve genel iş hacmini güçlendirmek istemiştir.

Çözüm

- Vietnam Merkez Bankası, ağ operasyonlarının daha iyi korunması için Proventia Network Active Bypass aygıtı dahil olmak üzere, bir IBM Security Network Intrusion Prevention System çözümü devreye almıştır.
- Müşteri aynı zamanda, ağ güvenliği desteği ile yönetim çabalarını birleştirmiştir.

İş Avantajları

- Müşteri, Vietnam Merkez Bankasının merkezi, çevresel ve uzak ağ kesimlerini kapsayan merkezileştirilmiş bir güvenlik stratejisine sahip olmuştur.
- IBM Security Network Intrusion Prevention System avantajlarından yararlanan banka, daha yüksek ağ kullanılabilirliği sağlarken, aynı zamanda maliyetleri ve yönetim gereksinimlerini azaltabilir.

SiteProtector

SiteProtector'un Misyonu: Güvenlik Yönetiminin Basitleştirilmesi

Daha fazla saldırı hedefi, yönetilecek daha fazla varlık ve daha az kaynak bulunmaktadır:

- **Genel Güvenlik Kullanıcıları, uzman eğitimine ve/veya güçlü araçlara gereksinim duyar**
  Karmaşık sistemlerin yönetilmesi, çeşitli, yüksek düzeyde uzman eğitimi almış personel veya birleşik bir konsol gerektirir.

- **Güvenlik Uzmanları, derinlemesine analitiğe ve ilişkilendirmeye gereksinim duyar**
  Bütünleştirilmiş olay analizi ve ilke düzenleme özelliklerine sahip özelleştirilebilir araçlar.
- **Güvenli İşlemsel Sistemler ayrıntılı araştırma gerektirir**
  Mevzuata uygunluk için hesap verebilirliğin, saydamlığın ve ölçülebilirliğin kanıtlanması, ayrıntılı ve esnek raporlar gerektirir.

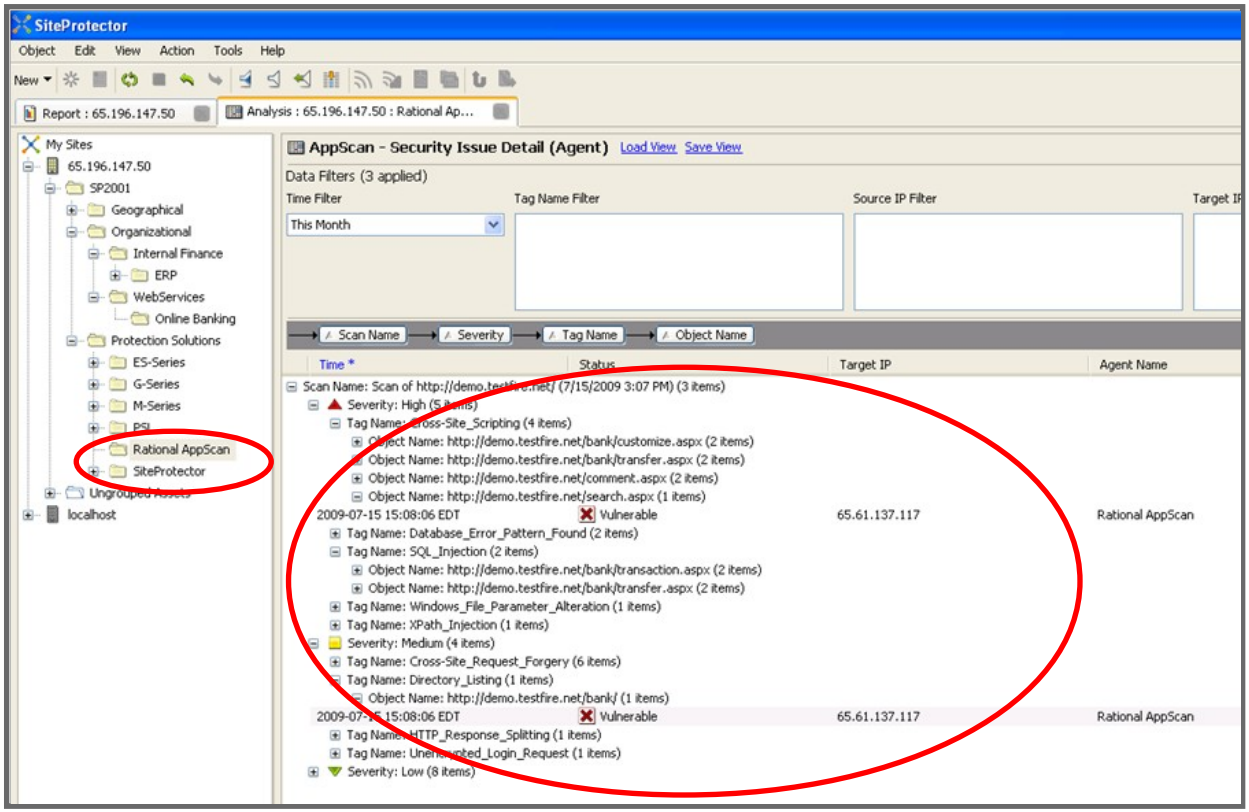
- **Çeşitli Teknolojiler ekonomik yönetim gerektirir**
  "Silolar" halindeki çok sayıda güvenlik yönetimi aracının, bağlantılı sunucuların ve lisans anahtarlarının yönetilmesi ve yönetimin maliyeti.
- **Genişleyen Evren etkin takip gerektirir**
  Kurumsal varlıkların tanımlanması, yönetilmesi ve güvenliğinin sağlanması.

- **Konu Uzmanlarının sayısı azdır**
  Sınırlı güvenlik kaynakları (zaman ve uzmanlık).

- **Çoğalan Veriler sistemleri boğar**
  Aşırı bilgi yüklemesi ve birleştirme.
- **Çakışan Öncelikler başarıları gölgeler**
  Güvenlik sürecinizin değerini nasıl duyurursunuz?

"Daha az ile daha fazlasını yapmayı kolaylaştırın"

SiteProtector, uygulama güvenlik açıklarını görüntüler



- ✓Ağ analisti, uygulama güvenlik açıklarını inceler
- ✓Ağ analisti, güvenlik açığı bulunan uygulama varlıklarını izler

SiteProtector SecurityFusion™ modülü, güvenlik zekası sağlar

Tag Name	Status	Severity	Event Count	Source Count
HTTP_POST_SQL_UnionSelect	Detected event	Medium	3	1
HTTP_POST_SQL_UnionSelect	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_POST_XP_Cmdshell	Detected event	High	48	1
HTTP_QuikStore	Attack failure (blocked by Proventia appliance)	Medium	5	1
HTTP_repeated_character	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Server_ID	Detected event	Low	21986	2
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)	Medium	1	1
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)	Medium	4	1
HTTP_testcgi	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)	Medium	48	1
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)	High	2	1
HTTP_Unify_UploadServelet	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Unix_Passwords	Detected event	High	12	1
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)	High	42	1
HTTP_URL_dotpath	Detected event	Low	4	1
HTTP_URL_Many_Slashes	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_URL_repeated_char	Detected event	Medium	1	1
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)	Medium	12	1
HTTP_URLscan	Detected event	Medium	2	1
HTTP_Webplus	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)	High	168	1
SQL_Injection	Attack likely successful (vulnerable)	High	73	2
XPath_Injection	Attack likely successful (vulnerable)	Medium	438	1

- ✓ **İzinsiz Girişi Belirleme/Önleme Sistemlerinin gerçek zamanlı olarak belirlediği kötü niyetli HTTP trafiği, güvenlik açığı bulunan varlıklarla ilişkilendirilir**
- ✓ **SiteProtector, saldırıların başarı olasılığı yüksek olduğunda ağ analistini uyarır**
- ✓ **Ağ analisti müdahale eder**

Başarıyı İleri Taşıyor – SiteProtector V2.9

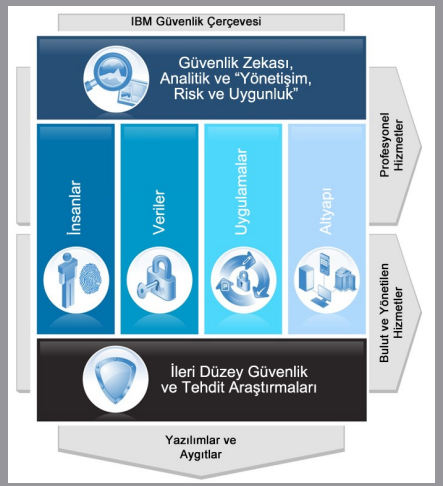
- **Çözüme Özgü Arabirimler** - Bağlama uyarlanmış, çözüme özgü arabirimler, eldeki görevle ilgili bilgiler sunar. Örneğin, "Aracıları Göster/Gizle" ayarlarıyla kullanılmayan tipleri gizleyebilirsiniz.
- **Geliştirilmiş Kullanıcı Arabirimi** - İyileştirilmiş menüler arabirimdeki karmaşayı azaltır, bu şekilde dikkatiniz dağılmadan önemli görevlere odaklanabilirsiniz.
- **İlke görünümü iyileştirmeleri** - İlke görünümü, ağınıza özgü aracı tiplerini içeren bir galeriyi, mevcut sürümler arasında seçim yapma olanağı ile görüntüler.
- **Analiz görünümü iyileştirmeleri** - Analiz görünümünde, görüntülenen herhangi bir sütun için bağlama uygun etkinlikler mevcuttur. Gereken şekilde ek sağ tıklatma etkinlikleri ve aramalar tanımlayabilirsiniz.
- **Otomatik sütun genişliği ayarı** - Sütunlar, görüntülenen veriler doğrultusunda otomatik olarak yeniden boyutlanır. Özelleştirilmiş ayarlar kaydedilebilir.
- **Ayrıntılara hızlı erişim** - Olay ayrıntılarına hızla erişmek için Analiz görünümünde bir olayı çift tıklatabilirsiniz.
- **Sistem yanıt süresi** - Özellikle Analiz görünümünde, büyük veri kümeleriyle çalışırken, geliştirilmiş veritabanı performansı.
- **Genişletilen sınırlar** - İki kat daha fazla olay kuralı; 400 adede kadar.
- **Güncellenen bileşenler** - En son güvenlik önlemlerine erişim için en son Java, Apache ve Geronimo sürümleri.

IBM'in benzersiz güvenlik uzmanlığının ve yaklaşımının avantajlarından yararlanın...

BENZERSİZ UZMANLIK

- Her gün izlenen 21 milyar olay
- 4.000'den fazla yönetilen hizmet müşterisi
- 10 güvenlik geliştirme laboratuvarı
- 9 güvenlik operasyonları merkezi
- 6.000'den fazla Güvenlik Mühendisi ve danışmanı
- 20'den fazla defa tasdik edilmiş liderlik
- 2010 Yılının Güvenlik Şirketi
- Ödüllü X-Force araştırma birimi
- Sektördeki en büyük güvenlik açığı veritabanı

SAĞLAMA BECERİSİ



- ✓ Zeka
- ✓ Bütünleşme
- ✓ Uzmanlık

Entegre Servis Yönetimi ve Güvenlik Çözümleri


Teşekkürler