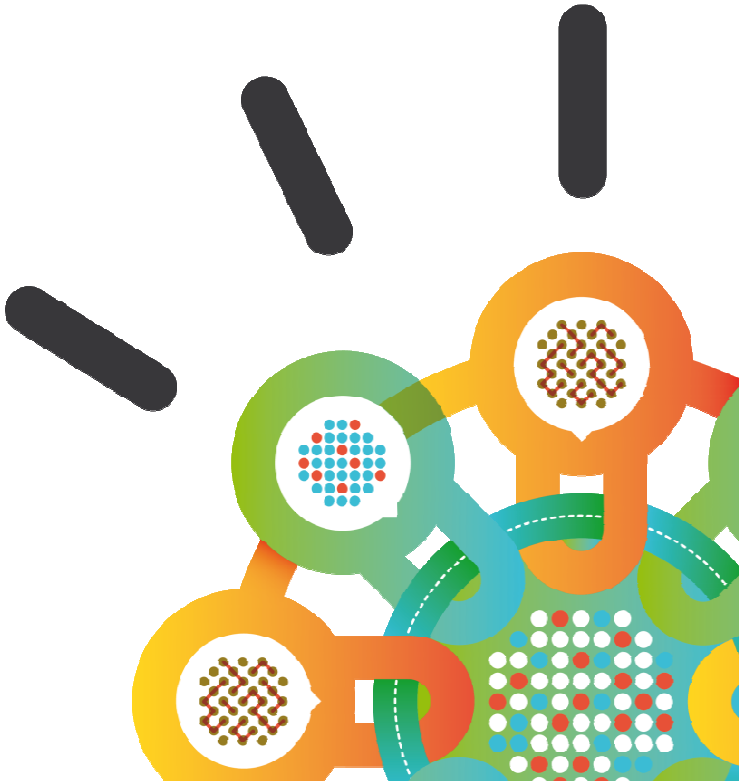
Security Intelligence.
Think Integrated.

Yeni Nesil Güvenlik Bilgisi Toplama ve Olay Yönetimi

Nurettin Erginöz
Client Technical Professional, CoP
CEE&Türkiye, IBM Security Systems
ERGINOZ@tr.ibm.com



Smarter Security

Security Intelligence.

Think Integrated.

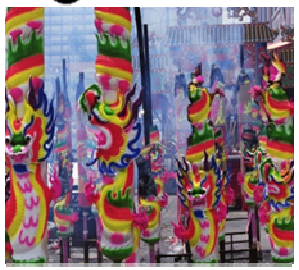
IBM

Security Intelligence.

Think Integrated.

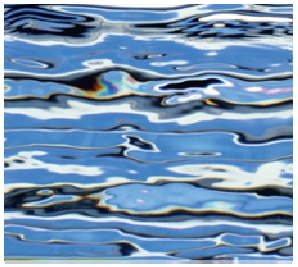
Akıllı Tedarik Zincirleri

Akıllı Ülkeler

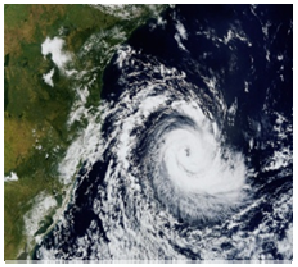


Akıllı Perakendecilik

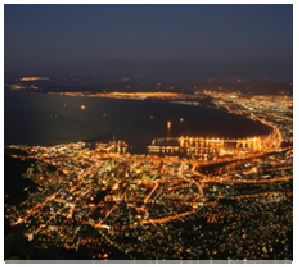
Akıllı Su Yönetimi



Akıllı Hava



Akıllı Enerji Şebekeleri



DONANIMLI

BİRBİRİYLE BAĞLANTILI

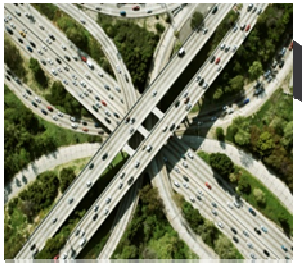
ZEKİ

Akıllı Petrol Sahası Teknolojileri

Akıllı Bölgeler

Akıllı Sağlık Hizmetleri

Akıllı Trafik Sistemleri



Akıllı şehirler

Akıllı Gıda Sistemleri

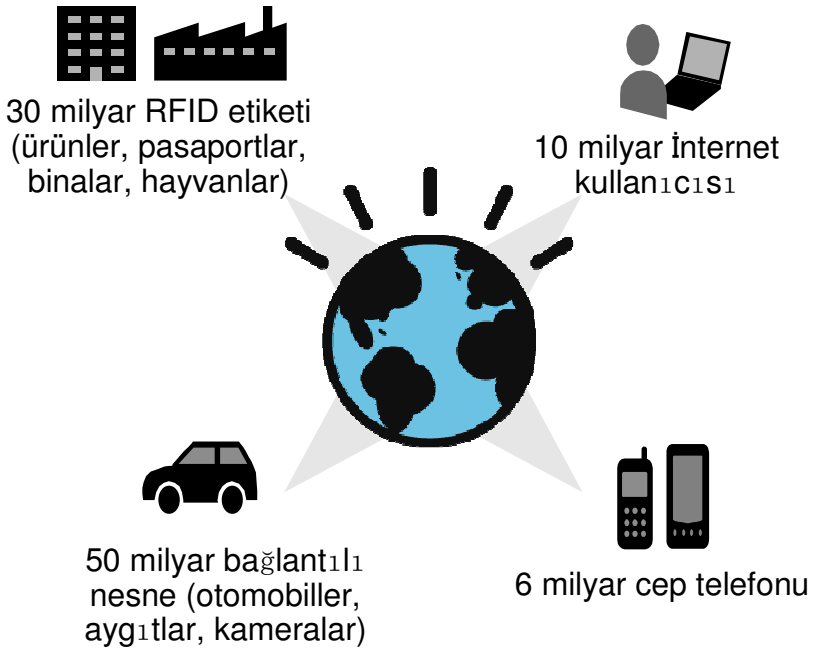
Security Intelligence.
Think Integrated.

Akıllı Çözümler…

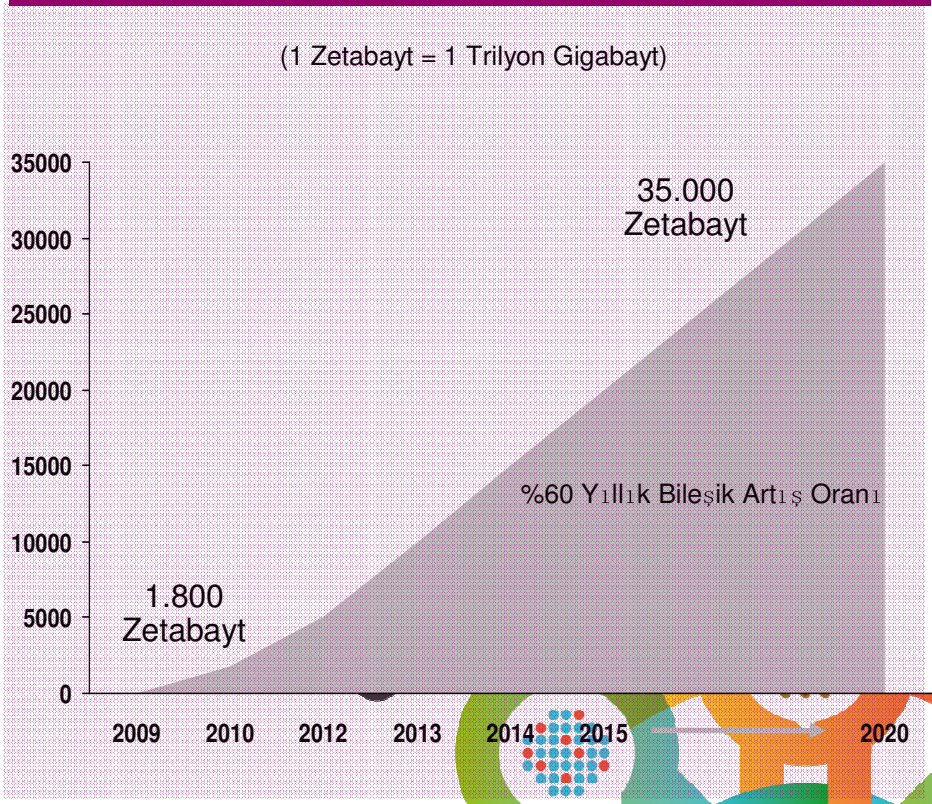
Dünya giderek daha donanımlı, birbiriyle bağlantılı ve zeki hale geliyor.

Security Intelligence.
Think Integrated.

Çok sayıda hedef içeren ortam



Dünya çapındaki veri patlaması



"Mobil tarayıcılarla bağlantılı olarak, henüz yeterince bilgi sahibi olmadığımız güvenlik sızıntıları bulunuyor."
Bilgi Teknolojileri Yöneticisi, Medya şirketi

Security Intelligence.
Think Integrated.

Big Big Big Big Data

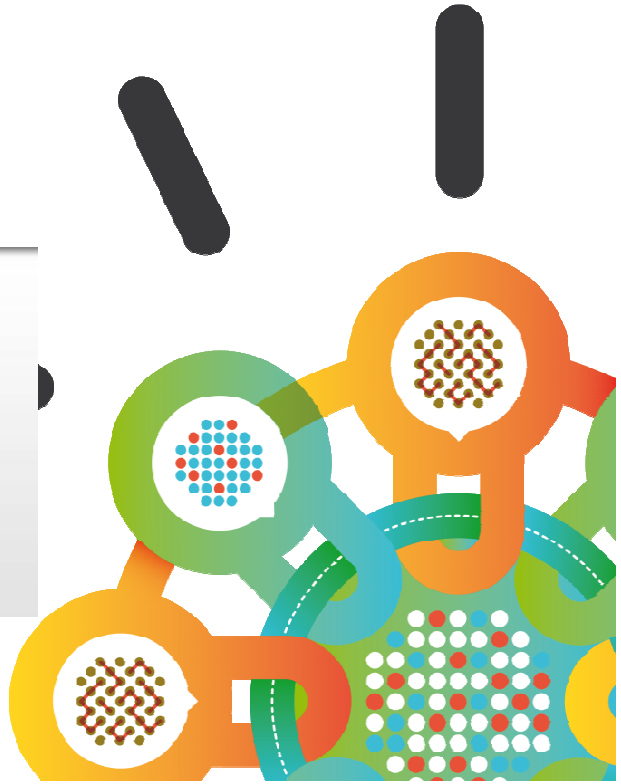
- Daha fazla hedef
- Daha fazla güvenlik açığı

Security Intelligence.
Think Integrated.

Güvenlik Yatırımları

Neden yatırım yapılıyor?

- Kim?
- Ne?
- Kanıt?



Security Intelligence.

VERİ PATLAMASI

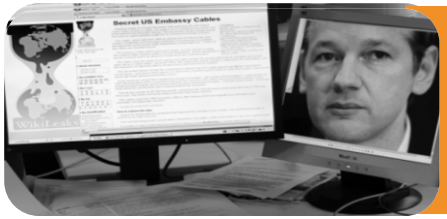
Hassas verilerine kimlerin baktığını bilmek bir yana, sadece tüm hassas verilerinin nerede bulunduğunu bilen müşteri sayısı bile çok az olduğundan, mevzuata uygunluk önemli bir zorluk oluşturmaktadır.

BT'NİN ÜRÜN HALİNE GETİRİLMESİ

Web 2.0'ın ve sosyal işin yaygınlaşması, önemli ölçüde yeni iş risklerinin ortaya çıkmasına neden olmaktadır.

HER ŞEY HER YERDE

Bulut, sanallaştırma ve diğerleri dahil olmak üzere yeni yenilikçi platformlar, karmaşıklık ve maliyet açısından daha da büyük zorluklara neden olmaktadır.

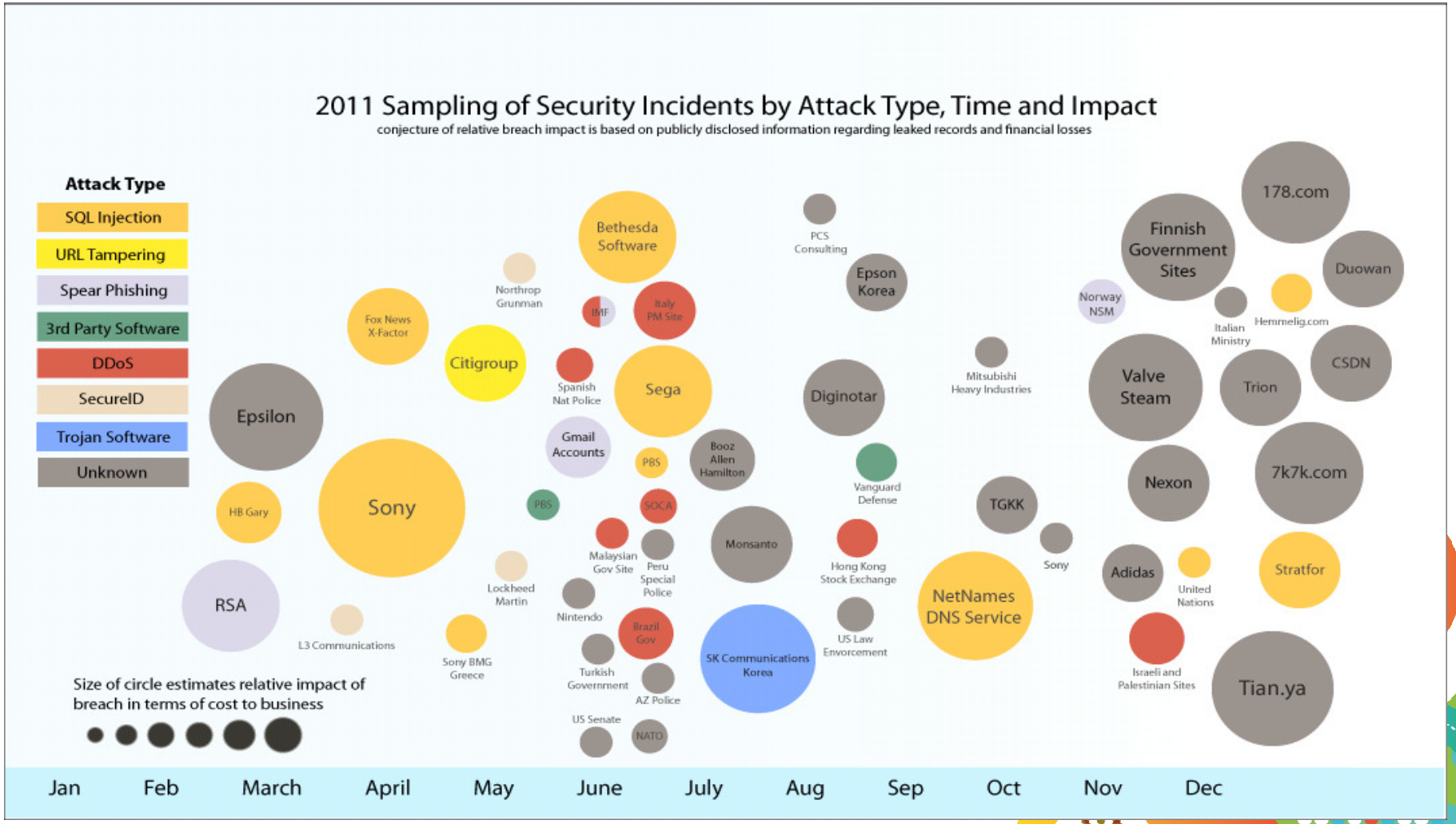


SOFİSTİKE SALDIRILAR

Saldırılar artık BT altyapısını değil, işin kendisini hedef almaktadır.

Security Intelligence.
Think Integrated.

2011 Yılı Raporu



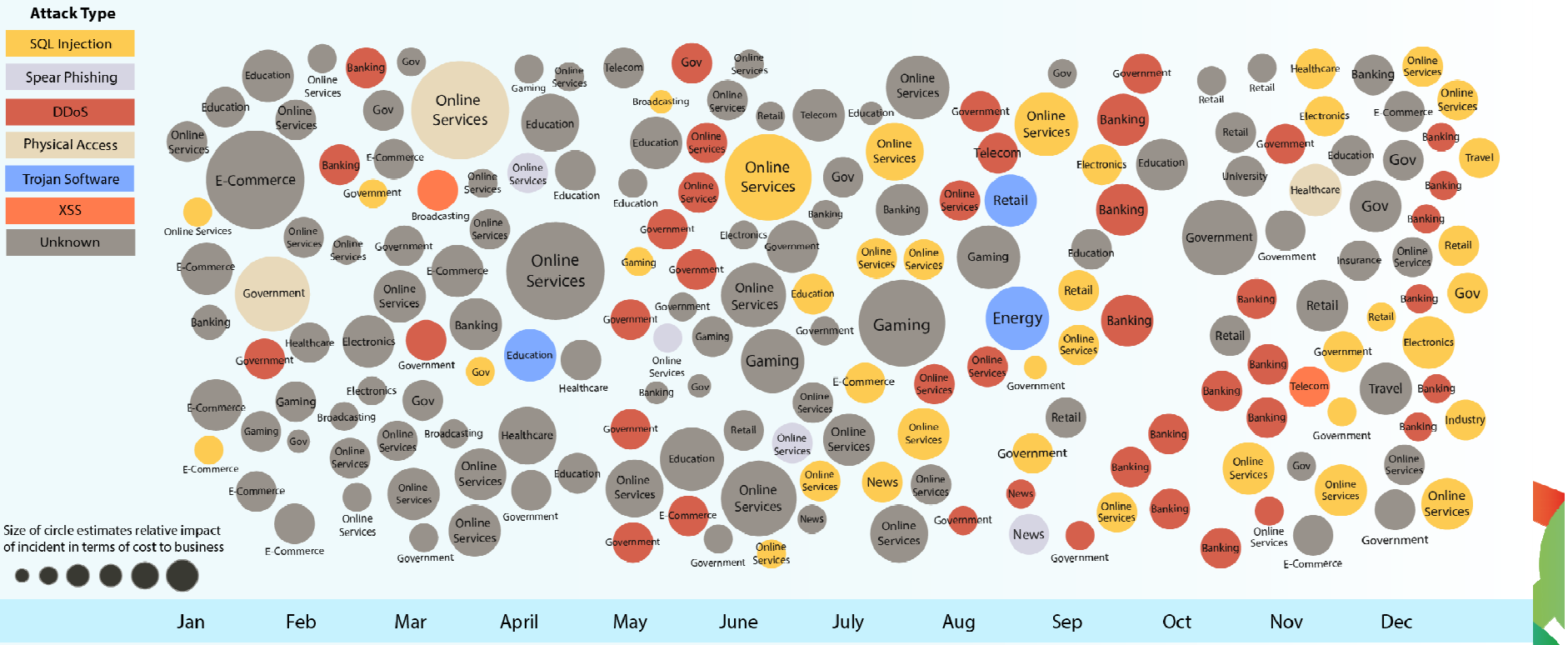
Source: IBM X-Force® 2011 Trend and Risk Report – March 2012

Security Intelligence.
Think Integrated.

2012 Ataklardaki artış ve değişim

2012 Sampling of Security Incidents by Attack Type, Time and Impact

Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



Security Intelligence
Think Inte

	Yönetim Kurulu Başkanı	Finans/Operasyon Yöneticisi	Bilgi Teknolojileri Yöneticisi	iK Yöneticisi	Pazarlama Yöneticisi
Yönetici önceliği	Rakiplerden farklılığın sürdürülmesi	Mevzuata uygunluk	Mobil aygıt kullanımının yaygınlaştırılması	Küresel çalışma esnekliğine olanak sağlanması	Markanın geliştirilmesi
Güvenlik riskleri	Fikri mülkiyetin suistimal edilmesi İş açısından hassas verilerin suistimal edilmesi	Yasal gereksinimlerin yerine getirilmemesi	Veri artışı Güvenli olmayan uç noktaları ve uygun olmayan erişim	Hassas verilerin açığa çıkması Çalışanların dikkatsizliği	Müşterilerin veya çalışanların kişisel bilgilerinin çalınması
Potansiyel etki	Pazar payı ve itibar kaybı Yasaların ihlali	Denetimlerin olumsuz sonuçlanması Para cezaları ve cezai kovuşturma Finansal zarar	Veri gizliliğinin, bütünlüğünün ve/veya kullanılabilirliğinin kaybı	Çalışan gizliliğinin ihlal edilmesi	Müşteri güveninin kaybı Marka itibarının kaybı

İşletmeler, giderek artan oranda Denetim Kuruluyla doğrudan bağlantılı Risk Yöneticileri ve Bilgi Güvenliği Yöneticileri atamaktadır.

*Kaynak: IBM Üst Düzey Yönetici Araştırmaları Serisi kapsamında 13.000'den fazla üst düzey yönetici ile yapılan görüşmeler

Siz hangi konumdasınız?

Security Intelligence.

Think Integrated.

Mevzuata uygunluk

1. Güvenlik risklerinizi değerlendirdiniz mi?
2. Güvenlik etkinliğini ölçmek için bir endüstri standardından yararlanıyor musunuz?
3. Mevzuata uygunluk için ortak bir denetim kümeniz var mı?
4. Güvenlik kanıtlarının bulunması için kritik kayıtları ve günlükleri saklıyor musunuz?

Dahili ve Harici Tehditler

5. Tehditlere ilişkin en son araştırmalardan yararlanıyor musunuz?
6. Verilerinize, uygulamalarınıza ve sistemlerinize kimler erişiyor?
7. Olaylara verilen yanıtları ve olağanüstü durumdan kurtarmayı nasıl yönetiyorsunuz?
8. Hassas verileri gizli olarak sınıflandırıp şifreliyor musunuz?
9. Yetkili kullanıcıların verilerinizle ne yaptıklarını biliyor musunuz?
10. Güvenlik, bulut bilgi işlem gibi yeni girişimlerde yerleşik hale getiriliyor mu?

Security Intelligence.
Think Integrated.

IBM Güvenlik Çerçevesi

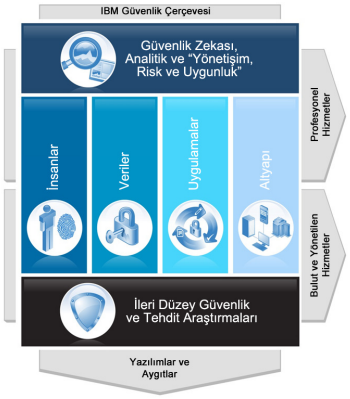
IBM Security Systems

- Pazarda temel güvenliği uçtan uca kapsayan tek satıcı firma
- Yenilikçi teknolojilere 1,8 milyar ABD doları yatırım
- 6.000'den fazla güvenlik mühendisi ve danışmanı
- Ödüllü X-Force® araştırma birimi
- Endüstrideki en büyük güvenlik açığı veritabanı

Zeka • Bütünleştirme • Uzmanlık

Security Intellige
Think Integrate

= IBM'in hizmet verdiği alanlar



Güvenlik Yönetişimi, Risk ve Mevzuata Uygunluk

SIEM (Güvenlik Zekası, Kurumsal Olarak Mevzuata Uygunluk)

Kimlik ve Erişim Yönetimi

Kimlik Yönetimi

Erişim Yönetimi

Veri Güvenliği

Veri Kaybının Önlenmesi

şifreleme ve Anahtar Yaşam Çevrimi Yönetimi

İleti Sistemi Güvenliği

E-posta Güvenliği

Veritabanı İzleme ve Koruma

Veri Gizleme

Uygulama Güvenliği

Uygulama Güvenlik Açığı Taraması

Web Uygulaması Güvenlik Duvarı

Uygulama Kaynak Kodu Taraması

Web / URL Adresi Süzme

Erişim ve Yetki Yönetimi

Hizmet Odaklı Mimari Güvenliği

Altyapı Güvenliği

Güvenlik Açığı Değerlendirmesi

Anabilgisayar Güvenliği

Tehdit Değerlendirmesi

Web / URL Adresi Süzme

İzinsiz Giriş Önleme Sistemi

Güvenlik duvarı, IDS/IPS, MFS, Uç Noktası Yönetimi

Güvenlik Olayı Yönetimi

Sanal Sistem Güvenliği

- ✓ X-Force Araştırma ve Geliştirme
- ✓ T.J. Watson ve diğer 8 güvenlik araştırmalar merkezi
- ✓ IBM Kassel içerik güvenliği ekibi
- ✓ Yönetilen Güvenlik Hizmetleri
- ✓ 11 merkezde 2.000'den fazla güvenlik mühendisi

IBM Research

Dünya Çapında Yönetilen Güvenlik Hizmetleri Kapsamı

- Sözleşme kapsamındaki 20.000'den fazla aygıt
- Tüm dünyada 3.700'den fazla yönetilen güvenlik hizmetleri müşterisi
- Her gün yönetilen 9 milyardan fazla olay
- 1.000'den fazla güvenlik patenti*
- 133 izlenen ülke (yönetilen güvenlik hizmetleri)

Güvenlik Operasyonları Merkezleri

Güvenlik Araştırmaları Merkezleri

Güvenlik Çözümü Geliştirme Merkezleri

İleri Güvenlik Dalları Enstitüsü

IBM İleri Güvenlik Enstitüsü

Siber güvenlik inovasyonuna ve işbirliğine olanak sağlıyor

Analiz edilen 10 milyar Web sayfası ve görüntü
Günde 150 milyon izinsiz giriş girişimi
40 milyon istenmeyen posta ve e-dolandırıcılık
46 bin belgelenmiş güvenlik açığı
Milyonlarca özgün kötü niyetli yazılım örneği

X FORCE

Riskleri Yönetebilmek

Security Intelligence.
Think Integrated.

Figure 42. Time between initial compromise and discovery – LARGER ORGS

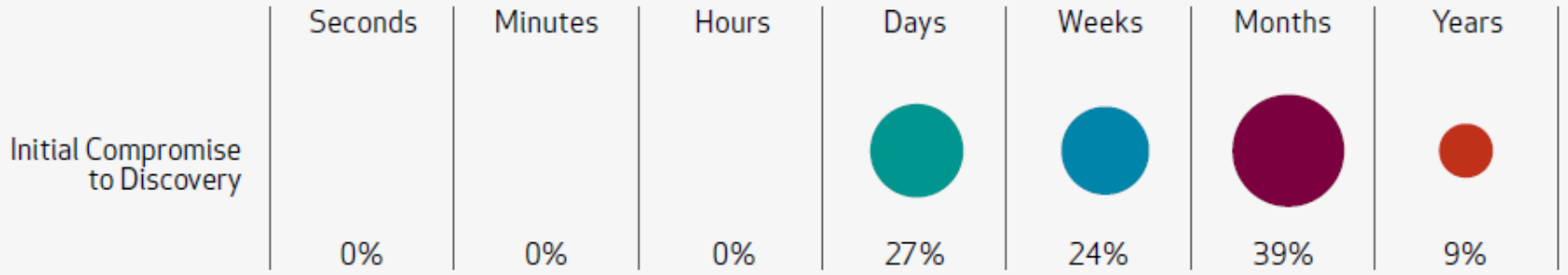
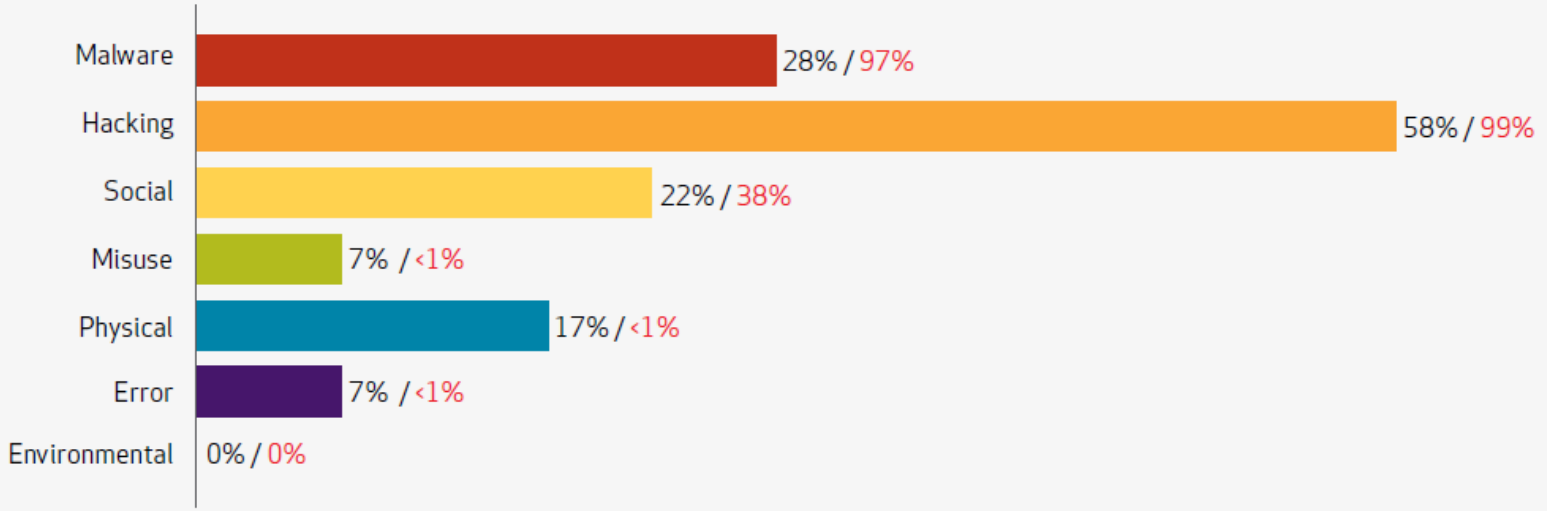


Figure 18. Threat action categories by percent of breaches and percent of records – LARGER ORGS



Charts from Verizon 2012Investigative Response Caseload Review

Security Intelligence.
Think Integrated.

IBM Security QRadar

QRadar:

- Ekim 2011 yılında IBM Ailesine katıldı
- IBM Security Systems

Ödüllü Çözüm:

- Yeni nesil Log Management, SIEM, Risk Management, security intelligence çözümleri
- Gartner raporlarında 2009 yılından bu yanı lider tarafta

Gelişim:

- +3000 müşteri, North America, EMEA and Asia Pacific ve dünyaya yayılmakta
- XForce entegrasyonu ile yazılım açıkılıkları, malware, spam, phishing, web-bazlı saldırılar ve genel siber aktiviteler

Gartner
Magic Quadrant

Security Intelligence.
Think Integrated.

Müşteri deneyimleri

Major Electric Utility	Detecting threats	• Discovered 500 hosts with “Here You Have” virus, which other solutions missed
Fortune 5 Energy Company	Consolidating data silos	• 2 Billion logs and events per day reduced to 25 high priority offenses
Branded Apparel Maker	Detecting insider fraud	• Trusted insider stealing and destroying key data
$100B Diversified Corporation	Predicting risks against your business	• Automating the policy monitoring and evaluation process for configuration change in the infrastructure
Industrial Distributor	Addressing regulatory mandates	• Real-time extensive monitoring of network activity, in addition to PCI mandates

Security Intelligence.
Think Integrated.

Güvenlik Zekası Zaman Çizelgesi

What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?

Vulnerability — PREDICTION / PREVENTION PHASE — Exploit — REACTION / REMEDIATION PHASE — Remediation

Pre-Exploit

Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

Post-Exploit

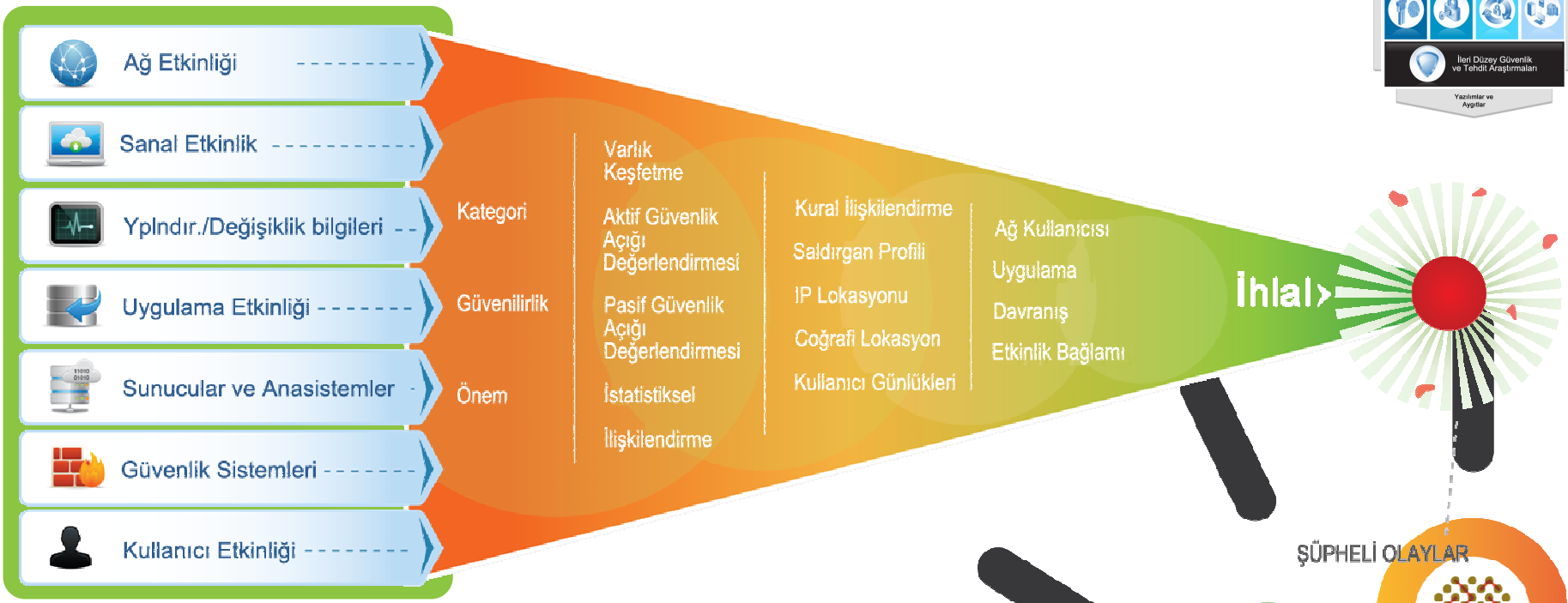
Reaction & Remediation

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
Security Information and Event Management.
Log Management. Incident Response.

Radar

Security Intelligence.
Think Integrated.

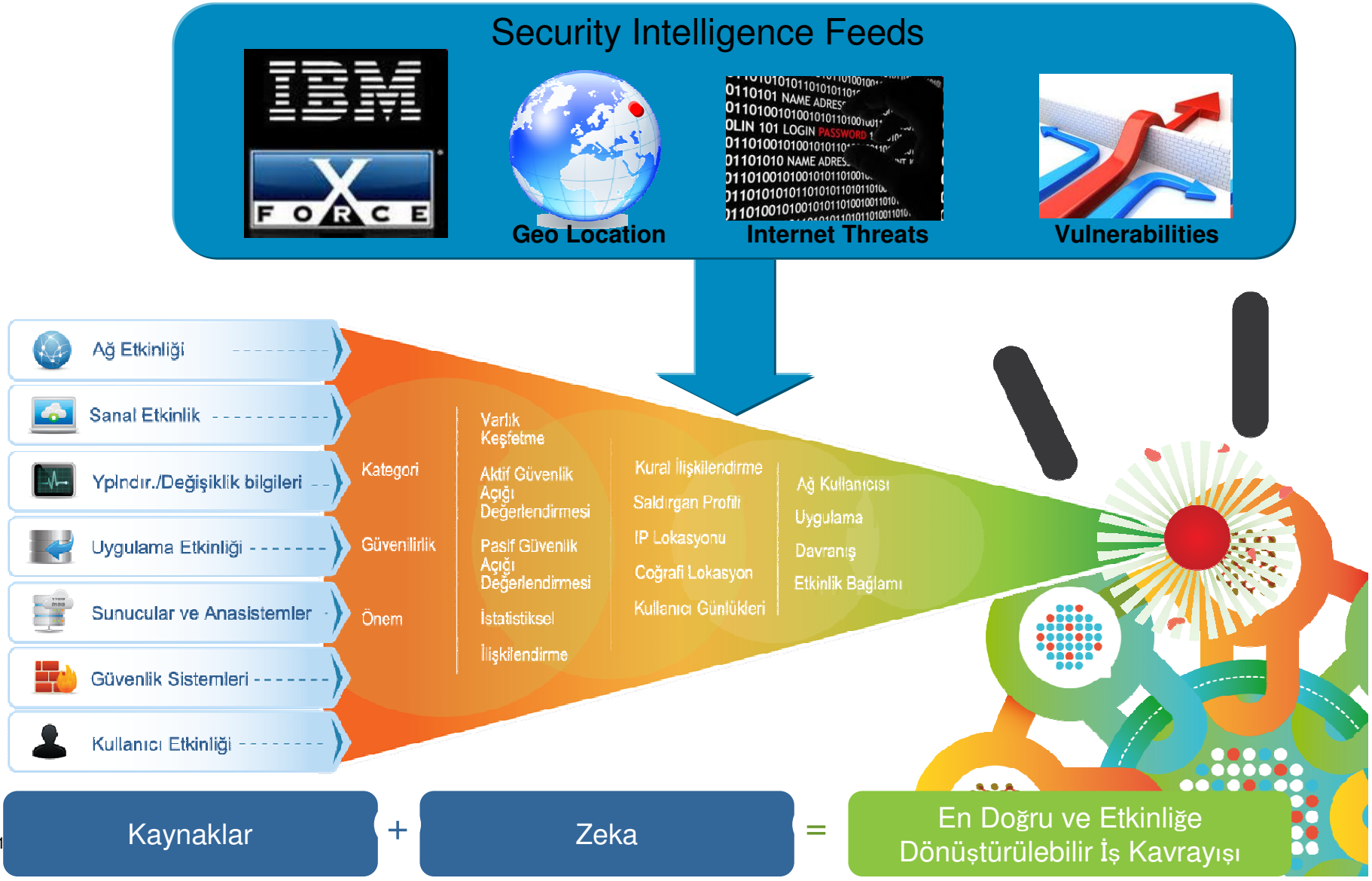
İş Akışında neler oluyor?



Kaynaklar + Zeka = En Doğru ve Etkinliğe Dönüştürülebilir İş Kavrayışı

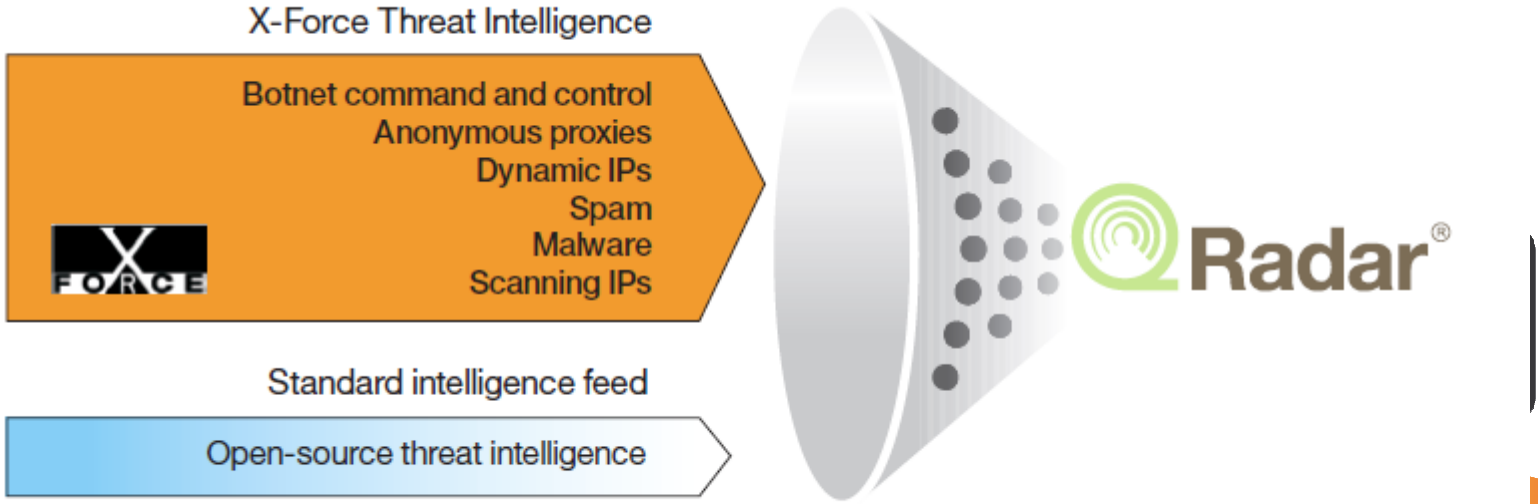
Security Intelligence.
Think Integrated.

Etkinliği Artıran Yaklaşım



Security Intelligence.
Think Integrated.

X-Force Verileri ve QRadar



X-Force Threat Intelligence:

- Son yenilikleri
- In-house analitikleri
- Güven derecesi
- Karşılaştırmalı Kapsam

Security Intelligence.
Think Integrated.

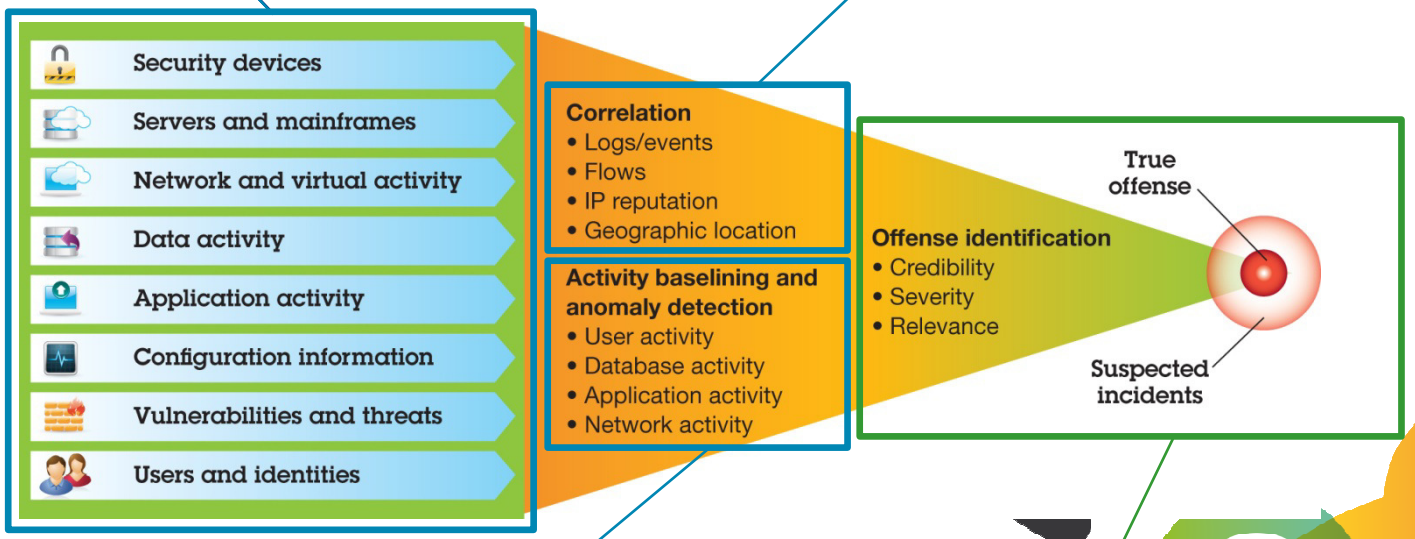
Atak Evreleri

Herşeyi İzleme

Loglar, ağ trafik akışı, kullanıcı aktiviteleri

Akıllı İlişkilendirme

Farklı aktiviteleri birleştirme



Anomalileri Saptama

Gizli davranışlar

Aksiyon için önceliklendirme

Security Intelligence.
Think Integrated.

Konumlandırma Mimarisi

Log Management	QRadar Log Manager 	• Turn-key log management and reporting • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	QRadar SIEM 	• Log, flow, vulnerability & identity correlation • Sophisticated asset profiling • Offense management and workflow
Configuration & Vulnerability Management	QRadar Risk Manager 	• Network security configuration monitoring • Vulnerability prioritization • Predictive threat modeling & simulation
Network Activity & Anomaly Detection	QRadar SIEM  QRadar QFlow 	• Network analytics • Behavioral anomaly detection • Fully integrated in SIEM
Network and Application Visibility	QRadar QFlow  QRadar VFlow 	• Layer 7 application monitoring (Nteflow) • Content capture for deep insight & forensics • Physical and virtual environments
Scale		• Event Processors • Network Activity Processors • High Availability & Disaster Recovery • Stackable Expansion

Security Intelligence. **Tek bir arayüz**

Think Integrated

- Log Management
- SIEM
- Configuration & Vulnerability Management
- Network Activity & Anomaly Detection
- Network and Application Visibility

One Console Security

Built on a Single Data Architecture

Security Intelligence.
Think Integrated.

Derinlemesine Güvenlik

IBM X-Force® Threat Information Center

Real-time Security Threats and Prioritized 'Offenses'

Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

Security Intelligence.
Think Integrated.

IBM Güvenlik Portfoyü

Guardium Database Security

AppScan Application Security

X-Force Threat Intelligence

Network Activity
Virtual Activity
Config/Change Info
Application Activity
Servers & Hosts
Security Systems
User Activity

Category
Credibility
Severity

Asset Discovery
Active Vulnerability Assessment
Passive Vulnerability Assessment
Statistical

Rules Corelation
Attacker Profile
IP Location
Geo Location
User Logs

Network User
Application
Behavior
Activity Context

Offense

TEM Endpoint Security

ISS Network Security

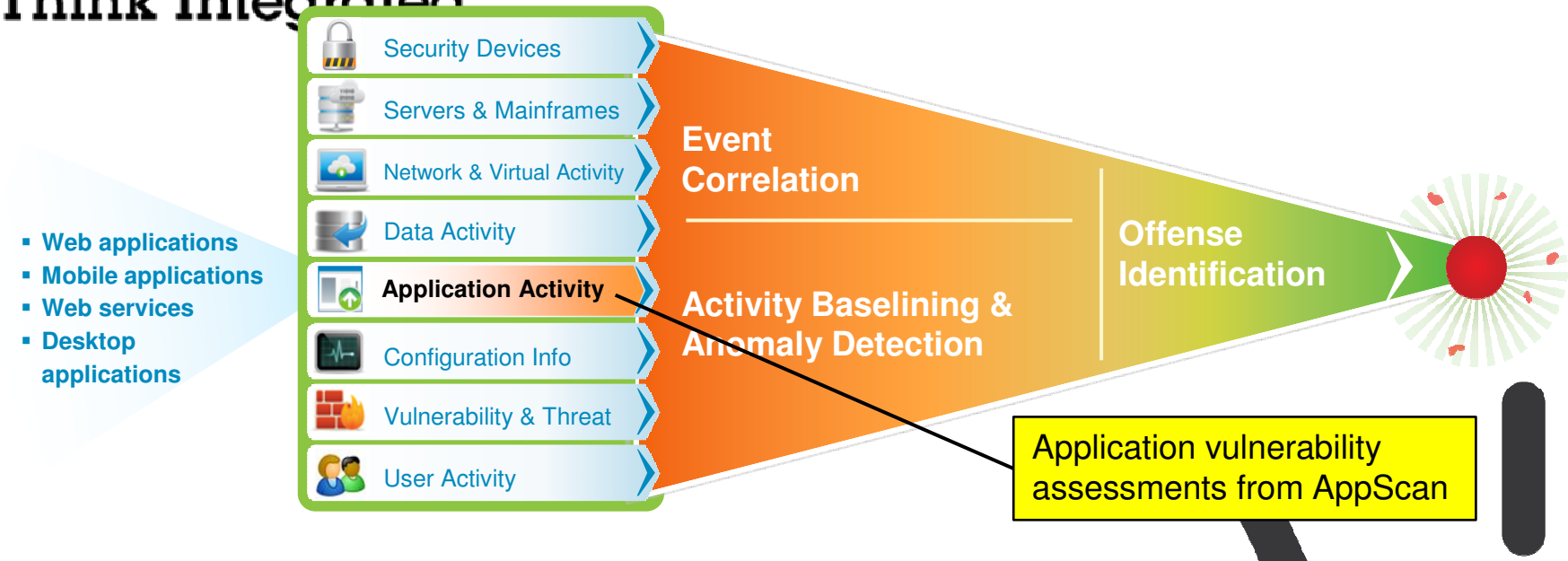
IAM Identity Security

SUSPECTED INCIDENTS

Sources + Intelligence = Most Accurate & Actionable Insight

Security Intelligence.
Think Integrated

AppScan & QRadar



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- Strengthens threat detection and offense scoring capabilities
- Correlates known application vulnerabilities with other real-time events and alerts to elevate meaningful offenses
- Enhances proactive risk management assessments by prioritizing critical application vulnerabilities

Security Intelligence.
Think Integrated

InfoSphere Guardium & QRadar

- Databases
- Data Warehouses
- Hadoop based systems
- File shares

Security Devices
Servers & Mainframes
Network & Virtual Activity
Data Activity
Application Activity
Configuration Info
Vulnerability & Threat
User Activity

Event Correlation

Activity Baselining & Anomaly Detection

Offense Identification

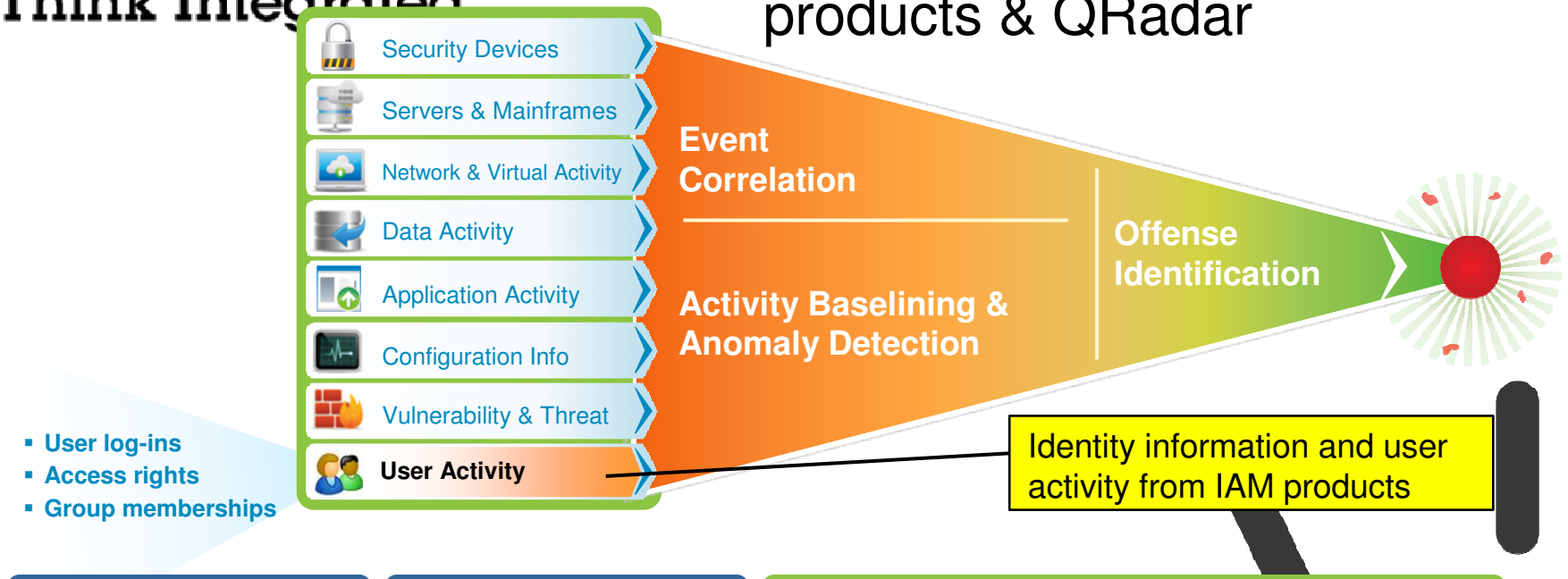
In-depth data activity monitoring and security insights from InfoSphere Guardium

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- Detects anomalistic behavior and malicious access to sensitive data
- Focuses customers on key data access events coming from InfoSphere Guardium while saving operational costs by not transmitting and storing insignificant events
- Provides broader, enterprise network security context for InfoSphere Guardium alerts and events helping identify advanced threats
- Improves compliance reporting with automated data access reports

Security Intelligence.
Think Integrated

Identity & Access Management products & QRadar

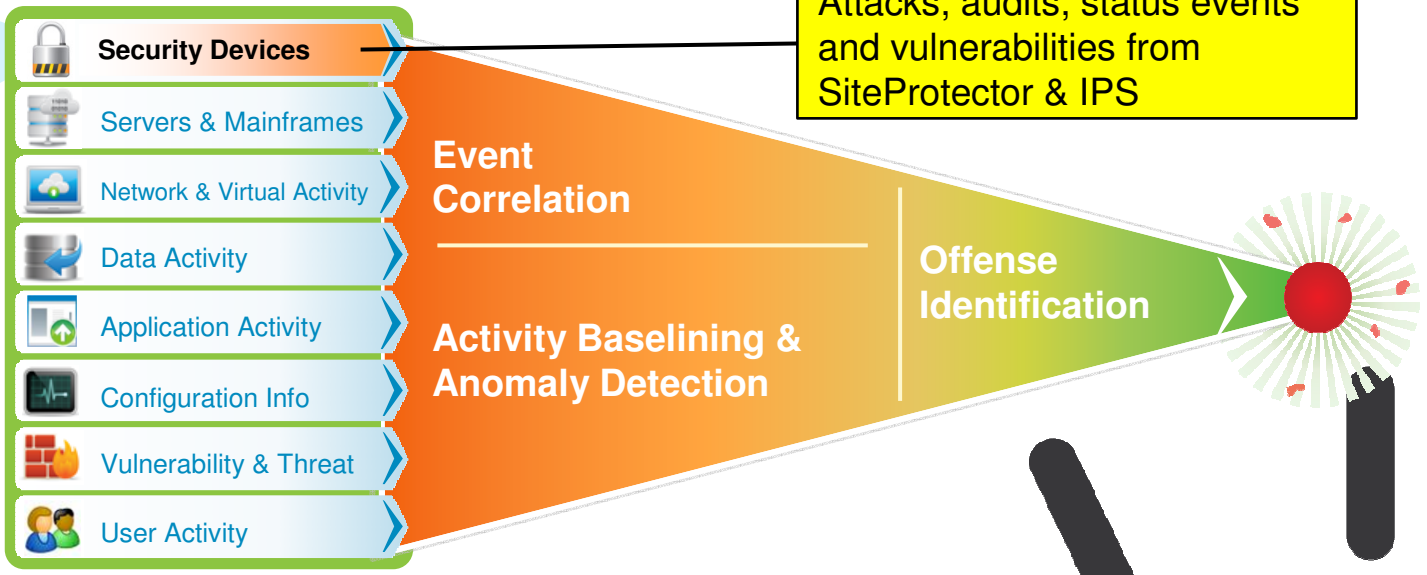


- Provides ability to insert user names into reference sets used for writing searches, reports, and rules
- Improves ability to defend against insider threats involving privilege escalations or inappropriate data access
- Facilitates compliance reporting by pairing user identities with access to sensitive data

Threat Protection & QRadar

Security Intelligence.
Integrated.

- Networks
- Servers
- Endpoints
- Applications
- Scanners



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- Helps find threats other SIEMs might miss by combining Network Protection's Protocol Analysis Module signature analysis and QRadar's anomaly detection capabilities
- Enables immediate real-time threat awareness and powerful threat and offense prioritization capabilities to establish definitive evidence of attack and visibility into all attacker communications
- Integrates X-Force security content
- Outstanding coverage available within full SIEM solution or targeted Network Anomaly Detection offering

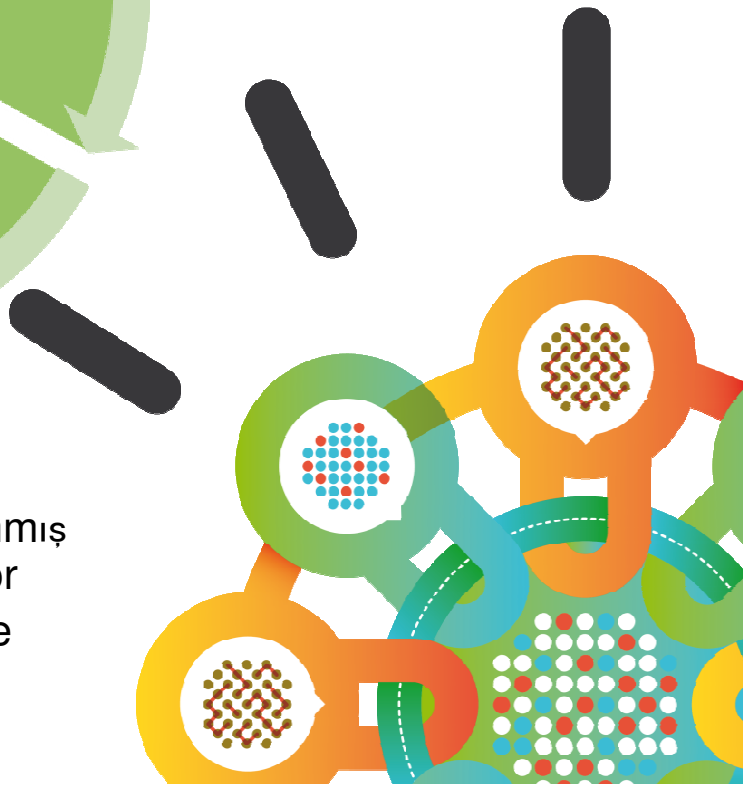
Security Intelligence.
Think Integrated.

Otomatikleştirilmiş: Ek personel gerektirmez

- Günlük kaynaklarının, uygulamaların ve varlıkların otomatik olarak keşfedilmesi
- Otomatik varlık gruplandırma
- Merkezileştirilmiş günlük yönetimi
- Otomatikleştirilmiş yapılandırma denetimleri

- Varlık tabanlı öncelik belirleme
- Otomatik tehdit güncelleme
- Otomatik müdahale
- Yönlendirilen iyileştirme

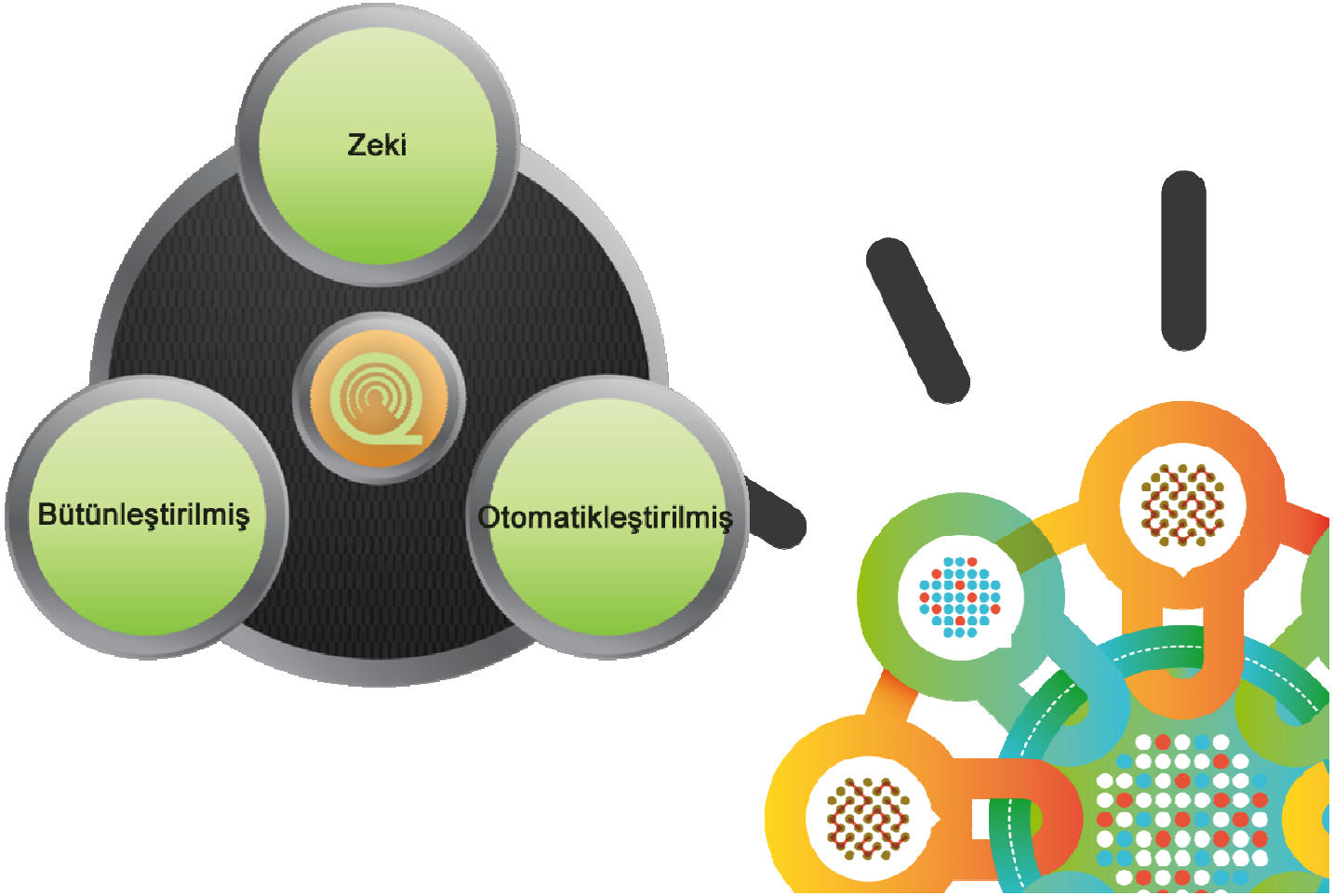
- Otomatik ayar
- Otomatik tehdit algılama
- Binlerce önceden tanımlanmış kural ve görev tabanlı rapor
- Kullanımı kolay olay süzme
- Gelişmiş güvenlik analitiği



Security Intelligence.
Think Integrated.

IBM Security QRadar:

Zeki, Bütünleştirilmiş, Otomatikleştirilmiş Güvenlik Zekası Platformu



Security Intelligence.
Think Integrated.

QRadar

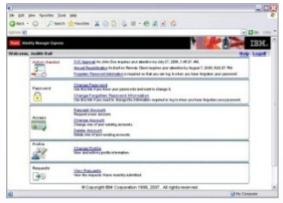
X-FORCE

Correlate new threats based on X-Force IP reputation feeds

Hundreds of 3rd party information sources

Guardium

Database assets, rule logic and database activity information



Identity and Access Management

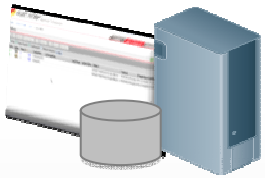
Identity context for all security domains w/ QRadar as the dashboard

Tivoli Endpoint Manager

Endpoint Management vulnerabilities enrich QRadar's vulnerability database

IBM Security Network Intrusion Prevention System

Flow data into QRadar turns NIPS devices into activity sensors



AppScan Enterprise

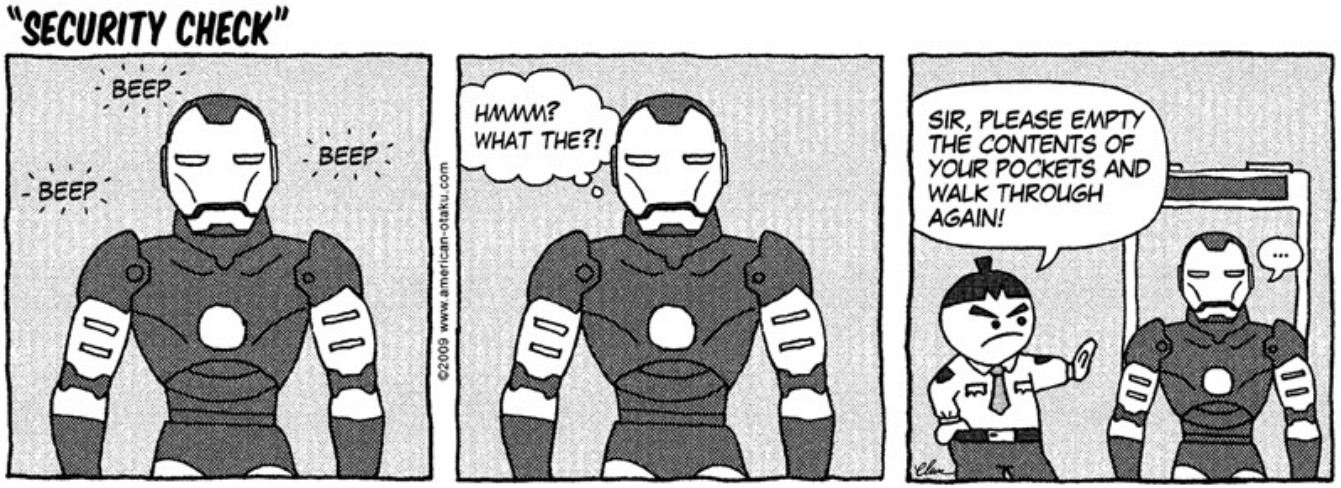
AppScan vulnerability results feed QRadar SIEM for improved asset risk assessment

Security Intelligence.
Think Integrated.

QRadar Tercih Etmenin En Önemli Nedenleri

1. En zeki, bütünleştirilmiş ve otomatikleştirilmiş çözüm
2. En gelişmiş tehdit analitiği ve mevzuata uygunluk otomasyonu
3. Az sayıda personel gereksinimi ile kısa değer elde etme süresi
4. Sistemler ve güvenlik verileri arttıkça kolaylıkla ölçeklenir
5. Köklü pazar liderliği ve mükemmel destek
6. En iyi kanal ilişkileriyle desteklenen birlikte iş yapma kolaylığı
7. IBM'in rakipsiz güvenlik uzmanlığı ve bütünleştirilmiş yeteneklerinin çeşitliliği

Securit
Think



TEŞEKKÜRLER

Nurettin Erginöz
Client Technical Professional, CoP
CEE&Türkiye, IBM Security Systems
ERGINOZ@tr.ibm.com