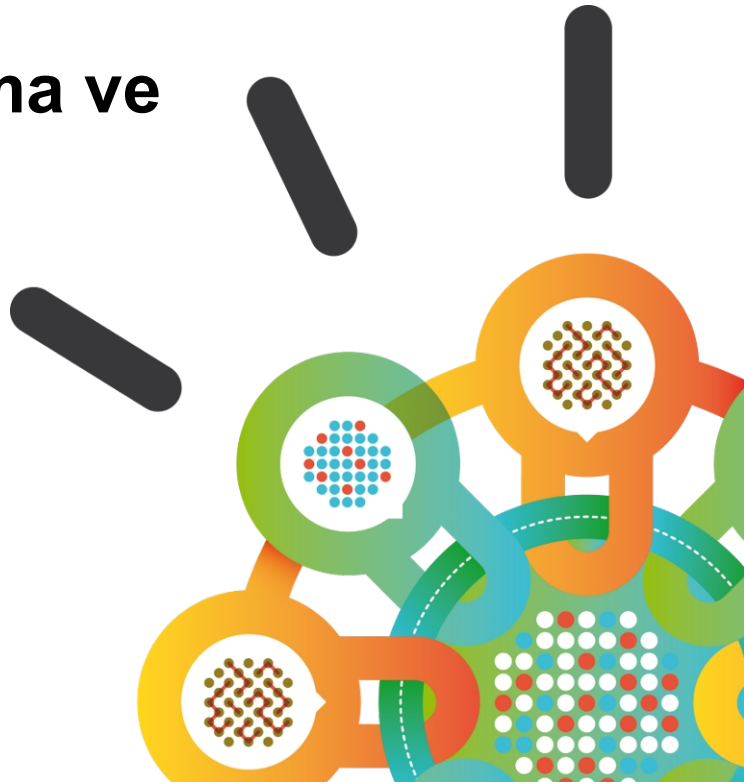
Security Intelligence.
Think Integrated.

IBM Güvenlik Sistemleri

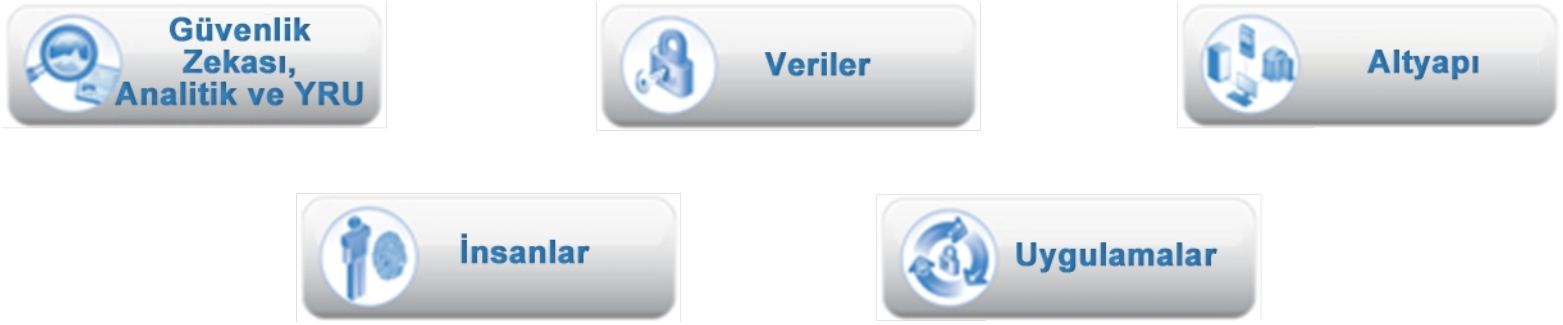
Yeni Nesil Güvenlik Bilgisi Toplama ve Olay Yönetimi

6 Aralık 2012



Gündem

- ✓ Günümüzde BT güvenliği gereksinimi
- ✓ IBM güvenlik çerçevesi



- ✓ QRadar: Yeni Nesil Güvenlik Bilgisi Toplama ve Olay Yönetimi

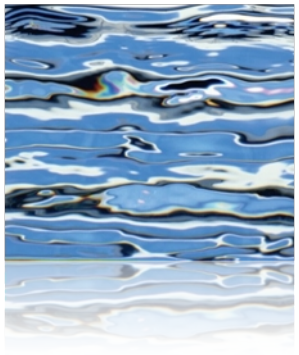
Dünya giderek daha donanımlı, birbiriyle bağlantılı ve zeki hale geliyor

Akıllı Tedarik Zincirleri

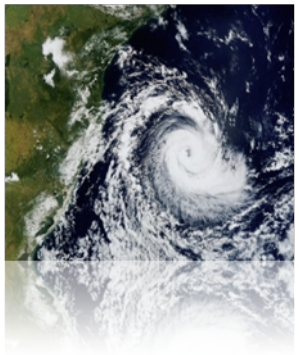
Akıllı Ülkeler

Akıllı Perakendecilik

Akıllı Su Yönetimi



Akıllı Hava



Akıllı Enerji Şebekeleri

DONANIMLI

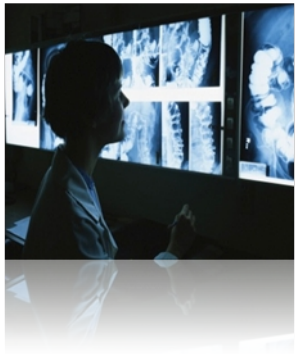
BİRBİRİYLE BAĞLANTILI

ZEKİ

Akıllı Petrol Sahası Teknolojileri

Akıllı Bölgeler

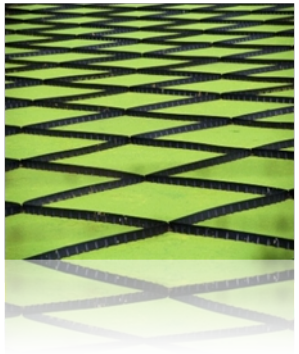
Akıllı Sağlık Hizmetleri



Akıllı Trafik Sistemleri

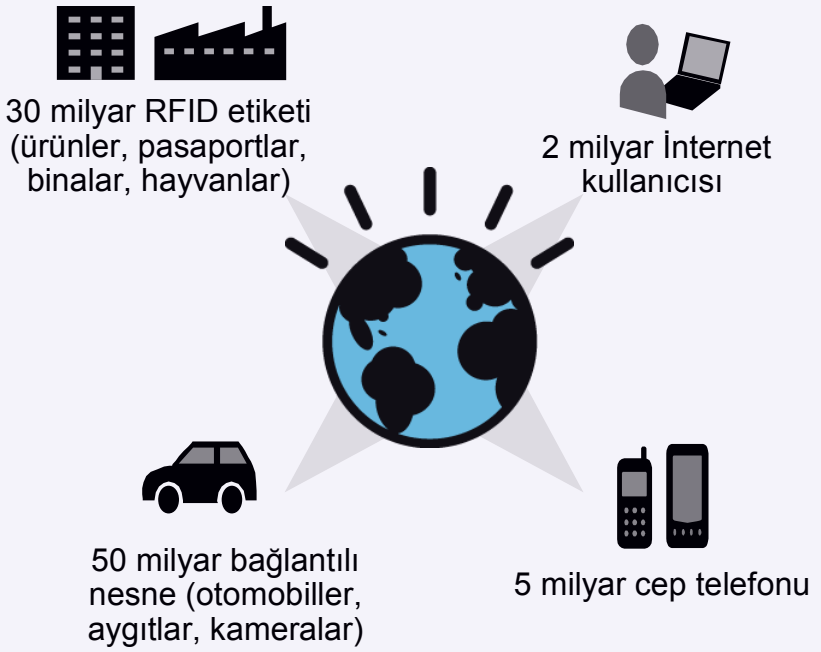
Akıllı Şehirler

Akıllı Gıda Sistemleri

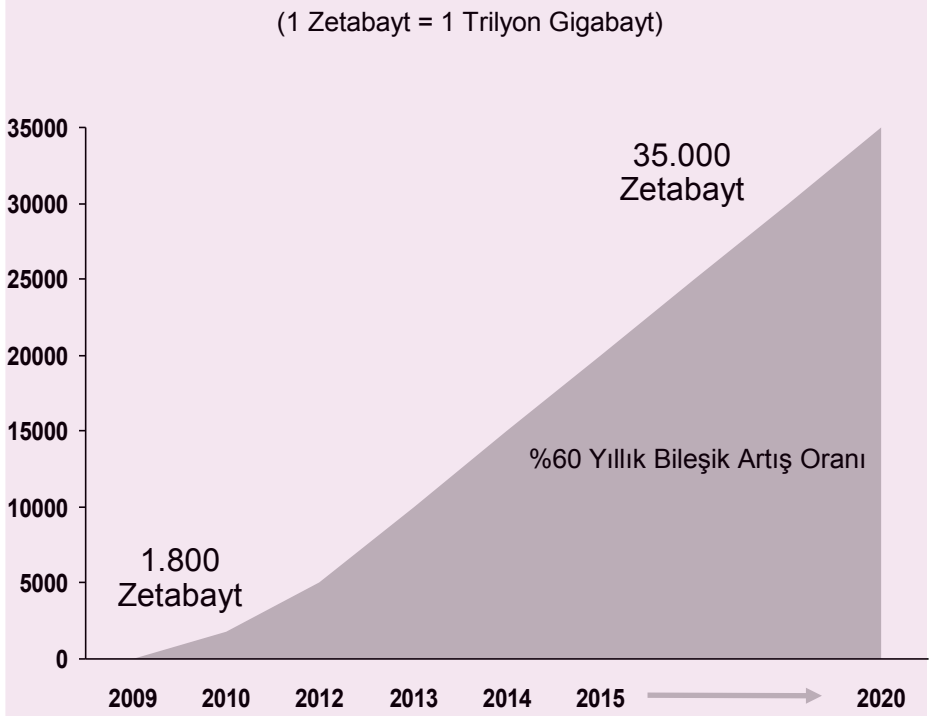


Bununla birlikte daha fazla hedef ve güvenlik açığı ortaya çıkıyor

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

... ve üst düzey yönetici önceliklerini etkilemektedir

	Yönetim Kurulu Başkanı	Finans/Operasyon Yöneticisi	Bilgi Teknolojileri Yöneticisi	İK 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

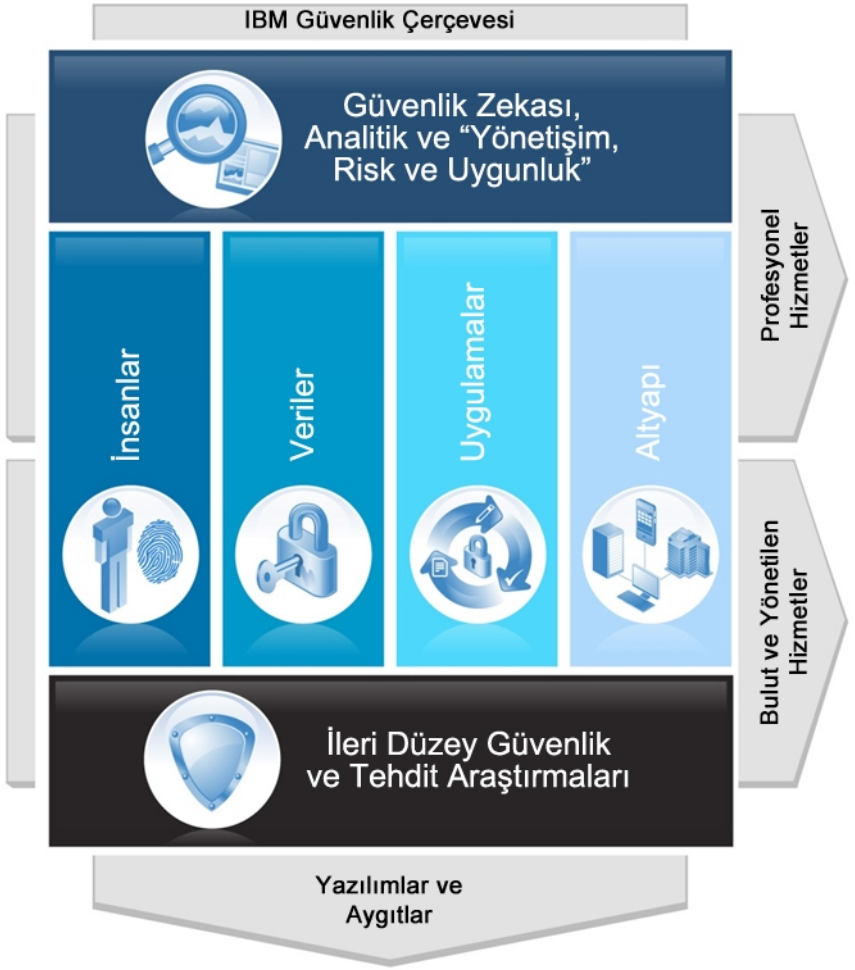
*Kaynak: IBM Üst Düzey Yönetici Araştırmaları Serisi kapsamında 13.000'den fazla üst düzey yönetici ile yapılan görüşmeler

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



QRadar: Tamamen Bütünleştirilmiş Güvenlik Zekası

Günlük Yönetimi

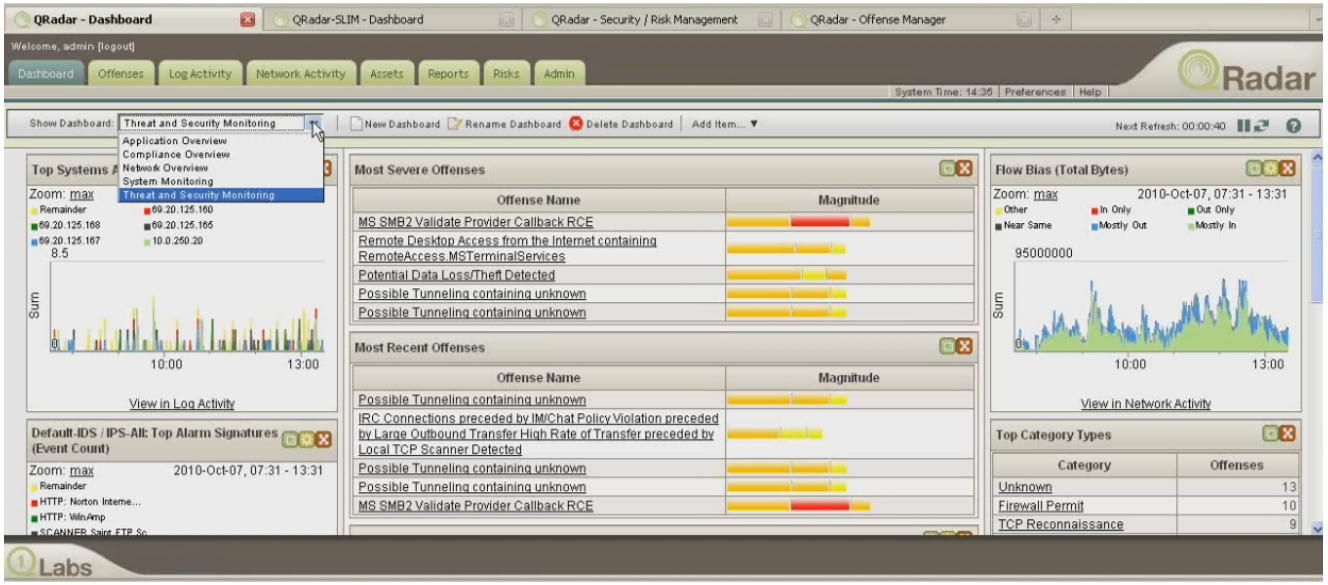
Güvenlik Bilgileri ve Olay Yönetimi

Risk Yönetimi

Ağ Etkinliği ve Anormallik Algılama

Ağ ve Uygulama Görünürlüğü

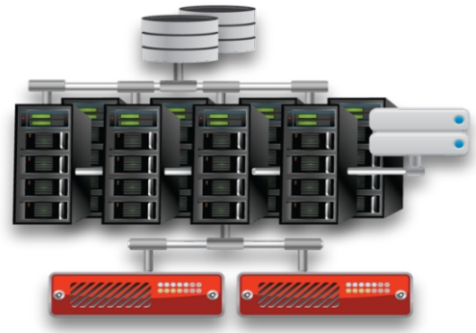
Tek Konsolla Güvenlik



Tek Veri Mimarisi Üzerine Kurulmuştur

Bütünleştirilmiş: Ölçeklendirme ve Kullanım Kolaylığı için Bütünleştirilmiş Platform

Birleştirilmiş Çözüm



- Ölçeklendirme sorunları
- Bütünleştirilmemiş raporlama ve arama
- Yerel karar yok
- Çok sayıda ürün ile yönetim
- Birbirinin kopyası günlük havuzları
  - ➢ ***İşletim darboğazları***

QRadar Bütünleştirilmiş Çözümü

- Yüksek düzeyde ölçeklenebilir
- Ortak raporlama ve arama
- Dağıtılmış ilişkilendirme
- Birleşik yönetim
- Tek kopya olarak saklanan günlükler
  - ➢ ***Tam görüş netliği***

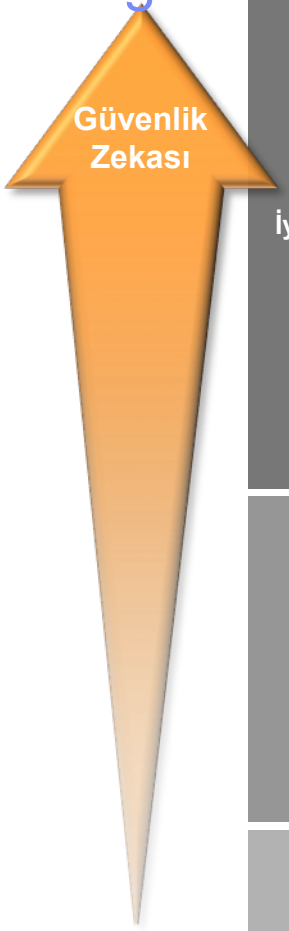
Tamamen Bütünleştirilmiş Güvenlik Zekası

Log Yönetimi	Radar Log Manager Radar Log Manager Free Edition	• Anahtar teslimi günlük yönetimi • KOBİ'lerden büyük kuruluşlara kadar • Kurumsal güvenlik bilgisi ve olayı yönetimine büyütülebilir
Güvenlik Bilgileri Toplama & Olay Yönetimi	Radar SIEM	• Bütünleştirilmiş günlük, tehdit, risk ve mevzuata uygunluk yönetimi • Gelişmiş olay analitiği • Varlık profili oluşturma ve akış analitiği • İhlal yönetimi ve iş akışı
Risk Yönetimi	Radar Risk Manager	• Tahmine dayalı tehdit modeli oluşturma ve benzetim • Ölçeklenebilir yapılandırma izleme ve denetimi • Gelişmiş tehdit görselleştirme ve etki analizi
Ağ Etkinliği ve Anormallik Algılama	Radar SIEM Radar QFlow	• Ağ analitiği • Davranışa ve anormallik algılama • Güvenlik bilgisi ve olayı yönetimi ile tam bütünleştirilmiş
Ağ ve Uygulama Görünürlüğü	Radar QFlow Radar VFlow	• Katman 7 uygulama izleme • İçerik toplama • Fiziksel ve sanal ortamlar

Müşterilemizin Q1 Labs'ı Tercih Etmesinin 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

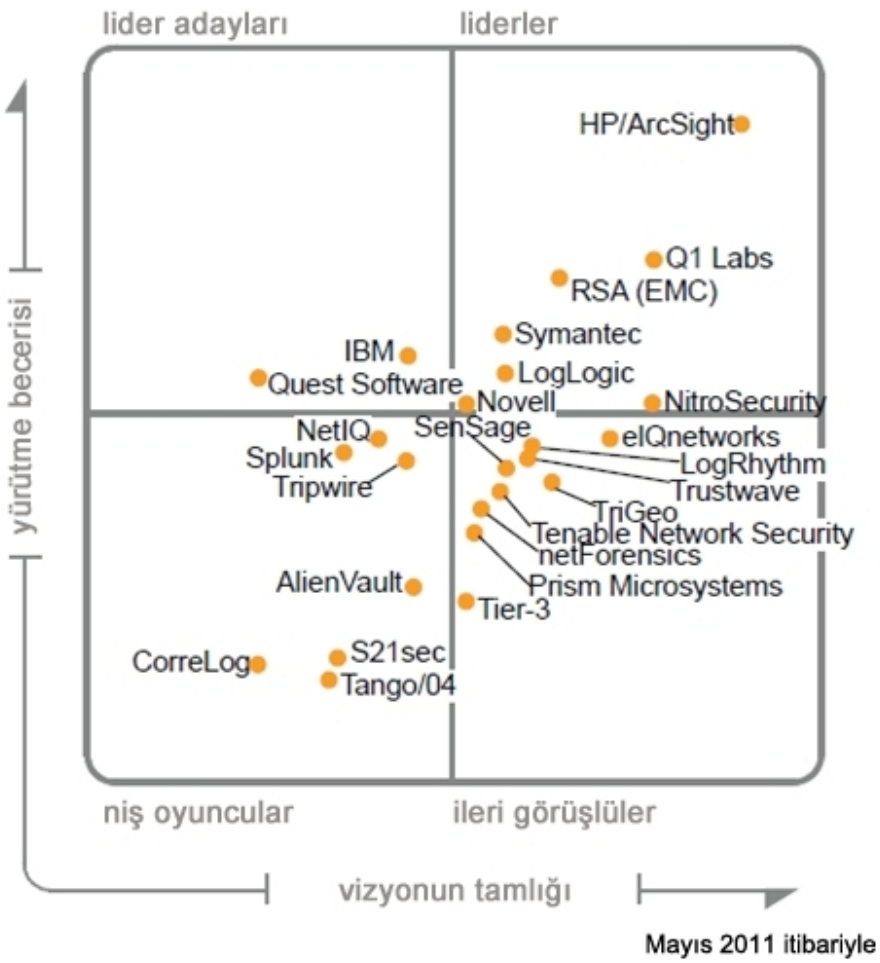
Güvenlik Zekası İyileştirilmiş Güvenliğe Doğru İlerlemeye Olanak Sağlar



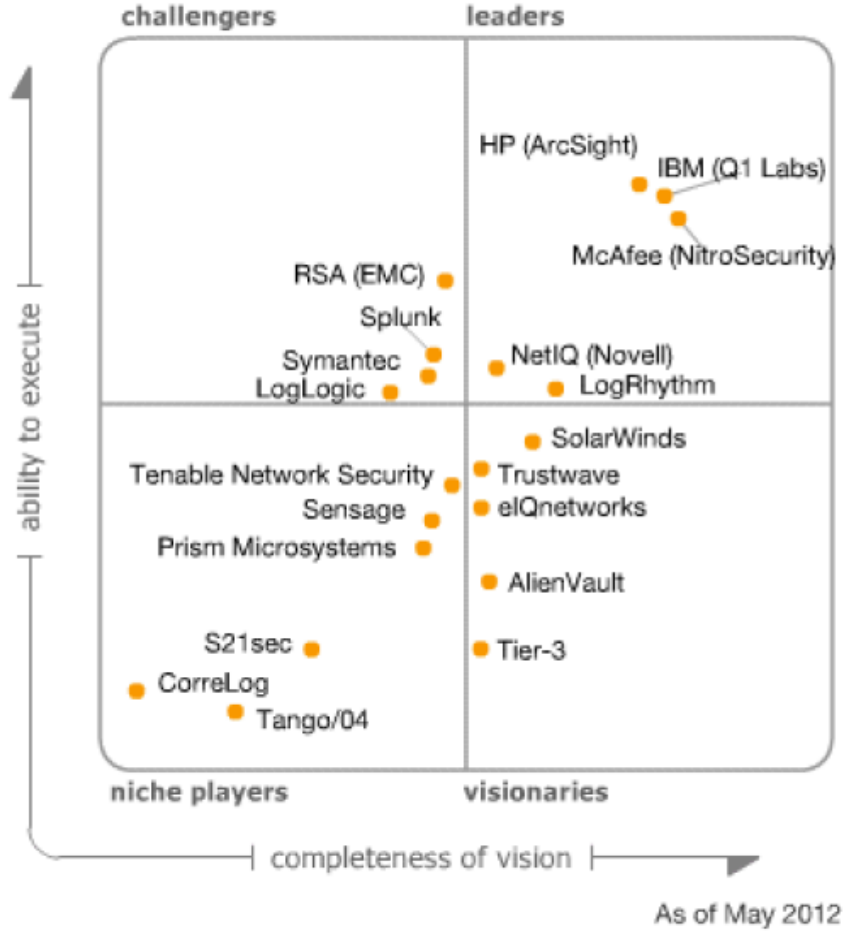
Güvenlik Zekası:
Bilgi ve olay yönetimi:
Gelişmiş ilişkilendirme ve ayrıntılı analitik
Harici tehdit araştırmaları

	İnsanlar	Veriler	Uygulamalar	Altyapı
İyileştirilmiş	- Görev tabanlı analitik - Kimlik yönetişimi - Ayrıcalıklı kullanıcı denetimleri	- Veri akışı analitiği - Veri yönetişimi	- Güvenli uygulama mühendisliği süreçleri - Dolandırıcılığın belirlenmesi	- Gelişmiş ağ izleme - Kanıt arama / veri madenciliği - Güvenli sistemler
Yetkin	- Kullanıcı yetkilendirme - Erişim yönetimi - Güçlü kimlik doğrulaması	- Erişim izleme - Veri kaybı önleme	- Uygulama güvenlik duvarı - Kaynak kodu tarama	- Sanallaştırma güvenliği - Varlık yönetimi - Uç noktası / ağ güvenliği yönetimi
Temel	- Merkezileştirilmiş dizin	- Şifreleme - Erişim denetimi	- Uygulama tarama	- Çevre güvenliği - Virüs önleme

Gartner Güvenlik Bilgisi Toplama ve Olay Yönetimi Magic Quadrant

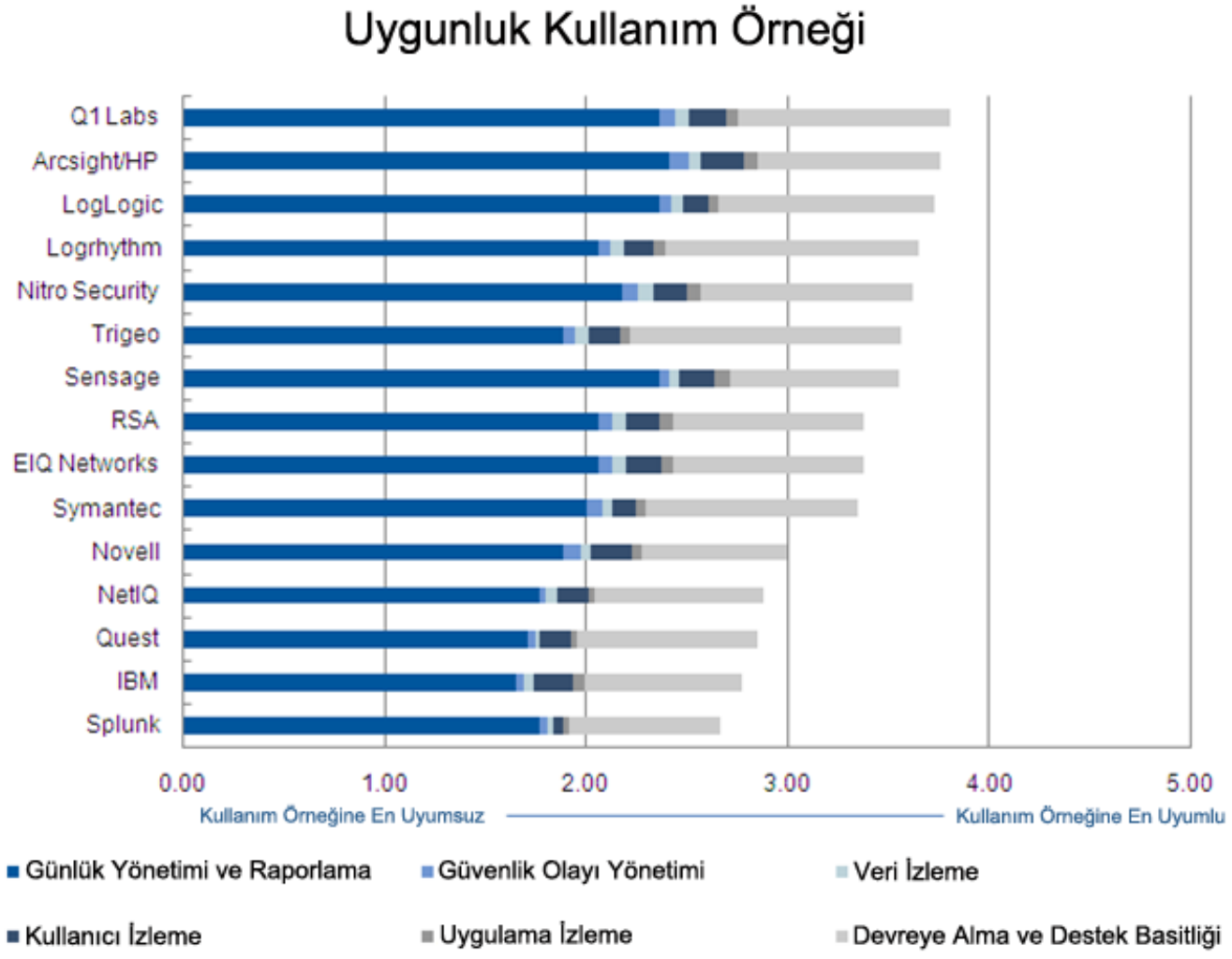


Kaynak: Gartner (Mayıs 2011)



Source: Gartner (May 2012)

Güvenlik Bilgileri Toplama ve Olay Yönetiminin (SIEM) en önemli etkeni olan mevzuata uygunlukta 1 numara



Üç başlıca kullanım örneği:
1.) Mevzuata uygunluk
2.) Tehdit yönetimi
3.) Genel devreye alma