IBM BusinessConnect
Vernetzter, intelligenter und informierter denn je

Security

IBM BusinessConnect
Vernetzter, intelligenter und informierter denn je

IBM Security Strategy

Diego Navarrete, Director, IBM Security Systems Europe

Four themes shape your world

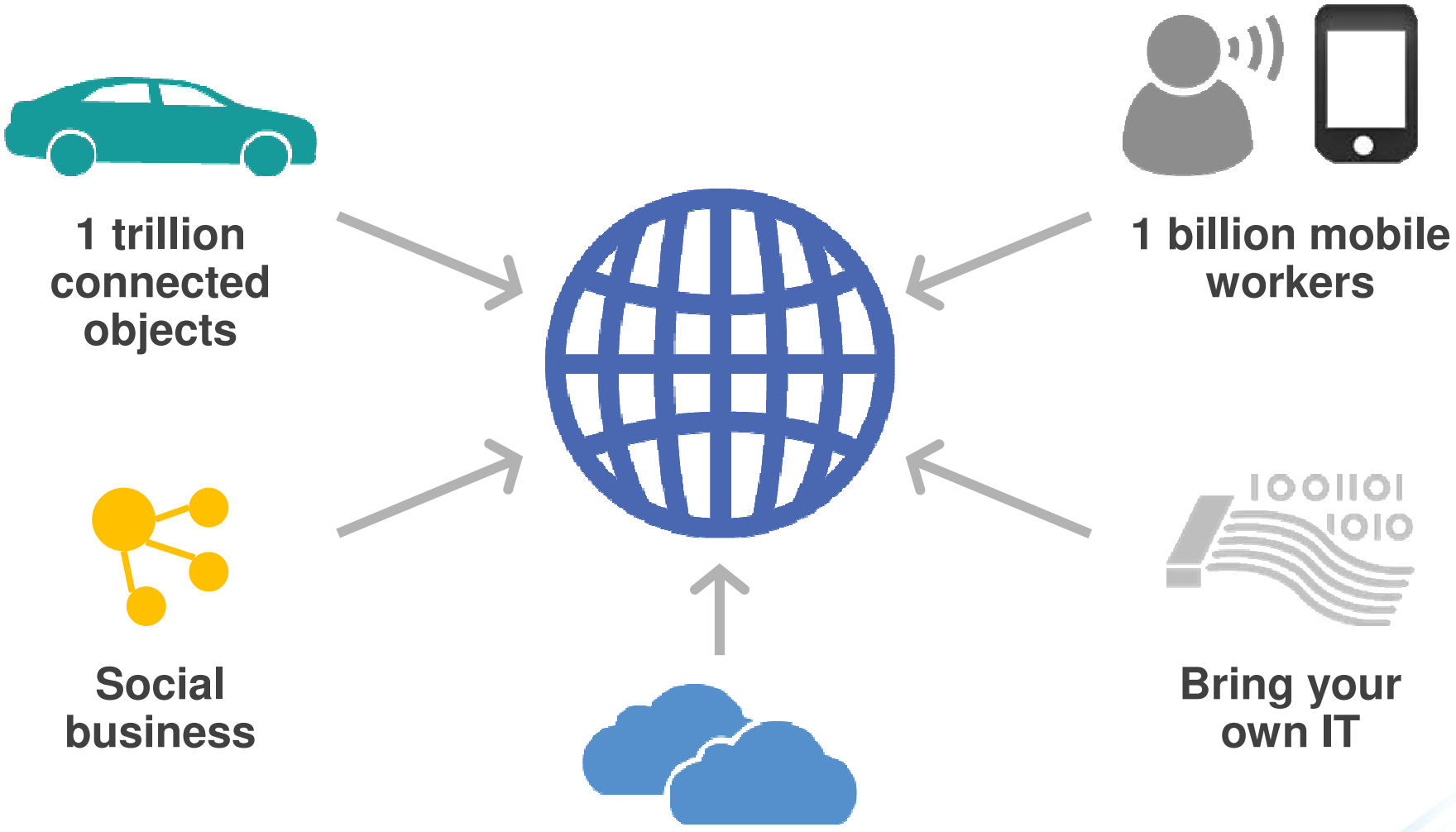
Innovative Technology

Extreme Threats

New Approach

New Leadership

Innovative technology changes everything



Motivations and sophistication are rapidly evolving

National Security

Nation-state actors
Stuxnet

Espionage, Activism

Competitors and Hacktivists
Aurora

Monetary Gain

Organized crime
Zeus

Revenge, Curiosity

Insiders and Script-kiddies
Code Red

What are we seeing? Key Findings from the 2012 X-Force Trend & Risk Report

Threats and Activity

- 40% increase in breach events for 2012
- Sophistication is not always about technology
- SQL Injection, DDoS, Phishing activity increased from 2011
- Java means to infect as many systems as possible

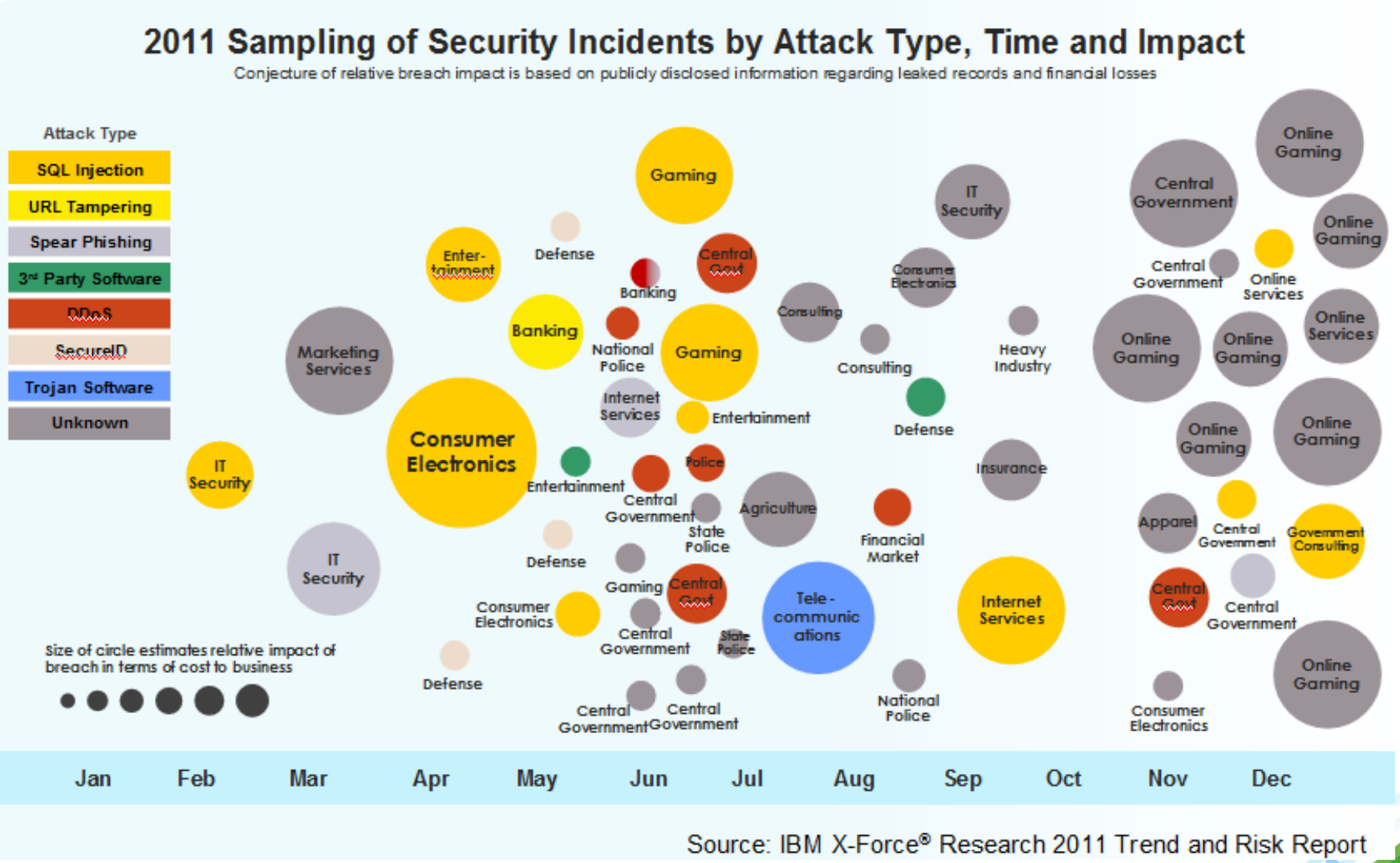
Operational Security

- Software vulnerability disclosures up in 2012
- Web application vulnerabilities surge upward
- XSS vulnerabilities highest ever seen at 53%
- Content Management Systems plug-ins provide soft target

Emerging Trends

- Social Media leveraged for enhanced spear-phishing techniques and intelligence gathering
- Mobile Security should be more secure than traditional user computing devices by 2014

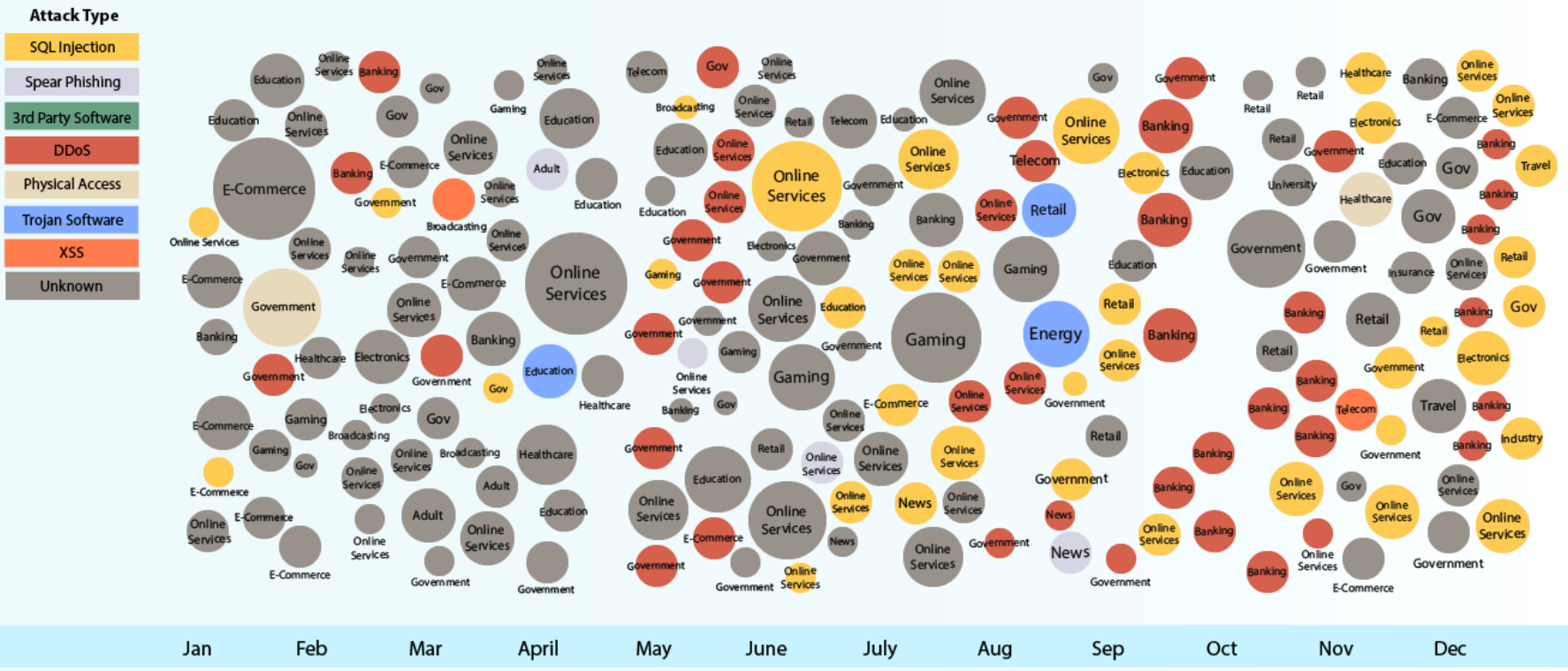
2011: The year of the targeted attack



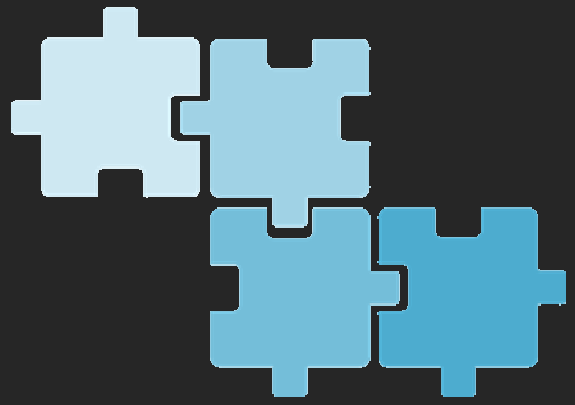
2012: The explosion of the breach continues!

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

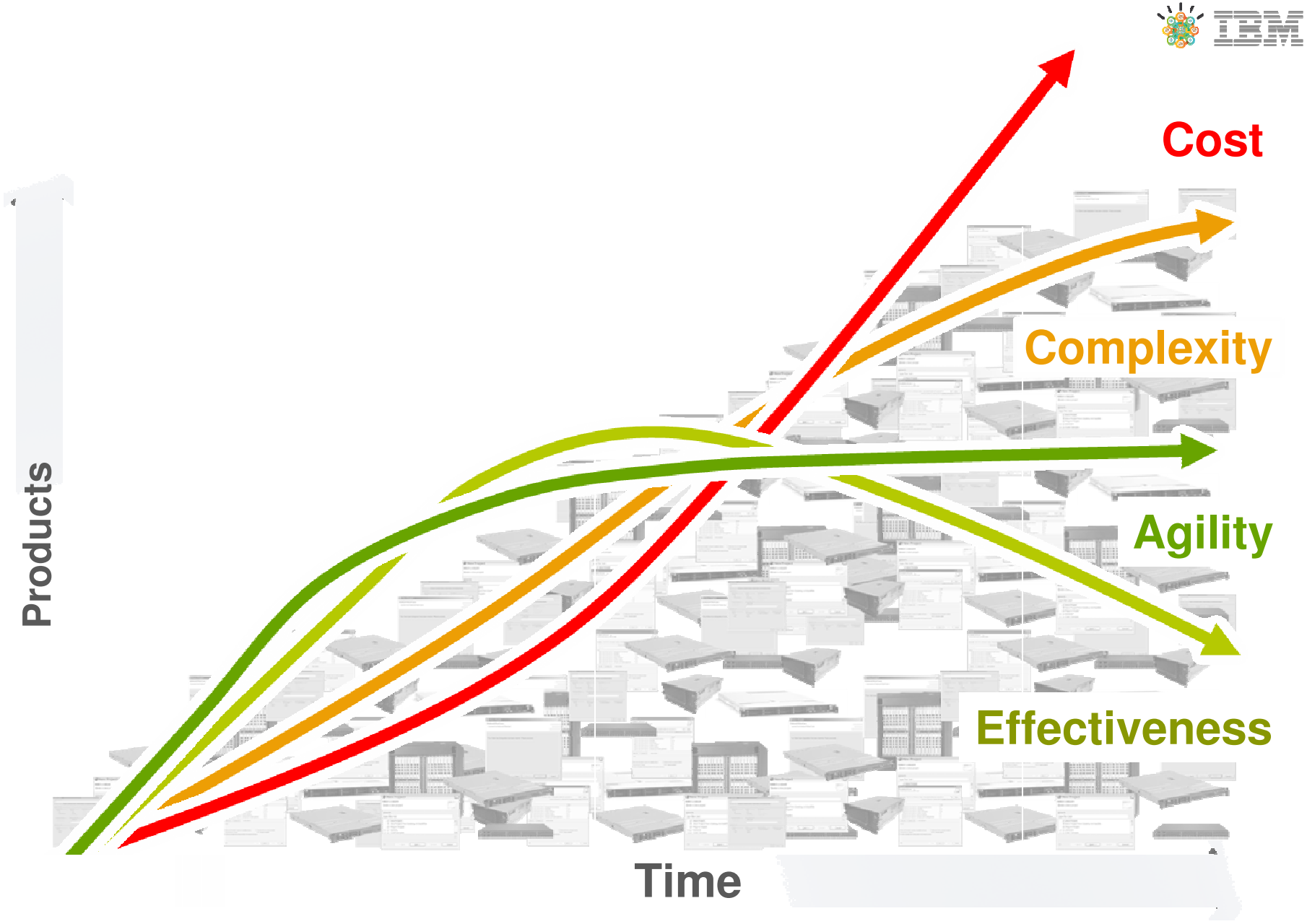


Source: IBM X-Force® Research 2012 Trend and Risk Report



How do we solve this?


Products
Time


Cost
Complexity
Agility
Effectiveness
Products
Time

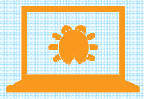
Your security team sees noise

They've been focusing on securing infrastructure...

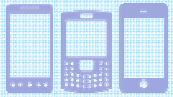
Infrastructure

Datacenters

PCs



Laptops

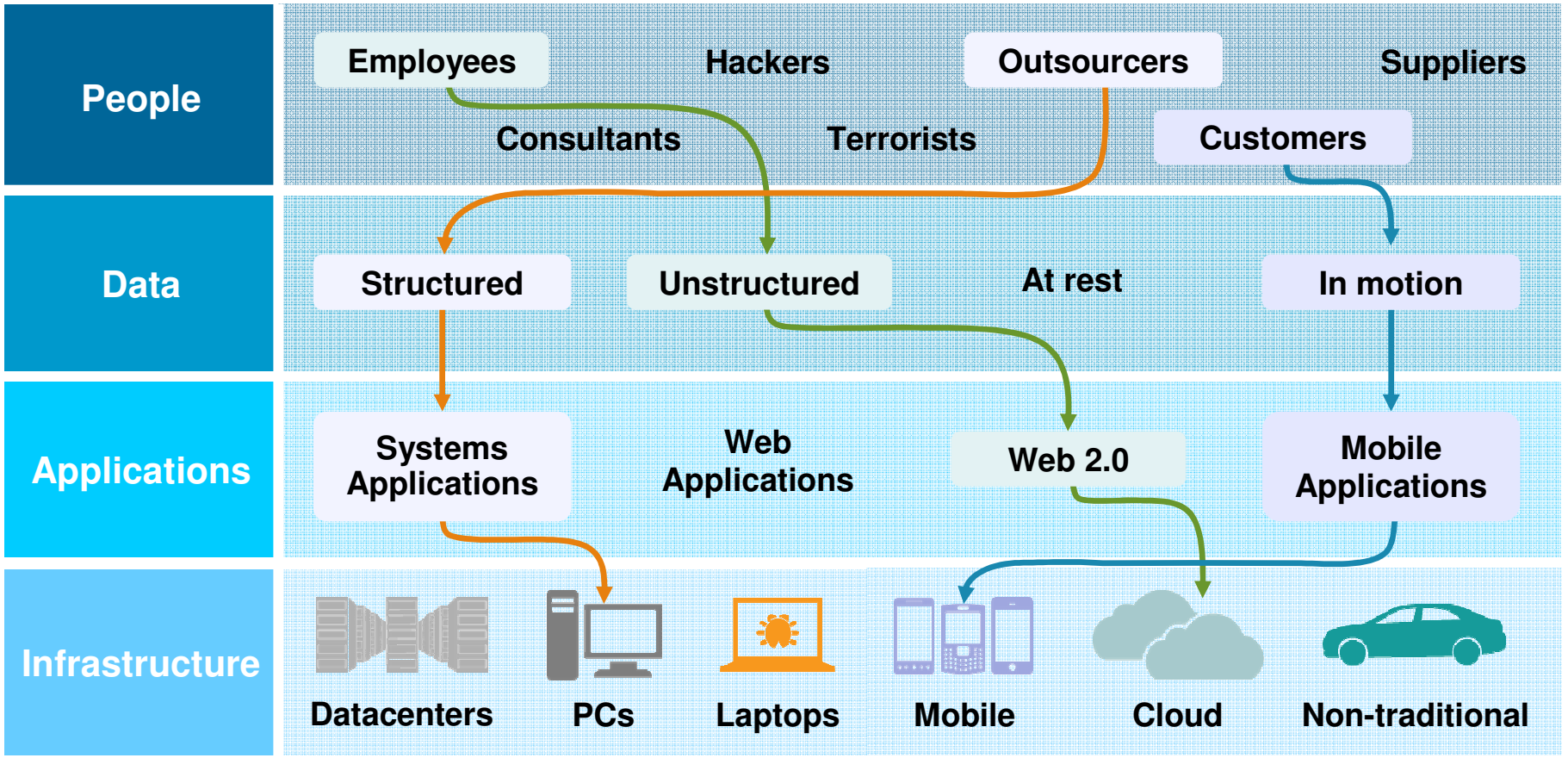


Mobile

Cloud

Non-traditional

They've been focusing on securing infrastructure...



but security challenges are a complex, four dimensional puzzle

People

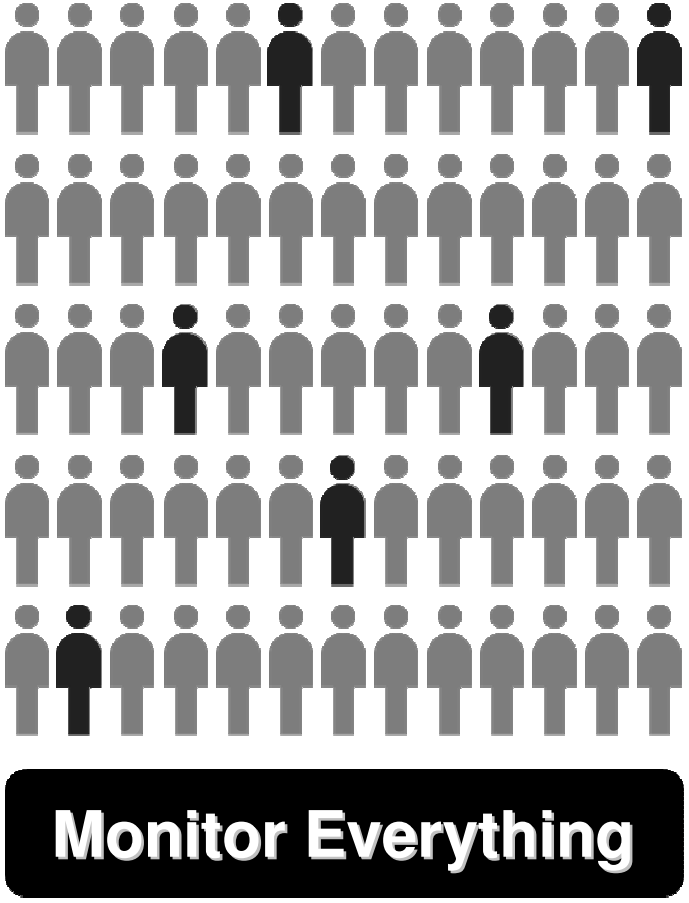
IBM

Then: **Administration**

- Identity management
- Cost control

Now: **Insight**

- Identify and monitor highest risk users
- Know who has access to sensitive data and systems
- Baseline normal behavior
- Prioritize privileged identities



Data

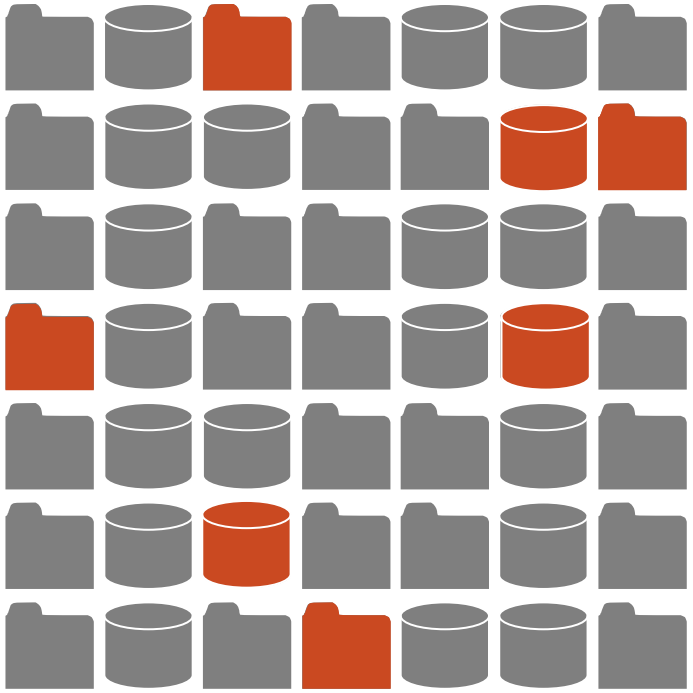
IBM

Then: **Basic Control**

- Simple access controls and encryption

Now: **Laser Focus**

- Discover and protect high-value data
- Understand who is accessing the data, at what time of day, from where, and in what role
- Baseline normal behavior



Monitor Everything

Applications

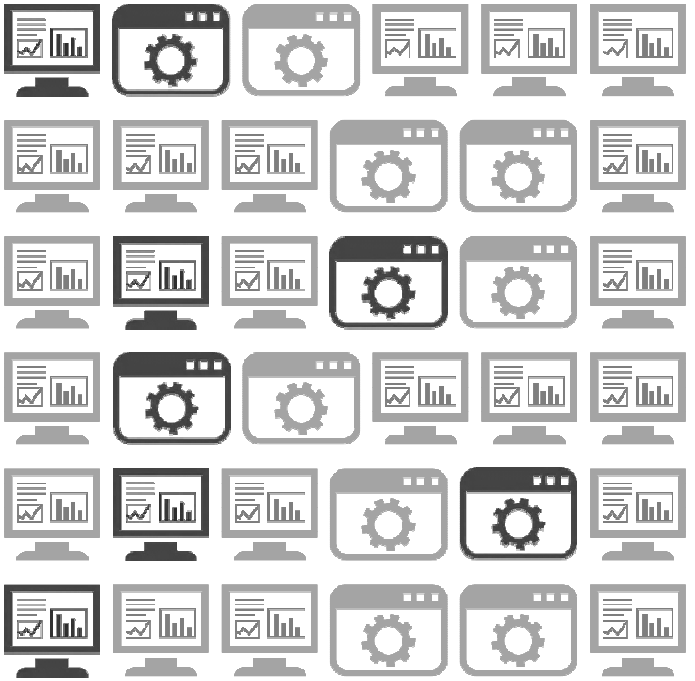
IBM

Then: **Bolt-on**

- Periodic scanning of Web applications

Now: **Built-in**

- Harden applications with access to sensitive data
- Scan source and real-time
- Baseline normal application behavior and alert



Monitor Everything

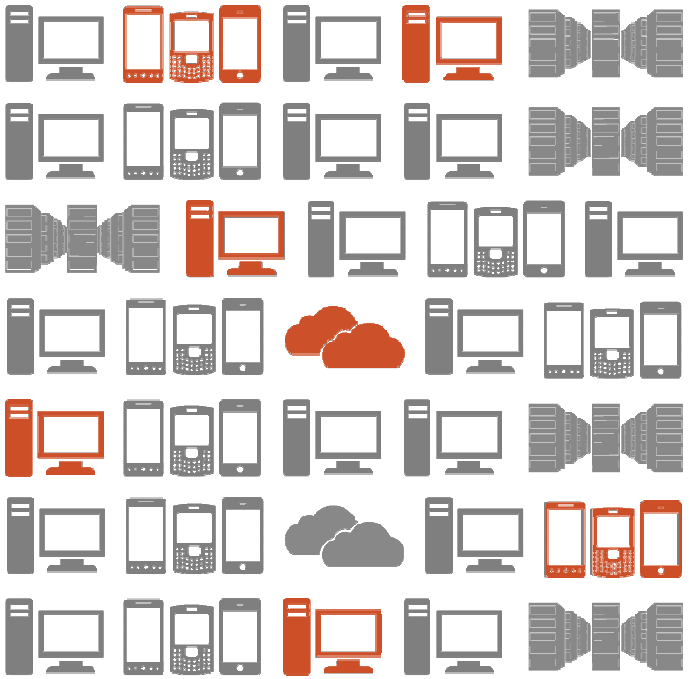
Infrastructure

Then: Thicker Walls

- Firewalls, manual patching, and antivirus
- Focus on perimeter security

Now: Smarter Defenses

- Baseline system and network behavior
- Analyze unknown threats using advanced heuristics
- Expand coverage into cloud and mobile environments



Monitor Everything


People
Data
Applications
Infrastructure
Advanced Security
and Threat Research

Advanced Research

Domain	IP Address	File Checksum
dogpile.com	**117.0.178.252**	c69d172078b439545dfff28f3d3aacc1
kewww.com.cn	83.14.12.218	**51e65e6c798b03452ef7ae3d03343d8f**
ynnsuue.com	94.23.71.55	**6bb6b9ce713a00d3773cfcecef515e02**

Monitor Everything

Then: **Reaction**

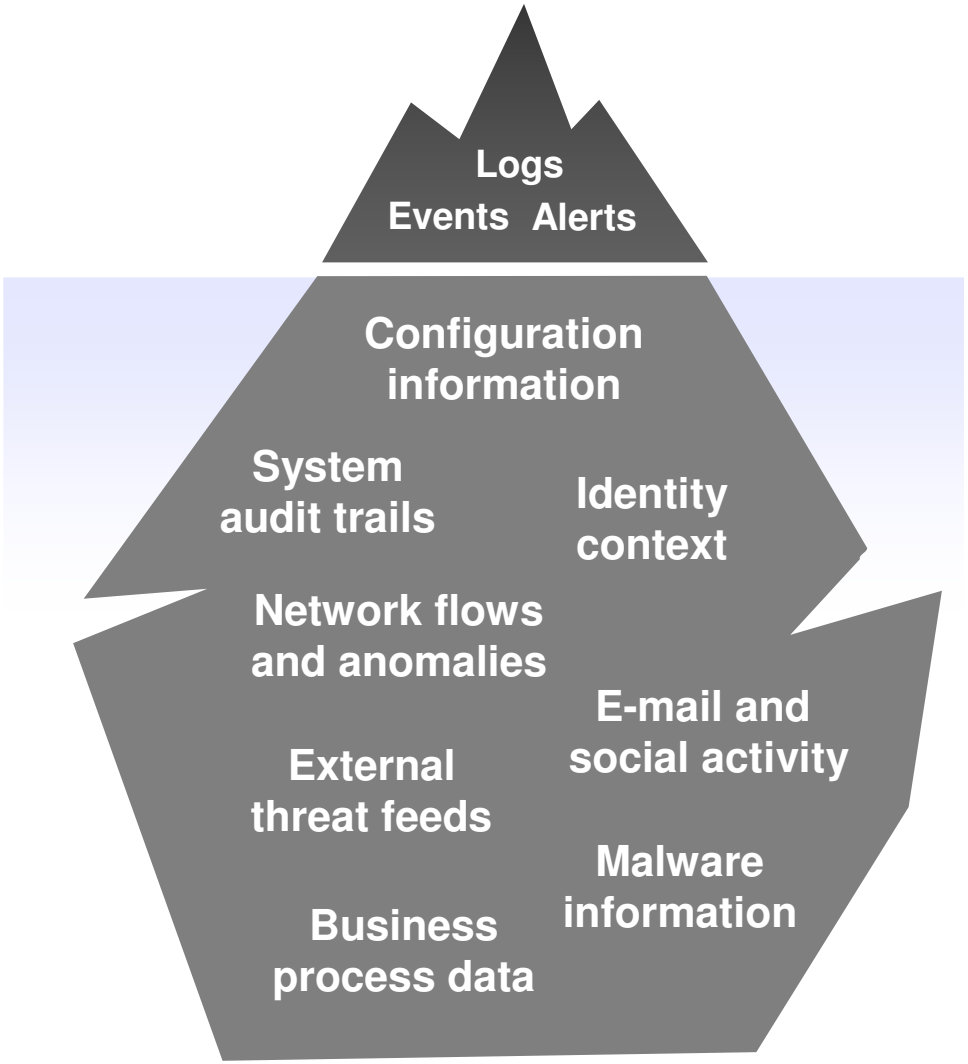
- Read about the latest threats from blogs and news
- Match against known signatures and bad actors

Now: **Situational Awareness**

- Consume real-time intelligence about the latest threats
- Correlate alerts against external behavior and reputation
- Proactively block bad domains, IP address and malware


Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

Security Intelligence

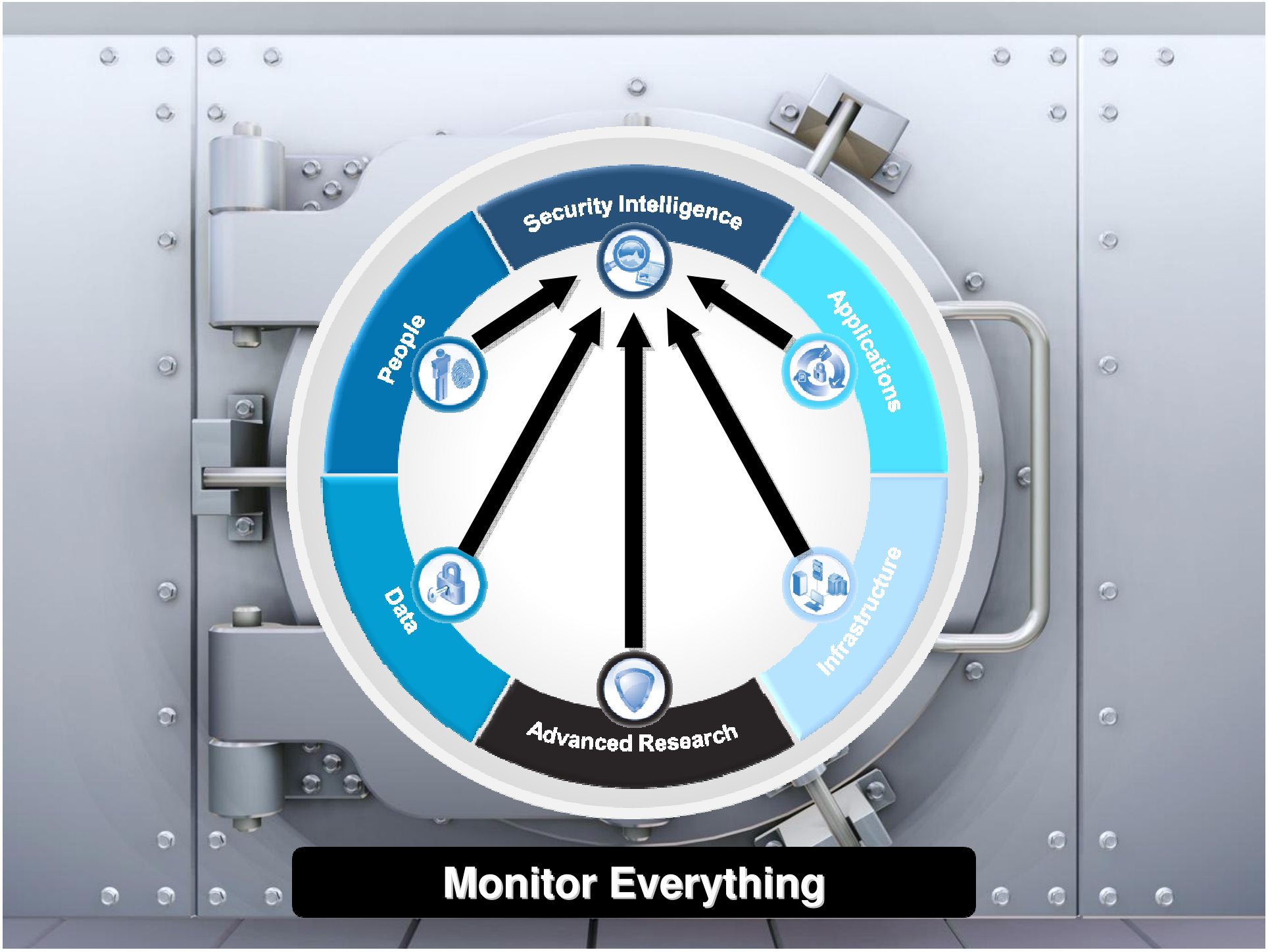


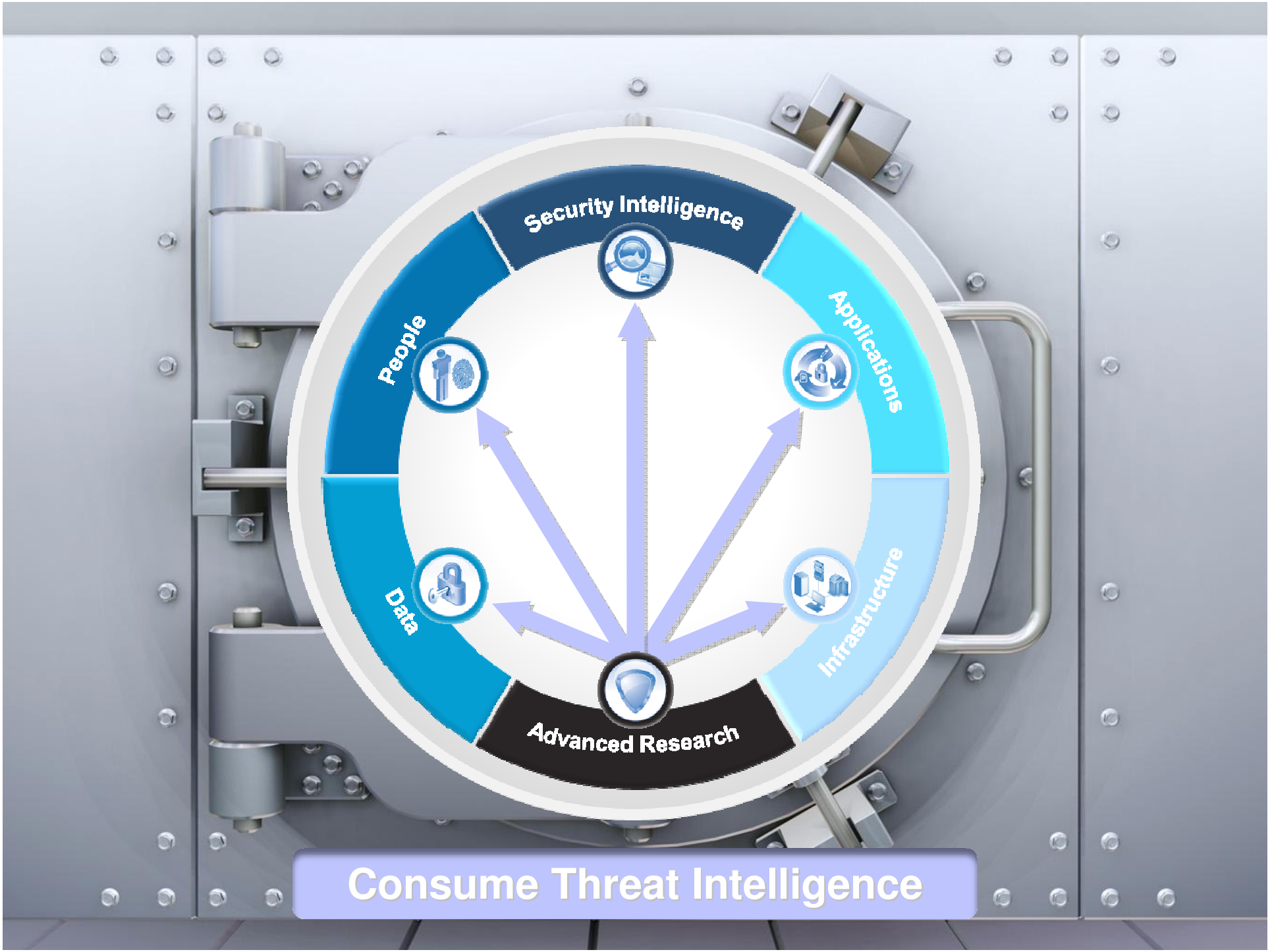
Then: **Collection**

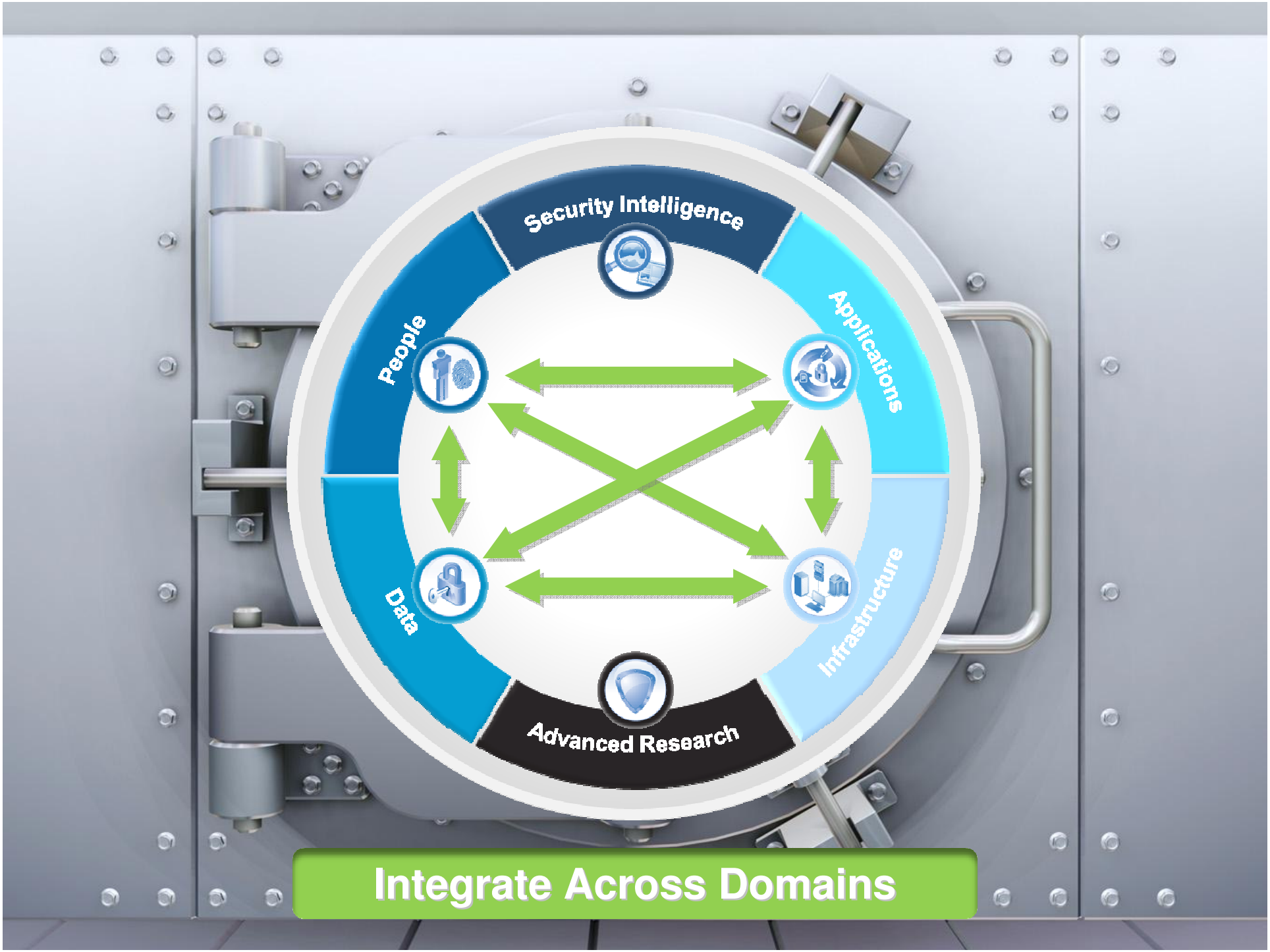
- Log collection
- Signature-based detection

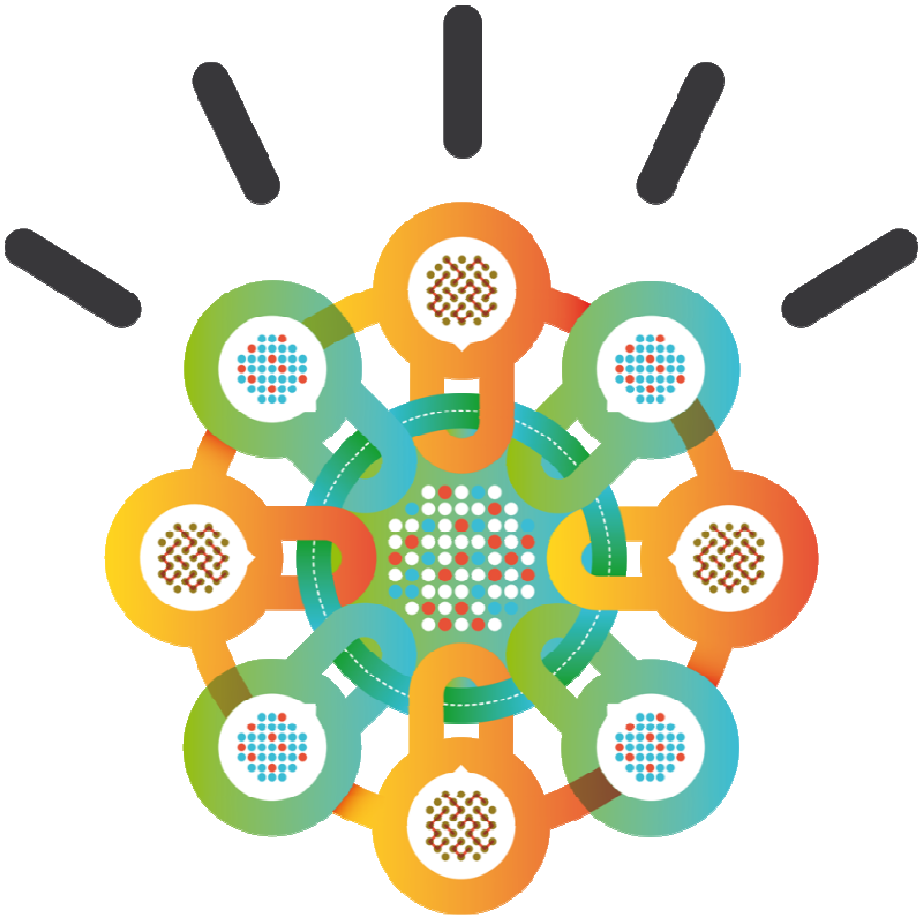
Now: **Intelligence**

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics

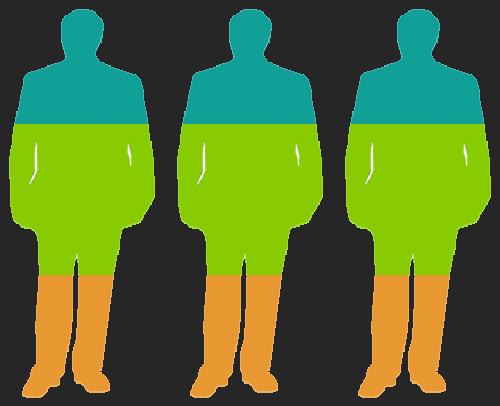

Security Intelligence
Applications
Infrastructure
Advanced Research
Data
People
Monitor Everything


Security Intelligence
Applications
Infrastructure
Advanced Research
Data
People
Consume Threat Intelligence


Security Intelligence
People
Applications
Data
Infrastructure
Advanced Research
Integrate Across Domains



Security Intelligence



Who is going to do this?

In a CISO study conducted by IBM, three groups emerged

Source: IBM Center for Applied Insights, *Finding a Strategic Voice: Insights from the 2012 IBM Chief Information Security Officer Assessment , May 2012*

Influencers

- Confident / prepared
- Strategic focus

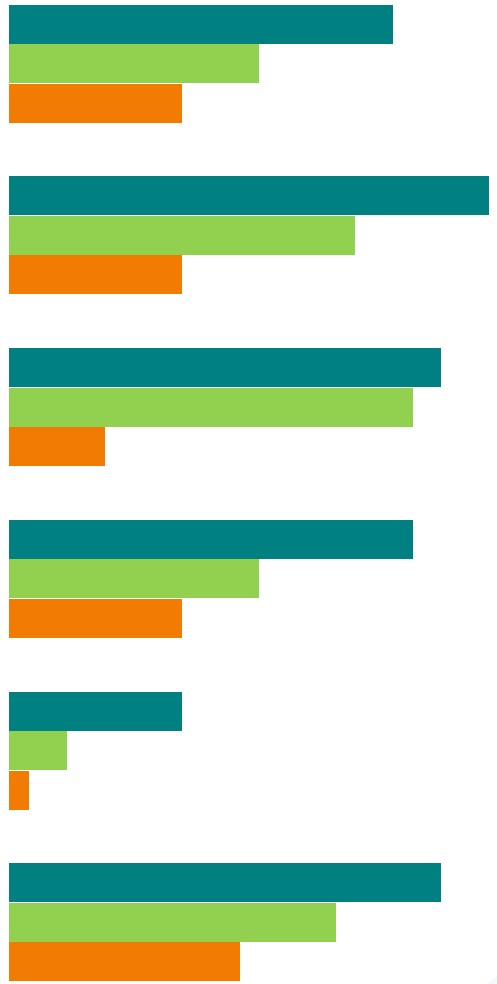
Protectors

- Less confident
- Somewhat strategic
- Lack necessary structural elements

Responders

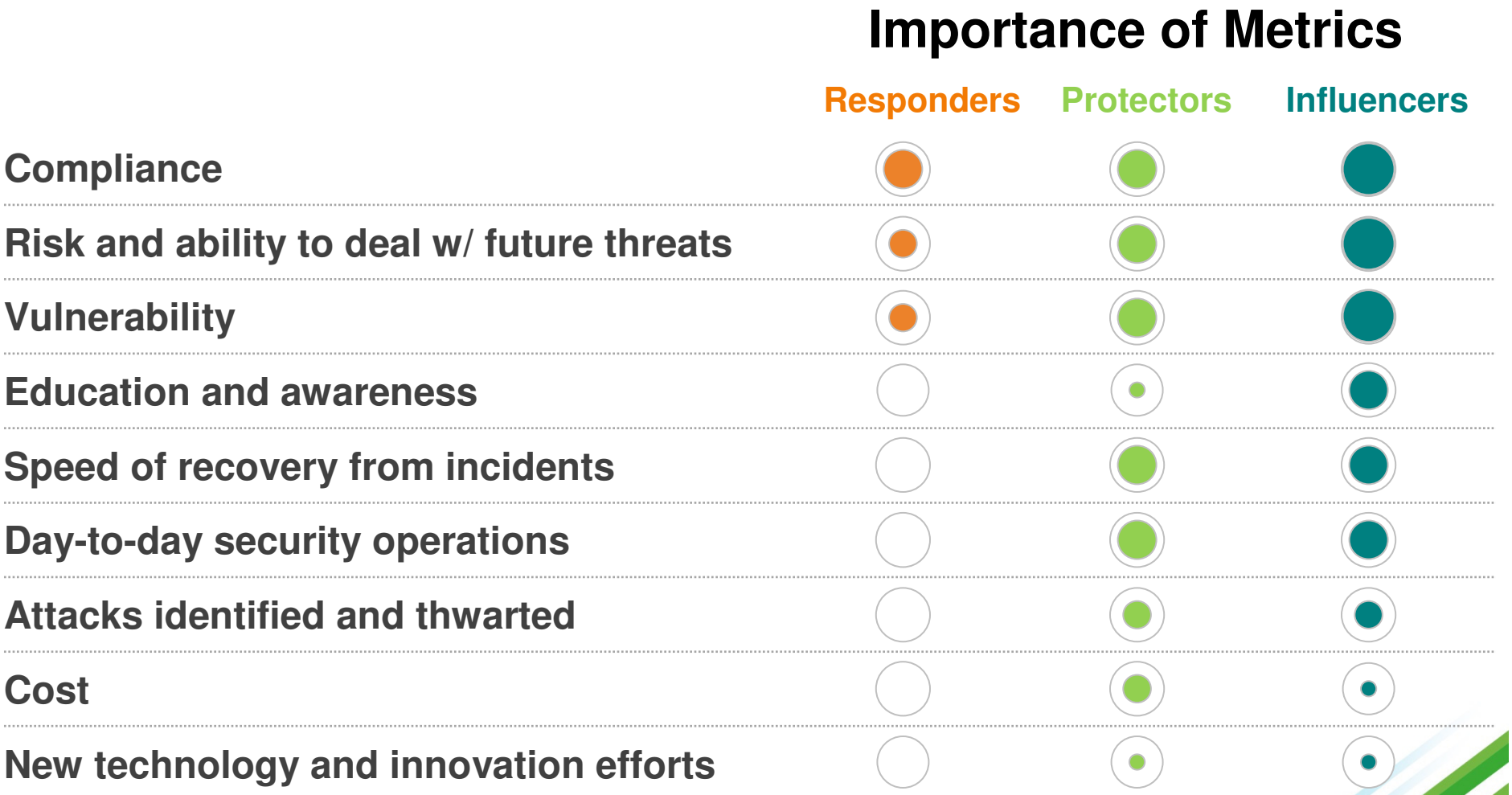
- Least confident
- Focus on protection and compliance

How they differ



Source: IBM Center for Applied Insights, *Finding a Strategic Voice: Insights from the 2012 IBM Chief Information Security Officer Assessment , May 2012*

Influencers use a wider variety of metrics and devote more attention to systemic change



Source: IBM Center for Applied Insights, *Finding a Strategic Voice: Insights from the 2012 IBM Chief Information Security Officer Assessment , May 2012*

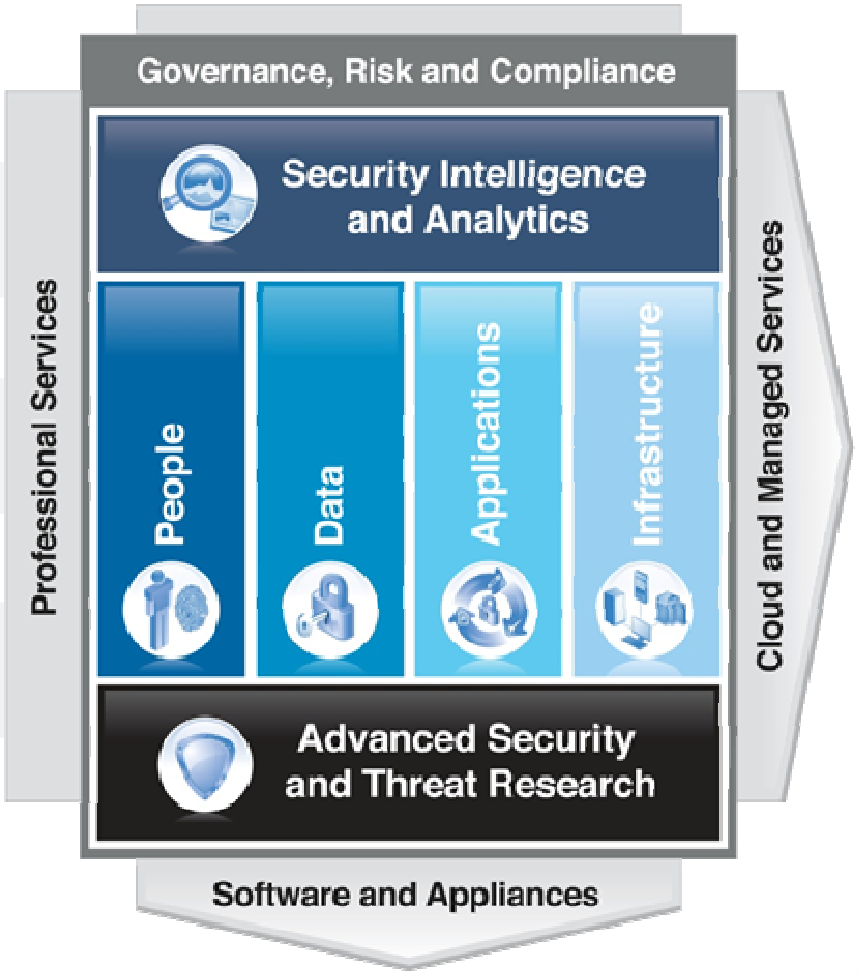
Applying these principles to our new world

IBM delivers security solutions across a comprehensive framework

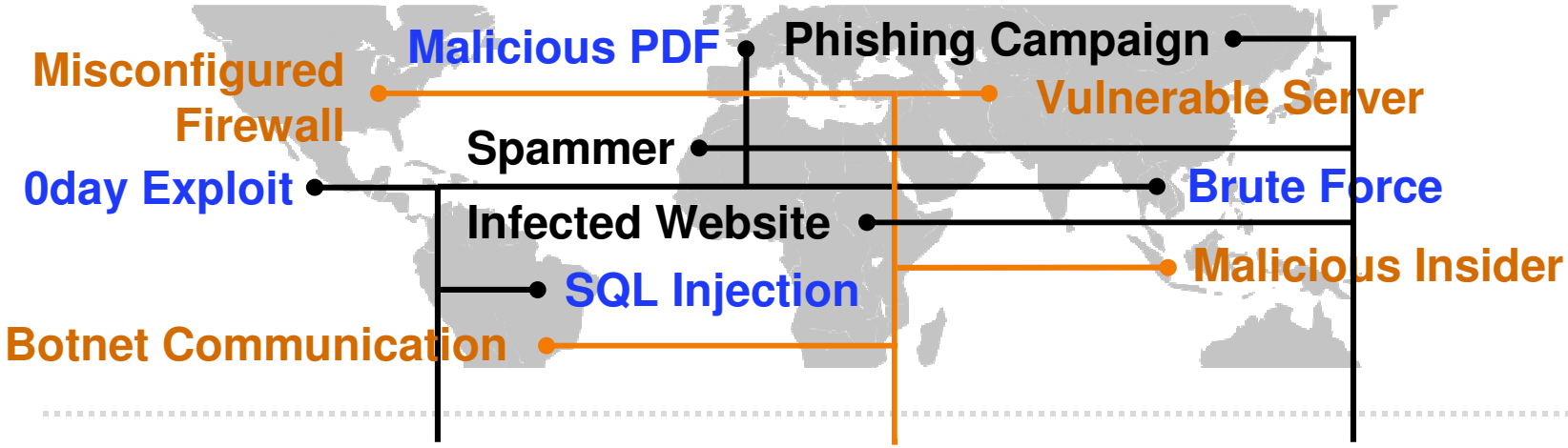
Intelligence

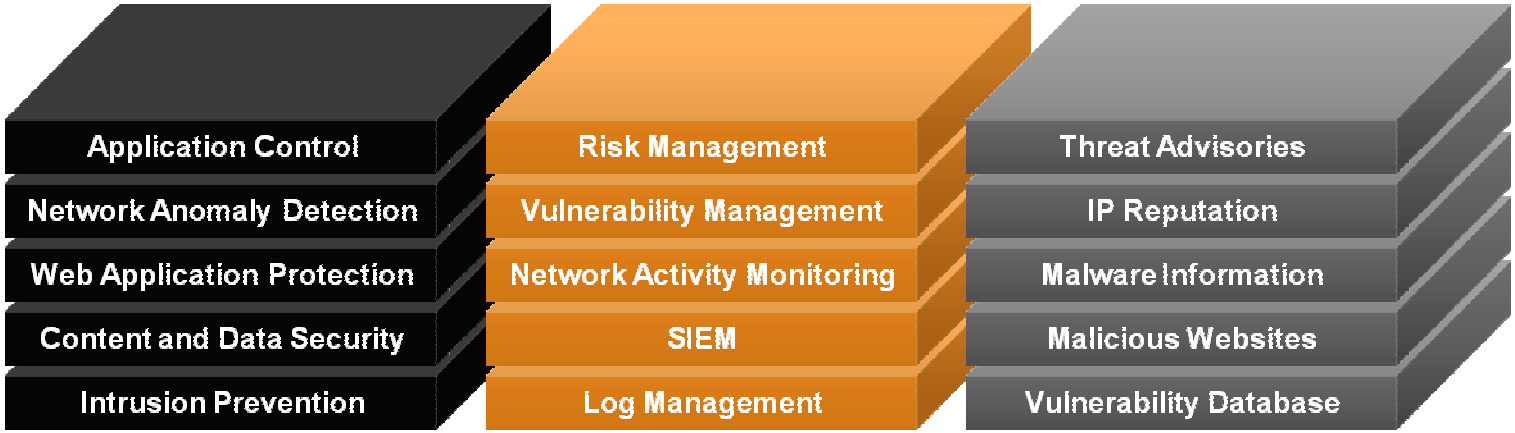
Integration

Expertise



Better protection against sophisticated attacks





On the Network

Across the Enterprise

Across the World

Better protection against sophisticated attacks

IBM Advanced Threat Protection Platform

International Financial Firm

Hardened defenses against threats and fraud

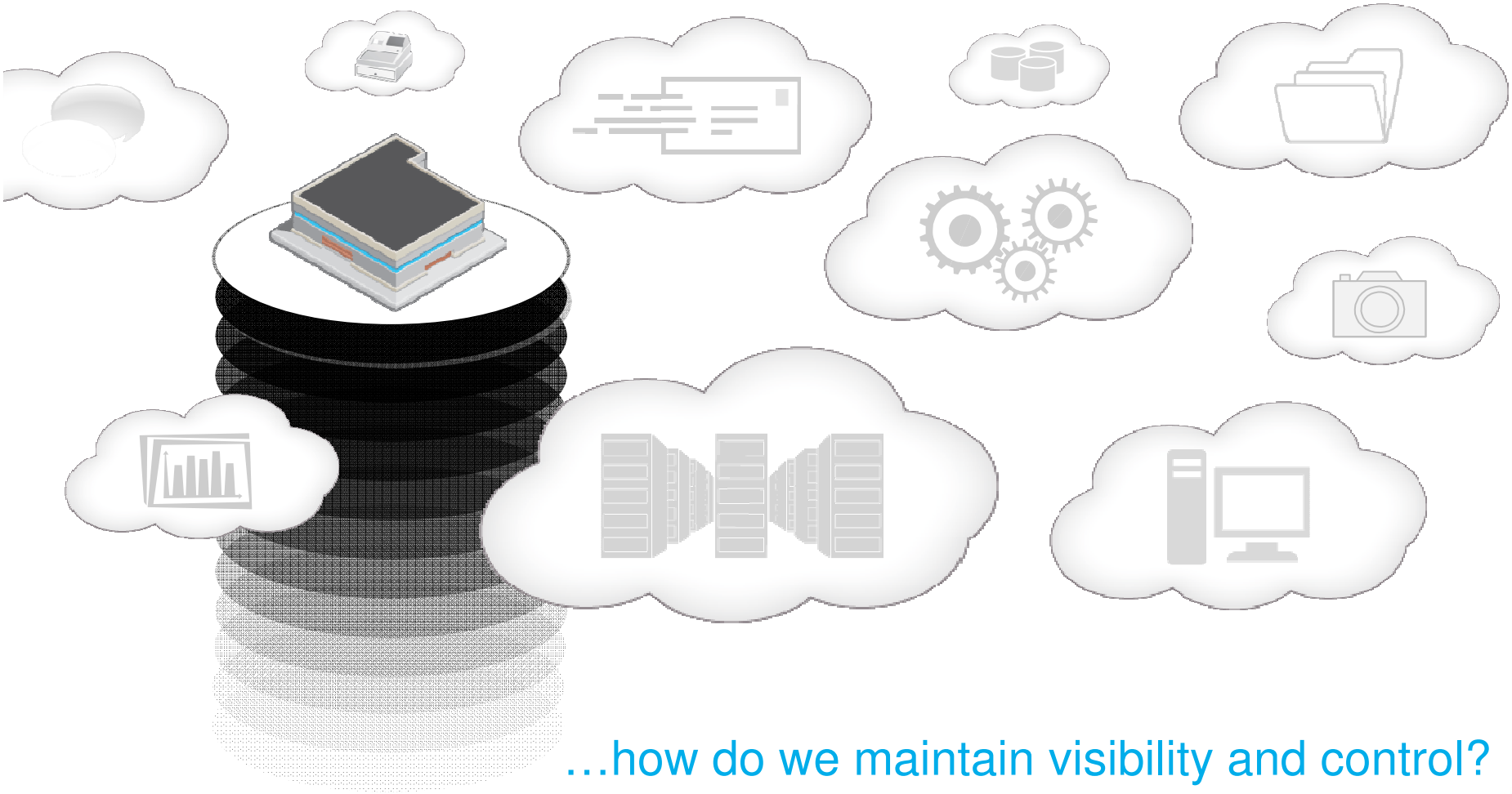
- Real-time correlation of hundreds of data sources
- Anomaly detection across 250 activity baselines to help identify “low and slow” threats

International Commodities Exchange

Analyzes and identifies threats in real time

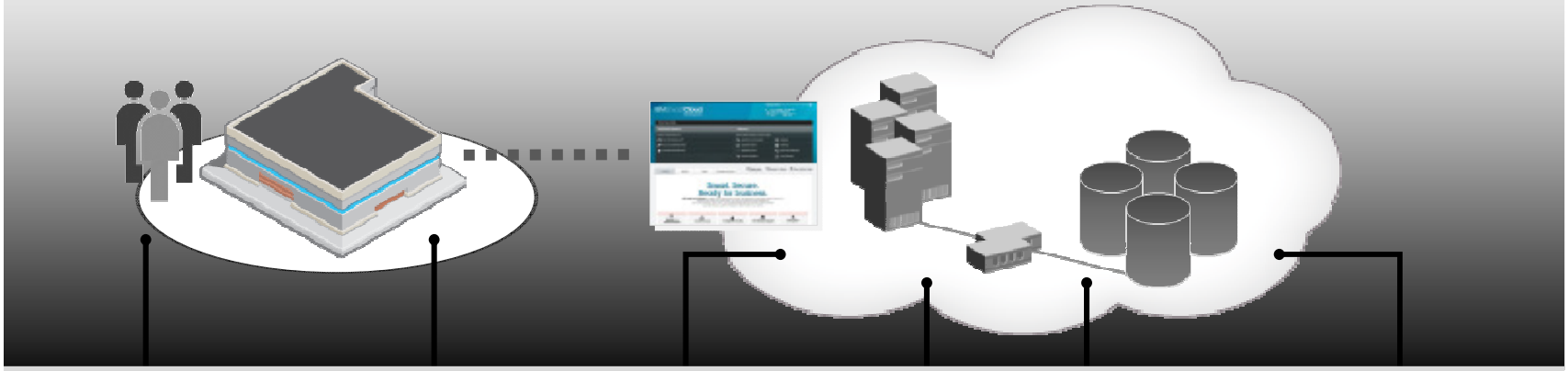
- Analyze worldwide traffic and transactions over multiple public and private networks
- Maintained >99% uptime
- 0 reported breaches in 3 years

Clouds are forming everywhere…



…how do we maintain visibility and control?

IBM Cloud Security



Identity Federation | Web Application Scanning | Virtualization Security | Network Security | Image & Patch Management | Database Monitoring

Security Intelligence

European Energy Company

Security for worldwide access to SaaS applications

- Reduced operational risk
- Provided security for access to Google Apps and Salesforce
- Seamlessly managing users in the providers' registry

Cloud Service Provider

Best-in-class security for an IaaS environment

- Shortened deployment cycles
- Reduced costs and energy use with virtual appliances
- Strengthened security with flexible protection

IBM Mobile Security

Device Management	Network, Data, and Access Security	Application Layer Security
Security for endpoint device and data	Achieve visibility and adaptive security policies	Develop and test applications

Major Australian Bank

Better protection for mobile banking transactions

- Over 1,500,000 mobile customer devices
- Centralized user security and policy management
- Single security infrastructure for multiple user touchpoints

IBM Corporation

Security for BYOD for a variety of platforms

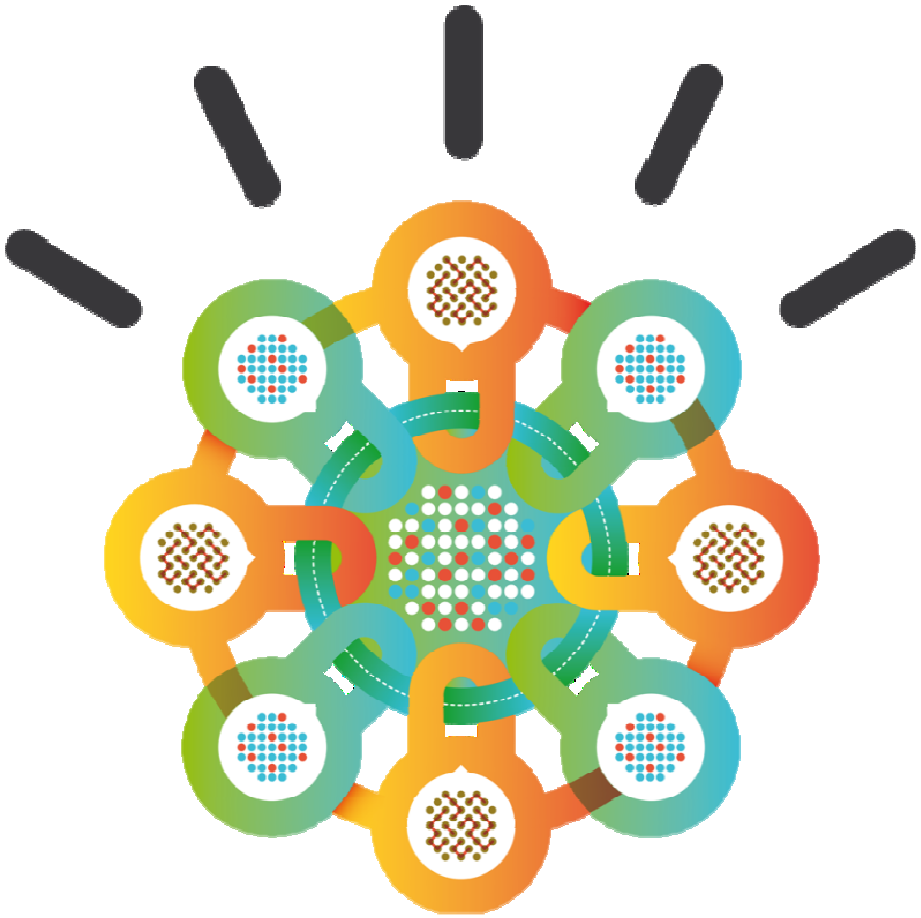
- 120,000 mobile devices deployed in months
- Reduced infections by 80-90%
- Achieve 98% patch compliance within 24 hours

Your security team sees…

Clarity…

Insights…

Everything…



Security Intelligence

Get Engaged with IBM

Follow us at @ibmsecurity

Download X-Force security trend & risk reports
http://www-03.ibm.com/security/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php

IBM BusinessConnect
Vernetzter, intelligenter und informierter denn je

Einführung und operativer Betrieb von IBM Network Intrusion Prevention Systemen beim Bundesrechenzentrum

Ing. Martin Krautschneider, Bundesrechenzentrum GmbH

Einführung und operativer Betrieb von IBM Network Intrusion Prevention Systemen

Ing. Martin Krautschneider

5. Juni 2013

AGENDA

Vorstellung Bundesrechenzentrum

- Rahmenbedingungen
- Kernkompetenzen & Markt
- Zahlen und Fakten
- Qualität und Sicherheit der Services

Intrusion Prevention beim Bundesrechenzentrum

- Rahmenbedingungen
- Vorgaben für Implementierung
- Implementierung
- Betriebliche Umsetzung
- Quo Vadis?

Vorstellung Bundesrechenzentrum

In öffentlicher Hand - Privatwirtschaftlich geführt

1997 Ausgliederung aus dem Finanzministerium mit dem Ziel

- Nutzung der Synergien durch Konsolidierung, Standardisierung und Bündelung von IT-Ressourcen und IT-Services
- Neustrukturierung der IT im Bund und Verwaltungsmodernisierung
- Flexibleres Gehaltsschema

Eigentümer ist die Republik Österreich, vertreten durch das Bundesministerium für Finanzen

Auftragsvergabe durch

- Gesetz – Betriebspflicht, Kostendeckungsprinzip, Umsatzsteuerbefreiung
- In-house Vergabe – ohne öffentliche Ausschreibung
- Vertrag – Gewinnerzielung

Als Full-Service Provider entwickelt, implementiert und betreibt das BRZ IT-Services für die Österreichische Bundesverwaltung

Unser Markt

- Bundesministerien und Bundeskanzleramt
- Universitäten
- Oberste Organe
- Ausgegliederte Organisationen

350 E-Government Anwendungen

- FinanzOnline, E-Finanz, Haushaltsverrechnung und Personalmanagement des Bundes, eZoll, Unternehmensserviceportal
- Firmen- und Grundbuch, Elektronisches Mahnverfahren
- ELAK – Elektronischer Akt, Help.gv.at, Data.gv.at
- Biometrischer Pass
- ÖH-Wahlen (e-voting)
- Gesundheitsportal

ZAHLEN & FAKTEN

Umsatz 2012	**265,3 Mio Euro**
Mitarbeiter/innen	**1.200**
Marktanteil	**ca. 55% der IT-Ausgaben der Bundesverwaltung**
Betreute IT-Arbeitsplätze	**> 30.000**
Server in Betrieb	**> 3.000**
Gespeicherte Daten	**> 1.800 Terabyte**
Output Services	**> 100 Mio Seiten pro Jahr**
IT Service-Provider Ranking	**Platz 2***

* Computerwelt, Top 1001, IKT-Services 2012

Laufende Optimierung der Informations- und Datensicherheit für unsere Kunden

Sicherheitsstandards auf internationalem Niveau

- Jährlicher Nachweis durch externe Zertifizierung
- Ausbau der Zusammenarbeit im Bereich Cybersecurity
  Mitglied bei A-SIT (Zentrum für sichere Informationstechnologie – Austria) und im CERT – Verbund (Computer Emergency Response Team Austria)

Qualität der Dienstleistungen erhöht

- Mit Kunden vereinbarte Service-Level eingehalten und Verfügbarkeit der Services deutlich erhöht

Intrusion Prevention beim Bundesrechenzentrum

Welche Herausforderungen gibt es zu beachten?

- Steigende Bedrohung durch immer intelligentere Angriffsszenarien
- 350 Anwendungen mit unterschiedlichem Schutzbedarf
- Netzsegmente mit unterschiedlichem Schutzbedarf
- Einsatz von Servervirtualisierung
- Unterschiedliche Anforderungen der Kunden bzgl. Sicherheit

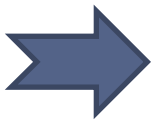
VORGABEN FÜR IMPLEMENTIERUNG

Allgemeine Anforderungen

- Investitionsschutz (kein sofortiger HW Tausch bei steigenden Bandbreiten)
- Größtmöglicher Nutzen bei möglichst geringem Personalaufwand
- Inline / passiver (Mirrorport) Betrieb muss möglich sein
- Entsprechende Performance um mehrere Netzsegmente gleichzeitig zu prüfen
- Hochverfügbare Implementierung
- IPv6 (Internet Protocol Version 6) Unterstützung

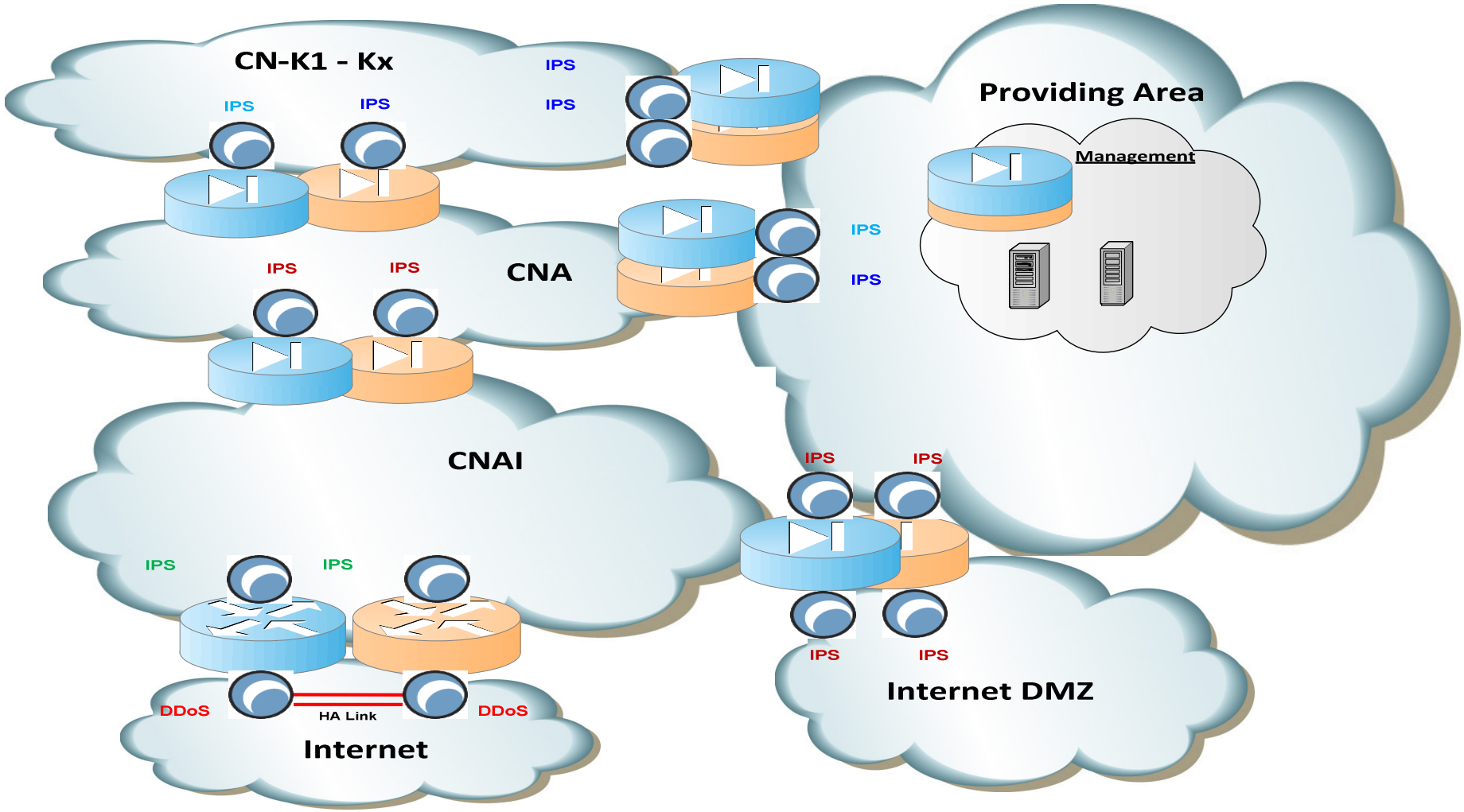
Security Anforderungen

- Aktualität der Signaturen (Operating Center oder ähnliches)
- Erkennung bekannter Applikationen
- Erkennung und Filterung von Anonymisierungsnetzwerken (TOR)
- Einfache Signaturpflege
- Aussagekräftigkeit von Alarmen bzw. Signaturbeschreibungen



Durchführung einer Marktanalyse mit Teststellungen

IMPLEMENTIERUNG



CNA…….Corparate Network Austria
CNAI……Corparate Network Austria Internet
CN-K1-Kx…Corparate Network Kunde1 – x

DMZ…….demilitarisierte Zone
IPS……Intrusion-Prevention-System
DDoS……..distributed denial-of-service

Die Intrusion Prevention Systeme sind an neuralgischen Punkten im Netzwerk implementiert.

Eingesetzte Hardware

- Proventia GX5008, G2000F und GX7412
- Cisco IPS
- Corero IPS

Virtualisierung

Um bei den verschiedenen Netzwerksegmenten einen voneinander unabhängigen Blocking - Schutz zu gewährleisten wurden die IPS Systeme der Type GX7412 entsprechend virtualisiert!

Pro Virtualisierung, bei IBM IPS spricht man von “Protection Domains”, können Signaturen unabhängig von anderen Protection Domains auf blocking gestellt werden.

Schutzmaßnahmen

- Unterschiedliche Protection Domains (Internet, Providing Area)
- Internet – nur Grundschutz
- Providing Area – blocken zusätzlicher Signaturen
- Zusätzliche Signaturen werden aufgrund von Beobachtungszeiträumen und Erfahrungswerten ausgewertet und aktiviert (false positives)

Upgrades

- Upgrades der Signaturen können sofort durchgeführt werden
- Erfolgt grundsätzlich in Abstimmung mit den betroffenen Kunden
- 24h Beobachtungszeitrum bevor blocking aktiviert wird
- Automatische Info über neue Signaturupgrades
- Firmwareupgrades nur in entsprechenden Wartungsfenstern

BETRIEBLICHE UMSETZUNG

Management

- Erfolgt grundsätzlich über die SiteProtector Console
- Sowohl Überwachung als auch Administration wird darüber abgewickelt
- Live View auf die Systeme ist möglich (Beobachtung aktueller Events)
- Erstellung diverser Reports für Kunden
- Events und Logs werden durch das zentrale Management in einer Datenbank gespeichert
- IPS Systeme können auch direkt administriert werden

Alarmierung

- Administration der Alarmierung über die SiteProtector Console
- Definition entsprechender Policies und Schwellwerte pro Signatur
- Bei Erfüllung der definierten Kriterien Alarme via eMail und SNMP (Simple Network Management Protocol)
- Außerhalb der Regelarbeitszeit wird außerdem ein Bereitschaftstechniker durch das Umbrella System verständigt
- Umfangreiches Regelwerk vorhanden um bei Penetrationstests einzelne Systeme aus der Alarmierung ausnehmen zu können

QUO VADIS?

Welche zukünftigen Herausforderungen kommen auf uns zu?

- Steigende Bandbreiten und komplexere Anwendungen
- Anzahl an verschlüsseltem Verkehr steigt stetig
- Immer stärkerer Einsatz von Virtualisierungstechnologien
- Schutzbedarfsanforderungen der Kunden werden komplexer
- Stärkere Verzahnung der verschiedenen Security Systeme (IPS, DDoS (distributed denial-of-service), HIPS (Host Intrusion Prevention System))

ÖSTERREICH RECHNET MIT UNS

Ing. Martin Krautschneider
Martin.Krautschneider@brz.gv.at

Danke!