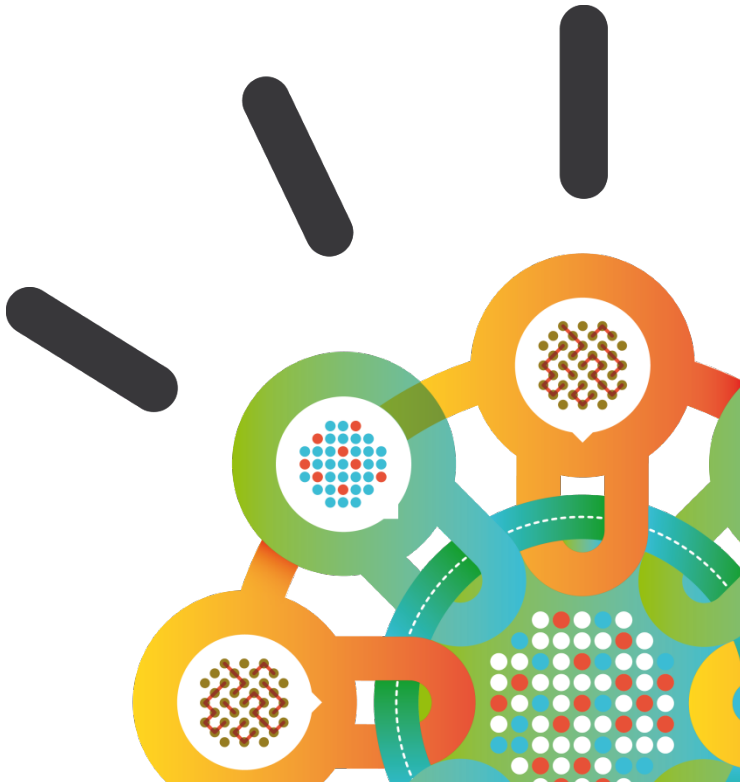
Impossibile trovare nel file la parte immagine con ID relazione rId16.

Security Intelligence.
Think Integrated.

Alberto Meneghini

Security Leader, IBM Italia

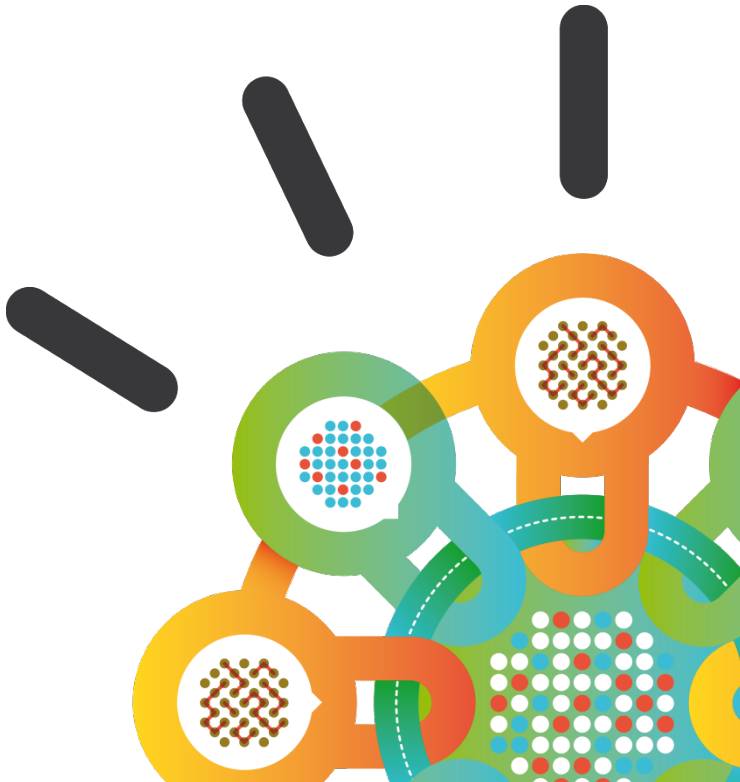


Impossibile trovare nel file la parte immagine con ID relazione rId16.

Security Intelligence.
Think Integrated.

Esistono istituzioni finanziarie che sanno cosa significa essere attaccate ed altre che neppure lo immaginano.

In quale vi riconoscete?



Alberto Meneghini
Security Leader, IBM Italia

L'ottantatre percento dei CISO afferma che le sfide poste dalle minacce esterne sono aumentate negli ultimi tre anni

Near Daily Leaks of Sensitive Data

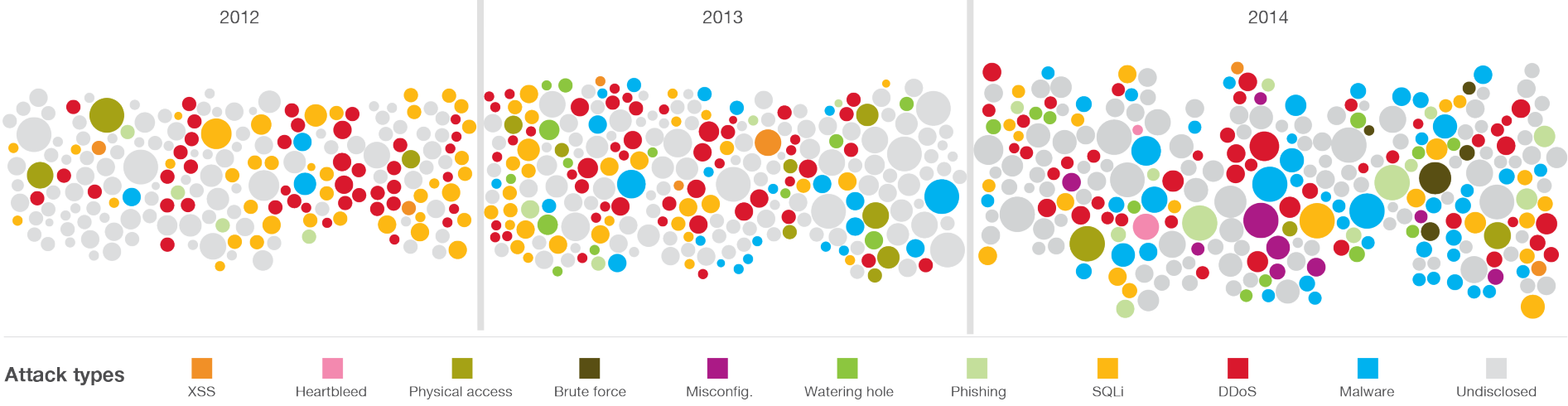
40% increase
in reported data breaches and incidents

Relentless Use of Multiple Methods

800,000,000+ records
were leaked, while the future shows no sign of change

"Insane" Amounts of Records Breached

42% of CISOs
claim the risk from external threats increased dramatically from prior years.



Size of circle estimates relative impact of incident in terms of cost to business.

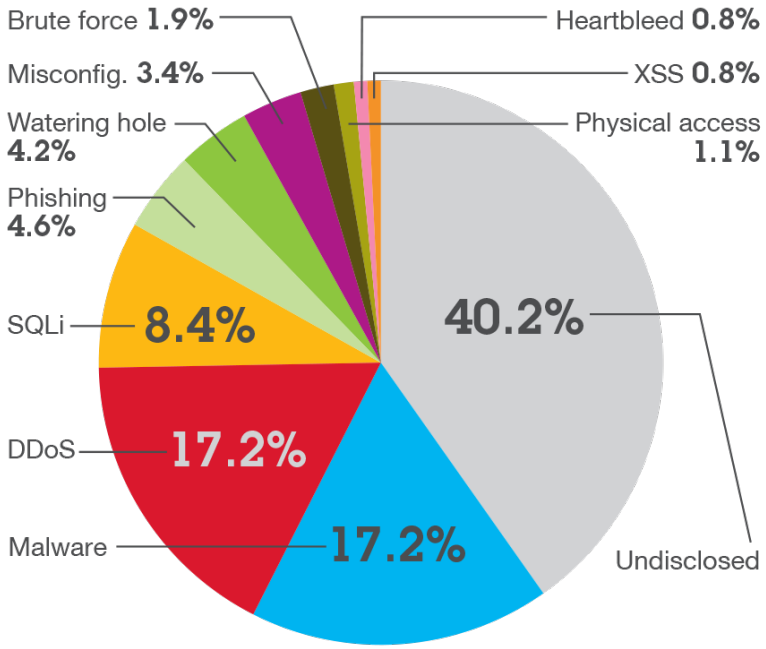
A historical look at security incidents by attack type, time and impact, 2012 through 2014

Source: IBM X-Force® Research and Development

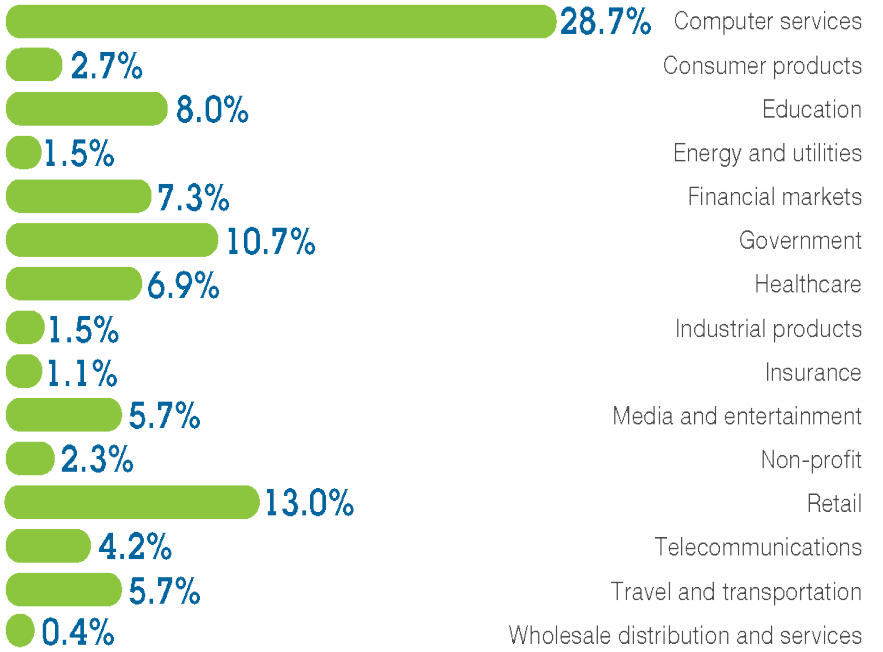
Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015 and 2014 IBM Chief Information Security Officer Assessment

Gli «aggressori» stanno attuando nuovi tipi di attacco in modo sempre più creativo. Violazioni di rilievo hanno interessato i settori della vendita al dettaglio e dei servizi informatici nel corso del 2014

Most-common attack types



Most-commonly attacked industries



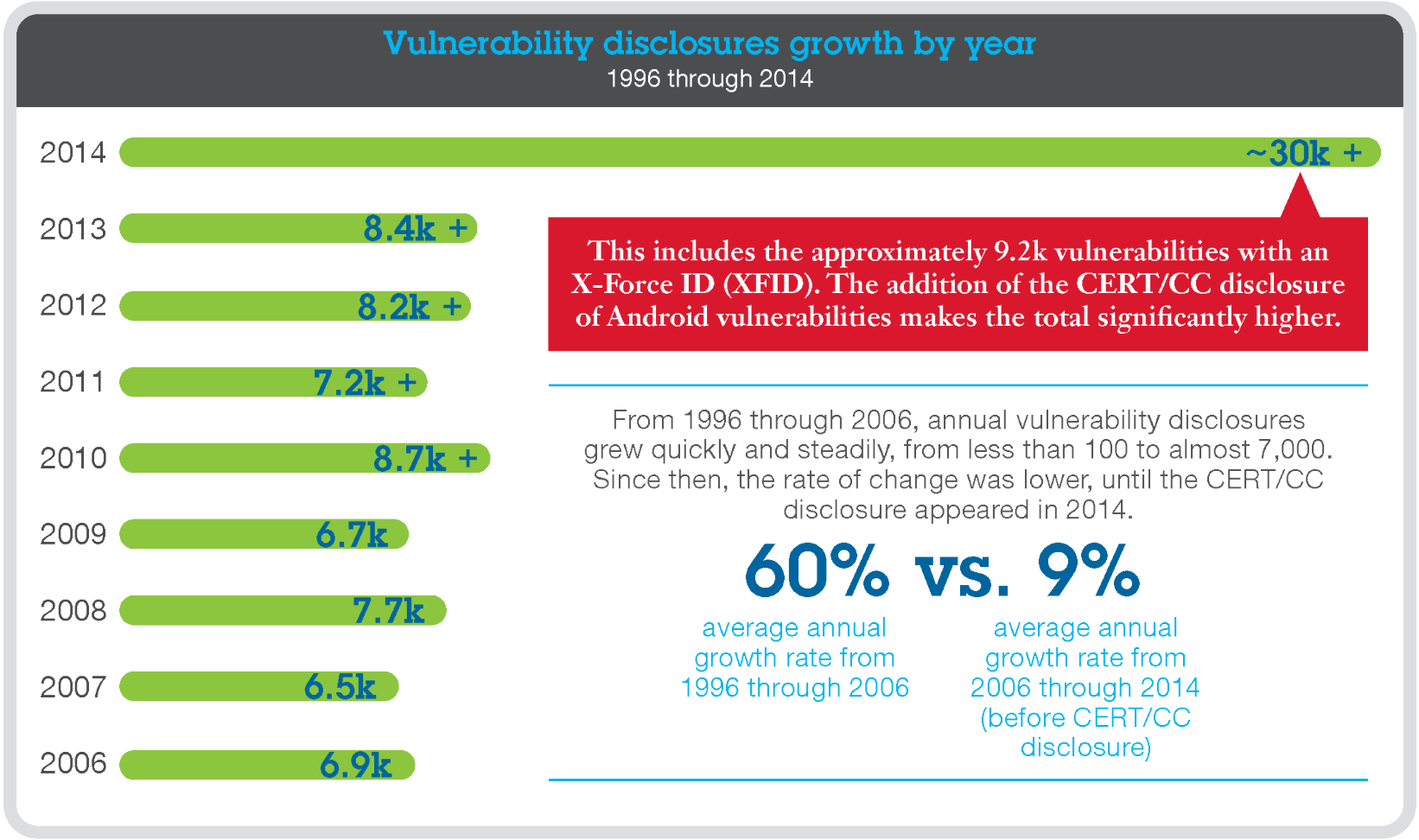
Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

Molteplici previsioni formulate nel corso degli ultimi due anni convergono nell'ipotizzare la diffusione di miliardi di dispositivi IoT connessi alla rete

IBM Center for Applied Insights

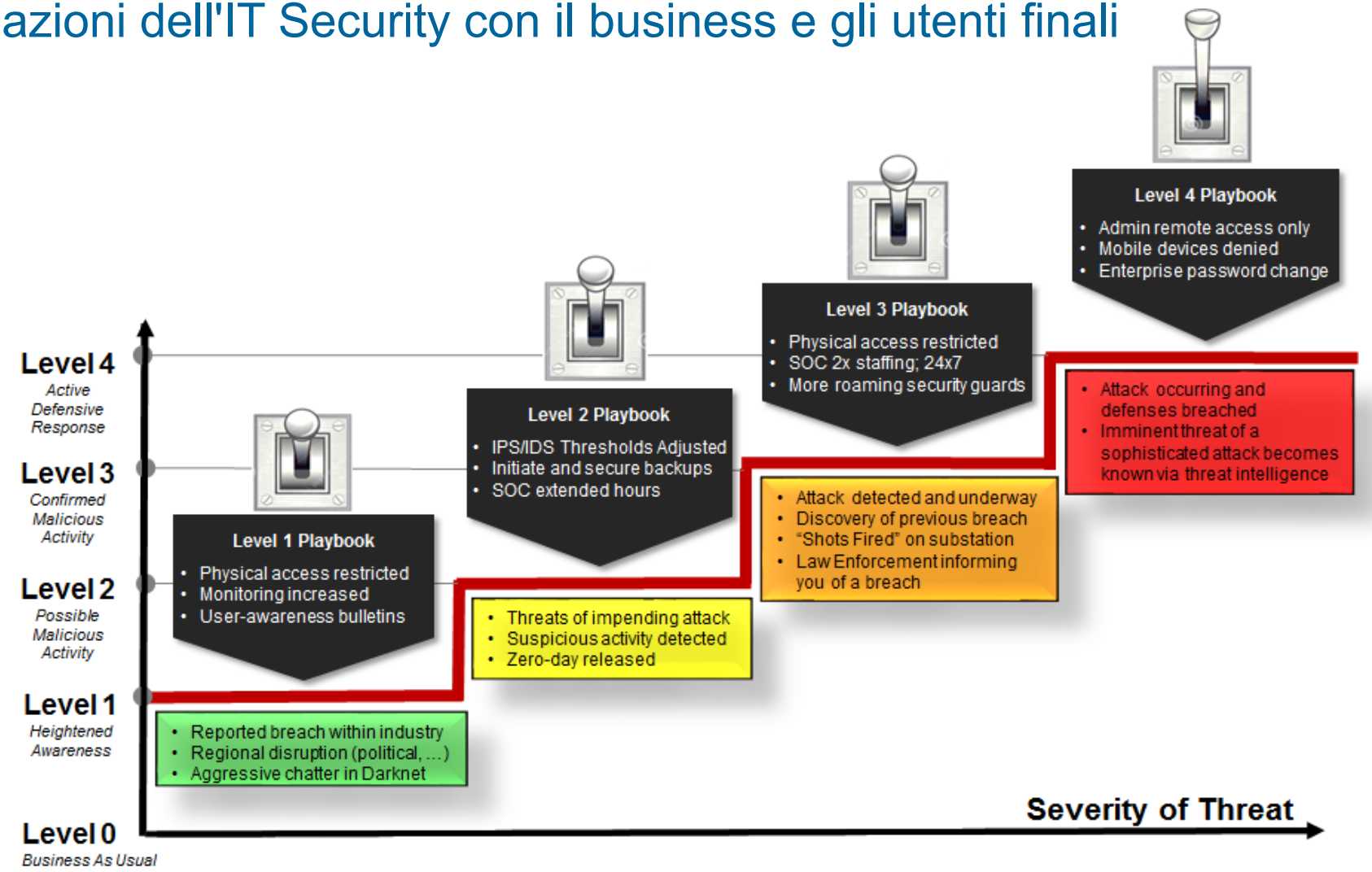
"IDC forecasts that there will be approximately 30 billion autonomous things attached to the Internet in 2020, which serve as the catalyst driving this significant revenue opportunity." IDC

Il 2014 si è chiuso con 9.200 nuove vulnerabilità registrate, ma il numero totale potrebbe raggiungere il picco di 30.000



Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

Il nuovo paradigma di sicurezza può essere rappresentato come un modello di risposta a più livelli, che mette in correlazione le azioni dell'IT Security con il business e gli utenti finali



I tipici processi di GRC sono manuali, inefficienti e inefficaci

Activities to Perform in SOX compliance)

Document Review → **Assessment Prep** → **Controls Walkthrough** → **Assessment** → **Risk review & Recommendation** → **Close-Out Meeting**

Without automated IT GRC tools

Refer to earlier risk review documents, work allocation and tracking in excel sheet.

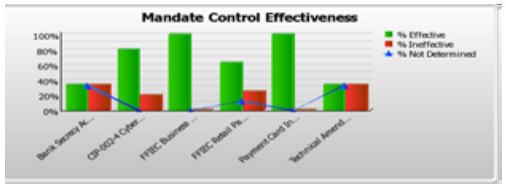
Interviews. Queries & Follow up (Email)

Take samples and assess. Status reporting through Excel sheet

Risk Findings & Reporting

With IT GRC Automation

Automated IT GRC Platform



Refer to earlier work papers in platform. Import templates, work allocation and tracking in workflow

Interviews. Queries & Follow up (Workflow)

Take samples and assess. Status reporting through Dashboard

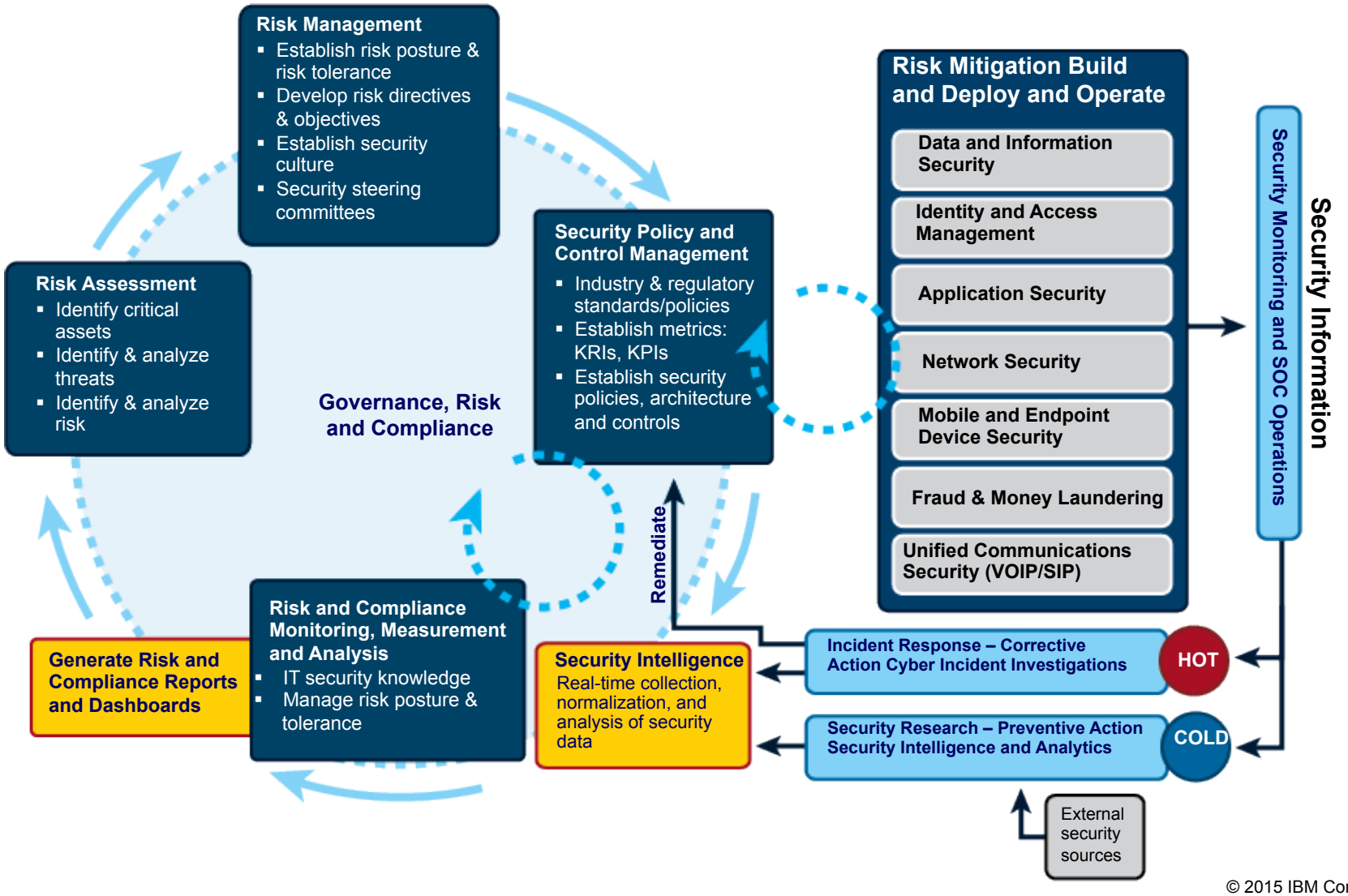
Risk Findings & Reporting: Dashboard

Document Review → **Assessment Prep** → **Controls Walkthrough** → **Assessment** → **Risk review & Recommendation** → **Close-Out Meeting**

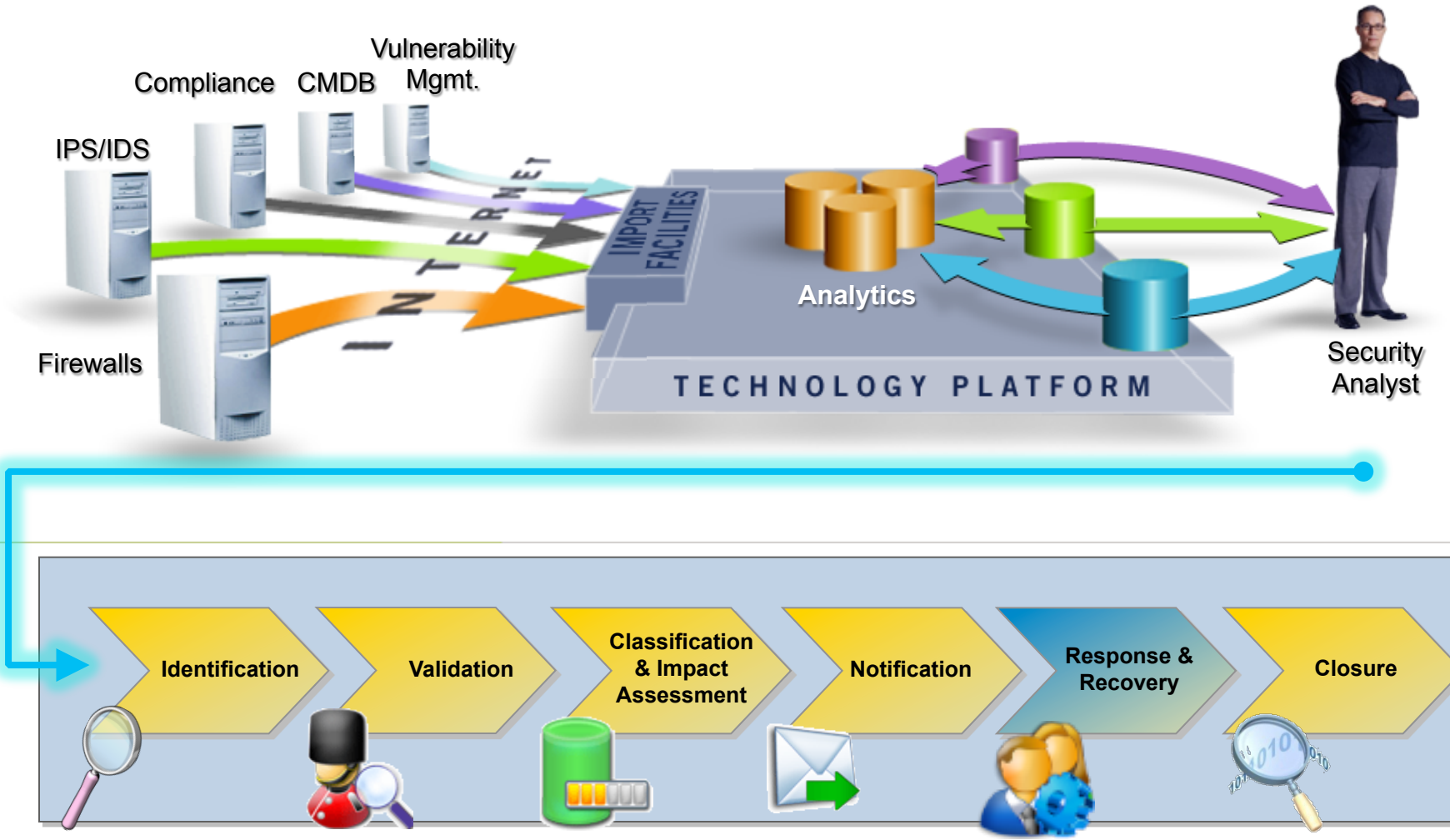
IBM risk reviewer

Client IT project owner

Un «Security Risk Management Life Cycle» integrato che opera in tempo reale è necessario per supportare il processo decisionale



Diverse funzioni SOC possono essere affidate a IBM per creare una soluzione "ibrida" di rapida implementazione, efficace e scalabile



In House vs Out-Tasking Service

	Traditional Software License	Managed Security Services Provider
Entry cost	High	Low
Installation and implementation	Requires in-house resources	MSSP handles implementation
Time to value	Long	Short
Skilled resources	Company must hire, train, and retain talent	MSS provides skilled resources
Efficiency and effectiveness	Limited scalability prohibits efficiency and effectiveness	Greater efficiencies via scalability (1:many) is inherent in SOC operations
Security posture	Dependent on skill, processes, and expertise of internal staff	Improved by diligence, guaranteed response times, security vulnerability research, and cumulative expertise of MSS team
Response	Dependent on skill, processes, and expertise of internal staff	24x7 protection, critical alert notification and levels of response per severity

IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanta vasta organizzazione globale per il delivery dei servizi di sicurezza

4,300
Strategic outsourcing security delivery resources

1,200
Professional services security consultants

650
Field security specialists

400
Security operations analysts

10
Security research centers

10
Security operations centers

15
SW Security development labs

IBM X-Force Expertise

- 150M intrusion attempts daily
- 83,000 documented vulnerabilities
- 40M unique phishing / spam attacks
- Millions of unique malware samples
- Billions of analyzed web pages
- 3000+ security patents

Managed Services Excellence

- 20,000+ devices under contract
- 3,700+ Security Svcs clients worldwide
- 20B+ events managed per day
- 133 monitored countries (MSS)
- Unique research and reports

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

X-FORCE

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security