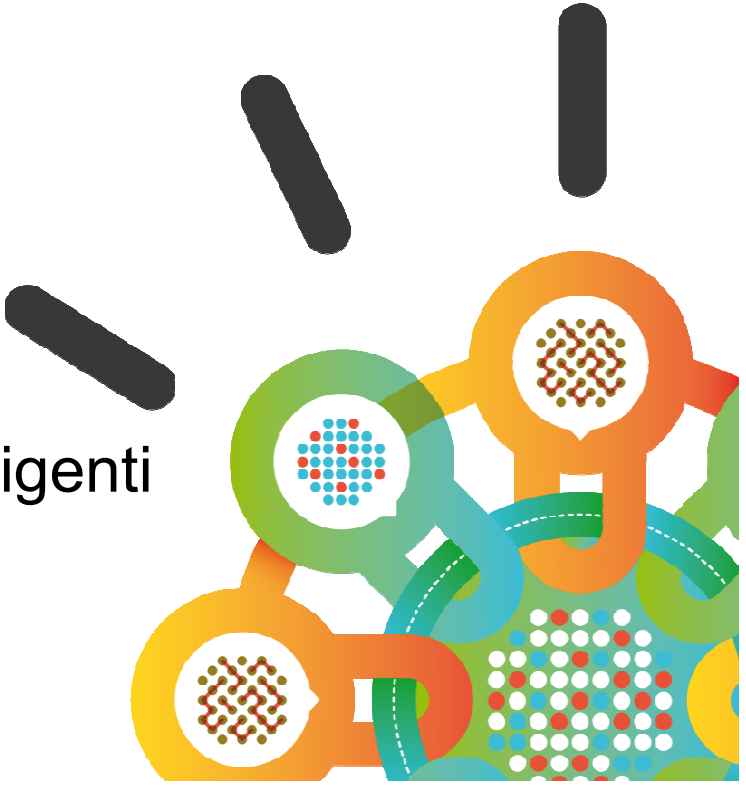
Security Intelligence.
Think Integrated.

Smarter Cities: Securing the new world of the Internet Of Things

Ing. Alberto Meneghini
IBM Italia

AFCEA Smart Cities:
Sicurezza e Protezione nelle Città intelligenti
Roma 26 marzo 2015



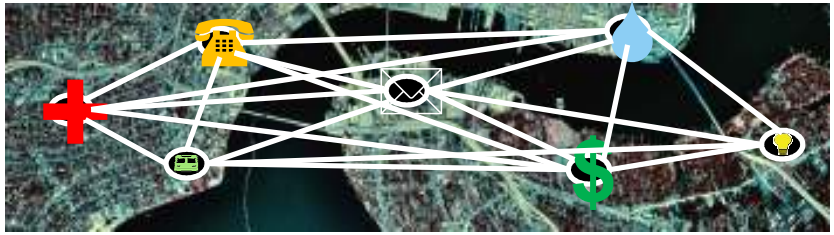
Agenda

- Smarter Cities: the dimension of «smart»
- Internet Of Things
- Security in the Internet Of Things
- IBM Security Model for the Internet Of Things
- Threats are still out there: X-Force Report
- About IBM X-Force: Monitoring and analyzing the changing threat Landscape

Smarter Cities: the three dimension of « smart »

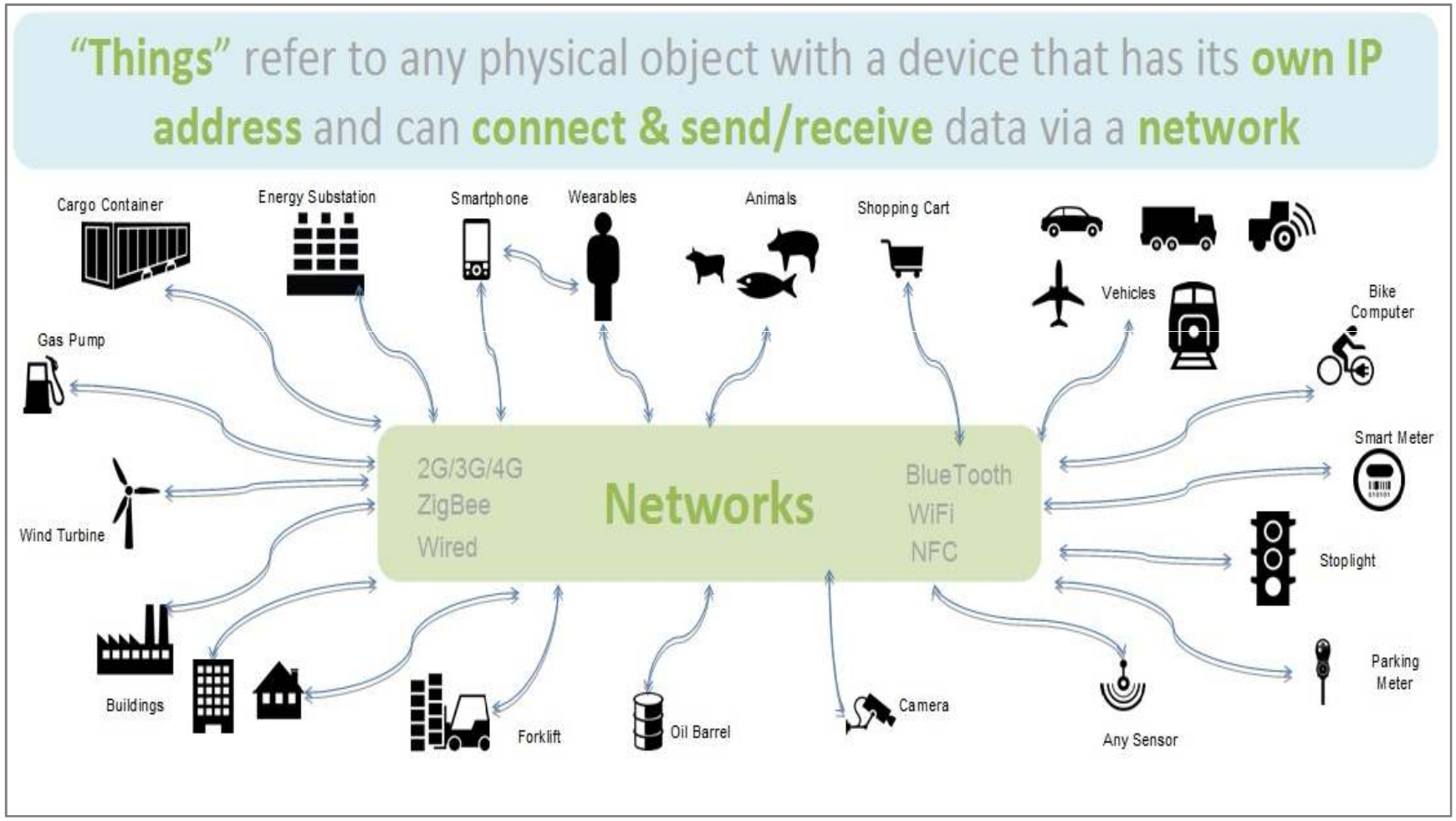
Our world is more
INSTRUMENTED

Our world is more
INTERCONNECTED



Virtually, all systems can become more and more
INTELLIGENT

The Internet of Things is all about physical objects that have the ability to compute, connect to networks, and communicate data



IBM Center for Applied Insights

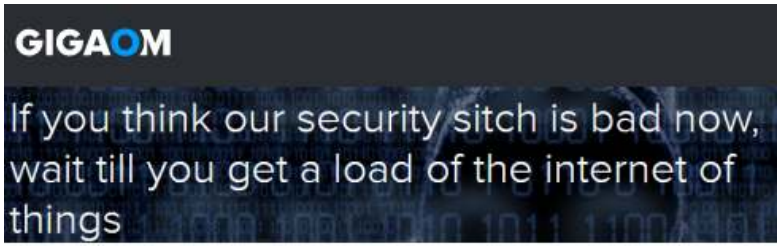
A variety of forecasts have come out over the past couple of years and all forecast billions of IoT connected devices

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

Security will be an increasingly hot topic within the IoT trend as enterprises look for ways to reduce risks of cyber attacks

"Securing the Internet of Things (IoT) is going to be a considerable challenge in the next decade, not least because the security implications are more varied than for traditional IT settings." *ABI Research*



GIGAOM

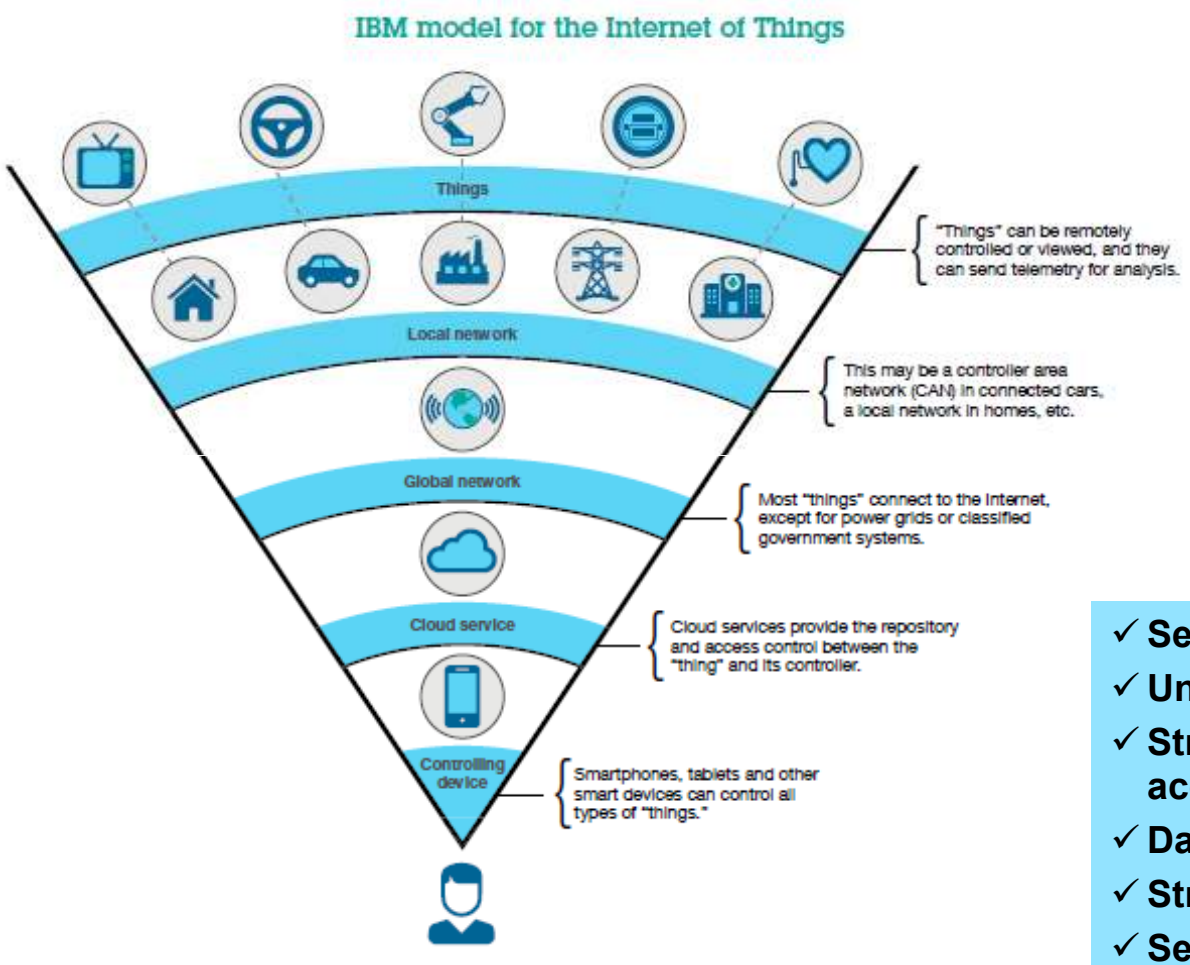
"The IoT is subject to numerous vulnerabilities at all of its core layers: perception, network, and application. The balance between cost and risk often means Things are less likely to employ more complex, resource-intensive security, such as access control and authentication." *ABI Research*

Dark Reading

"The potential damage to people, possessions, businesses and national critical infrastructure from a successful attack on cyber-physical systems through the rapidly emerging Internet of Things (IoT), cannot be underestimated." *Beecham Research*

"Malicious actors intent on taking control of data, identities and passwords have been investigating and making use of Internet connected devices that are not securely developed, making them easier targets than PCs, laptops or tablets." *IBM*

IBM has developed a security model for the Internet of Things



- ✓ **Secure operating system**
- ✓ **Unique Things Identifier**
- ✓ **Strong authentication and access control**
- ✓ **Data privacy protection**
- ✓ **Strong application security**
- ✓ **Security Intelligence**

Image Source: IBM

In this new era of security, the pace of technological change is colliding with increasingly sophisticated cyber threat actors

Your attack surface has grown and your network perimeter is unrecognizable

Adversaries have become more organized, aggressive and determined

BREACH

Narrow focus

National security,

Nation-state actors, APTs[1]

Stuxnet, Aurora, APT-1

Notoriety, activism,

Hactivists

Lulzsec, Anonymous

Monetary gain

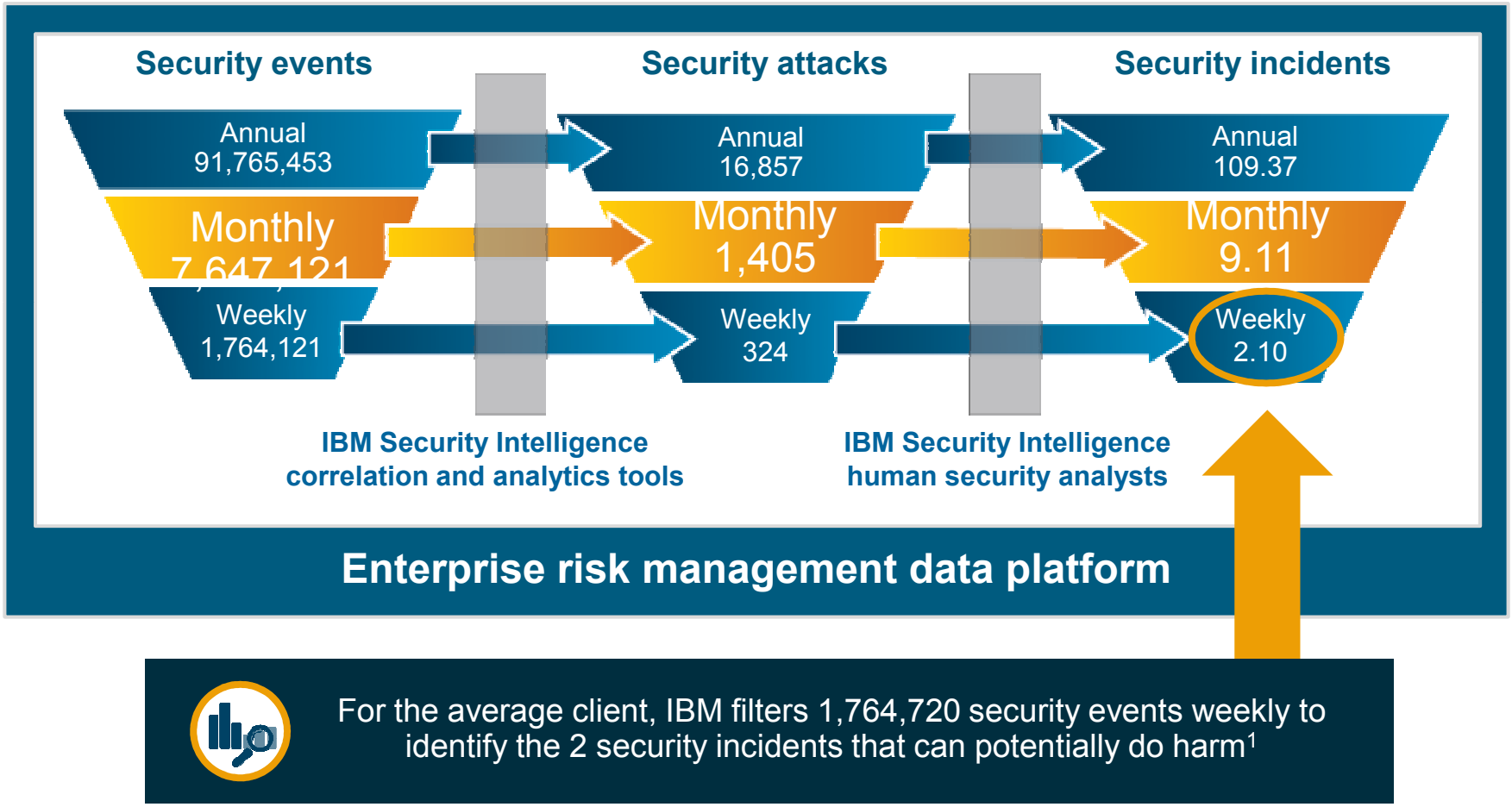
Organized crime

Zeus, ZeroAccess, Blackhole Exploit Pack

Broad focus

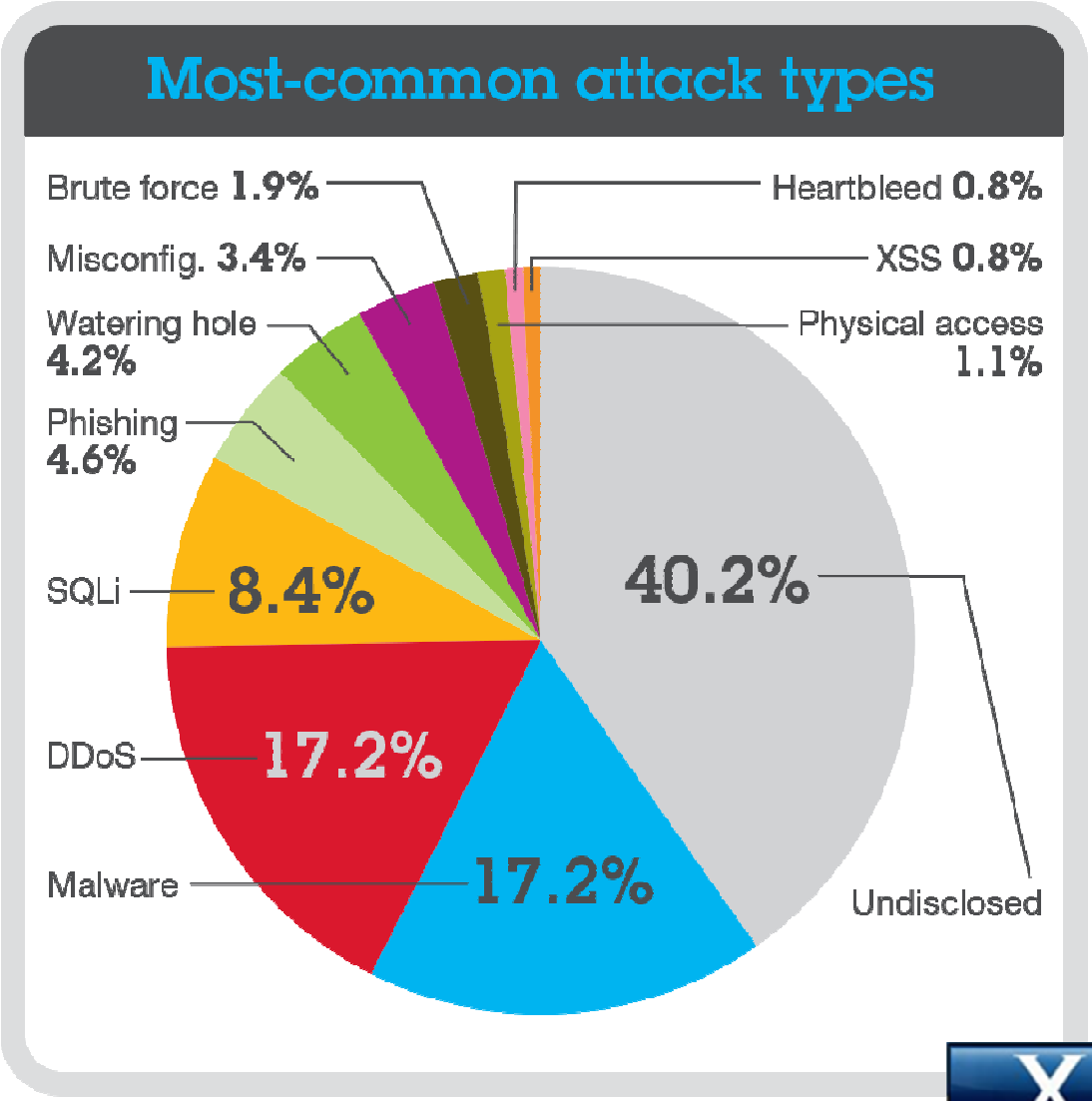
IBM X-Force experience: our clients need to know which threats are most relevant and potentially harmful to their organization

Which of those threats should I be most concerned about?



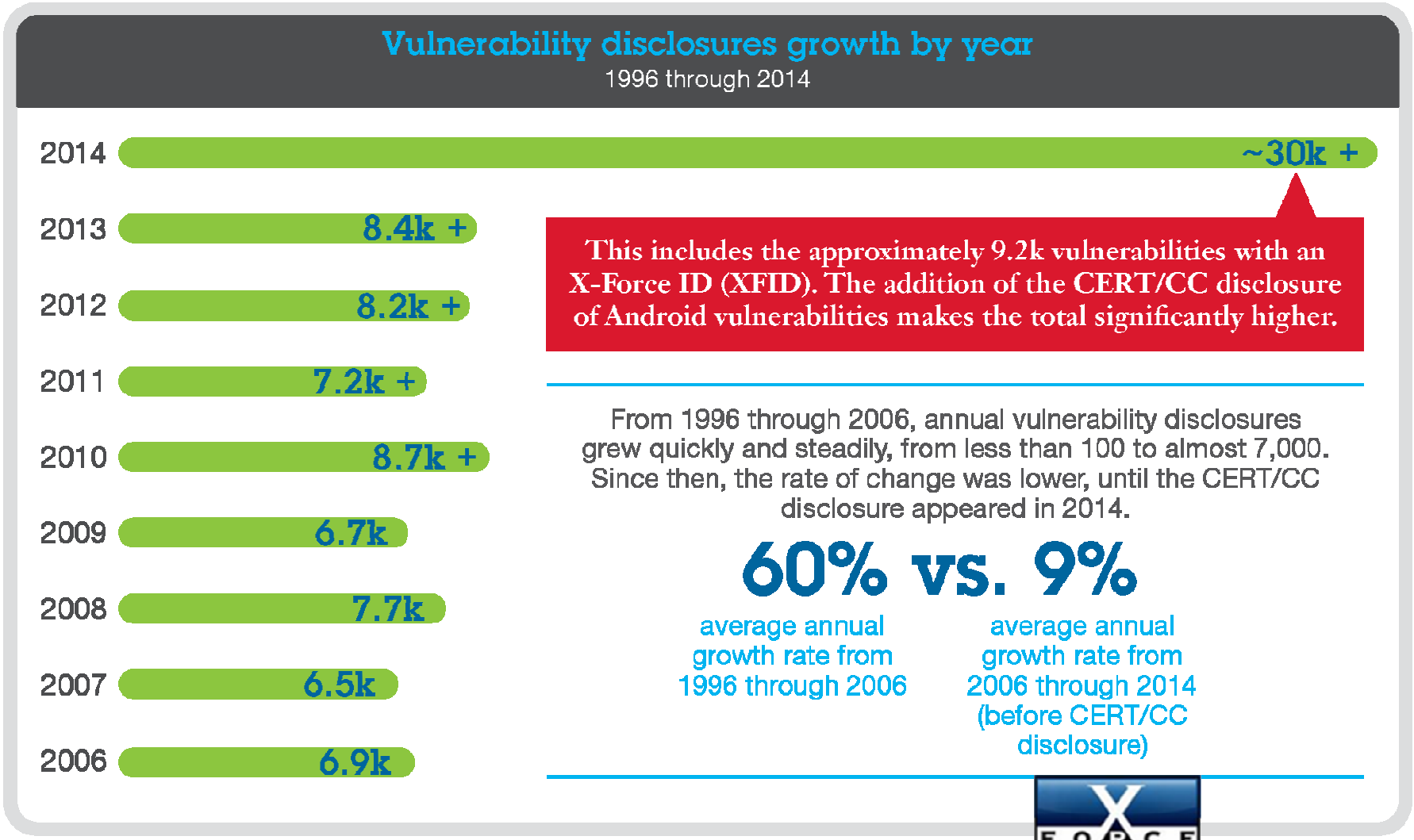
For the average client, IBM filters 1,764,720 security events weekly to identify the 2 security incidents that can potentially do harm[1]

Attackers are applying fundamental attack types in creative, new ways



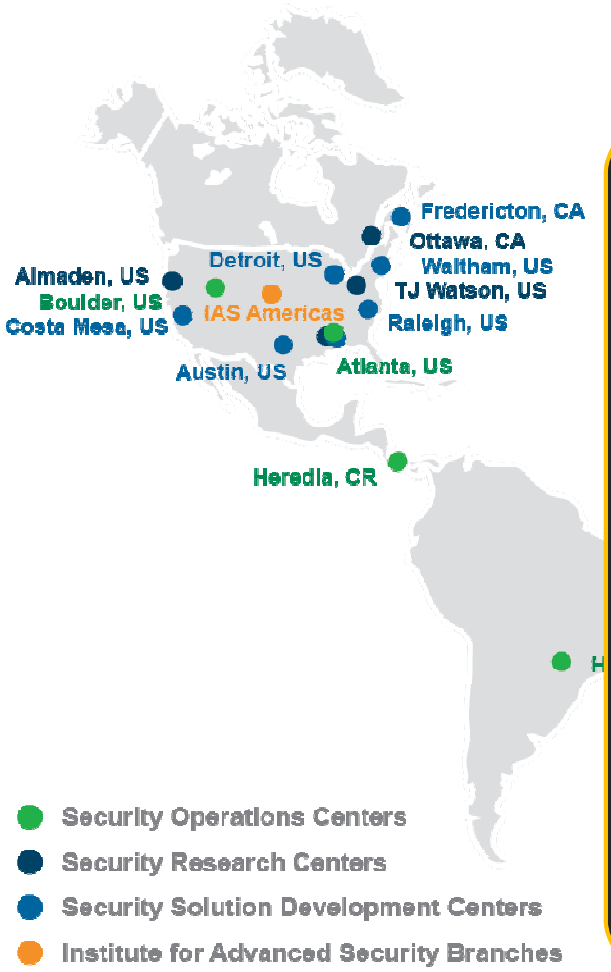
10 *Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015*

The 2014 vulnerability forecast shifted drastically when an automated tool identified a class of vulns affecting thousands of Android apps with improper SSL certificate validation



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

IBM X-Force monitors and analyzes the changing threat landscape



Coverage

20,000+ devices under contract

15B+ events managed per day

133 monitored countries (MSS)

3,000+ security related patents

270M+ endpoints reporting malware

Depth

25B+ analyzed web pages and images

12M+ spam and phishing attacks daily

96K+ documented vulnerabilities

860K+ malicious IP addresses

Millions of unique malware samples

Connect with IBM X-Force Research & Development

Twitter
@ibmsecurity and @ibmxforce

IBM X-Force Threat Intelligence
Quarterly and other research reports:
http://www.ibm.com/security/xforce/

IBM X-Force Security Insights Blog
www.SecurityIntelligence.com/topics/x-force

Find more on SecurityIntelligence.com

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security