ASSOCIAZIONE SPECIALISTI SISTEMI INFORMATIVI

Bologna, 23 gennaio 2019

Cyber Security e IoT

Gli attacchi digitali in Italia: presentazione del Rapporto 2018 OAD e dei dati inerenti l'IoT

Marco R. A. Bozzetti

Presidente AIPSI, Capitolo Italiano ISSA

Ideatore e realizzatore OAD

CEO Malabo Srl

m.bozzetti@aipsi.org

www.aipsi.org

www.oadweb.it

www.malaboadvisoring.it

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory

Indice

- Presentazione AIPSI ed iniziativa OAD
- I principali dati emersi dal Rapporto 2018 OAD
- IoT: considerazioni sui trend e sulla sicurezza IoT
  - Alcuni dati sugli attacchi IoT dal Rapporto 2018 OAD

Marco R. A. Bozzetti e Malabo Srl

- Ingegnere elettronico al Politecnico di Milano, è Presidente AIPSI e CEO di Malabo Srl
- Ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e Gea/Gealab, oltre ad essere stato il primo responsabile dei sistemi informativi (CIO) dell'intero Gruppo ENI (1995-2000).
- Nella seconda metà degli anni 70 è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, partecipando alla standardizzazione dei protocolli del modello OSI dell'ISO
- È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser"
- Commissario d'Esame per le certificazioni eCF (EN 16234 - UNI 11506).
- Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT

- Malabo Srl è stata creata da M. Bozzetti nel 2001
- una società di consulenza direzionale per l'ICT, che opera per Clienti lato domanda e lato offerta basandosi su una consolidata rete di esperti e di società ultra specializzate
- Obiettivo primario degli interventi di Malabo è di creare valore misurabile per il Cliente, bilanciando adeguatamente gli aspetti tecnici con quelli organizzativi nello specifico contesto del Cliente
- Dispone di un proprio laboratorio ICT con server e storage duali, virtualizzati, , collegati con switch a 10 G e connessi ad internet con fibra ottica a 100 Mbps, oltre ad uno spazio in cloud (IaaS)
- Per garantire un effettivo trasferimento di know-how, fornisce come servizio ai Clienti le proprie metodologie e gli strumenti informatici usati nell'intervento consulenziale

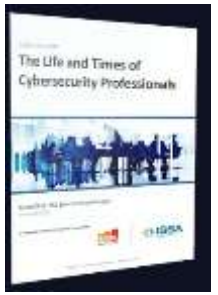
aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
servatorio
acchi Digitali
in Italia

ICT Advisory

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- Associazione apolitica e senza fini di lucro
- Capitolo Italiano di ISSA, Information Systems Security Association, (www.issa.org) che conta >>12.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo
- Obiettivo principale: aiutare i propri Soci nella crescita professionale → competenze →carriera e crescita business
  - Offrendo ai propri Soci servizi qualificati per tale crescita, che includono
    - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
    - ISSA Journal
    - Rapporti annuali e specifici; esempi:
      - Rapporto annuale OAD nel nuovo sito https://www.oadweb.it
      - ESG ISSA Survey "The Life and Times of Cyber Security Professionals"
    - Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016)
    - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
    - Gruppo Specialistico di Interesse CSWI, Cyber Security Women Italy, aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI)



OAD

OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

- *Che cosa è*
  - Indagine via web sugli attacchi digitali intenzionali ai sistemi informatici in Italia

- *Obiettivi iniziativa*
  - Fornire informazioni sulla reale situazione degli attacchi digitali in Italia
  - Contribuire alla creazione di una cultura della sicurezza informatica in Italia, sensibilizzando in particolare i vertici delle aziende/enti ed i decisori sulla sicurezza informatica

- *Che cosa fa*
  - Indagini annuali e specifiche su argomenti caldi, condotte attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende

- *Come*
  - Rigore, trasparenza, correttezza, assoluta indipendenza (anche dagli Sponsor)
  - Rigoroso anonimato per i rispondenti ai questionari
  - Collaborazione con numerose Associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori

2018
10 anni di indagini via web sugli attacchi ai sistemi informatici in Italia

Rapporto 2018 OAD

- 160 pagine A4
- 140 grafici
- 11 Capitoli → 131 pagine A4
  - Cap. 11: Dati dalla Polizia Postale e delle Telecomunicazioni, commentati dall'autore
- 9 Allegati →29 pagine A4
- Prefazione dott. ssa Nunzia Ciardi, Direttore Polizia Postale e delle Telecomunicazioni
- Executive Summary in italiano e in inglese

Per scaricare il Rapporto 2018 OAD (gratuito):

- Registrarsi a https://www.oadweb.it
- Consenso esplicito privacy
- Scaricare il file in pdf

OAD 2018

SPONSOR

PAT

Con la collaborazione della Polizia Postale e delle Comunicazioni
e con la Prefazione al Rapporto 2018 del Direttore dott.ssa Nunzia Ciardi

Le novità di OAD 2018

Chiara separazione tra **che cosa** e **come** attacco

Che cosa è attaccato	Come (tecniche attaccco)						
	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, pharming, hoax,scanning, indagini su Internet, ecc.)	Script e programmi maligni (ransomware, spyware, adware, ..)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	utilizzzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)
Distruzione fisica di dispositivi ICT o di loro parti							
Furto fisico di dispositivi ICT o di loro parti							
Furto informazioni da sistemi fissi (PC, server, storage system, ...)							
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)							
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori							
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS							
Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)							
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.							
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT							
Saturazione risorse digitali (DoS, DDoS)							
Attacchi ai propri sistemi in cloud o in hosting presso Fornitori							
Attacchi a dispositivi IoT (Internet of Thinks) in uso							
Attacchi ai propri sistemi di automazione (DCS, PLC, ..) e di robotica							
Attacchi a sistemi e/o servizi basati su blockchain							

- per ogni tipo di attacco (che cosa), se l'attacco è stato rilevato appaiono delle sotto domande che includono:
  - la frequenza di attacchi
  - le "macro" tecniche di attacco (come)
  - i principali impatti subiti dall'attacco più grave
  - le possibili motivazioni dell'attacco più grave
  - il tempo massimo richiesto per il ripristino ex ante nel caso del più grave attacco di quel tipo subito nell'anno
- se no si salta al tipo di attacco successivo

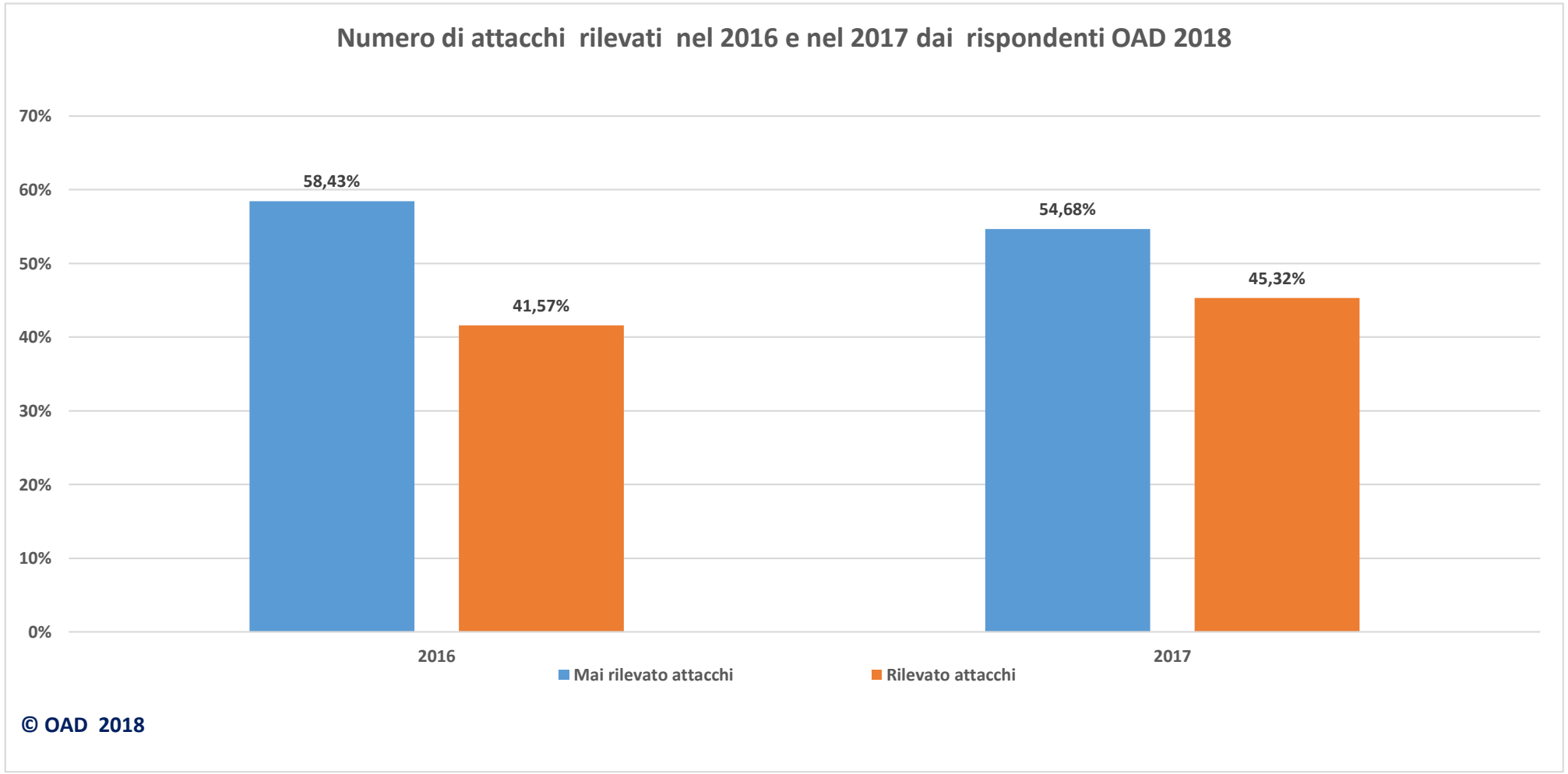
Attacchi ai servizi ICT terziarizzati

Attacchi a IoT

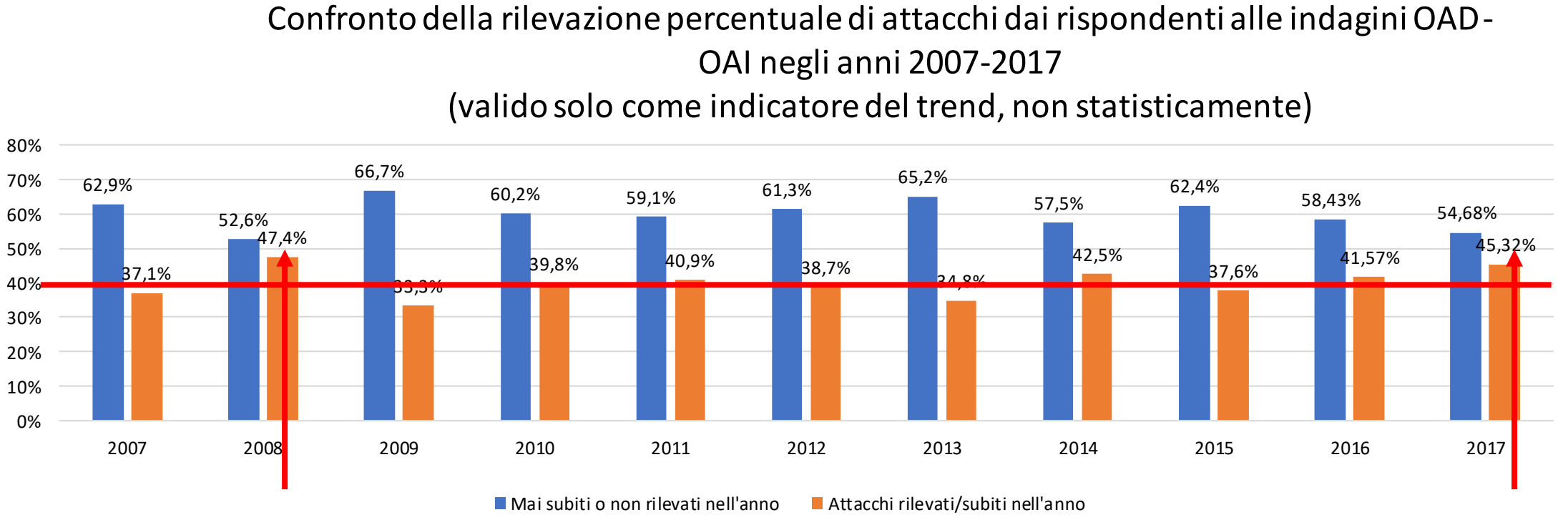
Attacchi sistemi aut. industriale e robotici

Attacchi alla blockchain

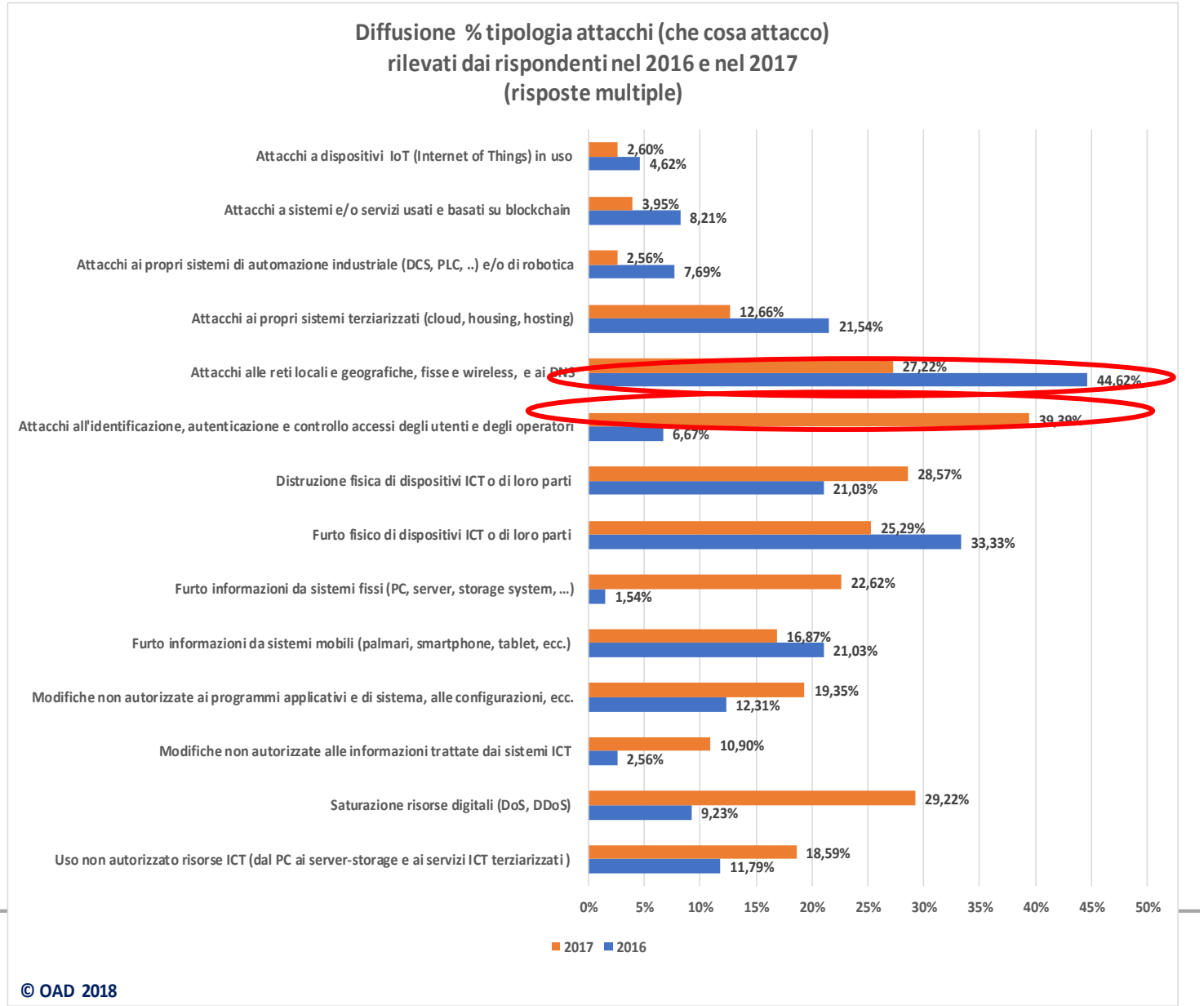
OAD 2018: attacchi rilevati 2016-17



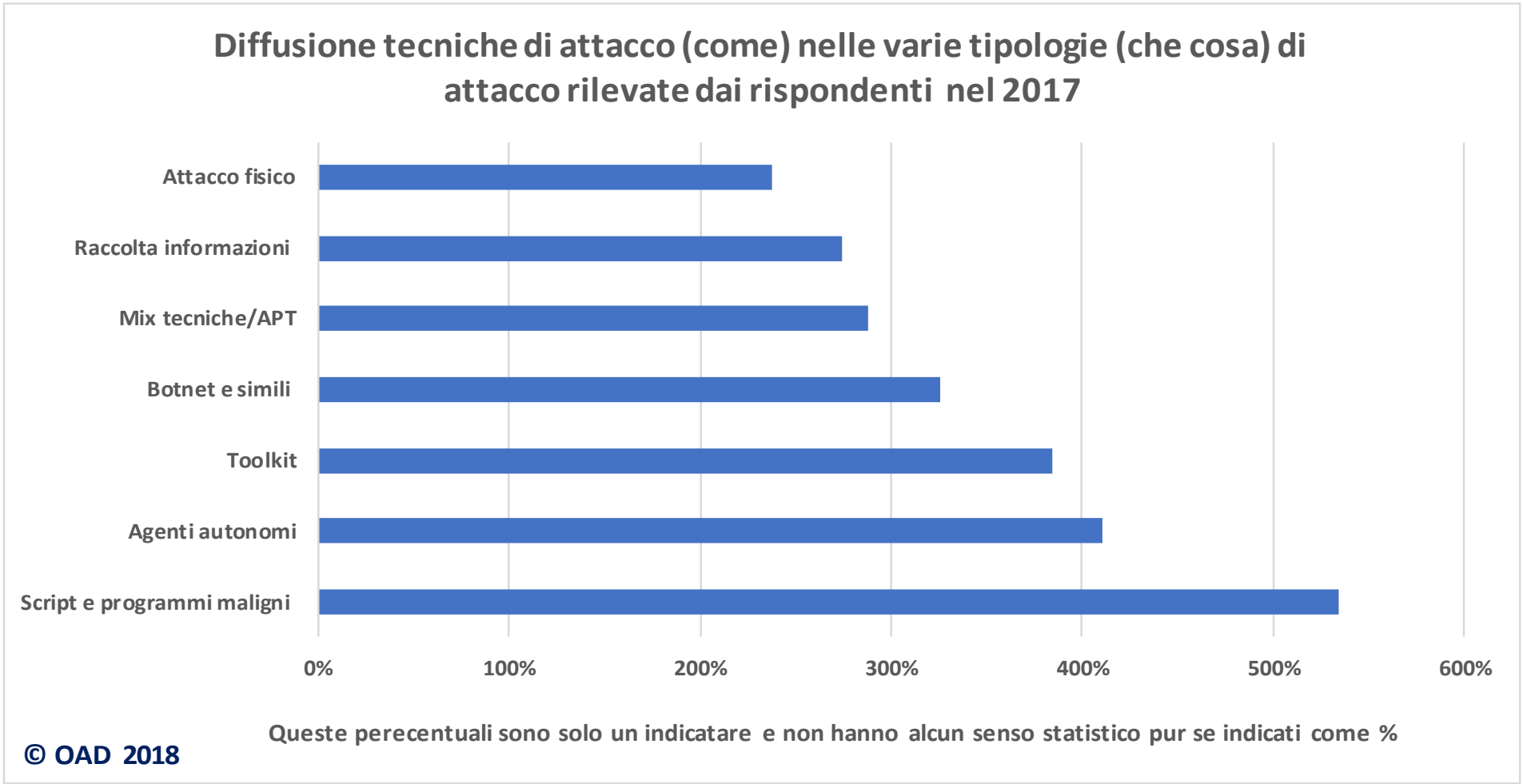
Un indicatore di confronto 2007-2017



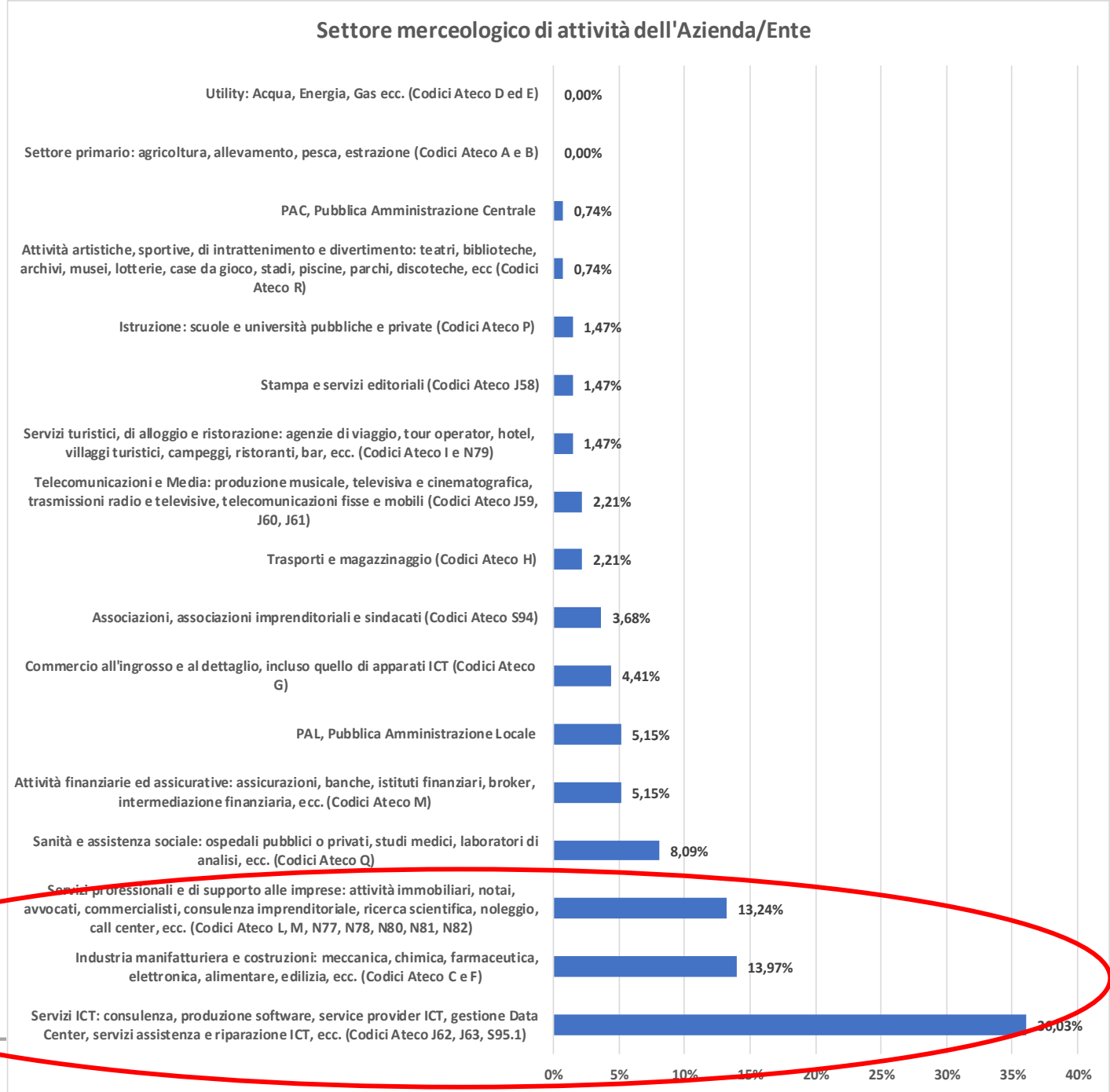
OAD 2018: diffusione tipologia attacchi rilevati 2016-17



OAD 2018: diffusione tecniche di attacco 2017

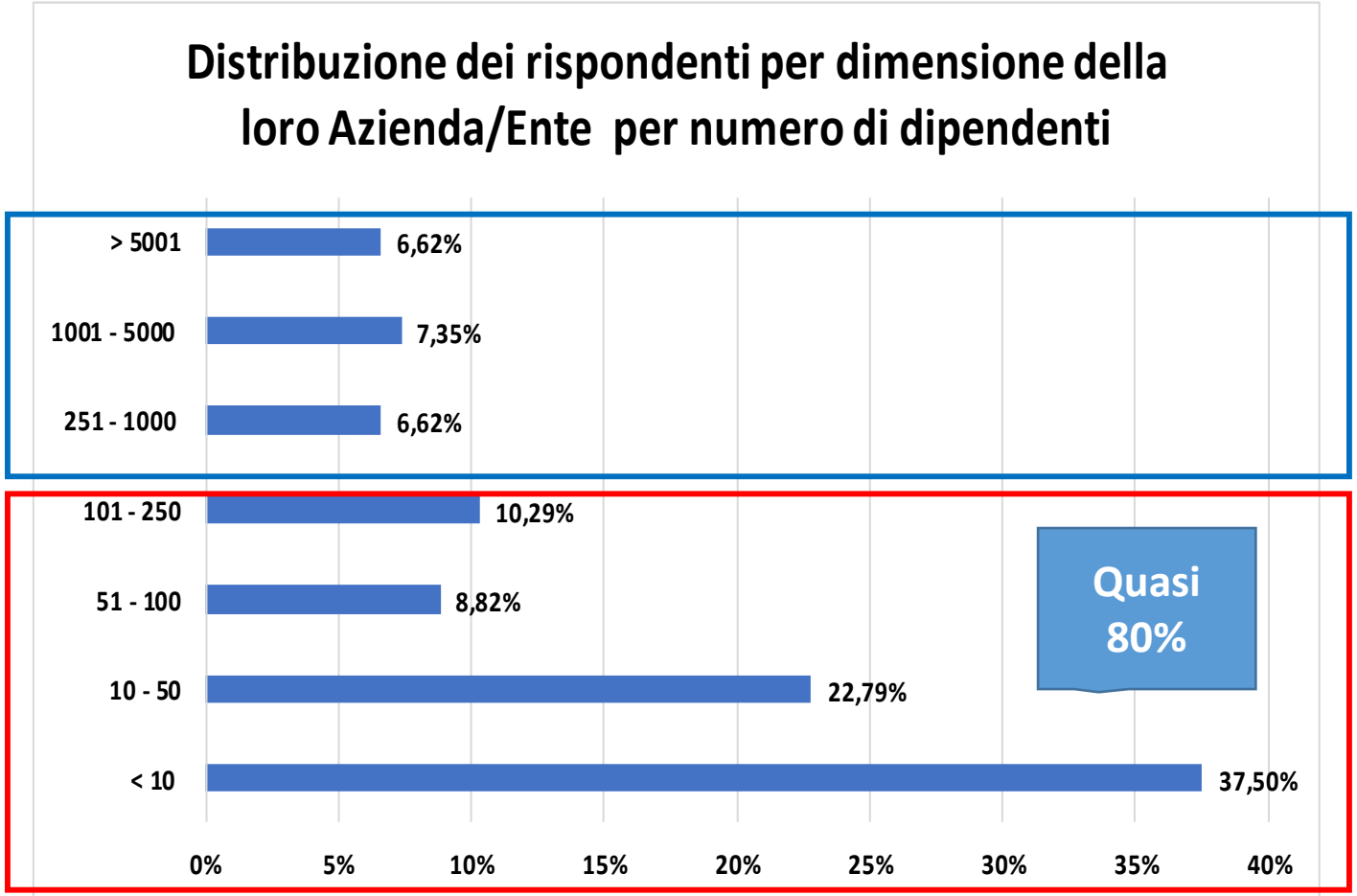


OAD 2018: settore merceologico aziende/enti dei rispondenti



aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD 2018: rispondenti per dimensioni azienda/ente



I più recenti dati ISTAT per le aziende:

- Fino a 9 dipendenti: **4.180.870**
- Da 10 a 49: 184.098
- Da 50 a 249: 22.156
- 250 e più: 3.787.

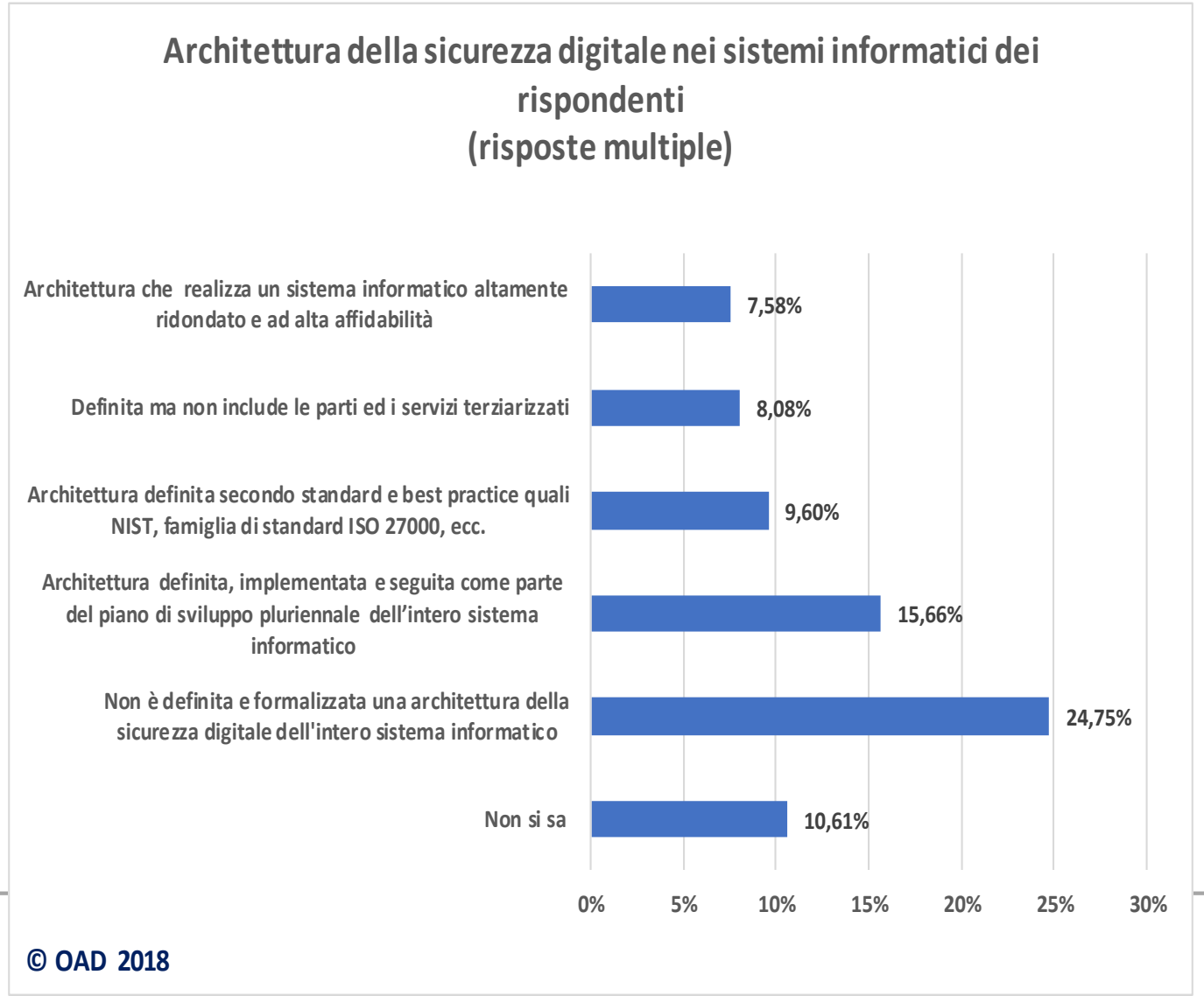
Pubbliche Amministrazioni:

- Circa **55.000**

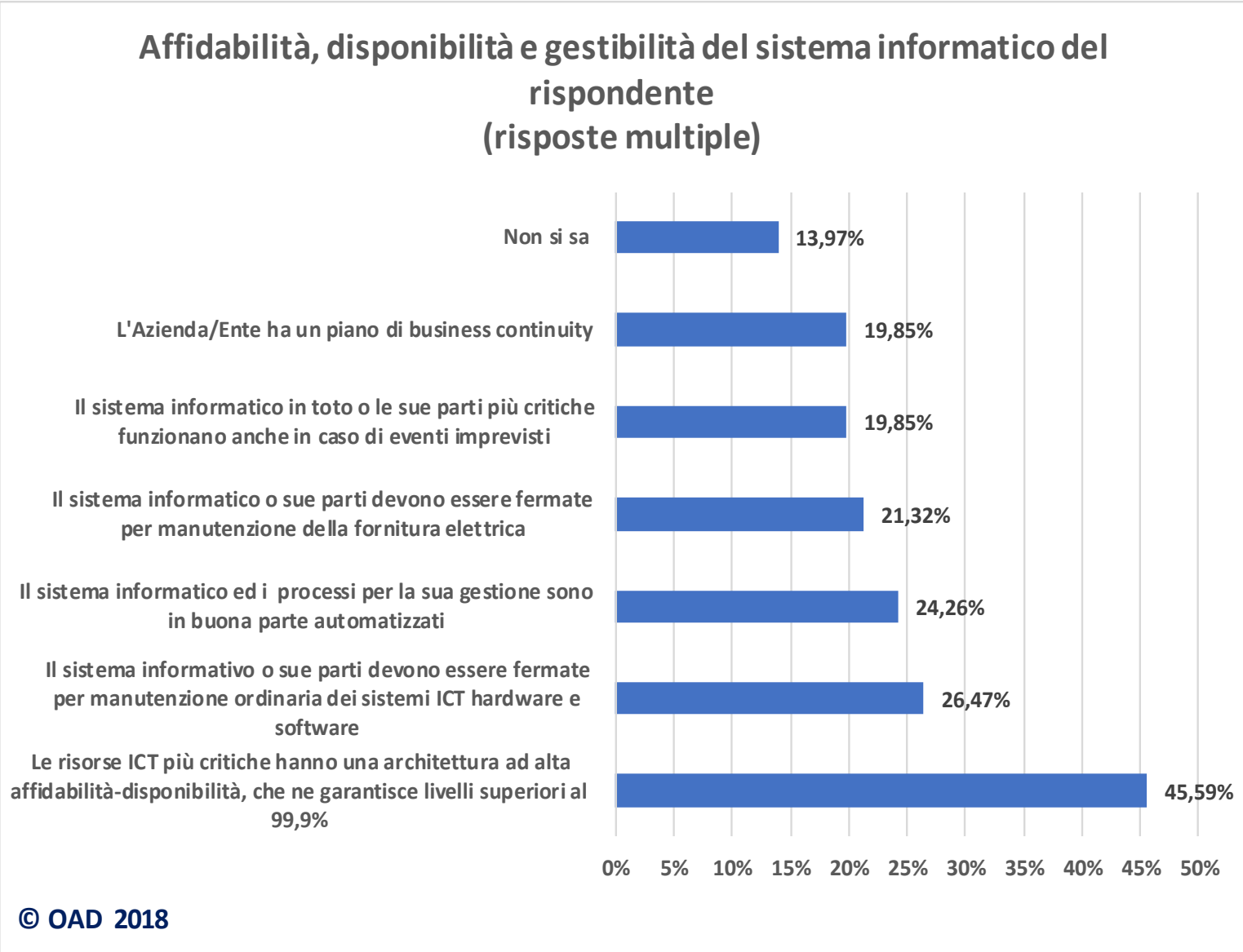
OAD 2018: le misure di sicurezza digitale delle aziende/enti dei rispondenti

- **Misure tecniche**
  - Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico
  - Contromisure fisiche
  - Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
  - Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
  - Contromisure tecniche per la protezione logica dei singoli sistemi ICT
  - Contromisure tecniche per la protezione degli applicativi
  - Contromisure per la protezione dei dati
- **Misure organizzative**
  - struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative
  - Contratti e clausole sicurezza digitale con le Terze Parti (GDPR dovrebbe aiutare!!)
  - Awarness sicurezza digitale
  - auditing
- **Misure di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

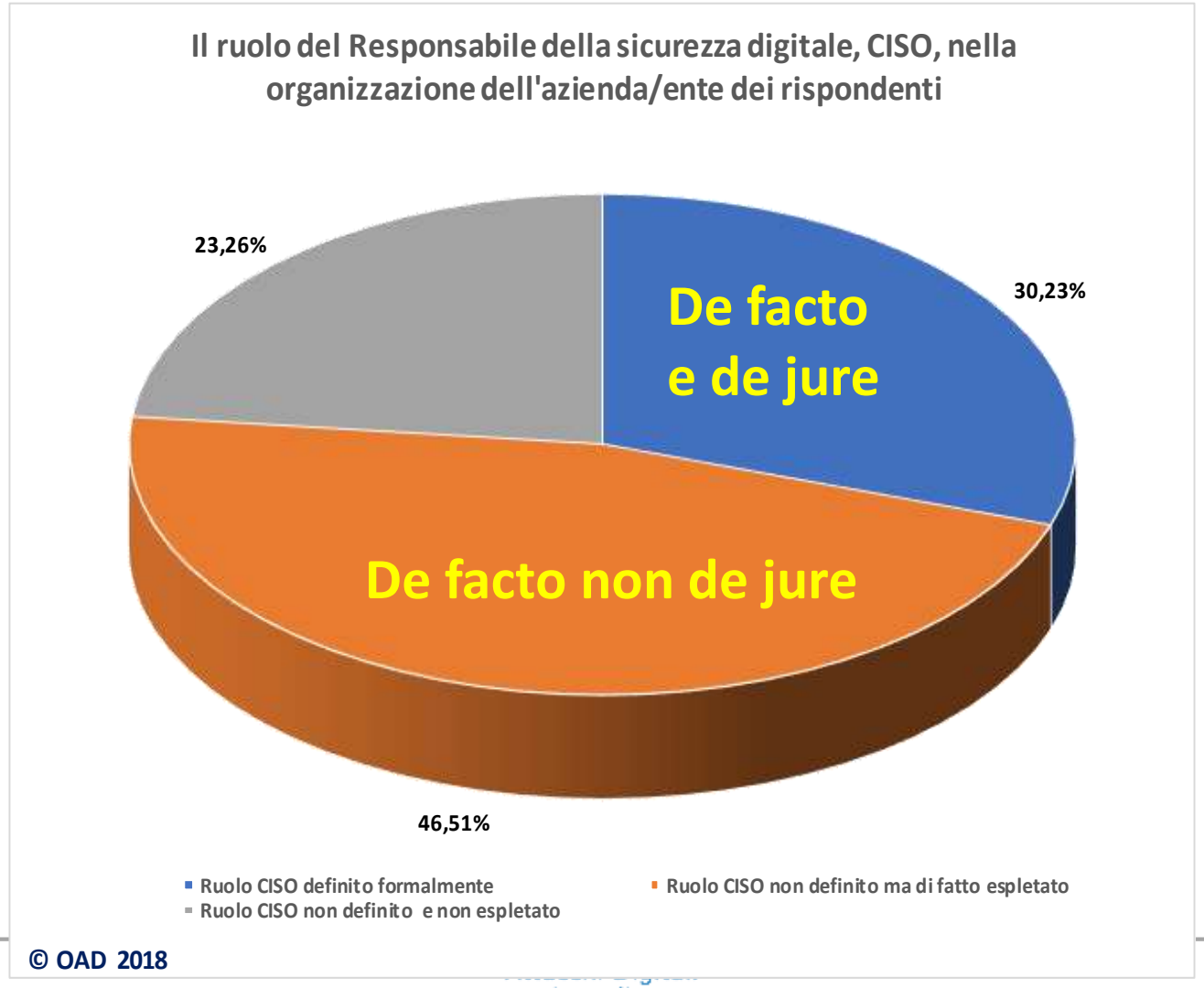
OAD 2018: architettura sicurezza digitale nei SI delle aziende/enti dei rispondenti



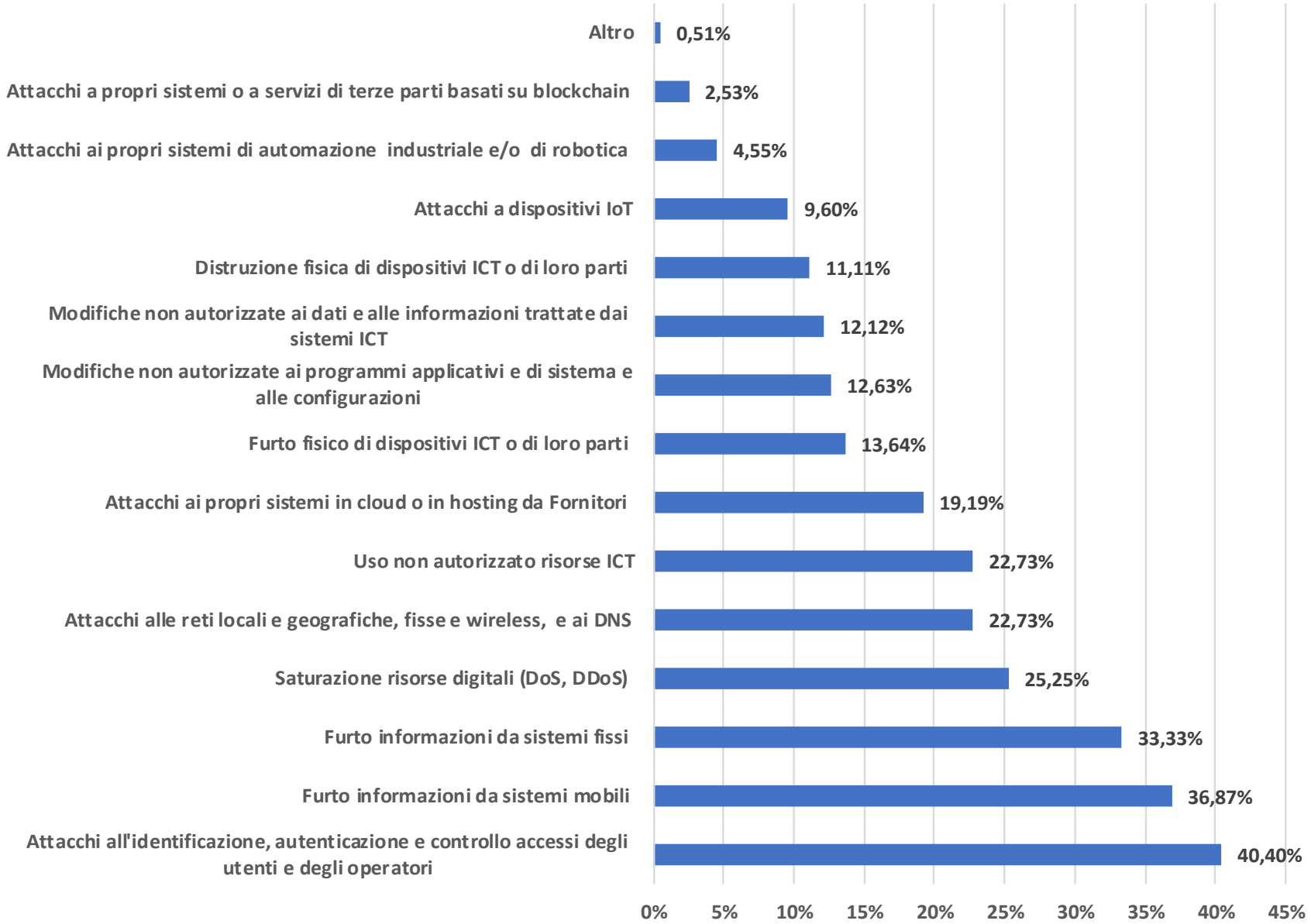
OAD 2018: livello sicurezza digitale dei SI delle aziende/enti dei rispondenti



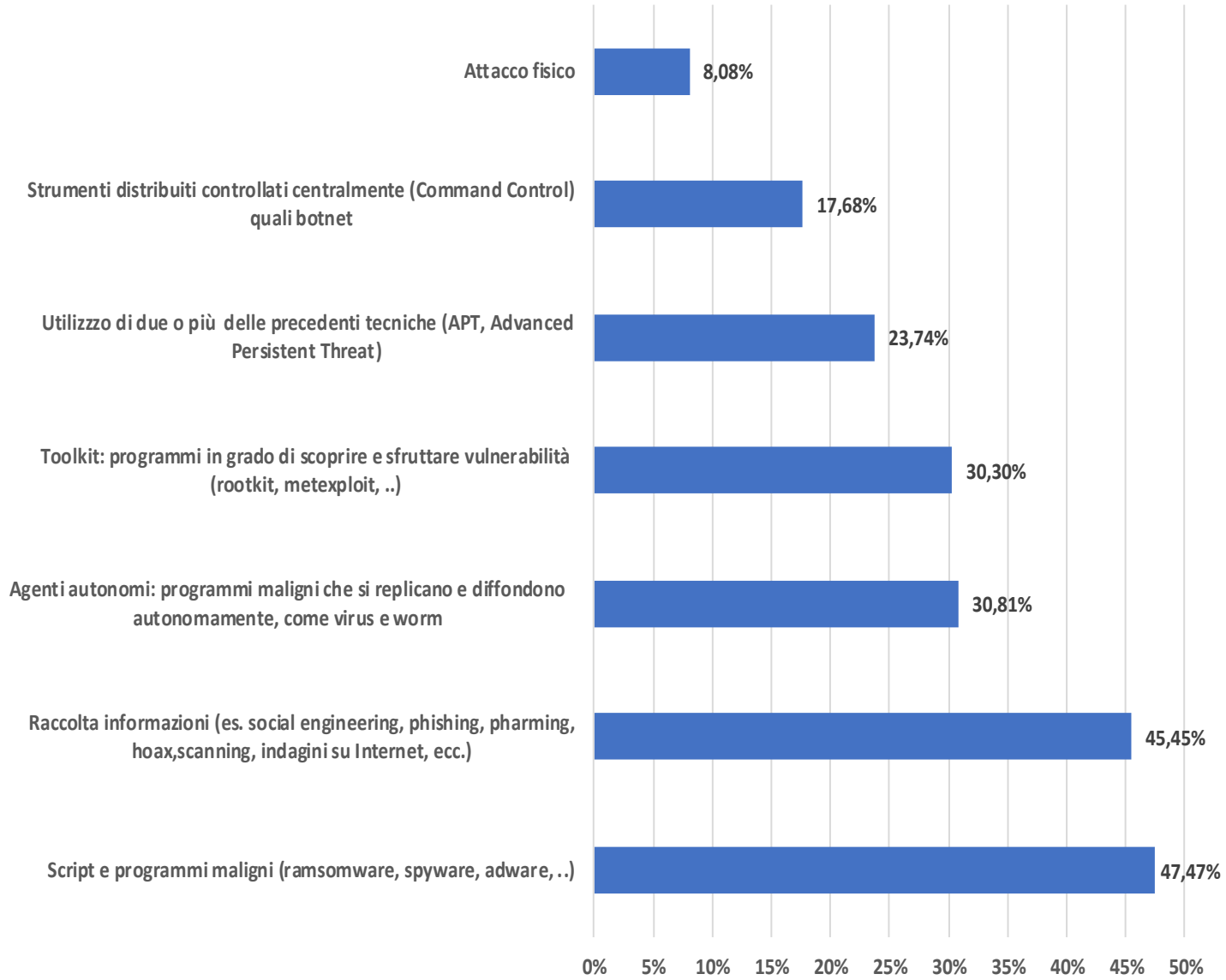
OAD 2018: CISO nella organizzazione per la sicurezza digitale delle aziende/enti dei rispondenti



Tipologia attacchi (che cosa) più temuti nel prossimo futuro (risposte multiple)



Tecniche di attacco (come) più temute nel prossimo futuro (risposte multiple)



OAD 2018: dati Polizia Postale - 1

C.N.A.I.P.I.C. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Protezione strutture critic	gen – 31 dic 201	gen – 31 dic 2016	Differenza %
Attacchi rilevati	1032	844	**22,27%**
Alert diramati	31524	6721	**369,04%**
Indagini avviate	72	70	**2,86%**
Persone arrestate	3	3	**0,00%**
Persone denunciate	1316	1226	**7,34%**
Perquisizioni	73	58	**25,86%**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	83	85	**-2,35%**

Indagini/ attacchi 6,89%

Indagini/ attacchi 8,29%

Arresti/ denunce 0,23%

Arresti/ denunce 0,24%

OAD 2018: dati Polizia Postale - 2

Financial Cyber Crime

Financial Cyber Crime	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Transazioni Fraudolente Bloccate in €	€ 20.839.576,00	€ 16.050.812,50	**29,84%**
Somme Recuperate	€ 862.000,00	=	
Arrestati	25	25	**0,00%**
Denunciati	2851	3772	**-24,42%**

Arresti/ denunce 0,88%

Arresti/ denunce 0,66%

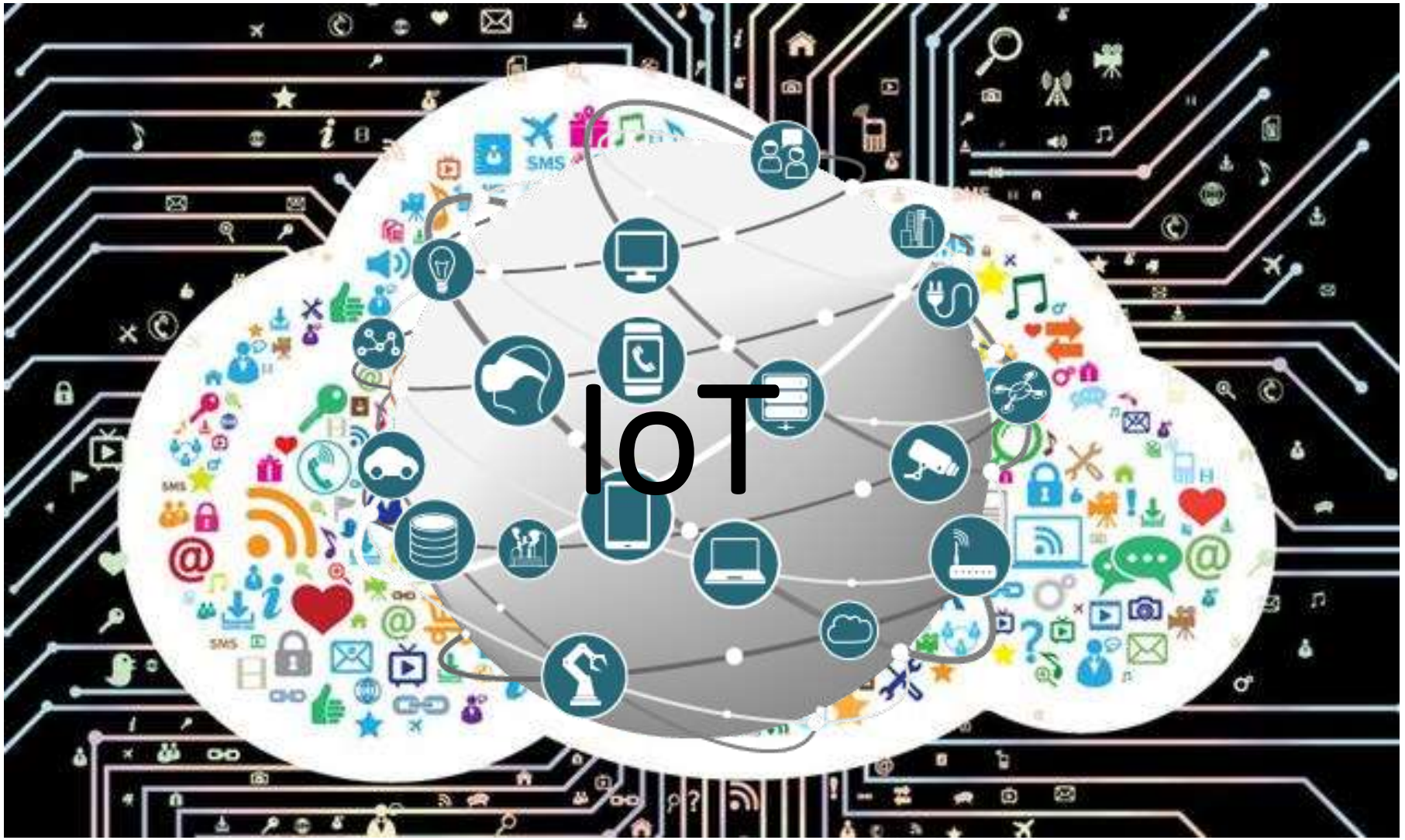
24

Cyber Terrorismo

Cyber Terrorismo	1 gen – 31 dic 2017	gen – 31 dic 2016	Differenza %
Arrestati	4	2	**100,00%**
Denunciati	18	9	**100,00%**

Arresti/ denunce 22%

Arresti/ denunce 22%


IoT

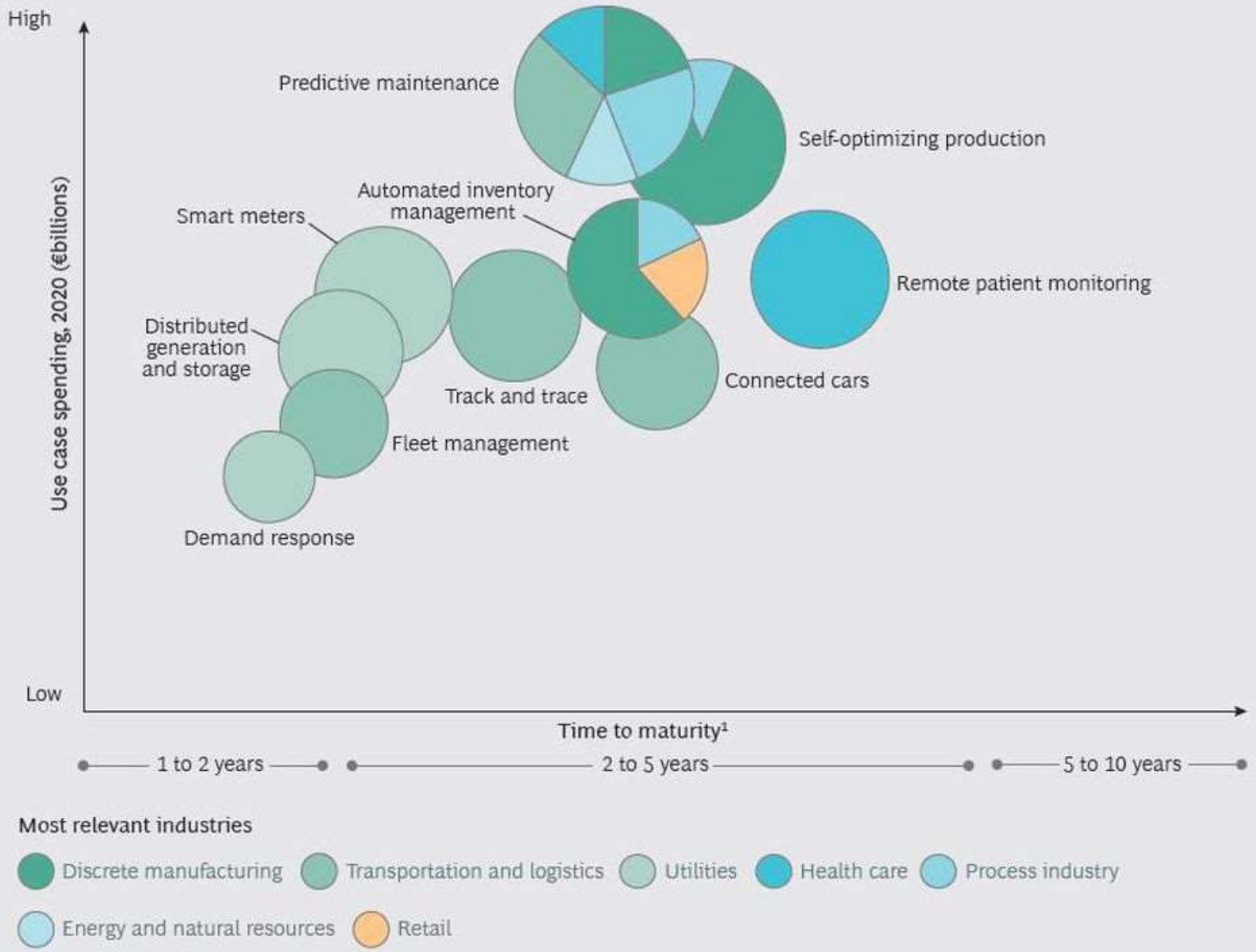
Il fenomeno IoT

- ***In Italia, dall'Osservatorio MIP: 3,7 miliardi di euro nel 2017 +32% rispetto al 2016), di cui:***
  - *26% contatori intelligenti*
  - *22% automobili connesse*
  - *14% Smart Building*
  - *9,7% Smart Logistics*
  - *8,6% Smart City*

- **L'impatto del Programma Industria 4.0**

- **A livello mondiale:**
  - B2B spending on IoT technologies, apps and solutions will reach €250B ($267B) by 2020 (BCG-Forbes)
  - By 2020, 50% of IoT spending will be driven by discrete manufacturing, transportation and logistics, and utilities (BCG-Forbes)
  - Between 2015 to 2020, BCG predicts revenue from all layers of the IoT technology stack will attain a least a +20% Compound Annual Growth Rate (CAGR)
  - McKinsey Global Institute predicts it could have an annual economic impact of $3.9 trillion to $11.1 trillion worldwide by 2025

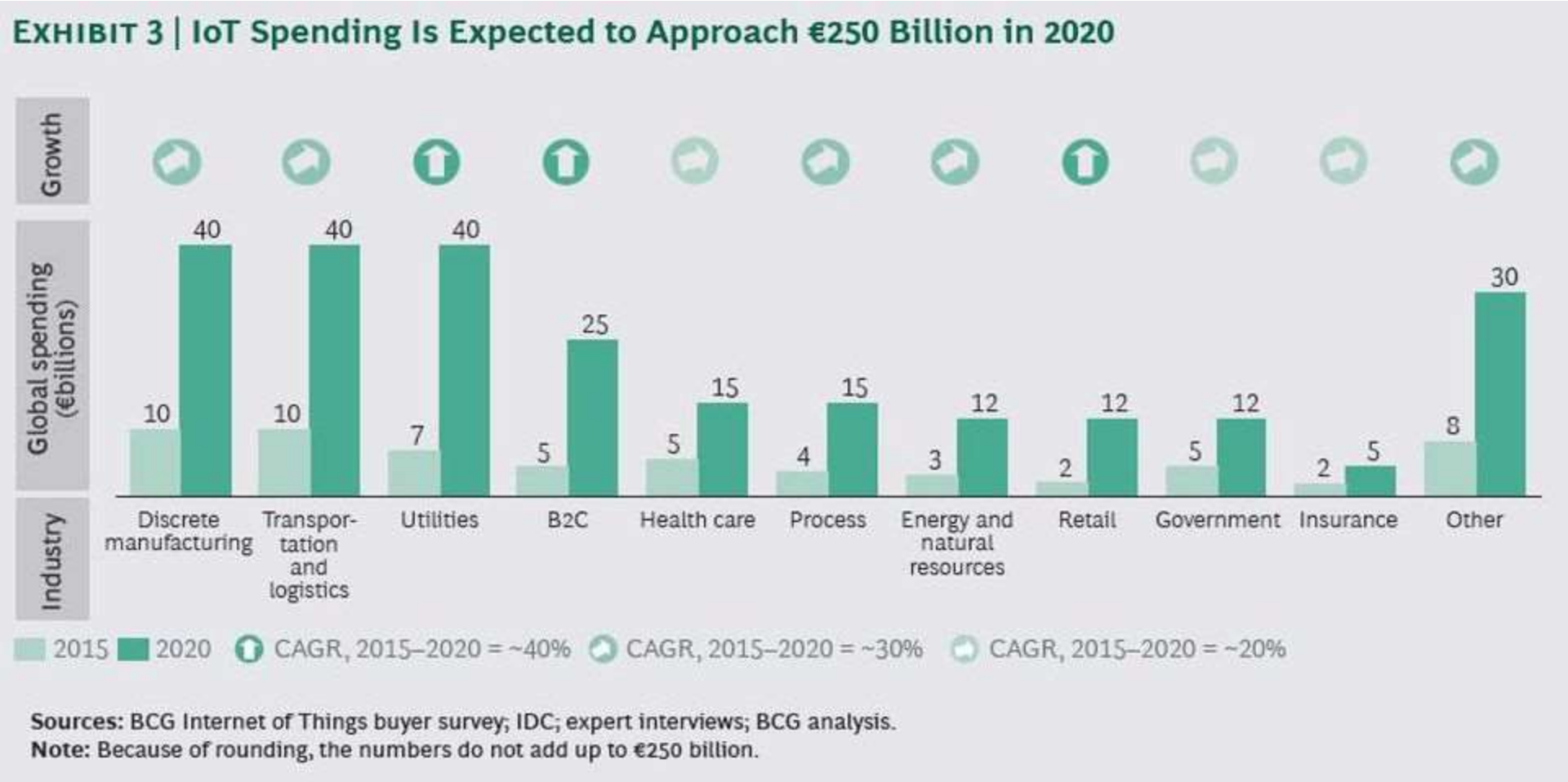
EXHIBIT 2 | Ten Use Cases Will Drive IoT Growth Through 2020



Sources: BCG Internet of Things buyer survey; IDC; expert interviews; BCG analysis.
Note: The bubble sizes indicate relative amounts of spending.
¹Productive and scaled use within real-life settings (that is, no pilots). To capture opportunities, vendors must quickly ramp up activities. The timing of commercial viability for these use cases was derived from responses to a survey question: "When do you expect to productively use [name of use case]?"

Fonte: BCG

Spesa IoT per settore a livello mondiale



Fonte: BCG

Internet delle cose: dove e come?

Dove? Dappertutto

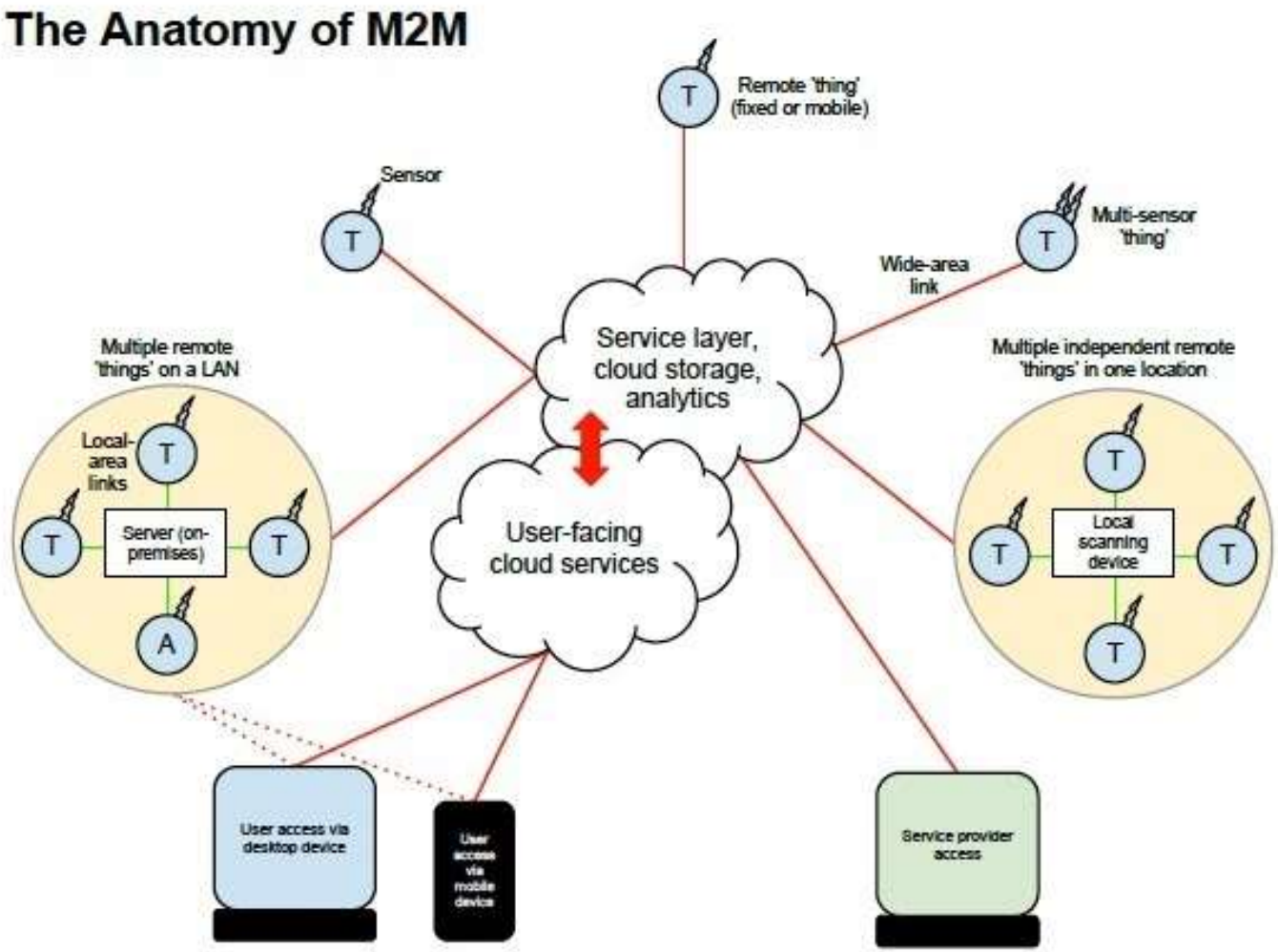
- **domotica**
- **elettrodomestici intelligenti**
- **Controlli mezzi di trasporto: dalle autovetture agli aerei**
- **Giochi (es. slot machine)**
- **sistemi di pagamento mobili da molteplicità di dispositivi**
- **Stampa 3D**
- **Logistica avanzata magazzini**
- **Armi int**
- **videosorv**
- **controlli in ture critiche**
- **Controlli med zati, sale operatorie robotizzate, e-health**
- **chioschi e colonne informative**
- **Contatori smart gas ed elettricità**
- **Smart city**
  - **Controllo e gestione viabilità, pulizia strade, safety, ….**

Come ? Con sistemi ICT

- Sistemi ad hoc ti e sistemi "g
- R S, e
- N
- enti
- diversi: SOA e ces
- emetria
- Autenticazione forte con KPI e «criptografia leggera»
- RFID e codici QR
- IETF 6LoWPAN, RPL, CoAP
- Protocolli specifici di comunicazione ed interoperabilità per i diversi ambienti d'uso (si veda NISTIR 8200)
- …….

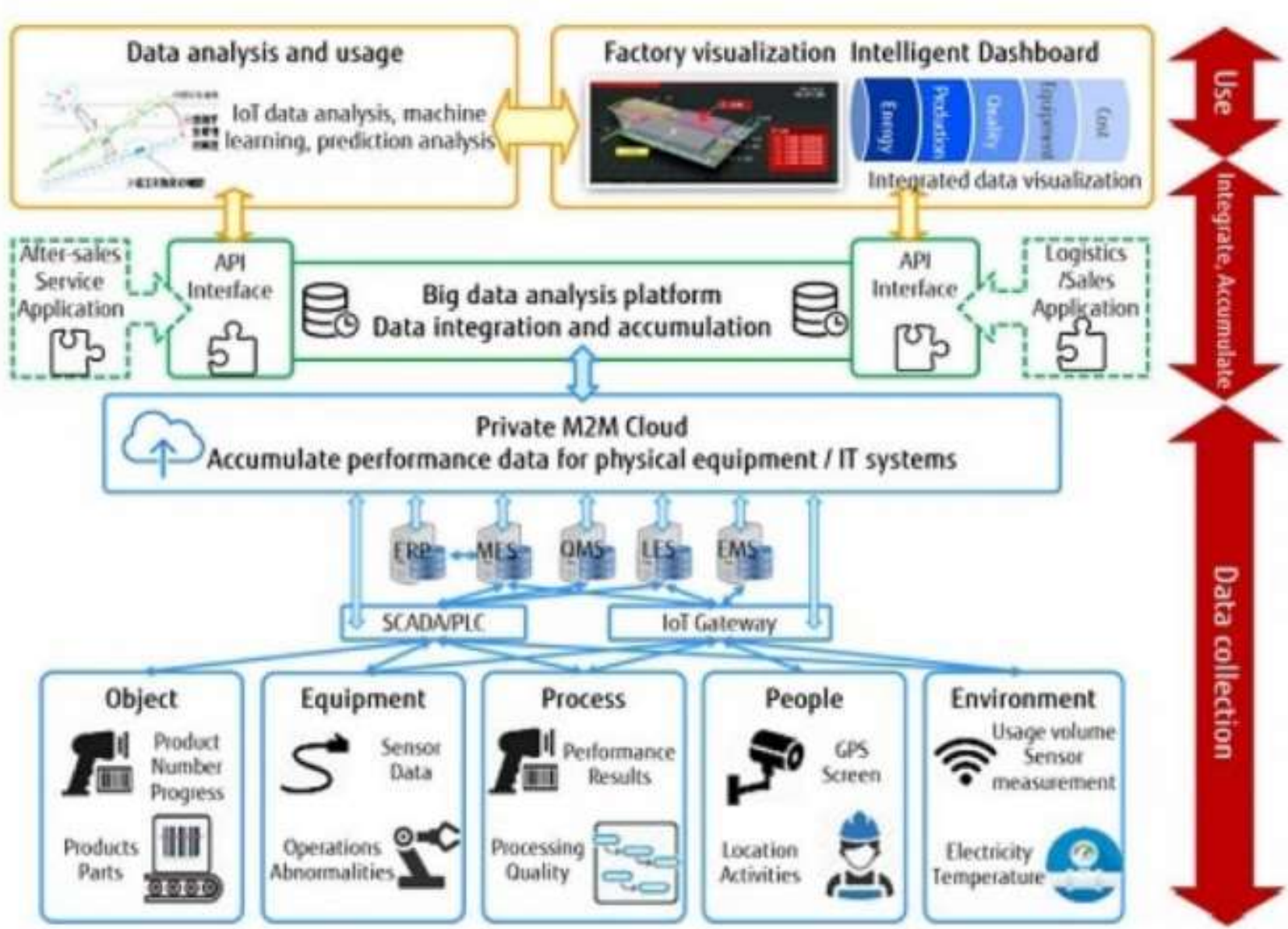
Ho tutti i problemi di sicurezza ICT
+ autenticazione sw
+ non presidio

IoT è un'interazione M2M, Machine to Machine



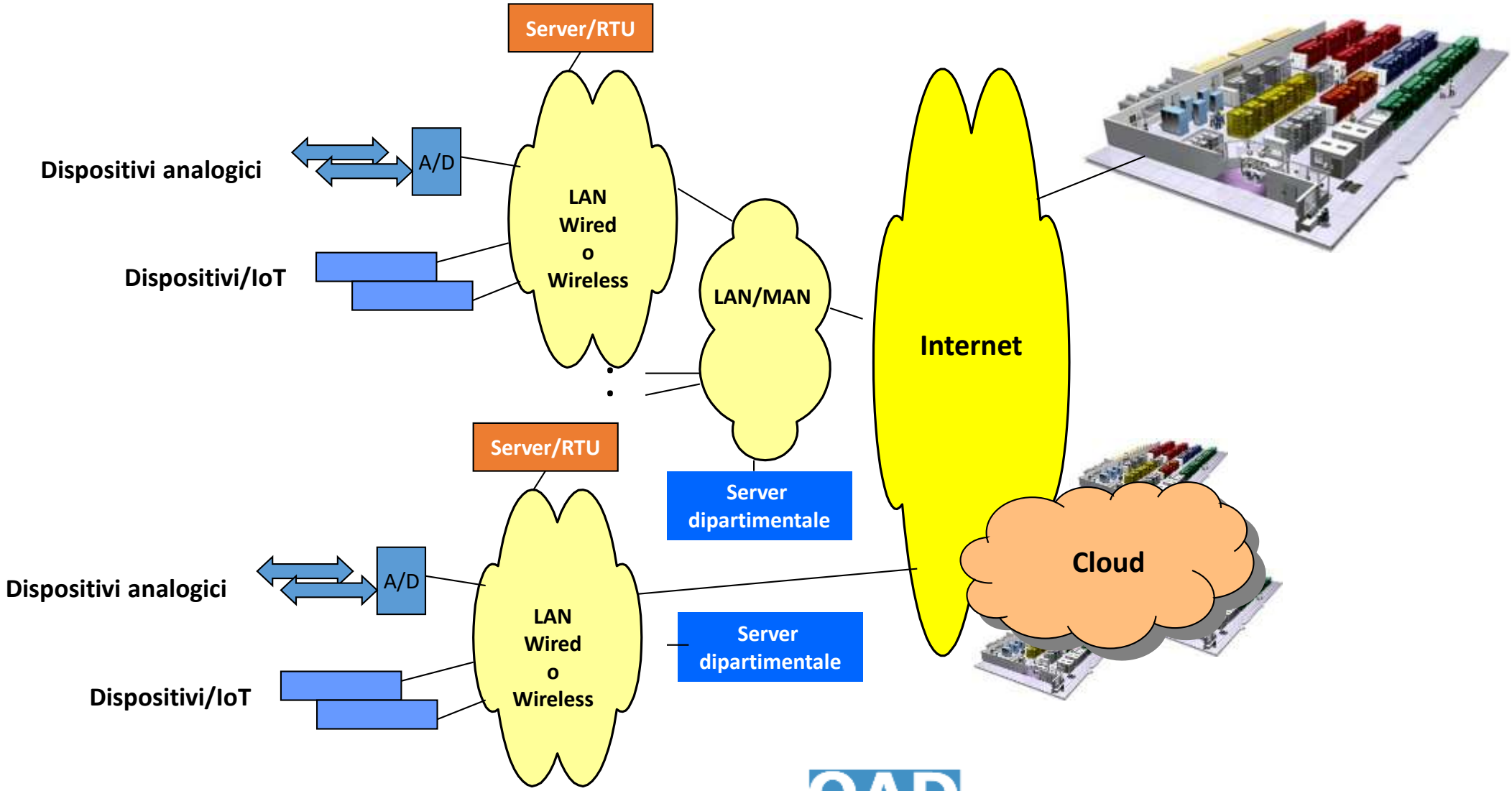
Fonte: ZDnet

Architettura esempio Smart Manufacturing Environment



Fonte:NIST

Schema esempio integrazione IoT con il sistema informatico



L’integrazione digitale dei sistemi di controllo/IoT con il sistema informatico

Pro

- Approccio architetturale unico
- Standardizzazione
- Utilizzo medesima infrastruttura a livello LAN/WAN
- Integrazione funzionale ed interoperabilità application-application e device-device
- Monitoraggio e controllo centralizzato e da remoto
- Maggior flessibilità, affidabilità e disponibilità
- Rilevazione criticità proattiva e dinamica quasi in tempo reale
- Segnalazione allarmi multifunzionale e multidevice
- Apertura a nuove funzionalità applicative → nuove opportunità di business

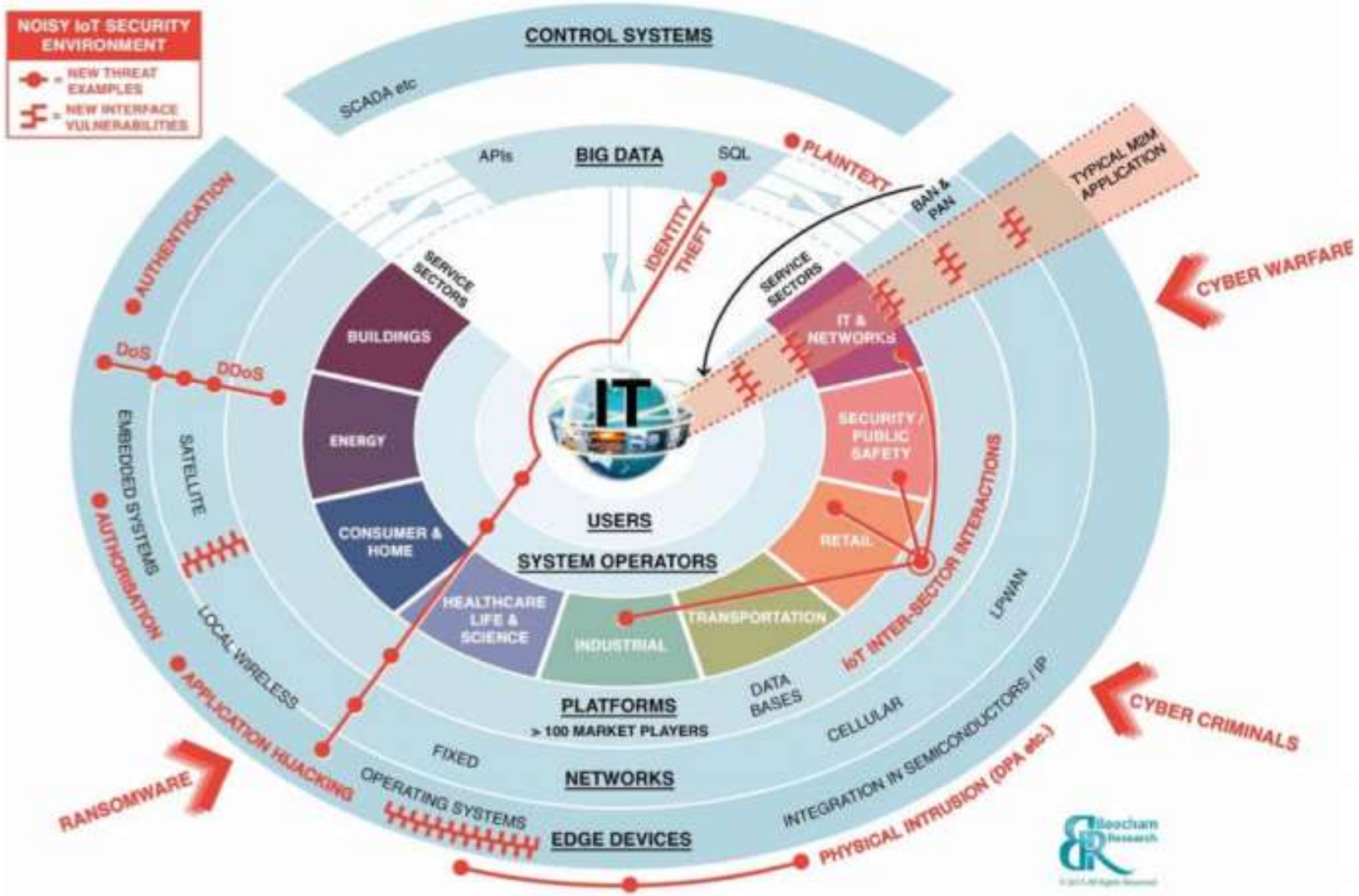
Contro

- Maggior complessità
  - Progettuale
  - gestionale
- Necessità di maggiori e più diversificate competenze
- apertura del mondo dei sistemi di controllo alle vulnerabilità ed agli attacchi tipici dei sistemi informatici (Stuxnet)
- Change management
  - Processi
  - Personale

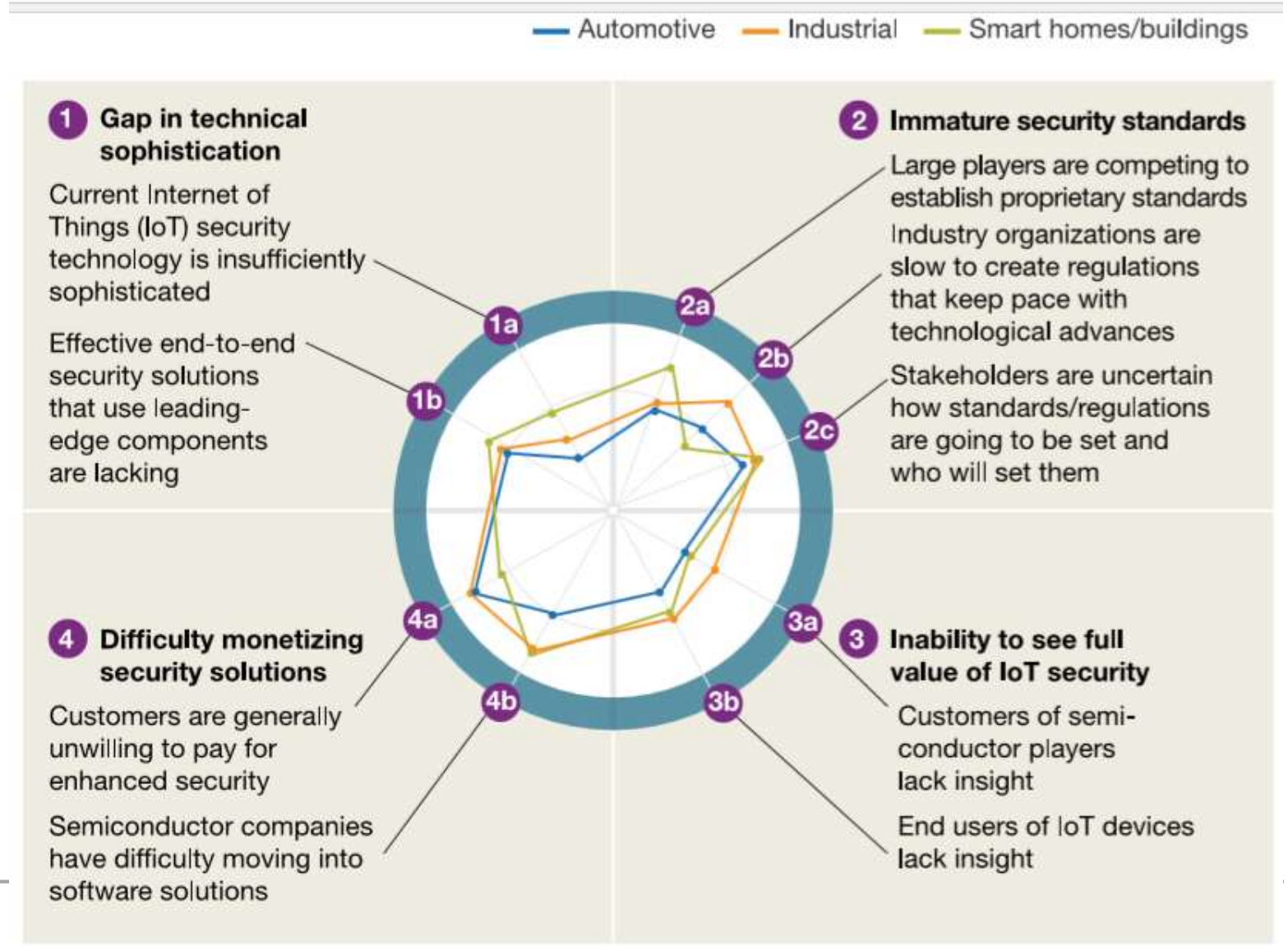
IoT: chip ovunque. E la sicurezza?

- **Orientamento alla vendita di massa (pochi $/chip) → minor qualità**
- **Orientamento al cloud per la raccolta di dati e per lo storage**
- **Sistemi non presidiati-custoditi (unattended) → richiederebbero un monitoraggio e controllo da remoto sofisticato**
- **Necessità di integrazione ed interoperabilità tra IoT e sistemi informatici**
  - **Aumento della complessità**
  - **Differenti (troppi??!!!) standard di protocolli ed interfacce**
- **<u>Tipici problemi sicurezza ICT in IoT</u>**
  - Sicurezza dei sistemi IoT e della loro integrazione/interazione con gli altri sistemi ICT
  - sicurezza ICT a livello progettuale
  - Problemi nell'identificazione ed autenticazione IoT (prevalentemente via certificati, essendo autonomi e non presidiati)
  - "Tradizionali" vulnerabilità tecniche, dalle reti al software e alla virtualizzazione
  - Vulnerabilità degli utenti privilegiati (gli utenti finali in ambito IoT praticamente non esistono)
  - Vulnerabilità della gestione
    - Difficoltà di/non aggiornamento versioni precedenti → i bachi rimangono → vengono sfruttati dagli attaccanti
    - Misure di sicurezza non attivate → dispositivi non protetti
      - Es: lasciare la password di default pre configurata nel dispositivo (Es: Pwd 0000 su Bluetooth)
    - Vulnerabilità cloud

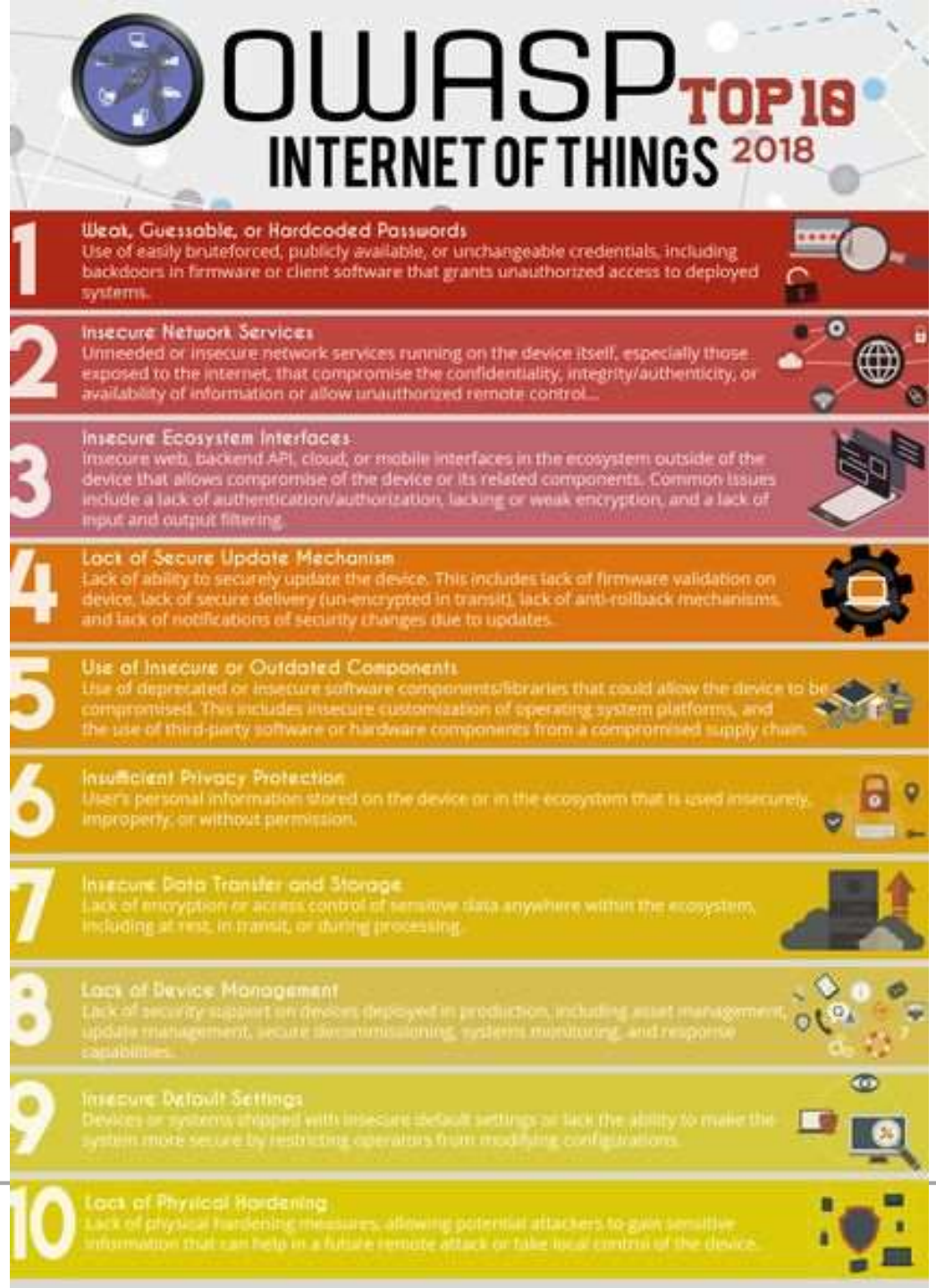
La mappa dei rischi nell'IoT
(Fonte: Beecham ripresa da NIST)



Per la sicurezza dei dispositivi IoT essenziale il ruolo dei semiconduttori (IC, ASIC): cosa pensano i fornitori (McKinsey)



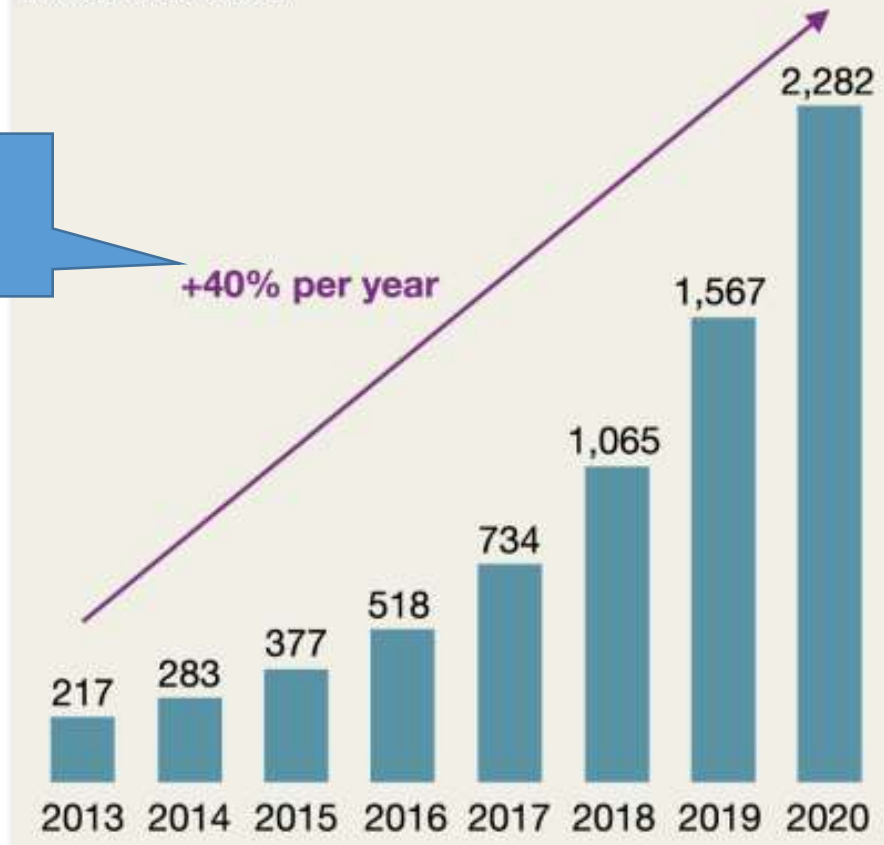
Fonte: McKinsey


OWASP TOP 10
INTERNET OF THINGS 2018
1
Weak, Guessable, or Hardcoded Passwords
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.
2
Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...
3
Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
4
Lack of Secure Update Mechanism
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
5
Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
6
Insufficient Privacy Protection
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7
Insecure Data Transfer and Storage
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8
Lack of Device Management
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9
Insecure Default Settings
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
10
Lack of Physical Hardening
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Smart home: pochi costruttori considerano la sicurezza IoT

IoT nella casa smart

Installed base of connected smart-building solutions is expanding rapidly ...



... but most building managers have not addressed cybersecurity risks

% of building facility managers (n = 224)

78% **Do not feel knowledgeable** about cybersecurity issues related to building-automation systems

46% **Do not monitor** their building-automation systems **for cyberattacks**

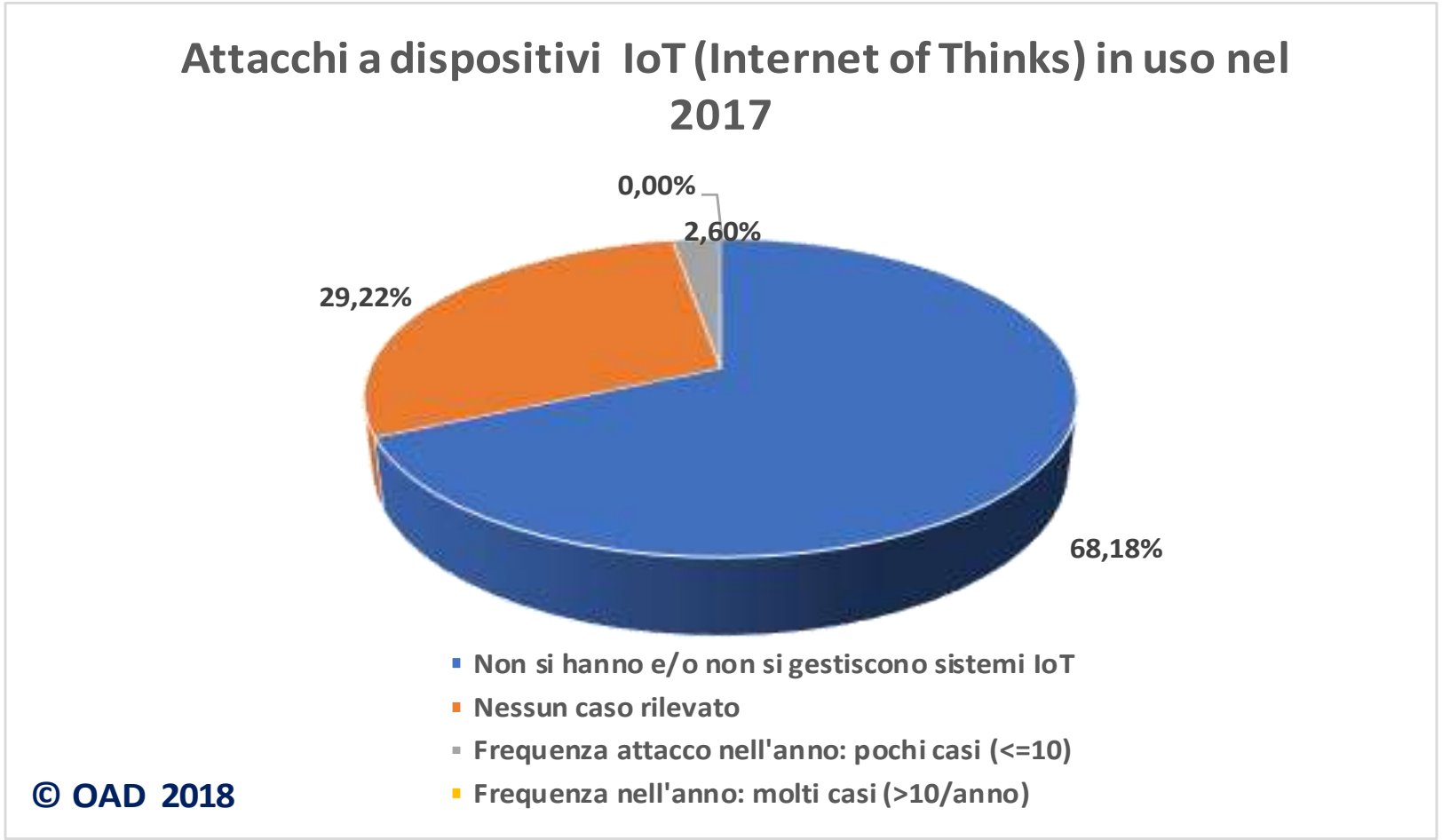
45% **Have not involved their company's IT department** in implementing security measures

63% **Have not developed a response plan** in event of cyberattack

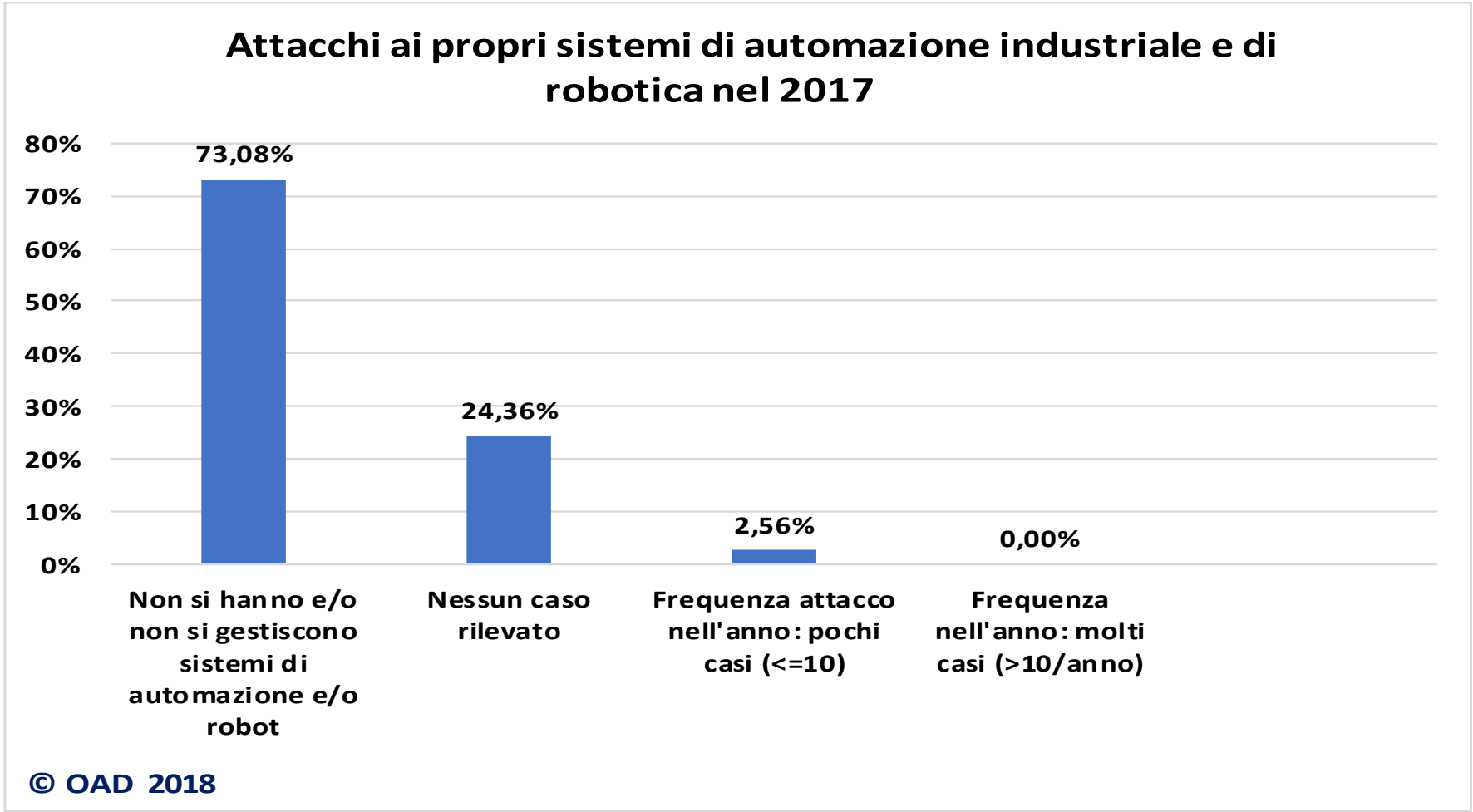
71% **Have not taken measures to improve cybersecurity**

Fonte: McKinsey

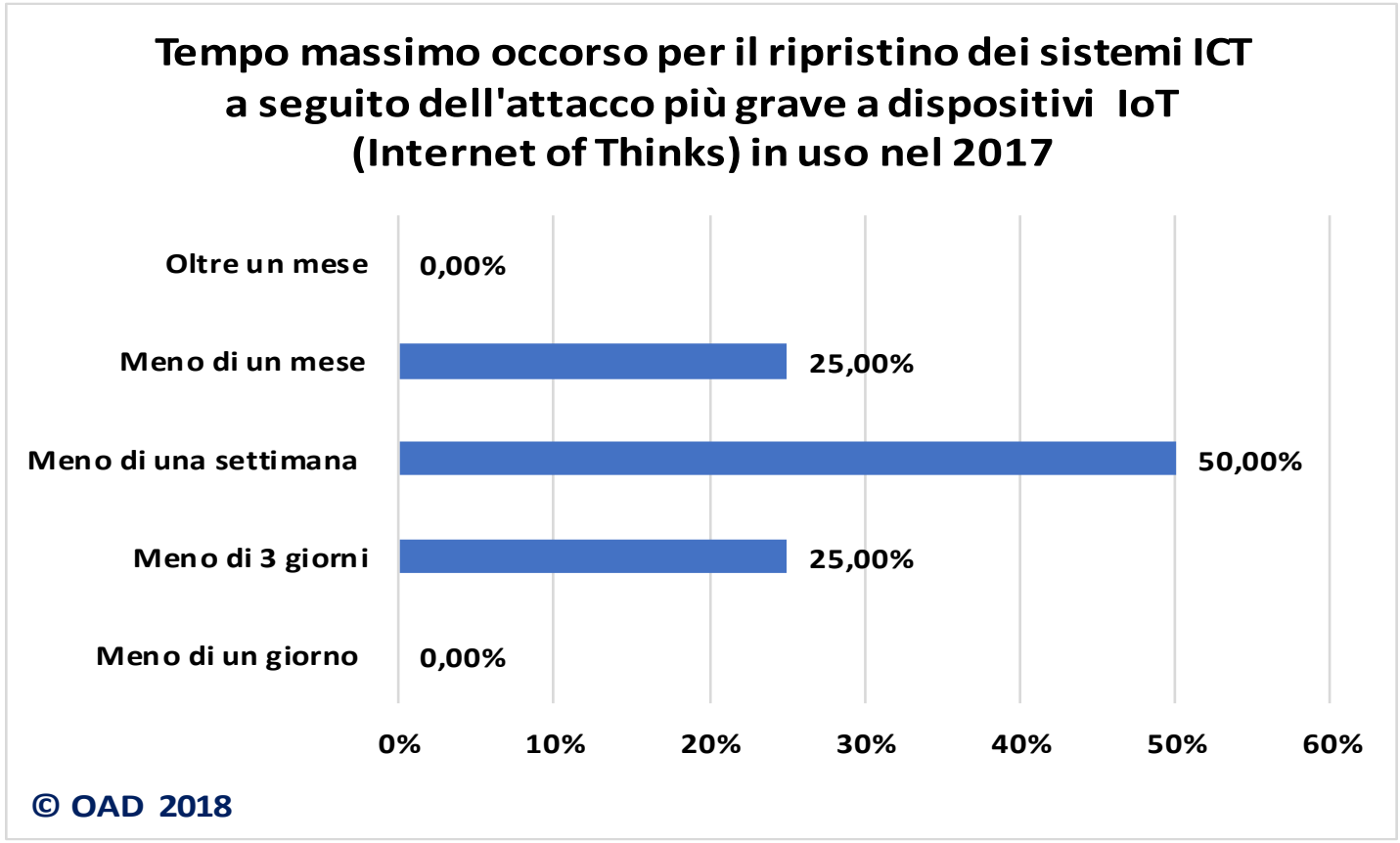
OAD 2018: Attacchi IoT



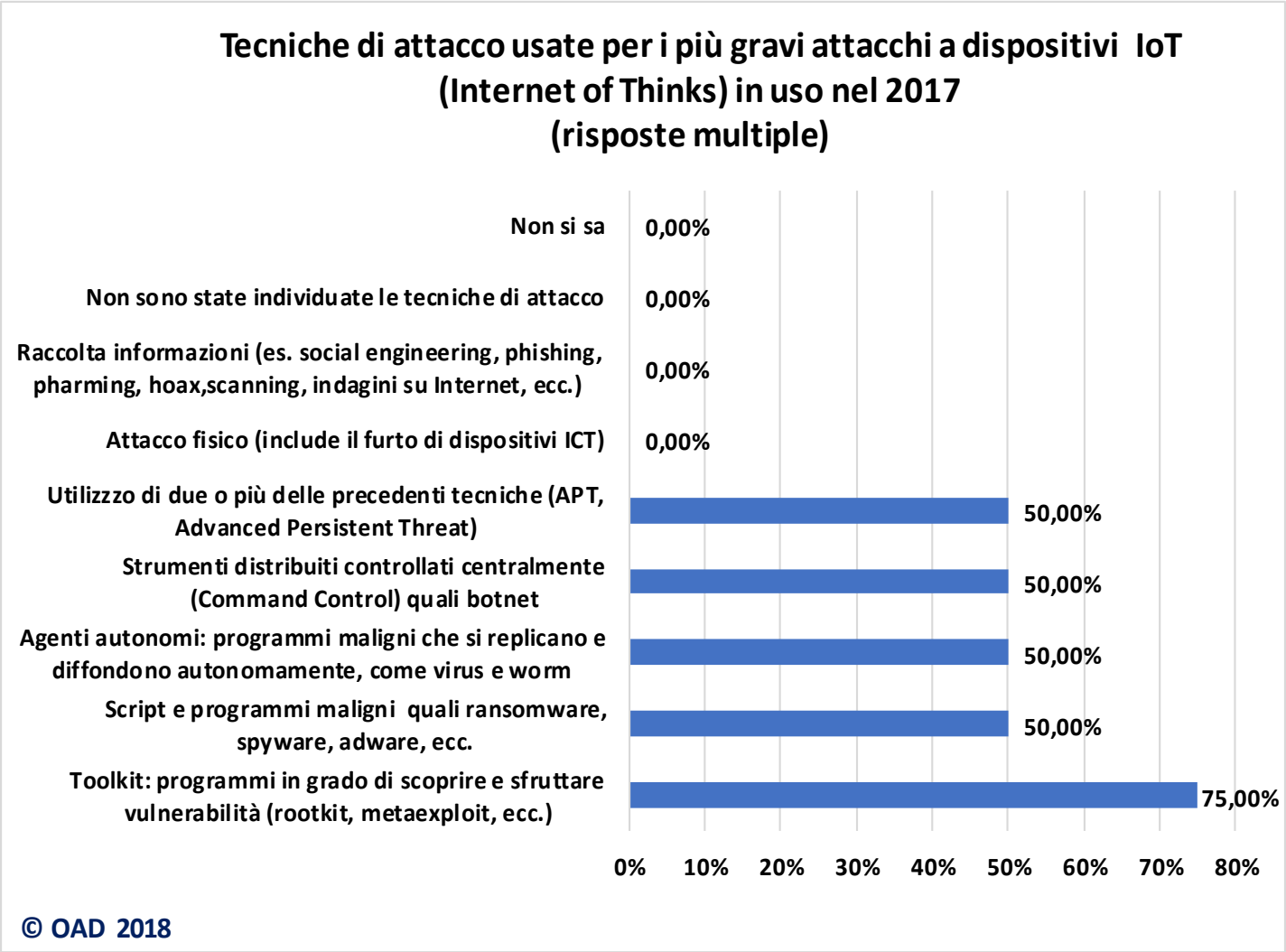
OAD 2018: Attacchi ai sistemi di automazione industriale e di robotica



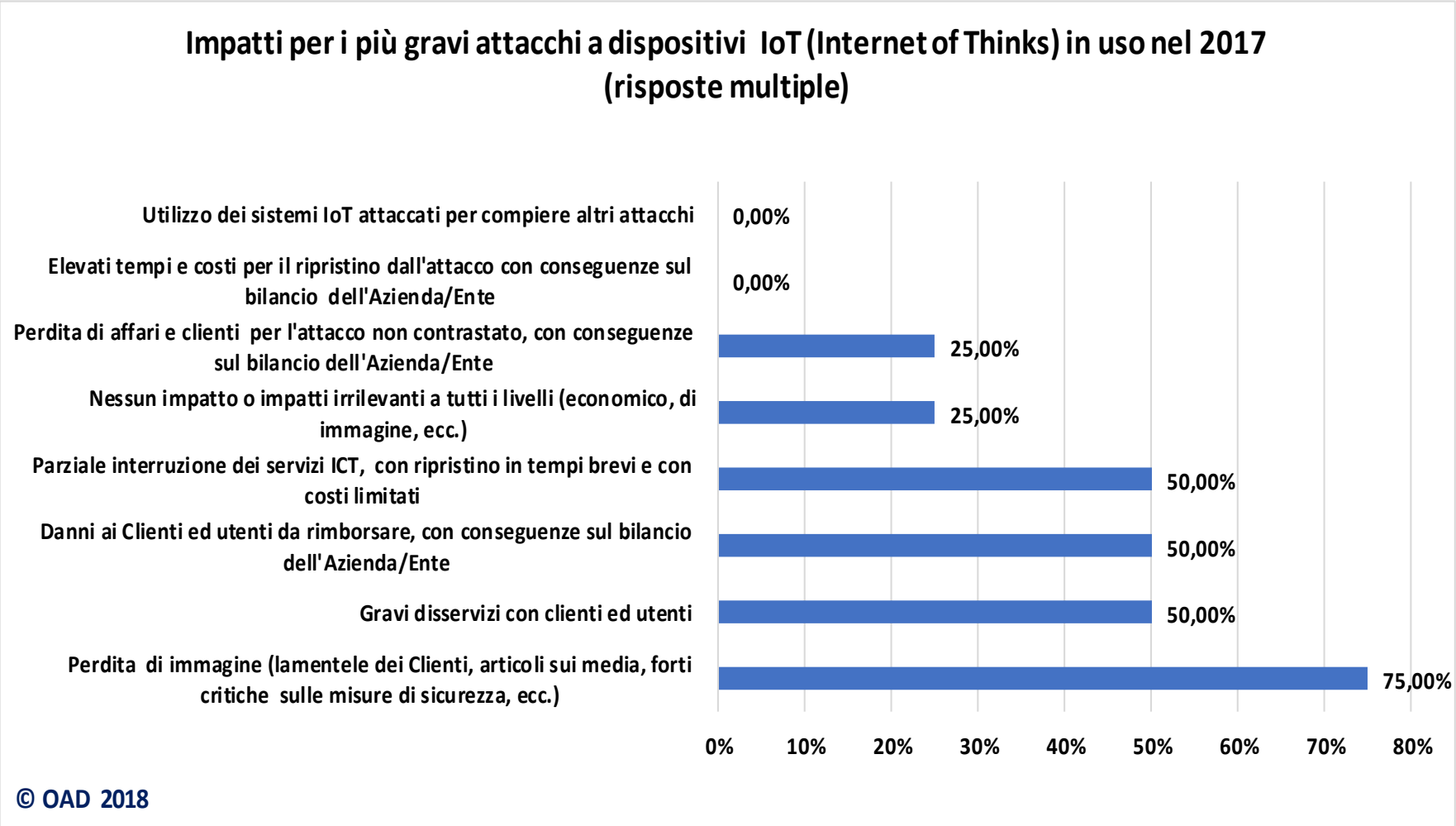
OAD 2018: Attacchi IoT



OAD 2018: Attacchi IoT



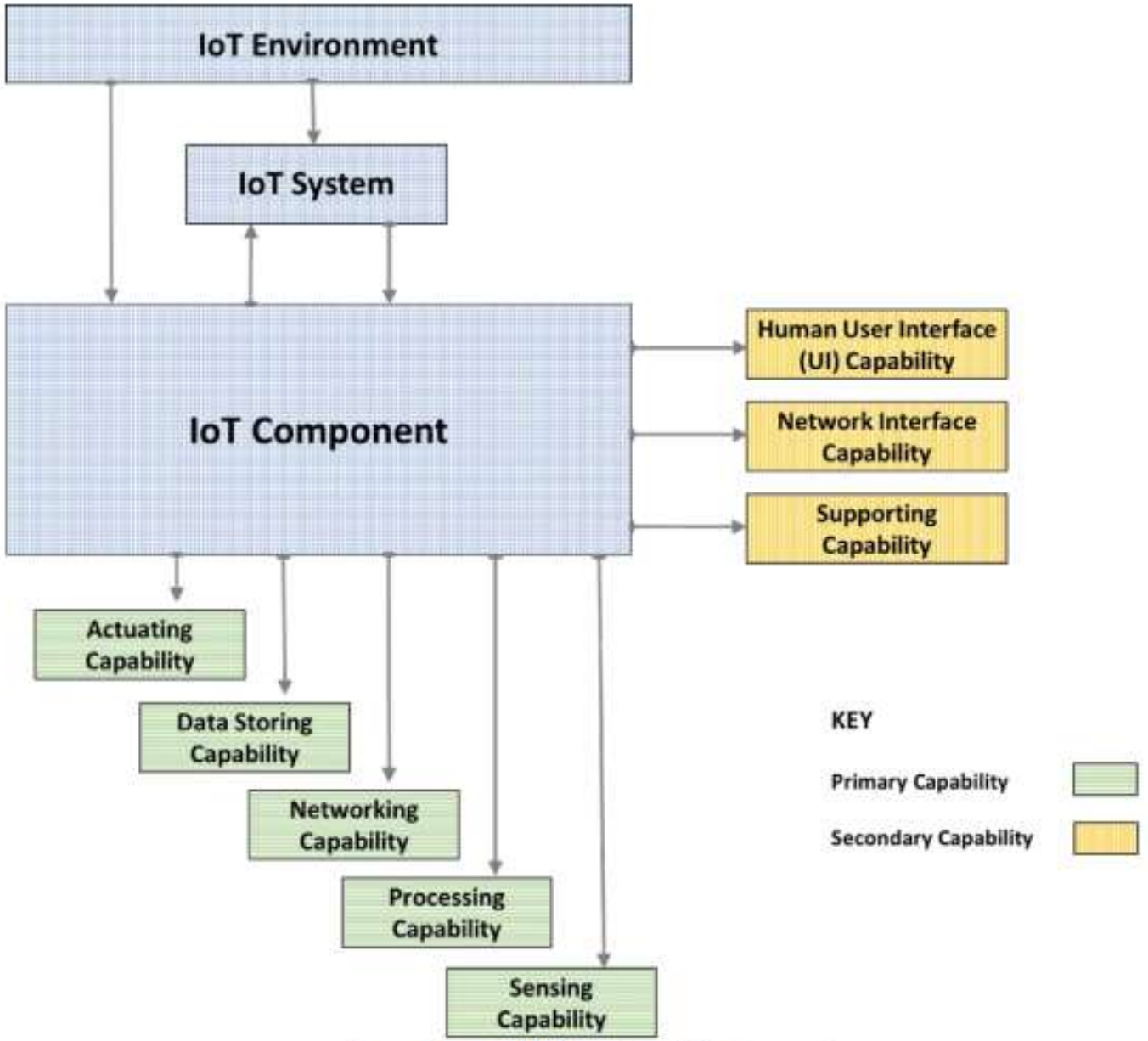
OAD 2018: Attacchi IoT



NIST IR 8200
Status of International Cybersecurity Standardization for IoT
Considerazioni tecniche

Consideration	Device Constraint	Security Concern
Power Consumption	Many IoT devices require a long battery life, without access to a permanent power supply.	Power-efficient hardware may lack additional capabilities like ability to support encryption or hardware security mechanisms.
Low Cost	The consumer's perceived value of a device greatly depends on the cost to purchase and implement the device. Market drivers often require that companies produce devices at a very low cost.	In meeting these price pressures, devices may have low processing power and constrained hardware space, offering limited support for security mechanisms.
Lifecycle	The lifespan of devices vary greatly, some devices (like simple sensors) are short-lived, while others are meant to last for decades.	Over time, devices may become hardware-constrained and cannot be updated. Built in security mechanisms may be found vulnerable or deprecated, like old encryption suites.

NISTIR 8200: schema componenti IoT



IoT Security Foundation
https://www.iotsecurityfoundation.org/

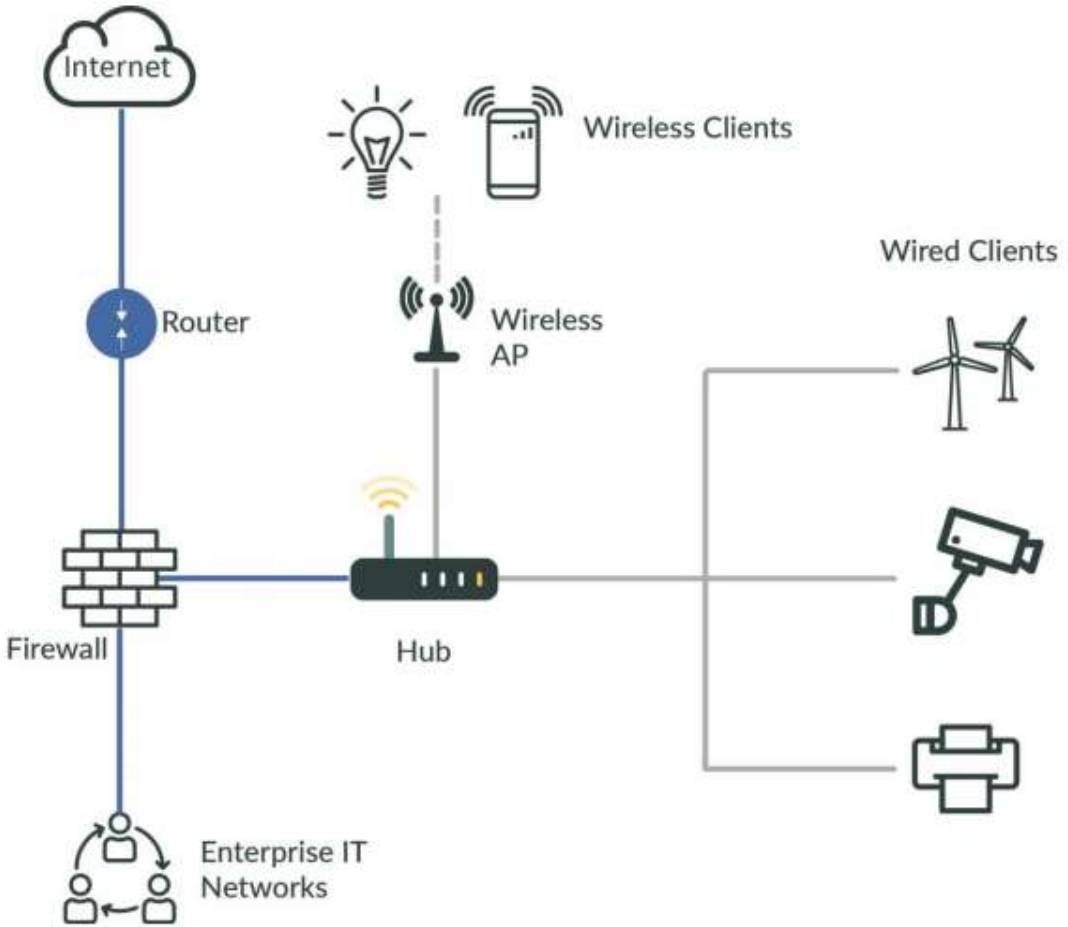
- Our Mission: *Make it Safe to Connect*

- <u>Pubblicazioni di riferimento:</u>
  - IoT Security Compliance Framework
  - IoT Security Compliance Questionnaire
  - Secure Design Best Practice Guides
  - Vulnerability Disclosure BPG
  - HOME IoT Security Architecture and Policy FOR OEM's
  - ENTERPRISE IoT Security Architecture and Policy FOR SECURITY ARCHITECTS
  - Establishing Principles for Internet of Things Security
  - IoT Cybersecurity: Regulation Ready – Full Version Nov 2018

I requisiti chiave per la compliance all'IoT Security di IoTSF

Key Requirement	Action Required	Framework Reference
Management governance	There must be a named executive responsible for product security, and privacy of customer information.	2.4.3, 2.4.11
Engineered for security	The hardware and software must be designed with attention to security threats.	2.4.4, 2.4.5, 2.4.6, 2.4.7
Fit for purpose cryptography	These functions should be from the best practice industry standards.	2.4.8 , 2.4.9
Secure network framework and applications	Precautions have been taken to secure Apps, web interfaces and server software	2.4.12, 2.4.13
Secure production processes and supply chain	Making sure the security of the product is not compromised in the manufacturing process or in the end customer delivery and installation.	2.4.10, 2.4.12, 2.4.13
Safe and secure for the customer	The product is safe and secure "out of the box" and in its day to day use. The configuration and control should guide the person managing the device into maintaining security and provide for software updates, vulnerability disclosure policy, and life cycle management.	2.4.14

IoTSF Hub-Based Architecture: esempio

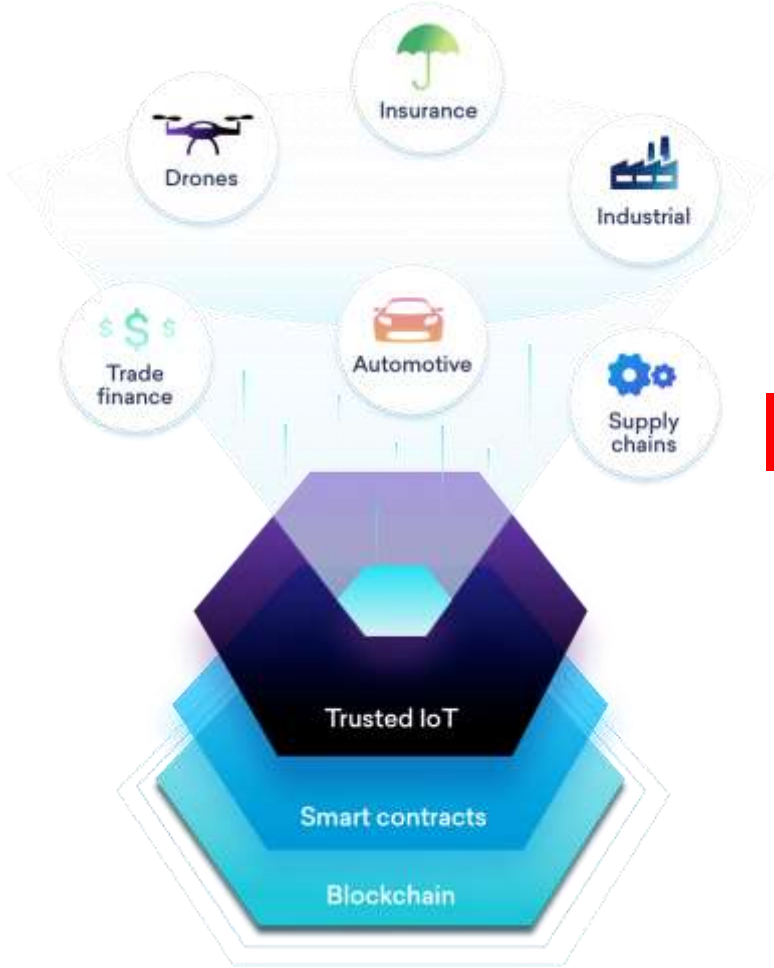


TrustedIoTAlliance (https://www.trusted-iot.org/)

- **Obiettivo utilizzare la tecnologia della blockchain per creare un protocollo di scambio sicuro per i dispositivi IoT. E creare un ecosistema sicuro , scalabile ed interoperante di sistemi sempre connessi**

- **Riferimenti**
  - **Chip BLE,** Bluetooth Low Energy, e **NFC,** Near Field Communication
  - **per la blockchain a Hyperledger, Bitcoin, Ethereum**

- **Casi d'uso in corso di sviluppo:**
  - **Trusted odometer**
  - **Supply chain event logging**
  - **Luxury goods identity verification**
  - **Smart vehicle charging**
  - **Router firmware verification**
  - **Deed of title registration**
  - **Trade finance automation**
  - **Data logger provenance**



GRAZIE DELL' ATTENZIONE

e …

- **Seguite le iniziative AIPSI e, se interessati, diventati Soci**
- **Scaricate il Rapporto 2018 OAD**
- **Rispondete al prossimo Questionario 2019 OAD (check annunci sul sito OAD**

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

OAD
Osservatorio
Attacchi Digitali
in Italia

malabo
ICT Advisory