convegno 6 cyber security 2018

mese europeo della sicurezza informatica

**Cyber Security e tecnologie intelligenti nella PA:** dal machine learning all'intelligenza artificiale

**Roma, 28 Novembre 2018 h. 9.00-13.30**

# *Cybersecurity –senza cultura e investimenti sarà Dark Future*


***Carlo Mauceli***

***carlo.mauceli@microsoft.com***


**organizzato e promosso da**

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

SAPIENZA UNIVERSITÀ DI ROMA DIPARTIMENTO DI INFORMATICA

PRS Planning Ricerche e Studi

# Agenda

- Dimensione di un Fenomeno
- Obiettivi degli Attaccanti
- Tipologia degli Attacchi
- Pubblica Amministrazione
- Catena d'Attacco Tipica
- Strategia di Sicurezza
- Conclusioni

# Dimensione del Fenomeno

**500B$**

Dal 2011 al 2017 i costi generati globalmente dalle sole attività del Cybercrime sono quintuplicatii

**1B di persone nel mondo**

Sono state colpite lo scorso anno da truffe, estorsioni, furti di denaro e dati personali

**180B$**

La perdita stimata ai soli privati cittadini

# E l'Italia ?

**10B€**

Si tratta di un valore dieci volte superiore a quello degli attuali investimenti in sicurezza informatica, che arrivano oggi a sfiorare il miliardo di euro

https://clusit.it/rapporto-clusit/

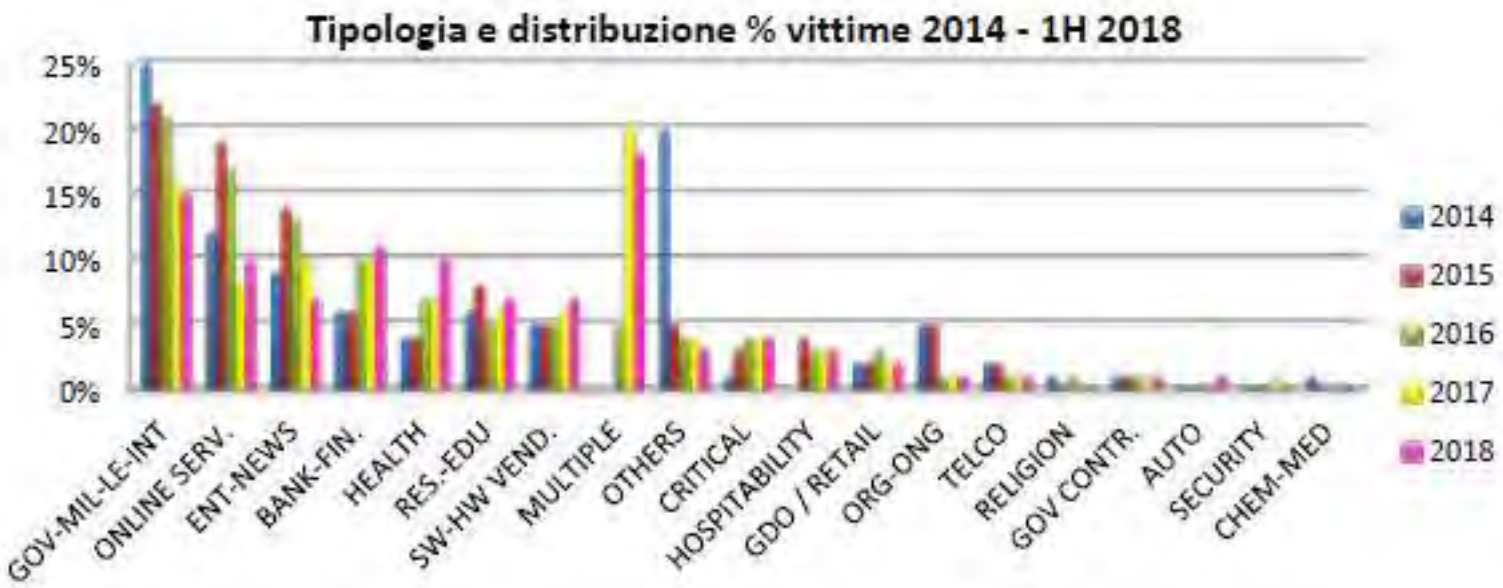
# Distribuzione degli Attaccanti per Tipologia – Primo Semestre 2018

| ATTACCANTI PER TIPOLOGIA | 2014 | 2015 | 2016 | 2017 | 2H 2017 | 1H 2018 | Variazioni 1H 2018 su 2H 2017 | Trend 1H 2018 |
|---|---|---|---|---|---|---|---|---|
| Cybercrime | 526 | 684 | 751 | 857 | 434 | 587 | 35,25% | ↑ |
| Hacktivism | 236 | 209 | 161 | 79 | 34 | 29 | -14,71% | ↓ |
| Espionage / Sabotage | 69 | 96 | 88 | 129 | 55 | 93 | 69,09% | ↑ |
| Information Warfare | 42 | 23 | 50 | 62 | 31 | 21 | -32,26% | ↓ |
| TOTALE | 873 | 1.012 | 1.050 | 1.127 | 554 | 730 | +31,77% | ↑ |

- Il numero di attacchi gravi cresce del 31,77%.
- Nel 2017 “Cybercrime”, “Cyber Espionage” e “Information Warfare” fanno registrare il numero di attacchi più elevato degli ultimi 7 anni.
- Nel 1H 2018 diminuisce ulteriormente la componente riferibile all’Hacktivism, sembra diminuire anche l’Information Warfare, mentre crescono in modo tangibile gli attacchi con motivazione cybercriminale (+35%) ed in modo impressionante quelli riferibili ad attività di cyber espionage (+69%).

https://clusit.it/rapporto-clusit/

# Un nuovo fenomeno: Multiple Targets




Tutti sono diventati bersagli e gli attaccanti sono diventati sempre più aggressivi e conducono operazioni con una logica “industriale” che prescinde sia da vincoli territoriali che dalla tipologia dei bersagli, puntando a massimizzare il risultato economico (furti di cryptovalute ai danni di grandi Exchange (Coincheck) o il danno inflitto alle vittime (NotPetya).

# Distribuzione delle Tecniche di Attacco

| TECNICHE DI ATTACCO PER TIPOLOGIA | 2014 | 2015 | 2016 | 2017 | 2H 2017 | 1H 2018 | Variazioni 1H 2018 su 2H 2017 | Trend 1H 2018 |
|---|---|---|---|---|---|---|---|---|
| SQL Injection | 110 | 184 | 35 | 7 | 1 | 0 | -100,00% | |
| Unknown | 199 | 232 | 338 | 277 | 137 | 212 | 54,74% | |
| DDoS | 81 | 101 | 115 | 38 | 19 | 20 | 5,26% | |
| Known Vulnerabilities / Misconfigurations | 195 | 184 | 136 | 127 | 56 | 77 | 37,50% | |
| Malware | 127 | 106 | 229 | 446 | 237 | 291 | 22,78% | |
| Account Cracking | 86 | 91 | 46 | 52 | 20 | 17 | -15,00% | |
| Phishing / Social Engineering | 4 | 6 | 76 | 102 | 50 | 61 | 22,00% | |
| Multiple Techniques / APT | 60 | 104 | 59 | 63 | 27 | 40 | 48,15% | |
| 0-day | 8 | 3 | 13 | 12 | 5 | 12 | 140,00% | |
| Phone Hacking | 3 | 1 | 3 | 3 | 2 | 0 | -100,00% | |

- Le tecniche sconosciute crescono del 54%;
- “Malware” che si conferma al primo posto;
- “Multiple Threats/APT” crescono del 48%
- I DDoS crescono del 5%
- Lo sfruttamento di vulnerabilità note ritorna a crescere: +37%;
- L’utilizzo di vulnerabilità “0-day”: +140%,

Gli attaccanti *riescono ancora a realizzare attacchi di successo contro le loro vittime con relativa semplicità e a costi molto bassi, oltretutto decrescenti* ☹☹☹

# 2017 - L'anno dell'insicurezza informatica

- Costi dell'insicurezza informatica quintuplicati negli ultimi 6 anni;
- Nel 2017 colpiti oltre 1 miliardo di persone
- Classe politica con scarsa attenzione al tema
- Il 29% della forza lavoro italiana ha elevate competenze digitali
- Cybercrime prima causa di attacchi gravi a livello mondiale
- Cyber espionage in crescita del 46%

| VITTIME PER TIPOLOGIA | 2014 | 2015 | 2016 | 2017 | Variazioni 2017 su 2016 | Trend 2017 |
|---|---|---|---|---|---|---|
| Institutions: Gov - Mil - LEAs - Intelligence | 213 | 223 | 220 | 179 | -18,64% | ↓ |
| Others | 172 | 51 | 38 | 40 | 5,26% | ↗ |
| Entertainment / News | 77 | 138 | 131 | 115 | -12,21% | ↘ |
| Online Services / Cloud | 103 | 187 | 179 | 95 | -46,93% | ↓ |
| Research - Education | 54 | 82 | 55 | 71 | 29,09% | ↑ |
| Banking / Finance | 50 | 64 | 105 | 117 | 11,43% | ↑ |
| Software / Hardware Vendor | 44 | 55 | 56 | 68 | 21,43% | ↑ |
| Telco | 18 | 18 | 14 | 13 | -7,14% | ↘ |
| Gov. Contractors / Consulting | 13 | 8 | 7 | 6 | -14,29% | ↘ |
| Security Industry | 2 | 3 | 0 | 11 | - | ↗ |
| Religion | 7 | 5 | 6 | 0 | - | ↓ |
| Health | 32 | 36 | 73 | 80 | 9,59% | ↑ |
| Chemical | 5 | 2 | 0 | 0 | - | → |
| Critical Infrastructures | 13 | 33 | 38 | 40 | 5,26% | ↗ |
| Automotive | 3 | 5 | 4 | 4 | - | → |
| Org / ONG | 47 | 46 | 13 | 8 | -38,46% | ↓ |
| Multiple Targets | - | - | 49 | 222 | 353,06% | ↑ |
| GDO / Retail | 20 | 17 | 29 | 24 | -17,24% | ↘ |
| Hospitability | - | 39 | 33 | 34 | 3,03% | ↗ |

Non è tanto il dato numerico a spaventare quanto il fatto che il fenomeno mira a interferire in maniera pesante non solo nella vita privata dei cittadini quanto, invece, sul piano finanziario e geopolitico. Insomma, il gioco si fa serio e un altro innalzamento del livello potrebbe non essere sopportabile.

- Pur essendo ancora la prima causa di attacco a livello globale e rappresentando un problema enorme, il Cybercrime è diventato ormai l'ultimo dei nostri problemi in ambito cibernetico dal punto di vista della sua pericolosità intrinseca.
- La novità del 2018 è stata rappresentata dalla tipologia e dalla distribuzione  delle vittime: Multiple Targets. Significa che nessuno è stato escluso dall'essere un obiettivo.
- Aumento della produzione e diffusione di malware che sfruttano i processori dei PC/Server colpiti per "minare" crypto-valute (BitCoin ma non solo…)
- Aumento degli attacchi per finalità di Espionage
- Aumento degli attacchi nel mondo industriale

Farnesina
Ministero degli Affari Esteri e della Cooperazione Internazionale

Ministero della Giustizia
Percorsi chiari e precisi: un tuo diritto

MINISTERO DELL'INTERNO

Accesso abusivo al sistema informatico». La sottrazione dei documenti dai sistemi informatici di palazzo Chigi, ministeri dell'Interno e della Difesa, della Marina Militare e del Parlamento europeo, finisce sotto inchiesta alla Procura della Repubblica di Roma.

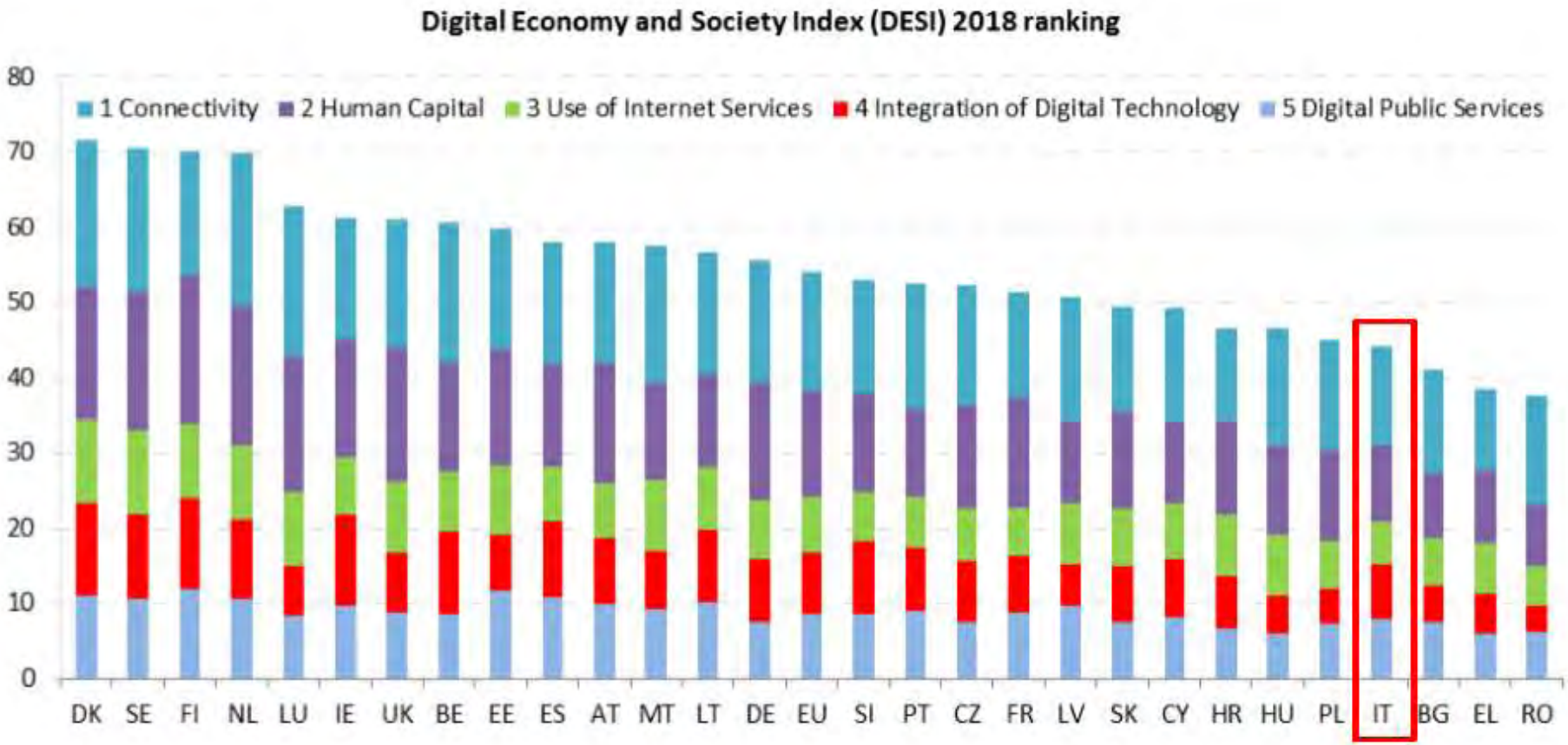
MINISTERO DELLA DIFESA

Ministero dell'Istruzione dell'Università e della Ricerca

I dati pubblicati non sono riconducibili a componenti dei sistemi informatici del MIUR, gestiti dalle società Almaviva-Fastweb e DXC-Leonardo. In particolare, non sono stati trafugati dati dai sistemi che gestiscono l'accesso alle caselle del dominio @istruzione.it.

Inasprire le norme penali a chi aggredisce la sicurezza informatica nazionale. Nominare un commissario straordinario per la Cyber security. Sono le due richieste che arrivano dal Movimento 5 Stelle al governo dopo l'attacco informatico contro le Pec del ministero dell'Interno e della Giustizia.

# Il Rapporto DESI – Una triste Realtà



# Catena d'Attacco




*Carlo Mauceli*
*CTO Microsoft Italia*

# MICROSOFT SECURE

End-to-end approach - safeguard data and prevent leakage – no interfering with user experience
Protect, detect & automatically respond to threats across endpoints, mails, files and IDs
Security capabilities are built in (not bolted on), comprehensive, and integrated

**Identity & access management**

Protect users' identities & control access to valuable resources based on user risk level

**Threat protection**

Protect against advanced threats and recover quickly when attacked

**Information protection**

Ensure documents and emails are seen only by authorized people

**Security management**

Gain visibility and control over security tools

# Strategia di Sicurezza – Aree d'attenzione

## Identity and access management

### Protect organizations from identity compromise

**Provide protection at the front door**
Move to more secure forms of multi-factor authentication such as PINs and biometric security protocols

**Simplify access to devices and apps**
Use passwordless access such as Windows Hello which provides secure single sign-on to all apps from any device that supports Windows 10.

**Stay safe in the cloud**
Prevent Pass the Hash attacks with Windows Defender Credential guard which protects single sign-in tokens.

## Threat protection

### Integrated, intelligent cybersecurity

**Built-in, not bolted on**
Native solutions across products, providing coordinated protection & remediation to maximize security

**Protect your organization**
Stop threats before they harm your business by securing identities, apps and data, devices, and workloads across a hybrid infrastructure.

**Detect threats with intelligence**
Use sophisticated machine learning models to quickly uncover suspicious behavior on-premises or in the cloud, harnessing advanced analytics about attacks.

**Rapidly respond**
Immediately investigate and remediate complex attacks across identities, apps, data, and devices, before they can cause damage.

## Security management

### Discover simplified and intelligent security management

**Understand your security posture**
Deliver effective threat detection and response using insights into your security state and the risks that impact your resources.

**Implement consistent security controls**
Create and customize consistent security policies and enable the controls that are critical to effective security management.

**Harden your security posture with intelligence**
Boost your organization's security with built-in intelligence, recommendations, and expert guidance.

## Information protection

### Strengthen your security posture

**Customize information protection policies**
Identify and classify sensitive data and apply the right level of protection

**Accelerate your path to compliance**
Enhance your security and privacy posture to comply with GDPR and other regulatory requirements

**Automatically protect your sensitive data**
Encrypt data, restrict access, and remotely wipe devices to prevent data leaks

**Understand how users access data files and software as a service (SaaS) apps**
Gain visibility into how users distribute data to effectively respond to security events



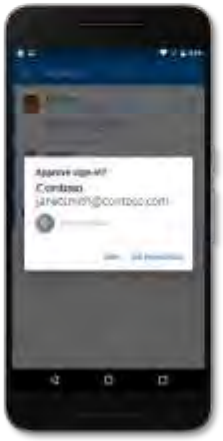
*Carlo Mauceli*
*CTO Microsoft Italia*

# Protezione dell'Identità

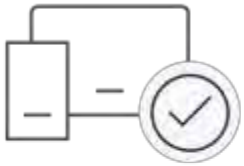
Prove users are authenticated, authorized and secure before granting access to apps, data, and devices

Password-less Authentication

Windows Hello



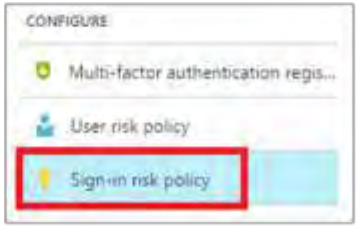
MS Authenticator



Conditional Access

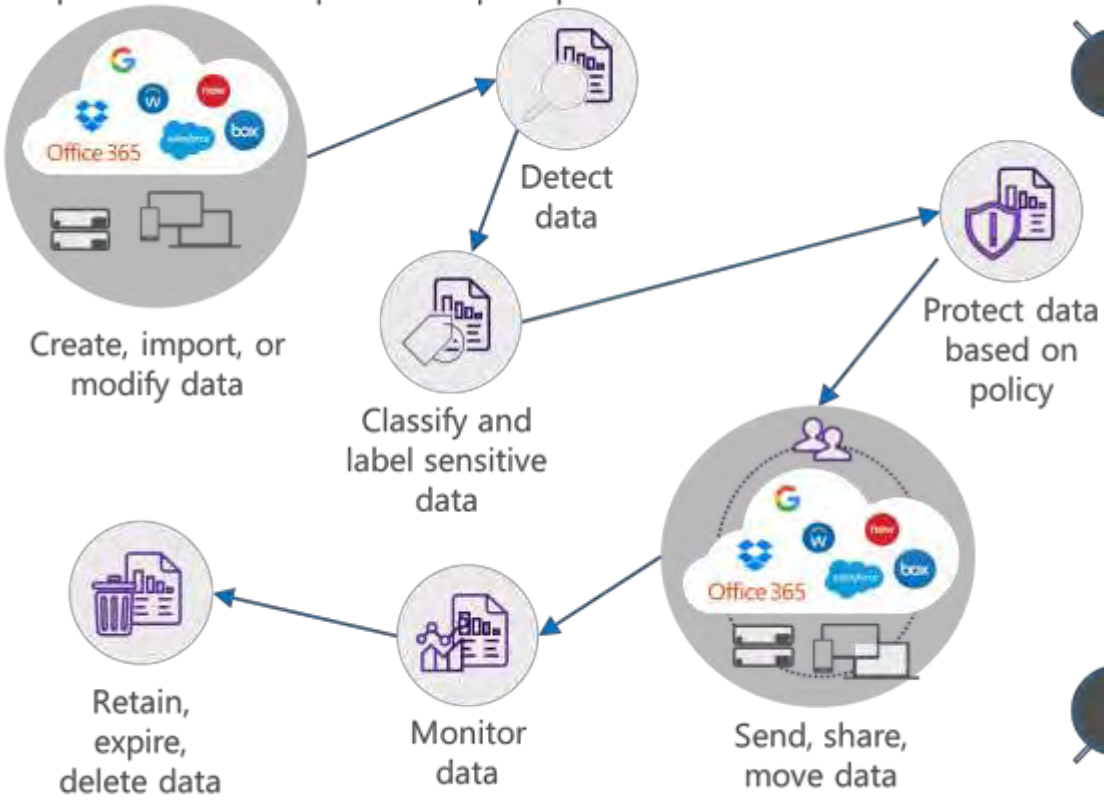

Identity Protection

Safeguard credentials when they are used in an OS or application session



# Protezione dell'Informazione

Dictates to put in place appropriate technical and organizational measures to implement the data protection principles




GDPR compliance use cases

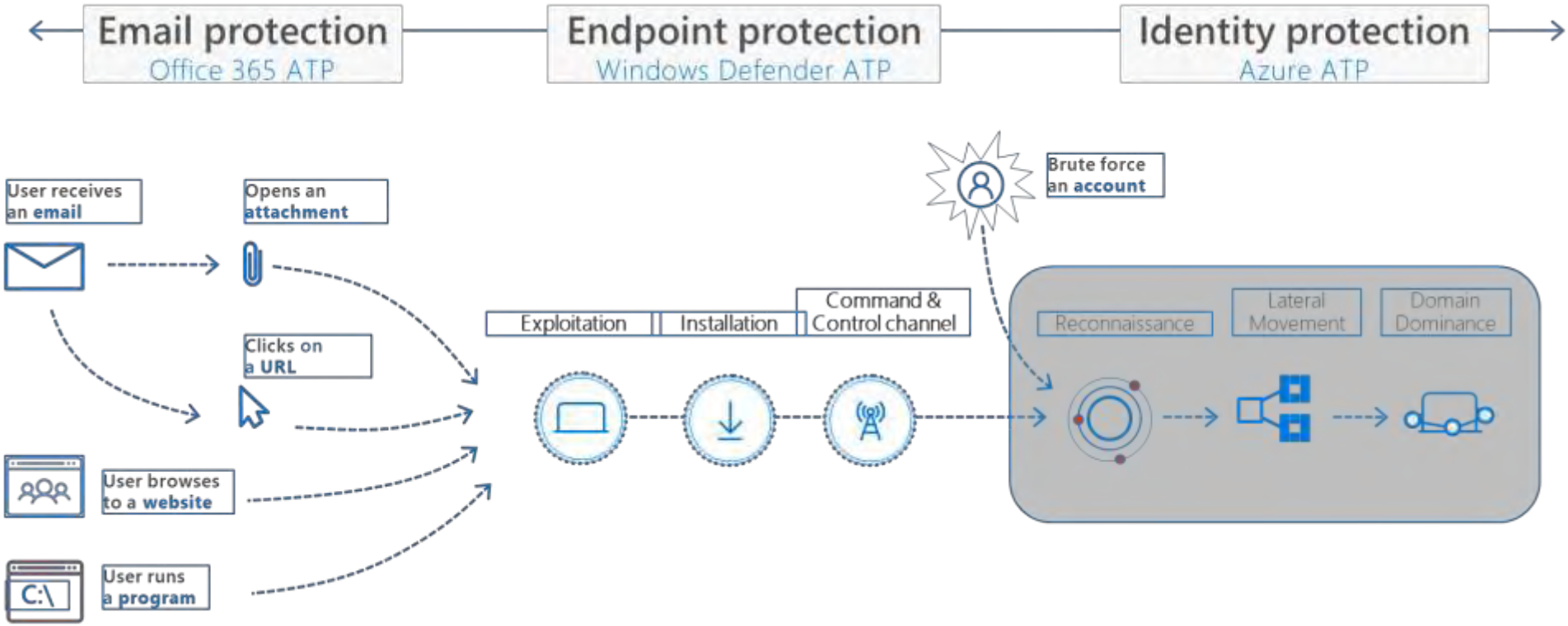
- Discover personal data (PII) in unstructured data
- Ensure data is protected on-premises, in the cloud and on mobile devices
- Grant and restrict access to data
- Gain visibility and control of data stored in cloud apps
- Detect data breaches before they cause damage
- Prove the right things are in place for good faith effort to be compliant
- Manage Data Subject Requests

Adopted on 14 April 2016, enforced on 25 May 2018



Carlo Mauceli
CTO Microsoft Italia

# Copertura della Superficie d'Attacco






Carlo Mauceli
CTO Microsoft Italia

# Risposta alla catena d'attacco secondo Microsoft

## Killchain

**Azure / EMS Technology**
- Azure AD / Intune / Conditional access
- Azure Security Center
- Azure Operations Management Suite

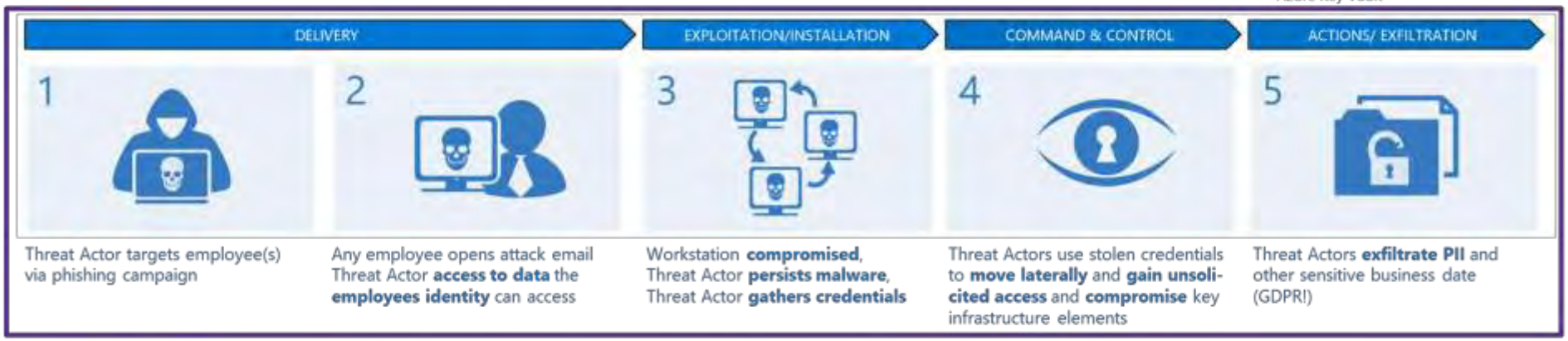
**Azure / EMS Technology**
- Azure AD / Intune / Conditional access
- Azure Security Center / Azure OMS
- Azure Advanced Threat Protection

**Advanced Threat Analytics**
- Advanced Threat Analytics (in EMS E3)

**Azure / EMS Technology**
- Azure Advanced Threat Protection
- Azure Security Center / OMS

**Office 365 Technology**
- Data Loss Prevention

**Azure / EMS Technology**
- Azure Information Protection (E5 feat.)
- Azure Advanced Threat Protection
- Disk, Storage, SQL Encryption
- Azure Key Vault




**Microsoft Security Initiatives**
- Cyber Defence Operations Center
- Security Response Center
- Malware Protection Center
- Digital Crimes Unit
- Cyber Threat Intelligence Program

**Professional Service Solutions**
- Cloud Security Planning for O365
- Cloud Securtiy Planning for Azure
- Cybersecurity Architect / Advisor

**Professional Service Solutions**
- Persistent Adversary Threat Detection (PADS) – new COS
- Priviileged Admin Workstation (PAW)
- Applocker (POP-Applocker)
- Win10 Security Implementation Service
- Securing Windows Client WorkshopPlus
- ~~Cybersecurity Architect / Advisor~~

**Professional Service Solutions**
- ATA Implementation Service (ATA-IS)
- Security Foundation
- Enhanced Security Admin Environment (ESAE)
- Privileged Access Workstation (PAW)
- Active Directory Hardening (ADH)
- Secure Lateral Account Movement (SLAM)
- Cybersecurity Architect / Advisor



Carlo Mauceli
CTO Microsoft Italia

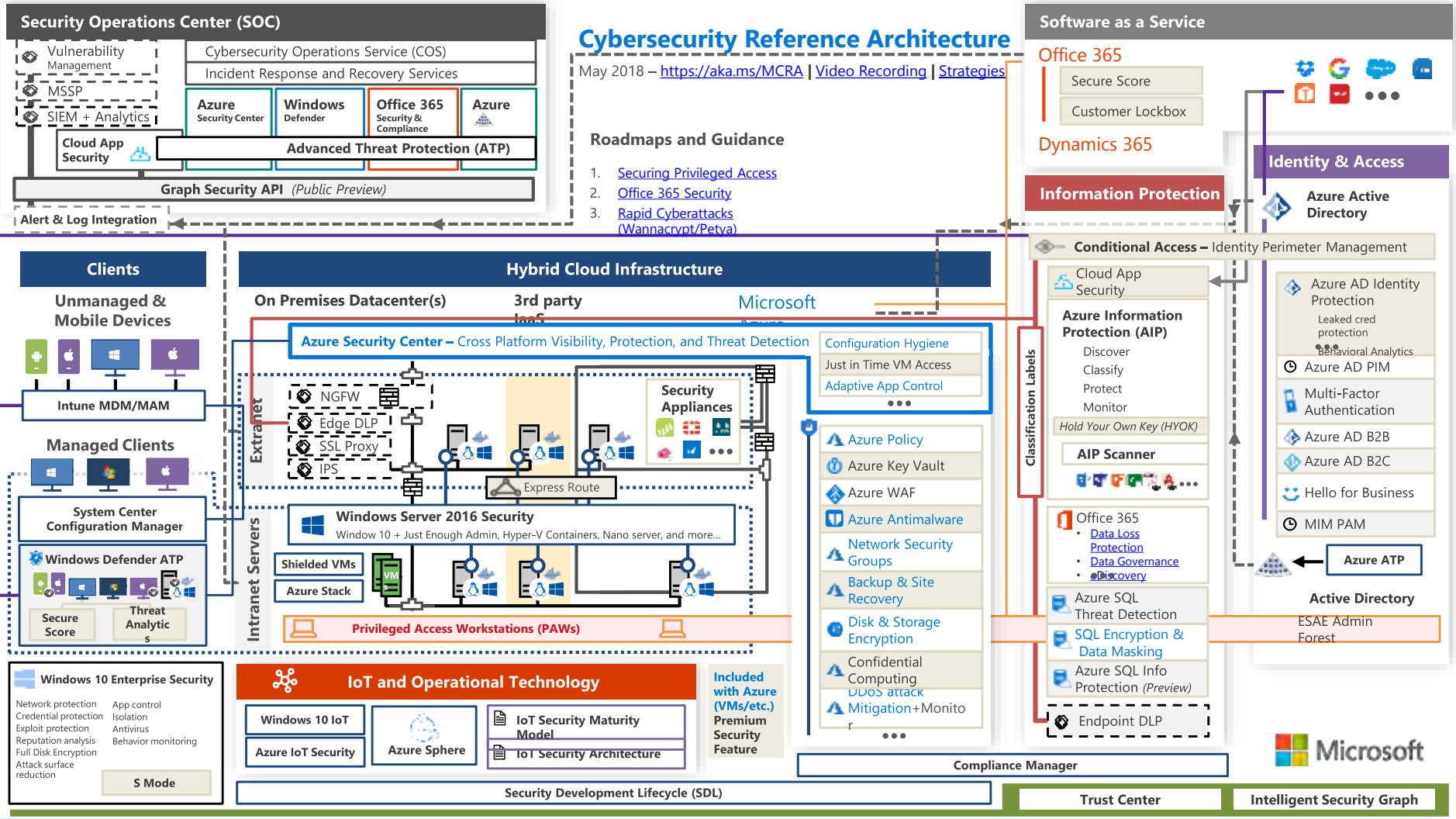
# Il Cloud come leva per la Mitigazione del Rischio





Carlo Mauceli
CTO Microsoft Italia

# Cybersecurity Reference Architecturee




organizzato e promosso da

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

CIS SAPIENZA

PRS Planning Ricerca e Studi

Carlo Mauceli
CTO Microsoft Italia

# Conclusioni

- Definire gli asset da proteggere in maniera chiara
- Pianificare un «Security Journey»: Roma non è stata costruita in un giorno !!!
- Bisogna pensare come pensa chi ci attacca
- Non si può combattere con tecnologie e armi vecchie !!!
- *«New ideas are not only the enemy of old ones; they also appear often in an extremely unacceptable form»* (Carl Gustav Jung)

- Grazie
- Q&A