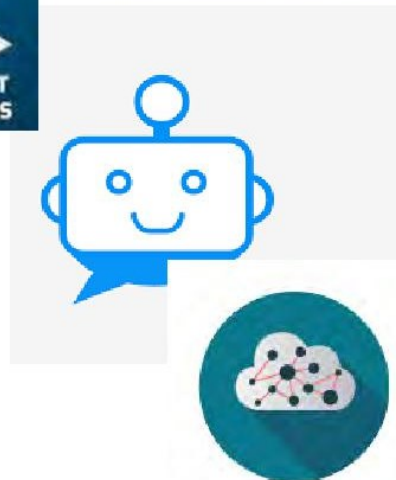


*Perché cyber security e
tecnologie intelligenti
nella PA*

Perché

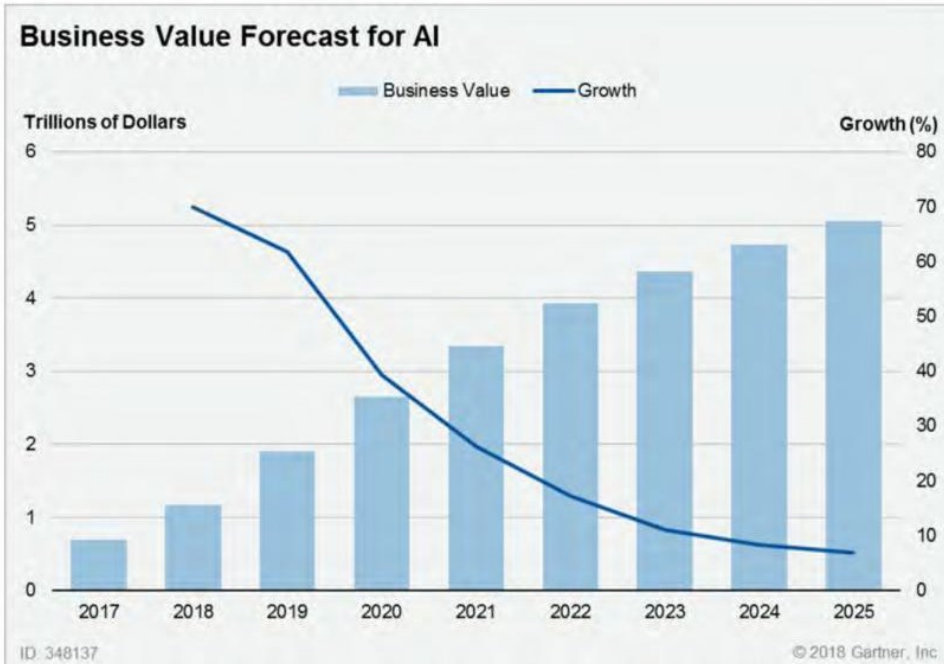
l'intelligenza artificiale è
**già presente nella nostra
vita**

- ❑ elettrodomestici
- ❑ automobili
- ❑ smartphone
- ❑ laptop
- ❑ assistenti virtuali
- ❑ etc.



Perché

è un tema **in rapida crescita**: nell'anno in corso si stima un incremento del giro di affari mondiale del 70% sul 2017, con una tendenza a triplicarsi nel 2022



Fonte: Gartner marzo 2018



Perché

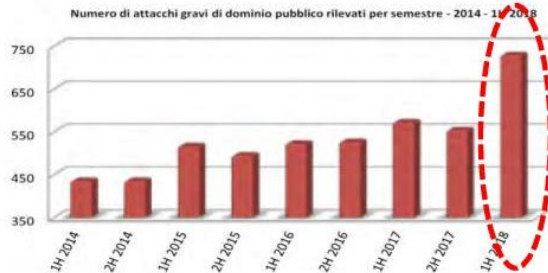
Sono attesi nei prossimi 30 anni progressi che potrebbero comportare rilevanti impatti sociali

Fonte: world economic forum (www.weforum.org/agenda/2018/03/timeline-of-creative-ai/)



Perché

- Oltre agli aspetti tecnologici ed algoritmici c'è una forte attenzione del settore pubblico ai **risvolti etici e sociali** e al carattere **«umanocentrico»** dell'intelligenza artificiale con l'obiettivo di integrare le capacità umane e non sostituirle



Grave cyber attacco alla Pubblica Amministrazione in Italia tramite la PEC

20 novembre 2018 - Francesco Bussolini - Aziende, Cyber, Difesa e Sicurezza

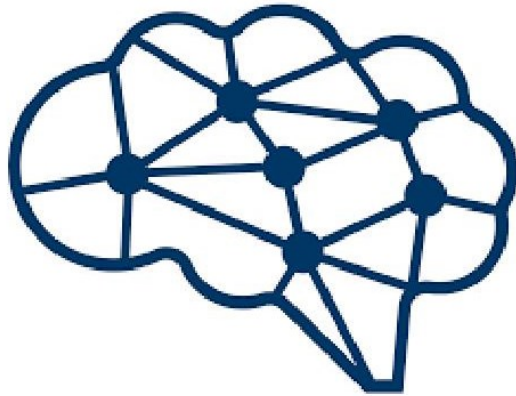


Perché

- l'IA riduce i costi degli attacchi esistenti, permettendo attacchi prima sconosciuti e rendendo sempre più difficile capire chi sia l'attaccante
- per difendersi diventa sempre più importante analizzare una enorme mole di dati che può essere fatto solo con l'ausilio dell'IA
- la Pubblica Amministrazione ha il dovere di proteggere efficacemente i propri asset (dati) e garantire ai propri utenti un utilizzo sicuro e affidabile dei servizi erogati on-line

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2H 2017	1H 2018	Variazioni 1H 2018 su 2H 2017	Trend 1H 2018
Institutions: Gov - Mil - LEAs - Intelligence	213	223	220	179	73	111	+52%	

Quali obiettivi



Comprendere

- **Stato dell'arte** e nuovi paradigmi dell'Intelligenza Artificiale e della cyber security
- **Nuove frontiere** della ricerca su IA e Cyber security
- Come Intelligenza Artificiale e Machine Learning possono contribuire al **miglioramento dei servizi e della sicurezza nella PA**

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

Milestone

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

500B\$

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

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 ?

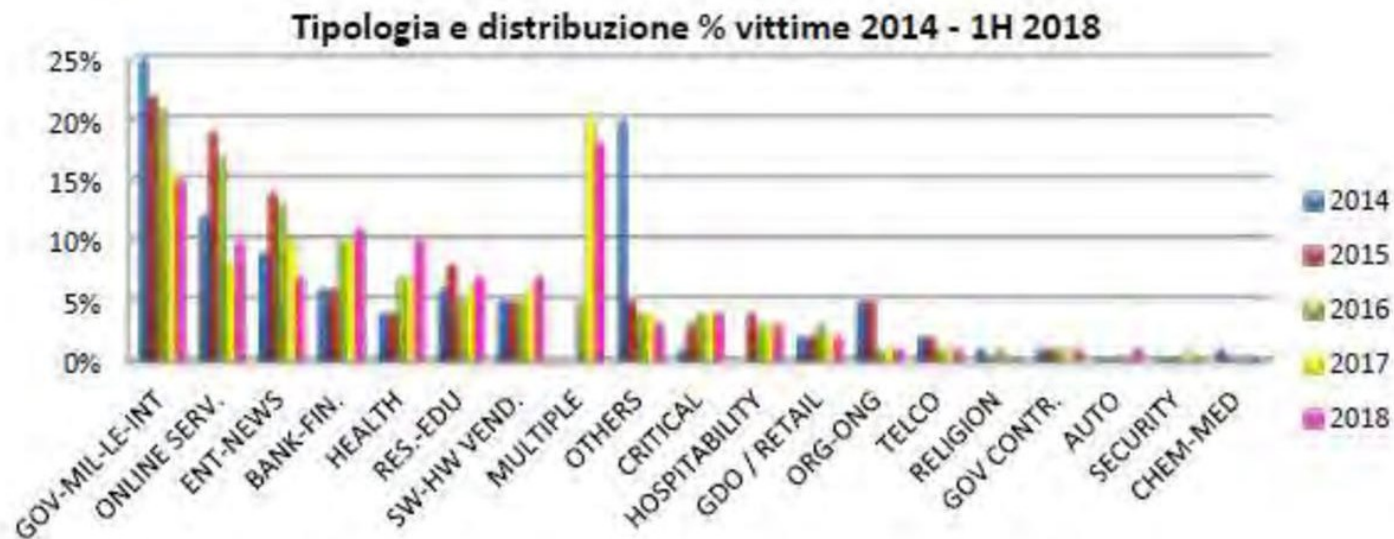
10B€

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



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%).



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](#)).

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 😞😞😞

- 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%	↔
Hospitality	-	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



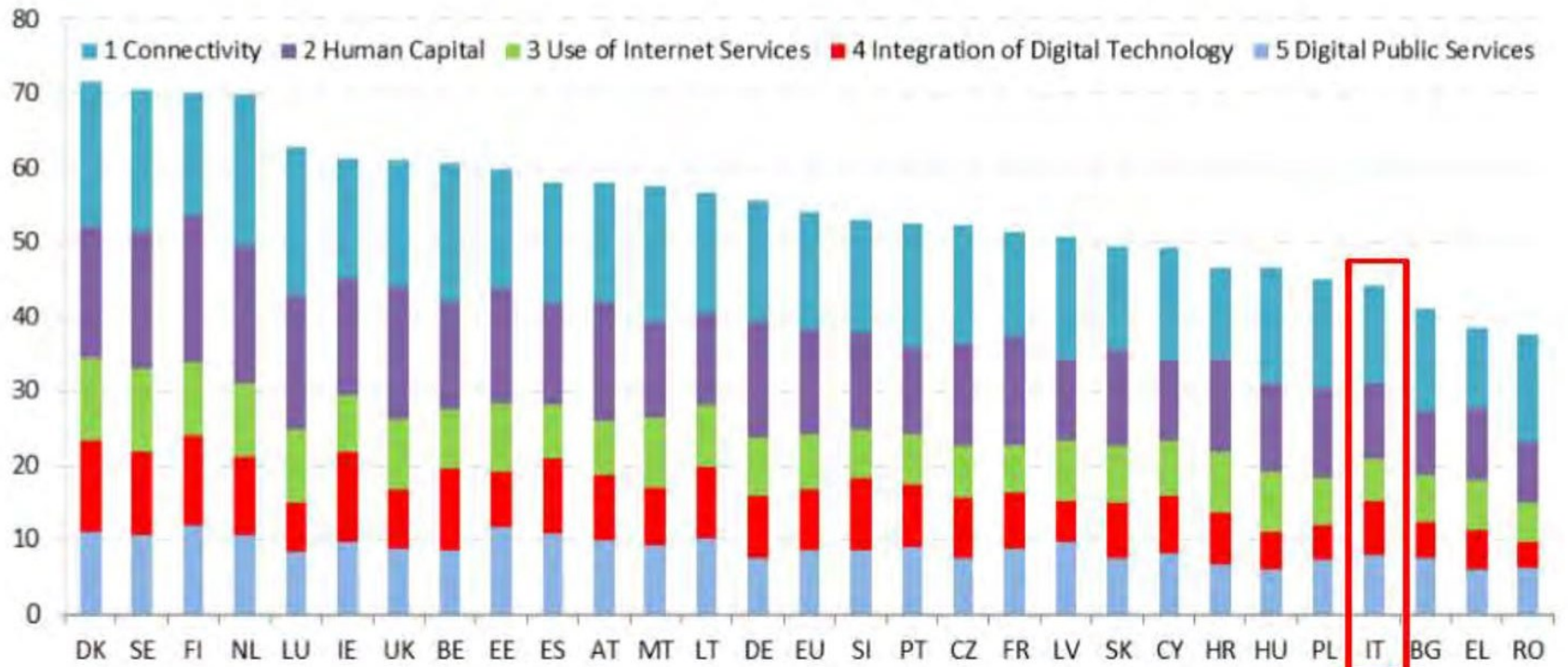
Accesso abusivo al sistema informatico». La sottrazione dei documenti dai sistemi informatici di palazzo Chigi, ministeri dell'Interno e della Difesa, della Marina Militare e del Parlamento europeo, finisce sotto inchiesta alla Procura della Repubblica di Roma.



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.

Digital Economy and Society Index (DESI) 2018 ranking



Catena d'attacco



I pilastri della sicurezza

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

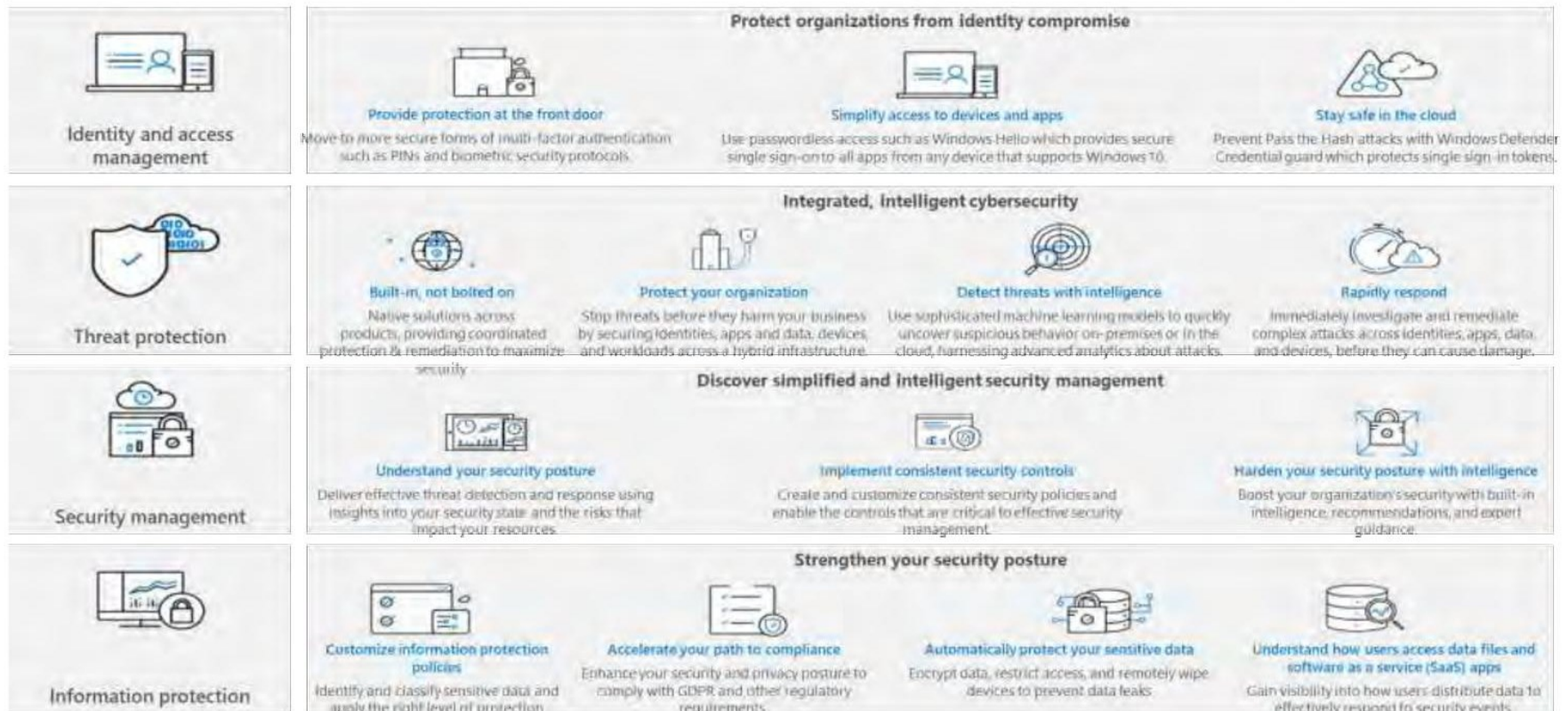
Ensure documents and emails are seen only by authorized people



Security management

Gain visibility and control over security tools

Strategie di sicurezza

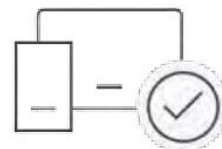


Protezione dell'identità

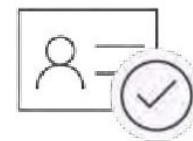
Prove users are authenticated, authorized and secure before granting access to apps, data, and devices



Password-less Authentication



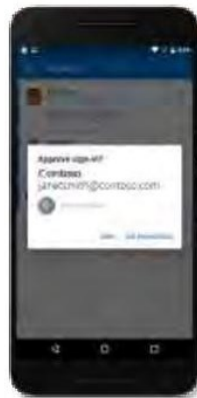
Conditional Access



Identity Protection



Windows Hello



MS Authenticator

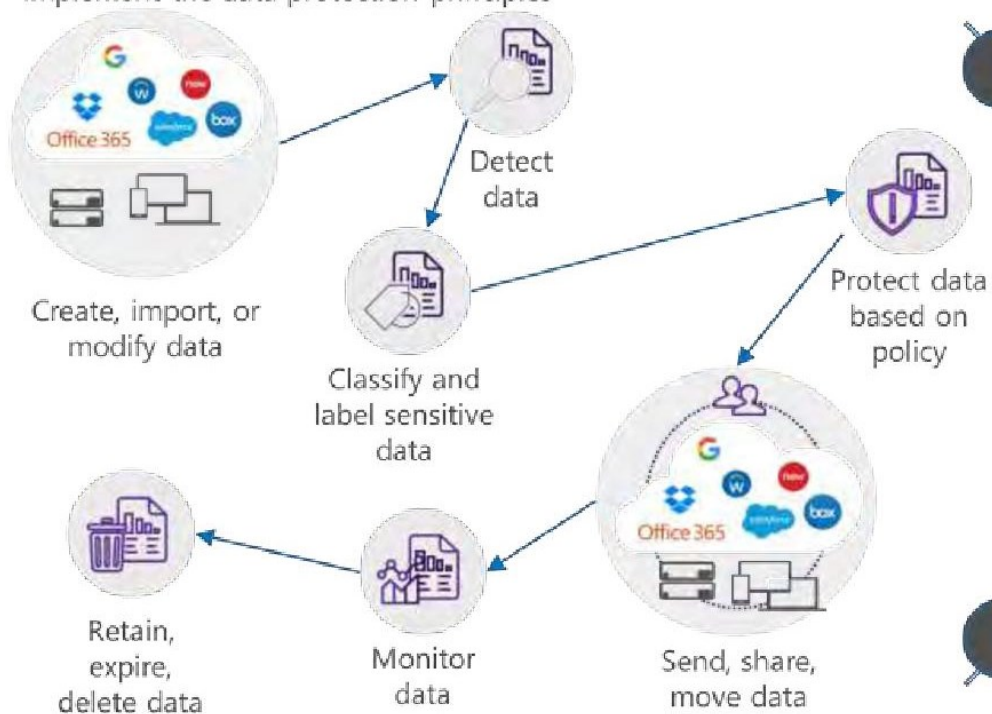


Safeguard credentials when they are used in an OS or application session



Protezione dell'Informazione

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

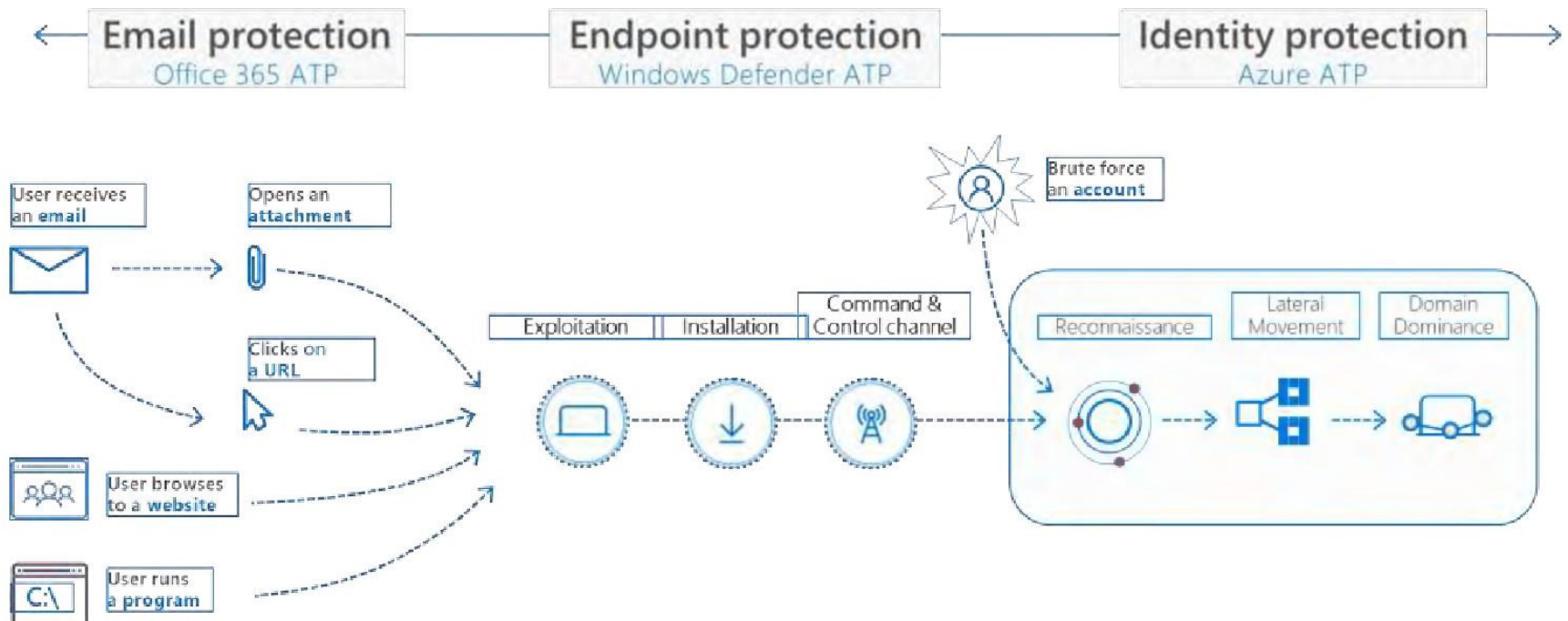


GDPR compliance use cases



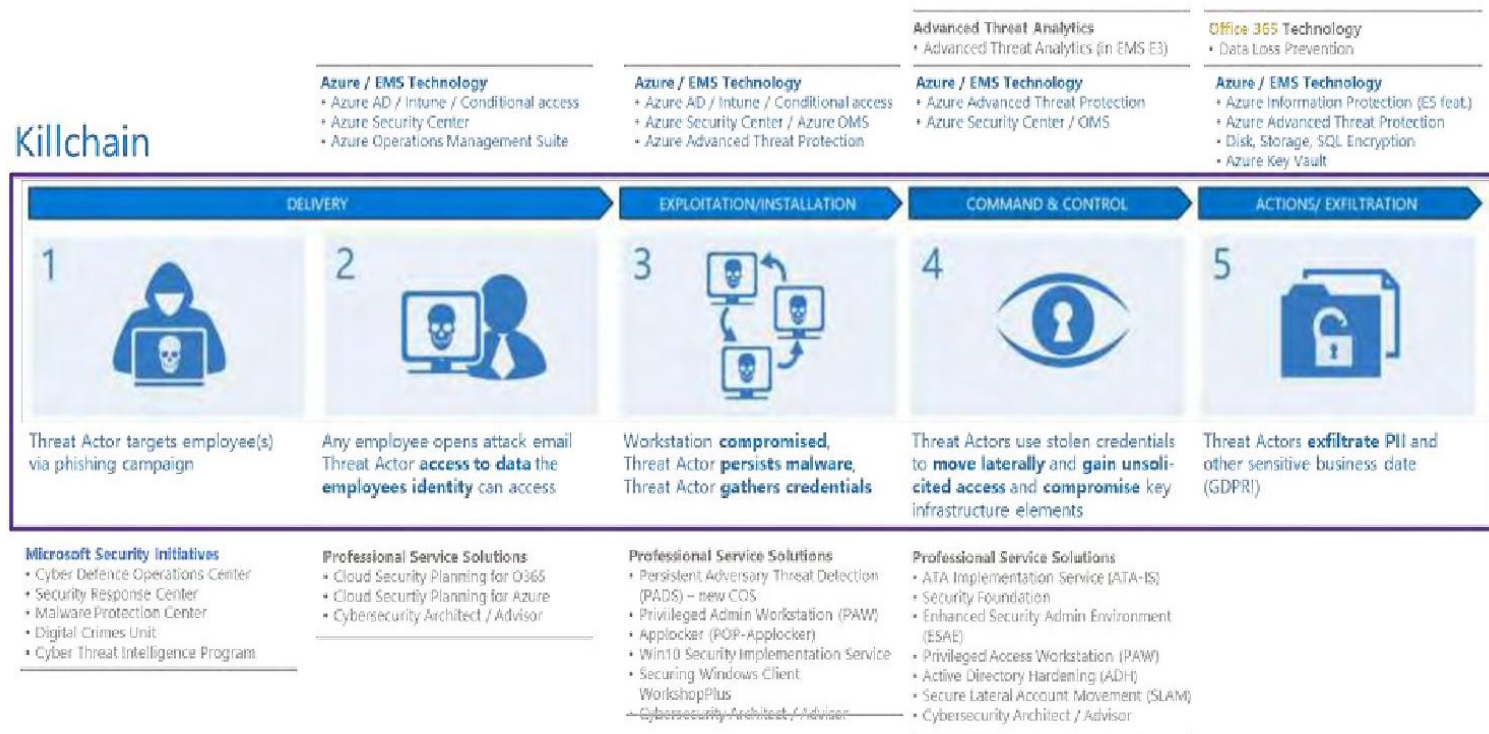
Adopted on 14 April 2016, enforced on 25 May 2018

Copertura della superficie d'attacco



Risposta alla catena d'attacco

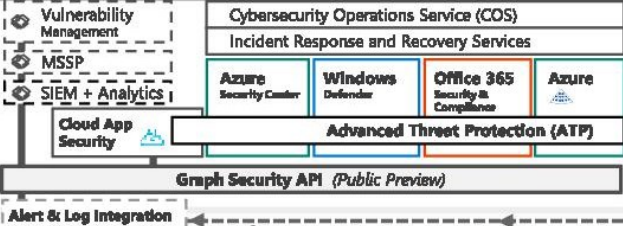
Killchain



Il Cloud come leva per la mitigazione del rischio



Security Operations Center (SOC)



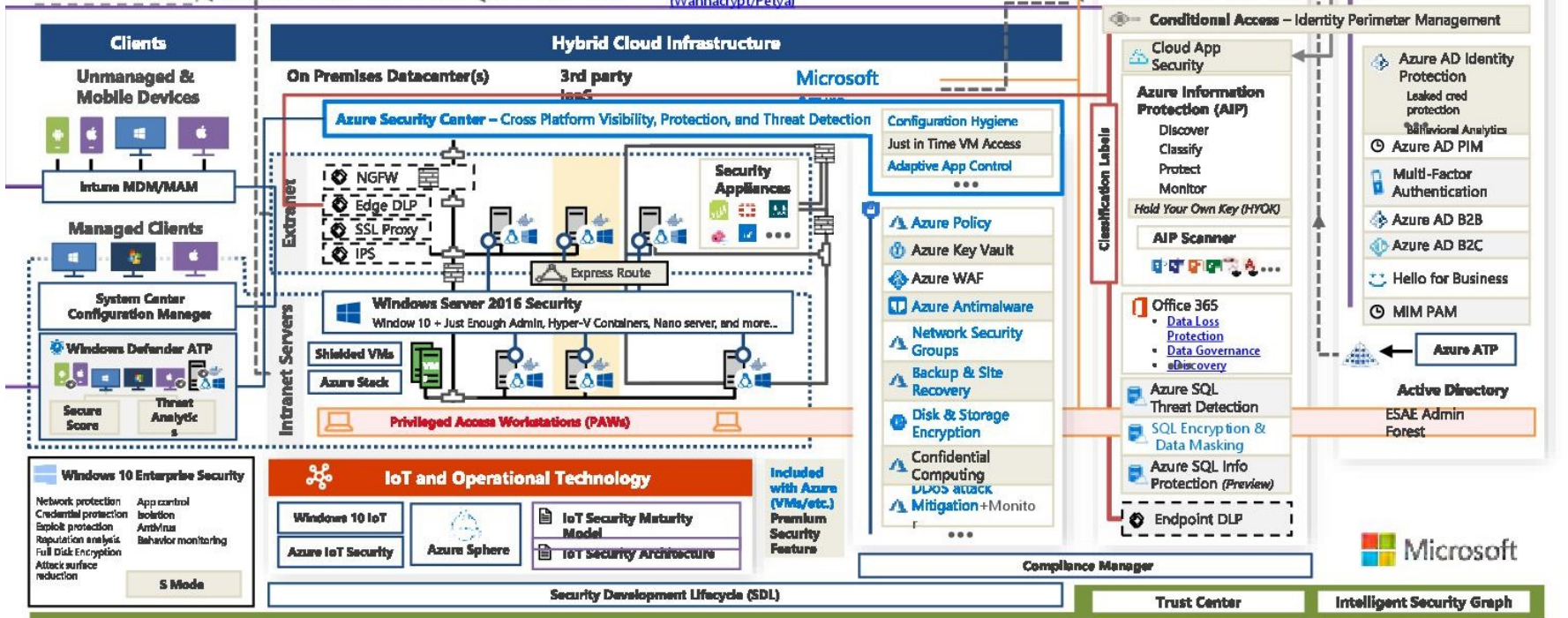
Cybersecurity Reference Architecture

May 2018 – <https://aka.ms/MCRA> | [Video Recording](#) | [Strategies](#)

Roadmaps and Guidance

1. [Securing Privileged Access](#)
2. [Office 365 Security](#)
3. [Rapid Cyberattacks \(Wannacrypt/Petya\)](#)

Software as a Service



- 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)



*Nuovi Paradigmi basati
sull'intelligenza artificiale nella
protezione degli asset informatici*

- Le minacce informatiche di nuova generazione: come siamo arrivati allo stato attuale
- Come le nuove tecnologie e le nuove minacce impattano utenti e infrastrutture
- Perché il Machine Learning è indispensabile e quali sono le difficoltà di applicazione nella Cybersecurity

1994

1
NEW VIRUS
EVERY HOUR



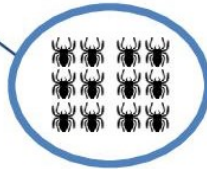
2006

1
NEW VIRUS EVERY
MINUTE



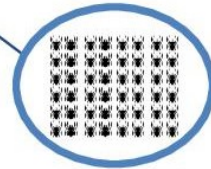
2011

1
NEW VIRUS EVERY
SECOND



2018

360,000
NEW SAMPLES
EVERY DAY



Kaspersky Lab: The Big Numbers of 2017

Online threats

Information for : 2017 | 2016

A **billion** malicious online attacks: 1 billion **↑** | 758 million



15,714,700 unique malicious objects (scripts, exploits, executable files, etc.) detected by Kaspersky Lab's web antivirus in 2017



22% of computers where our web antivirus was triggered hit by advertising programs and their components



88% of attacks originated in 10 countries



Ransomware



More than **96,000** modifications of crypto-ransomware detected



38 new families discovered



939,722 unique KSN users attacked by encryptors, including



>240,000 corporate users

Banking malware



1,126,701 devices saw attempted attacks to launch malware capable of stealing money via online banking

Applications most targeted by exploits



MS Office: 17.6% **↑** | 13%

Adobe Flash: 4.5% **↓** | 8%

APTs ; 0-Days

0.1%



Cyber-weapons

Attacchi Non malware

9.9%



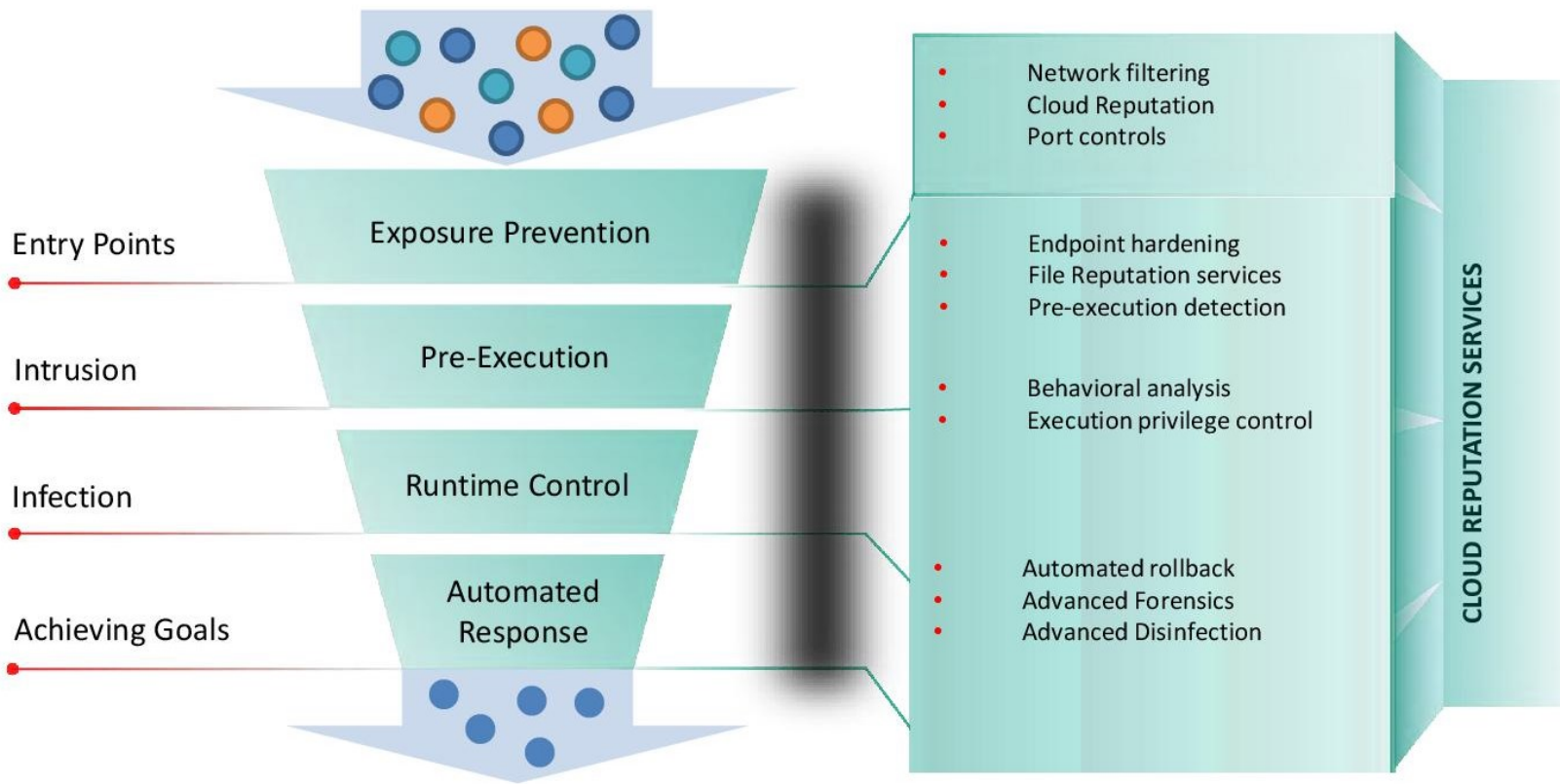
Attacchi Mirati

90%



Cybercrime Tradizionale

- Maggiore complessità delle minacce informatiche dovuta a:
 - Business model efficienti aperti a criminali non avanzati tecnicamente
 - Malware avanzato reperibile in vendita o sottratto a grandi organizzazioni
 - Utilizzo di tecniche proprie degli attacchi mirati per attacchi su larga scala
 - Semplicità di anonimizzazione (Tor – Bitcoin – Darkweb)
 - Utilizzo di minacce non sofisticate abbinate a tecniche di Social Engineering



STAGES OF AN ATTACK

ORDER OF DEFENSE

LAYERS OF PROTECTION

● Unsupervised Learning

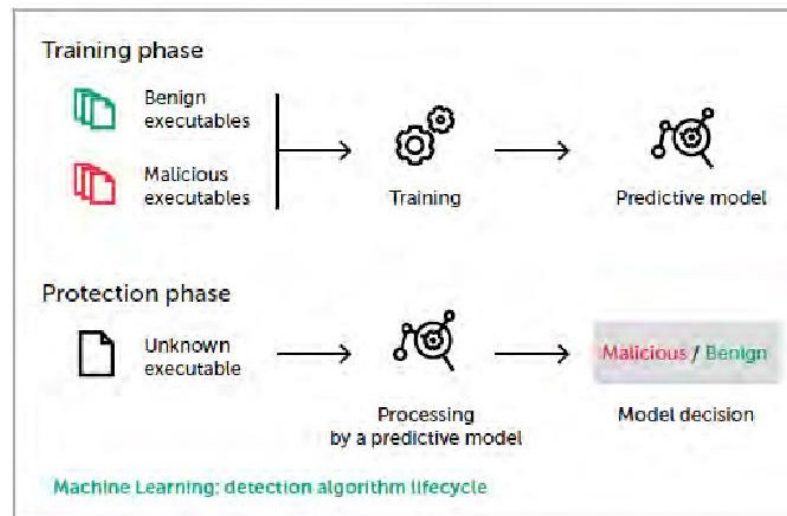
- Ha lo scopo di individuare la struttura dei dati o la legge di generazione del dato
- Apprendimento basato su data set privi delle risposte corrette

● Supervised Learning

- Ha lo scopo di individuare il modello che produrrà la risposta corretta per i nuovi oggetti
- Viene usato quando sono disponibili sia i dati che le risposte giuste
- Si compone di due stadi:
 - Apprendimento e adattamento di un modello ai dati disponibili
 - Applicazione del modello ai nuovi sample e ottenimento di predizioni

● Deep Learning

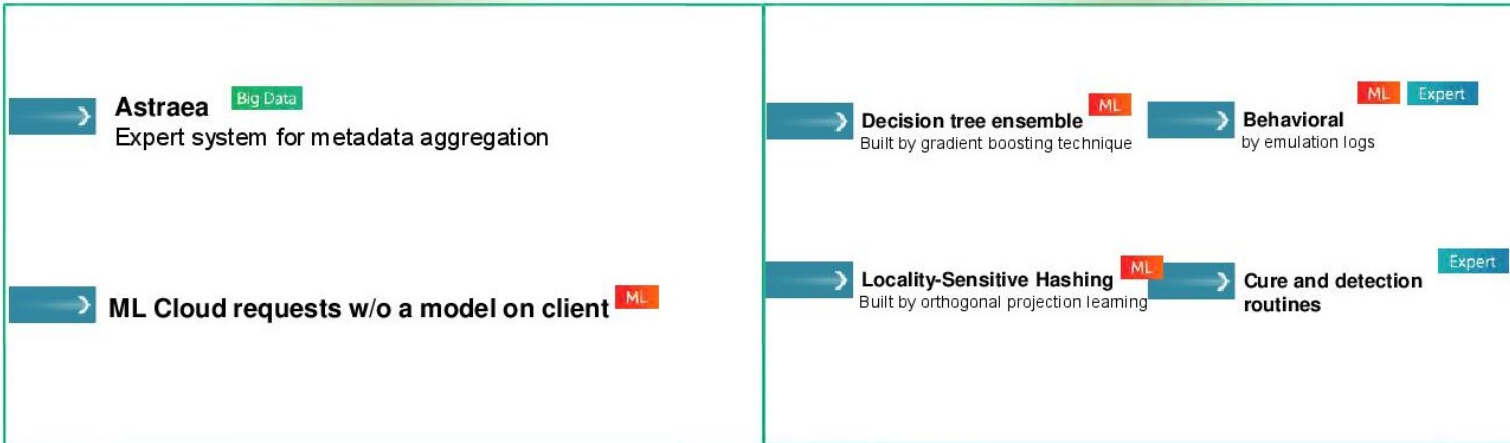
- Approccio che facilita l'estrazione di funzionalità ad un alto livello di astrazione da dati di basso livello (Ex. speech recon, face recon.)
- Utilizzato per identificare malware dai dati di basso livello (Ex. Gerarchie di funzioni, detection multi stadio...)



- Necessità di un Dataset molto ampio
 - La necessità è di addestrare il nostro modello attraverso un dataset rappresentativo delle condizioni reali in cui dovrà operare.
- Trained Model deve essere interpretabile
 - Solitamente i modelli di ML sono delle Black Box non interpretabili dagli umani, questo non va bene in cybersecurity perché non permette l'analisi di una serie di casi (ex. Falsi positivi)
- False Positive Rate pari a zero
 - Necessità non comune nel ML, che richiede di impostare requisiti molto alti nella fase di training, sia per il modello che per le metriche.
 - Il modello deve permettere la correzione dei FP «on the fly» in caso di rilevamenti errati basati su dati sconosciuti, senza dover addestrare di nuovo il modello. Gli algoritmi devono potersi adattare alle reazioni dei Cybercriminali – distribuzione dei dati variabile
 - Gli avversari scrivono nuovi malware con nuove tecniche
 - Migliaia di Software House producono nuovi tipi di eseguibili benigni

IN CLOUD

ON CLIENT

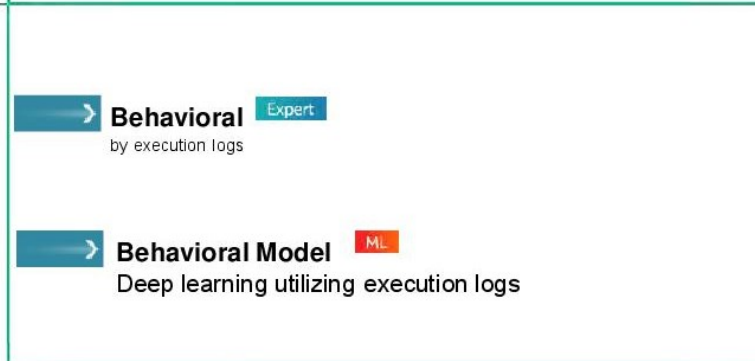


PRE
EXECUTION

ML — Content is generated automatically by machine-learning techniques

Expert — Content is generated by experts

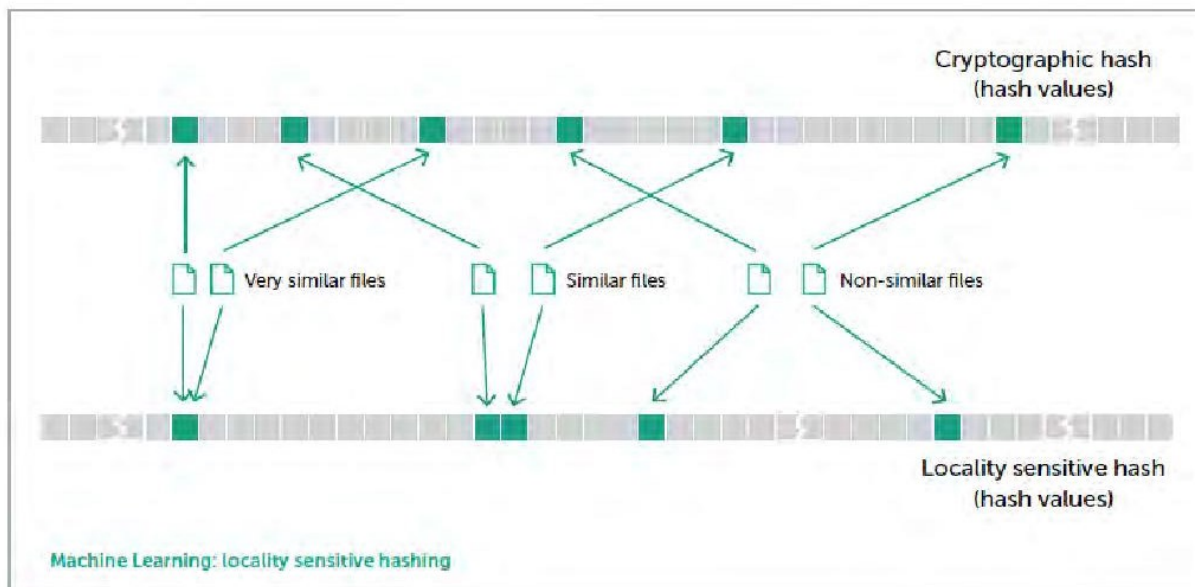
Big Data — Suspicious files' metadata from millions of endpoints collected and processed



POST
EXECUTION

- Pre-Execution:

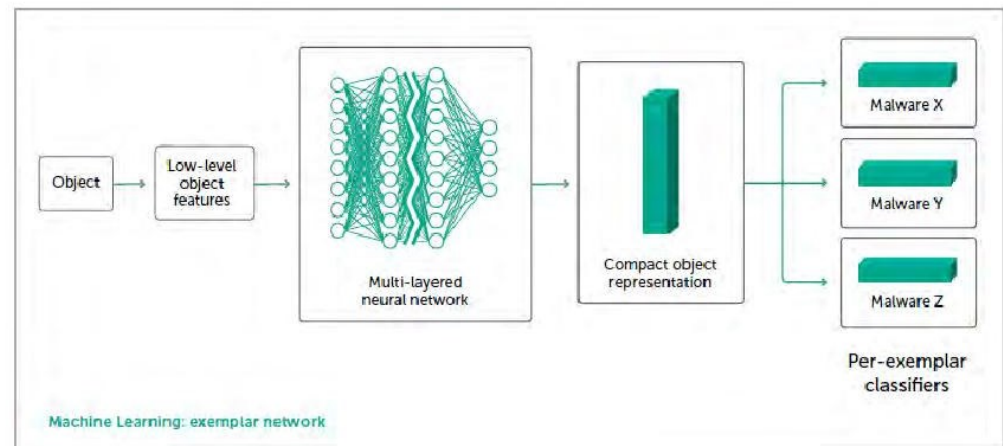
- Similarity Hashing (LSH) basato sulla struttura del file, molto utile per identificare varianti di varie tipologie di malware.
- Viene utilizzato in combinazione con altri algoritmi in uno schema a due stadi, allo scopo di ridurre il carico computazionale sull'endpoint e limitare i falsi positivi.



Deep Learning contro gli attacchi mirati:

- Nel caso di un sample singolo viene usato l'approccio **Exemplar Network (ExNet)**

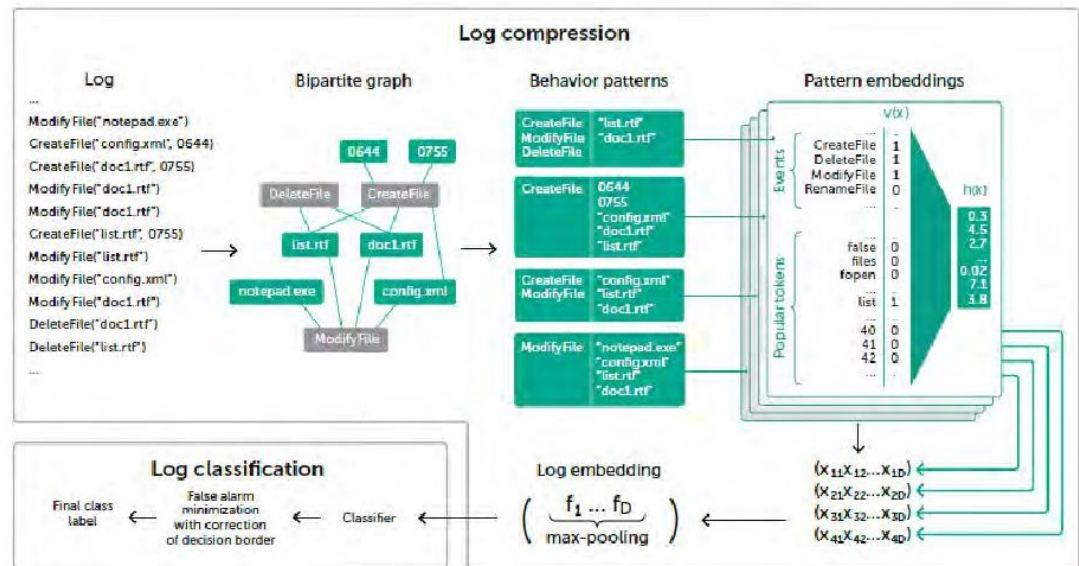
Permette di combinare più passaggi (estrazione di funzionalità, rappresentazione compatta e creazione di un modello per esemplari) **in una singola pipeline con le discriminanti di vari tipi di malware**



Deep Learning in Post-Execution:

- Log forniti dai motori di analisi comportamentale
- **Il modello comprime la sequenza di eventi in un set di vettori binari che vengono forniti ad una rete neurale per distinguere i comportamenti leciti da quelli pericolosi**

Permette di addestrare una rete neurale capace di operare con concetti comportamentali di alto livello. Può adattarsi a diversi ambienti utente e incorpora funzionalità di correzioni di falsi allarmi by design.



Conclusioni

- Avere i dati giusti
- Conoscere la teoria del ML e come applicarla in cybersecurity
- Conoscere i bisogni degli utenti e essere esperti nella tecnologia
- Avere una giusta quantità di dati
- Applicare un approccio multi livello per il rilevamento delle minacce

Grazie per l'attenzione

Vincenzo Calabrò

www.vincenzocalabro.it

LinkedIn / vincenzocalabro