



IRIDEOS

connessi al domani

Sicurezza degli algoritmi:
criticità e vulnerabilità per Aziende, Nazioni e utenti

17 maggio 2019



Il progetto IRIDEOS

Un nuovo polo che aggrega e consolida gli operatori ICT italiani nel mondo B2B



F2i SGR (*Fondi italiani per le infrastrutture*) è il più grande Fondo infrastrutturale operante in Italia e tra i maggiori in Europa. Circa 2,5 miliardi di euro investiti in infrastrutture nazionali (aeroporti, distribuzione gas, servizi idrici, energie rinnovabili). Nelle telecomunicazioni ha acquisito Metroweb nel 2011, poi ceduta a OpenFiber a fine 2016.



Marguerite (*the 2020 European Fund for Energy, Climate Change and Infrastructure*), è un fondo creato con il sostegno di sei istituzioni finanziarie pubbliche europee e della Commissione Europea per investimenti capital-intensive nell'Unione Europea.

-----> **78,3%**



IRIDEOS



-----> **19,6%**

Fusione in
IRIDEOS
agosto '18



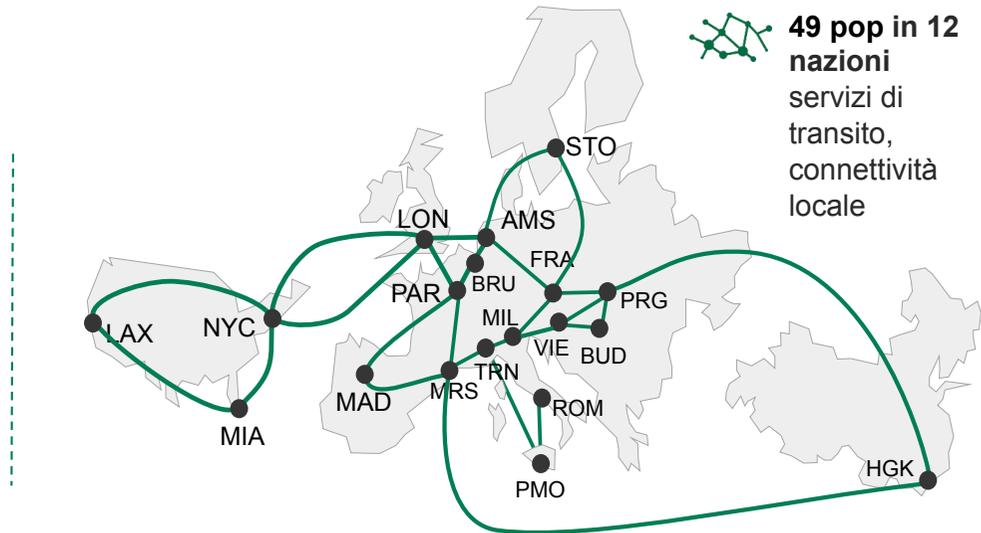
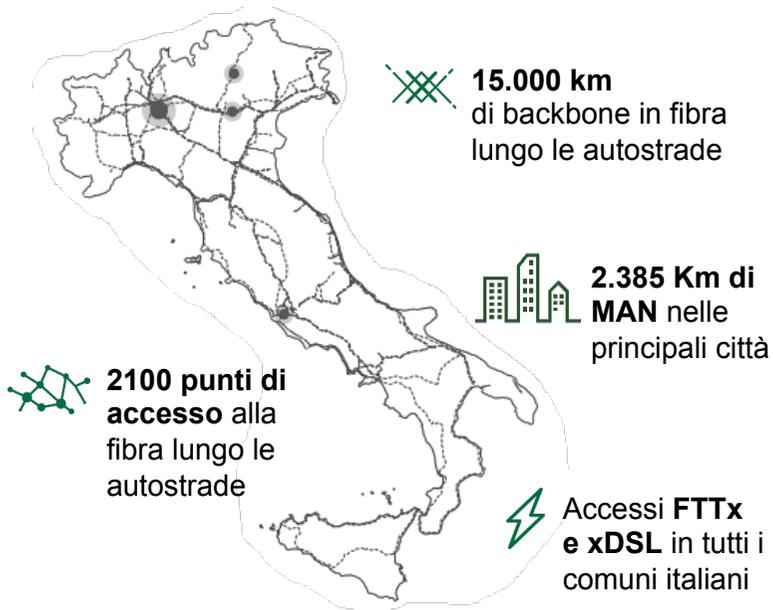
100%





La rete

Rete in fibra lungo le autostrade e presenza internazionale



Interconnessi con i maggiori Internet Exchange europei

IRIDEOS



I Data Center

12 data center in 4 città, forte presenza in Caldera



Milano.Caldera
[Avalon Campus]

8	Data center
8.900	mq
23	sale

- TIA-942 (tier III)
- POP MIX in sala

SAP® Certified in SAP HANA® Operations **SAP®** Certified in Hosting Services



Roma.Tiburtina

2	Data center
550	mq
3	sale



1 DC certificato:
Tier IV - Design



Trento.Dolomiti

1	Data center
425	mq
7	sale

Accesso privilegiato a
fonti energetiche



Verona.Brennero

1	Data center
500	mq
1	sala

Interconnessioni con cloud provider

Microsoft Express Route - AWS Direct Connect - Oracle Fast Connect - Google Cloud Interconnect - Salesforce Express Connect - City Cloud Connect - IBM Direct Link - Tencent Direct Connect - Alibaba Cloud
Attive primo trimestre 2019



Avalon Campus

Il più grande hub italiano per la «neutral colocation»

Unico punto in Italia per connettersi con tutti gli operatori nazionali ed internazionali

- oltre **155 operatori** ospitati
- **11.000 link** in fibra ottica installati



Accesso diretto al backbone di Internet

- 2 accessi in fibra separati
- POP MIX in sala

Milano – via Caldera

- 8900 m²
- 23 sale in 4 edifici



Tre piattaforme Cloud

Prestazioni elevatissime e soluzioni per ogni esigenza



V.Cloud

- Adatto ai **carichi stabili** ad alte prestazioni
- Storage "**ultraperformante**" (fino a 1M Iops)
- Disaster recovery "Zerto based"
- **Alta affidabilità** grazie all'infrastruttura distribuita su 3 data center interconnessi

vmware[®]



O.Cloud

- Adatto ai **carichi dinamici** ad alte prestazioni
- Nativamente distribuito a livello europeo: Milano, Francoforte, Amsterdam
- Supporto architetture a **microservizi** e **DevOps Cloud Automation**

 **openstack.**



S.Cloud

- Specifico per **ambienti SAP Hana**
- Alta affidabilità inclusa nel servizio
- Progetti di migrazione da ambienti "in house" disponibili
- Servizi di gestione SAP opzionali

Certificazioni:

SAP[®] Certified
in SAP HANA[®] Operations

SAP[®] Certified
in Hosting Services

Centinaia di aziende "già a bordo" e migliaia di applicazioni attive



Alcune referenze

Carrier

Akamai	Epsilon Telecommunications	Level 3	Telecom Italia Sparkle
Aria	Fastweb	N.G.I. - Eolo	Telespazio
BT Italia - British Telecom	Globecast	NTT Communications	T-Systems Italia
C&W - Cable & Wireless	GTT	Orange	Vanco
Cogent Communications	H3G	Skylogic	Vodafone
Colt Telecom	KPN	Tata Communications	Wind Telecomunicazioni

OTT

Nella Avalon telehouse sono presenti i più grandi Over The Top e Content Delivery Network internazionali.

Automotive

Volkswagen
Audi
BMW

Finanza e assicurazioni

ACRI
Banca del territorio Lombardo
BB Tech Group s.r.l.
BCC Pordenone
Cattolica
Fineco
Natixis
Toyota Financial Services
Vittoria Assicurazioni

Industria e Servizi

Aeroporto Valerio Catullo	CPL Concordia	Gruppo Italiano Vini	Marelli Motori	SCORPION BAY S.P.A.
Autostrada	Daikin Applied Europe	Gruppo Poli Supermercati	MD Spa	Sifte Berti
Autostrade Meridionali	Dedagroup	GSK	Moto.it	Sistemi Spa
AXIOMA	Deloitte	HALLEY Informatica	MyChef	Sittam
Bisazza	DHL International	ICAR	OIA Services Ltd.	Subito.it
BS-PD	Exalogic	I-Faber	OMEGA Software	TotalErg
Calzedonia	Exprivia	I Grandi Viaggi S.p.A	OPENJOBMETIS SPA	TT Tecnosistemi S.p.A
Carrefour	F2A	Immobiliare.it	Pixartprinting	Unicef
Cementir Holding	GlaxoSmithkline	Iper supermercati	Profexional Srl	Univeg
Centro Epson Meteo	Golden Lady	LD Market	Quadriga	Valassis
Co.Ge.Di International S.p.a.	Golden Point	Like	Reply S.p.A	
Comparameglio.it	Grimaldi Group SpA		Salmoiraghi & Viganò	

PA, Utility e Sanità

Comune Verdello (BG)	ISISS Valle Seriana	AMA Roma	Unigas Distribuzione	Uniacque	San Raffaele Roma
Consorzio Parco dei Colli di Bergamo	Provincia di Treviso	Dolomiti Energia	Cogeide	Istituti Ospedalieri Bergamaschi – Gruppo San Donato	Cliniche Habilita



Raffaele Regni

Cyber Security Manager in Irideos

- Cos'è la Cyber Security?

Alla conferenza di Black Hat del 2014, il generale Keith Alexander, allora direttore della NSA, usò la frase Computer Network Operations (CNO).

CNO è il termine generico per le tre diverse componenti coinvolte nella guerra informatica tradizionale:

- *Computer Network Defense (CND),*
- *Sfruttamento della rete informatica (CNE),*
- *Computer Network Attack (CNA).*

CNO = Cyberwarfare

CNE + CNA = cyberwarfare offensivo.

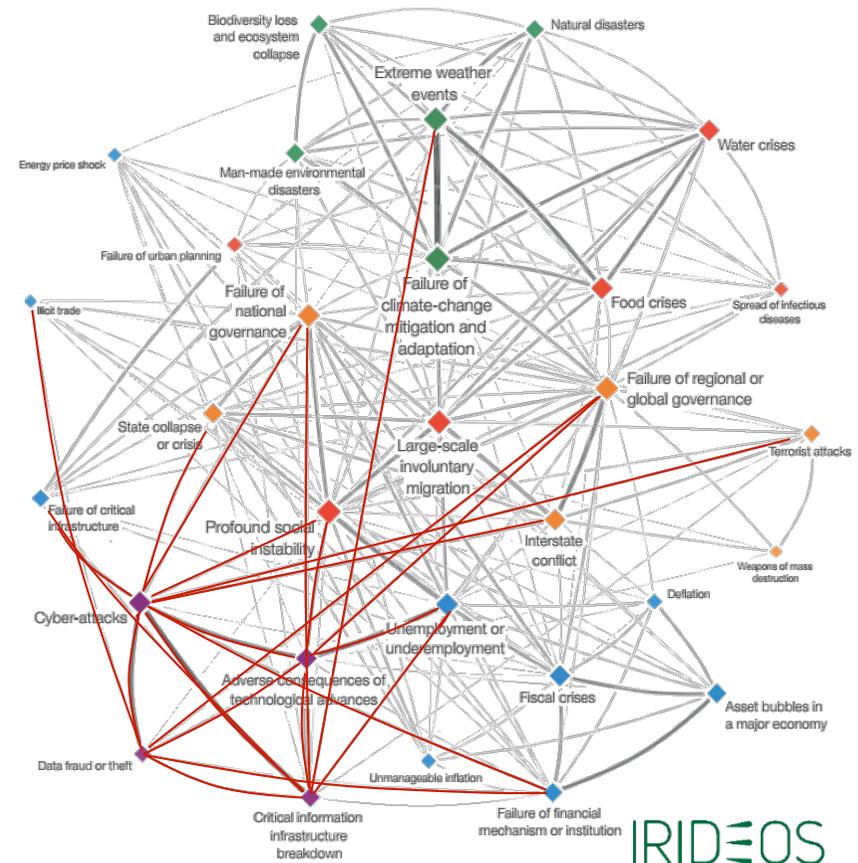
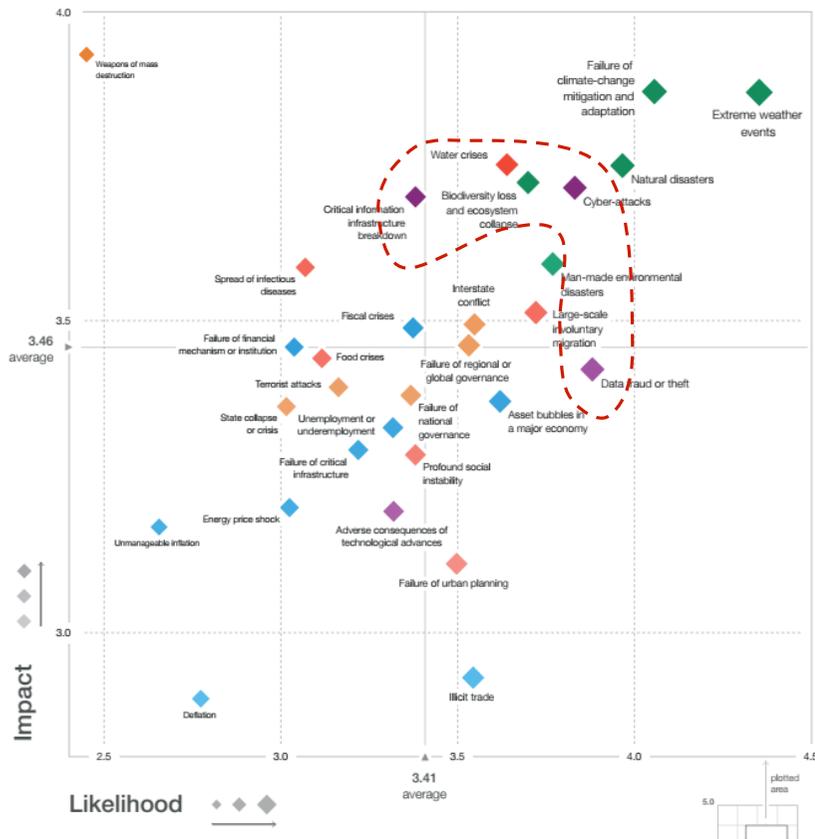
CND = cyberwarfare difensivo.

Questa è la Cyber Security



Panorama delle minacce

Il World Economic Forum ha pubblicato il Global Risks Report 2019



IRIDEOS



Contesto di riferimento

Danno reale Vs. Minaccia Percepita

Rischio percepito

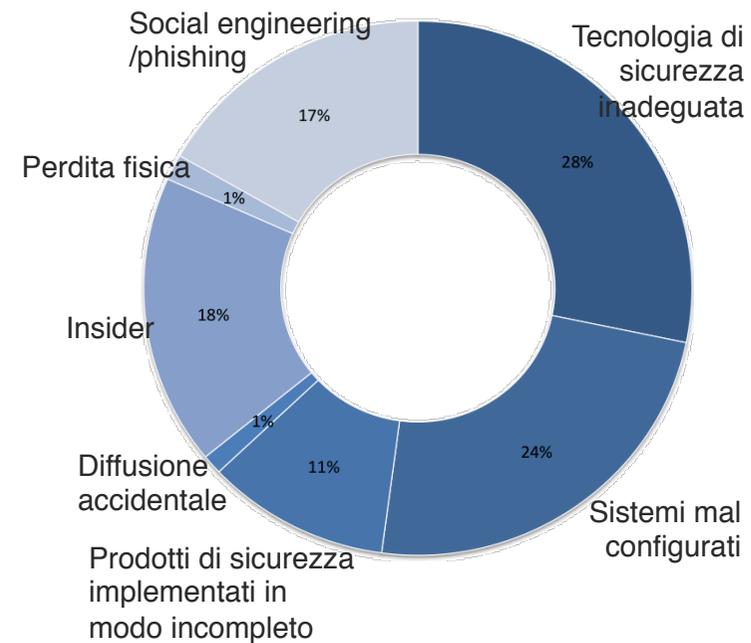
32%
Delle società ritengono il rischio Cyber come uno dei principali rischi

28%
Delle aziende ha subito un attacco cyber negli ultimi 12 mesi

24%
Delle organizzazioni vede la Business Interruption come la minaccia numero 1 della propria attività

Source: Continental European Cyber Risk Survey 2016

Reali cause di danno



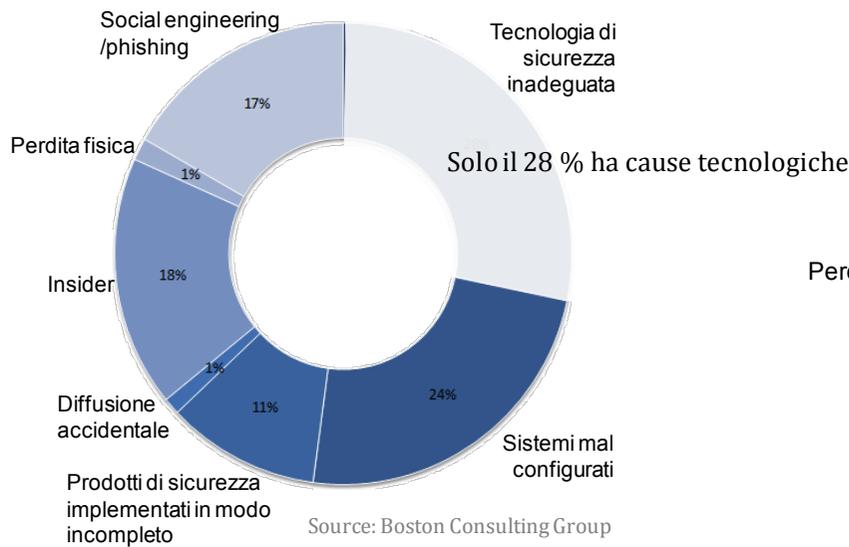
Source: Boston Consulting Group 2017



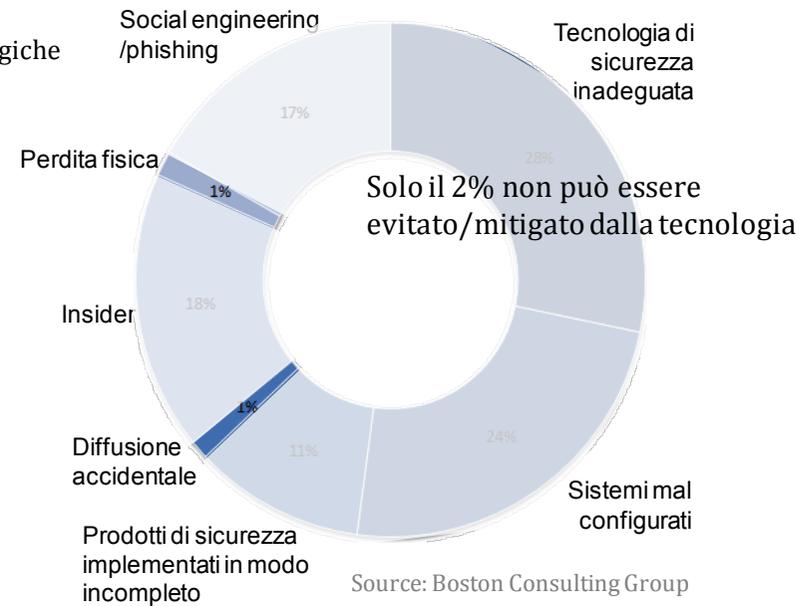
Contesto di riferimento

Danno reale Vs. Minaccia Percepita

Reali cause di danno



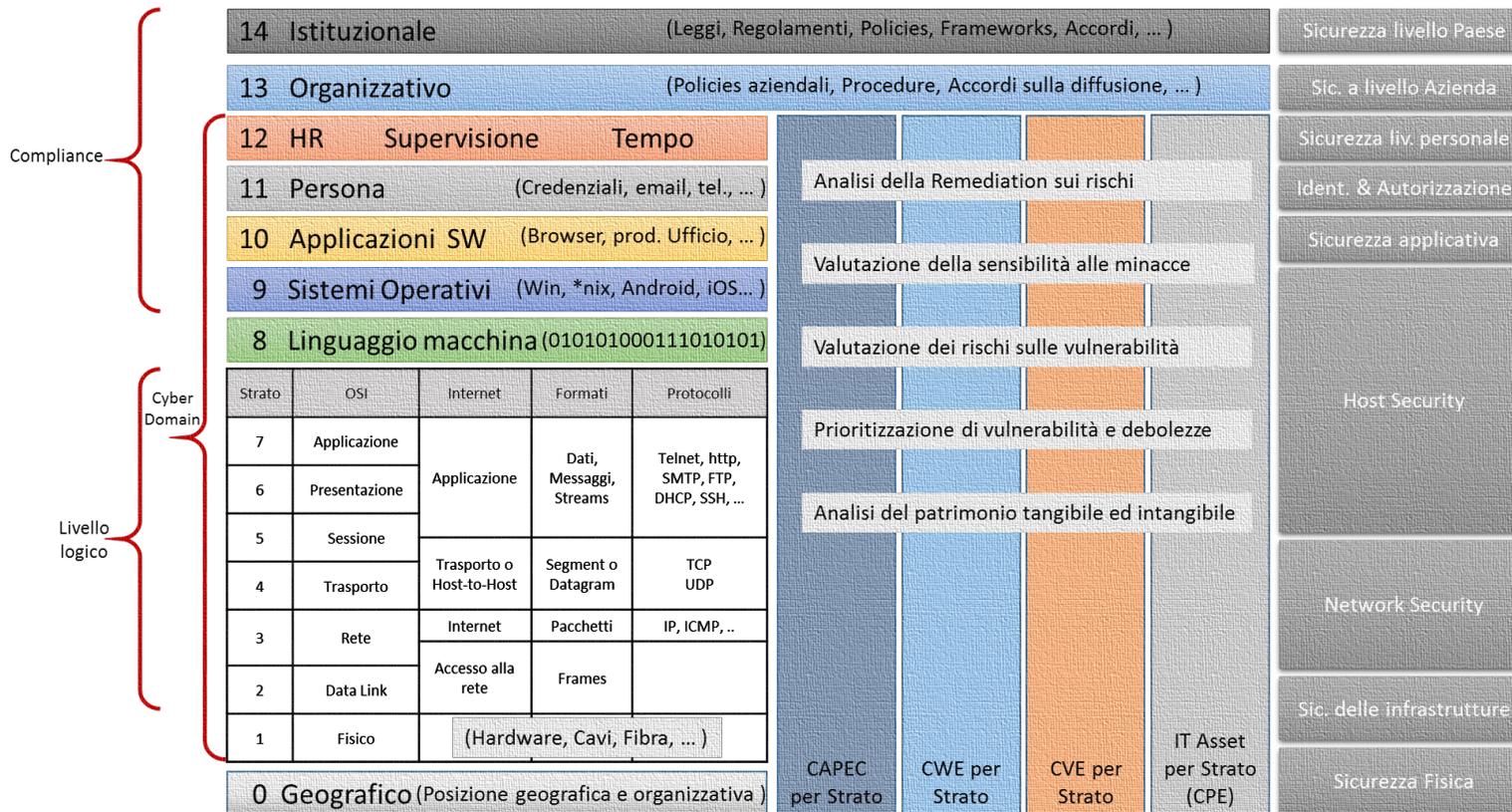
Reali cause di danno





La nuova Cyber Security

Snowden e il Datagate hanno cambiato il modo di vedere la Cyber Security

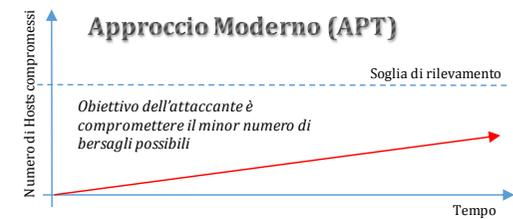
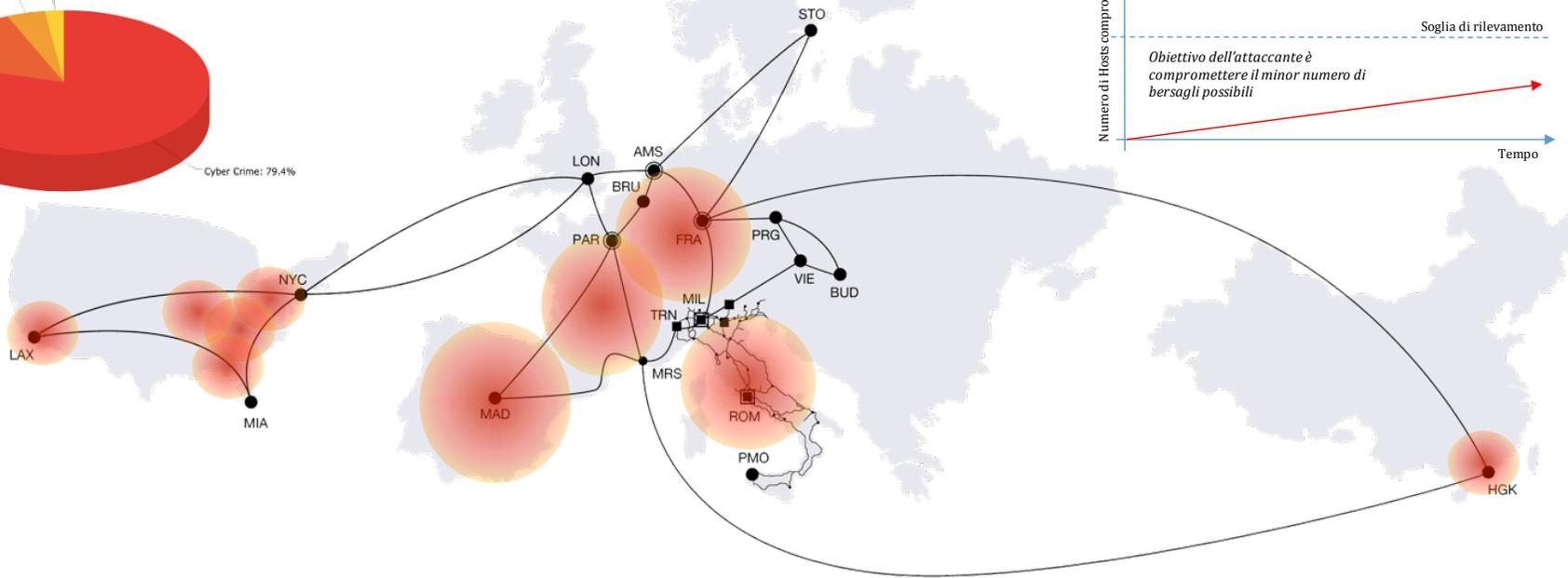
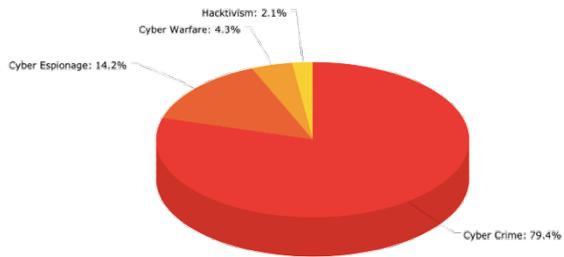




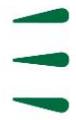
Architettura Irideos

Un mondo da proteggere

Motivations Behind Attacks (March 2019)
hackmaggeddon.com



- **A chi attacca basta avere successo una volta**, chi si difende deve vincere sempre..
- **Chi attacca ha a disposizione molte più risorse di chi si difende**, violare i sistemi è il suo core business



Approccio di difesa (in prestito dal mondo militare)

Presupposto: Nessun sistema è impenetrabile

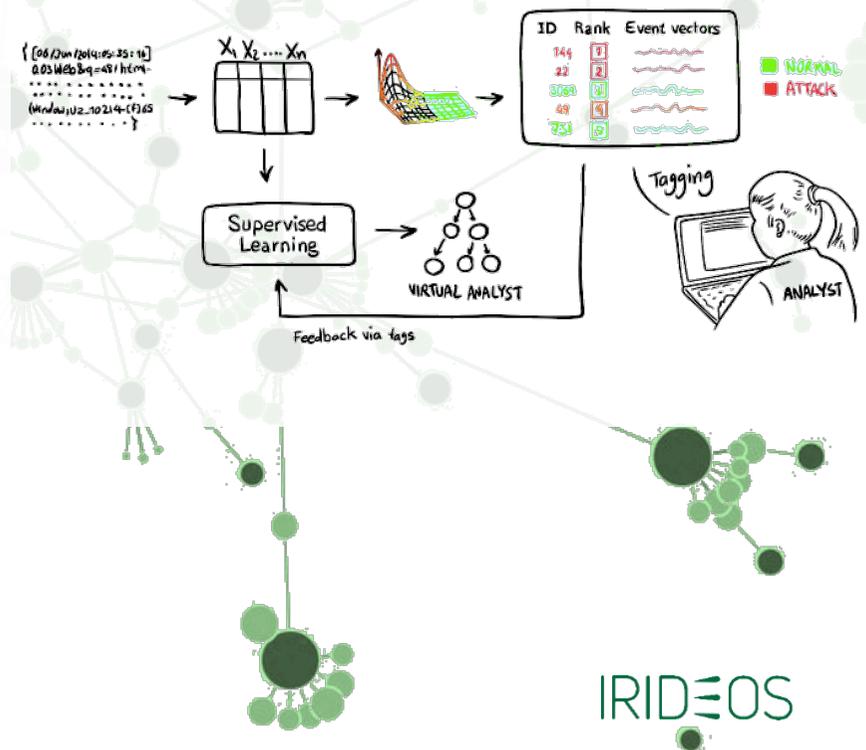


Le minacce cambiano => Il sistema evolve

Processo di difesa

Perché Irideos si rivolge al Machine Learning

- Le piattaforme informative compongono un grafo
- Ogni nodo è affetto da vulnerabilità e soggetto a minacce
- Attraverso l'analisi del rischio cumulato sono gestite le priorità di mitigation (**sicurezza Proattiva**)
- Behavior Analysis e correlazione di eventi identificano i possibili attacchi (**sicurezza Reattiva**)
- Identificato un potenziale agente malevolo sono calcolati i possibili alberi di attacco
- Dai possibili alberi di attacco sono identificati i nodi critici, intervenendo sui quali si isola l'attaccante
- Isolato l'attaccante è possibile procedere all'hardening delle piattaforme violate



IRIDEOS

IRIDEOS

 info@irideos.it

 800.585.383

 irideos.it