DEFENSIS

MILANO, 22 MARZO 2018

CYBERSECURITY E GDPR

DEFENSIS

GRUPPO ITALIANO 1972

INTELLENET
International Intelligence Network

WAD
World Associations of Detectives

CII
Council of International Investigators

GIDP
Associazione Direttori Risorse Umane

COMPLIANCE / CYBER SECURITY

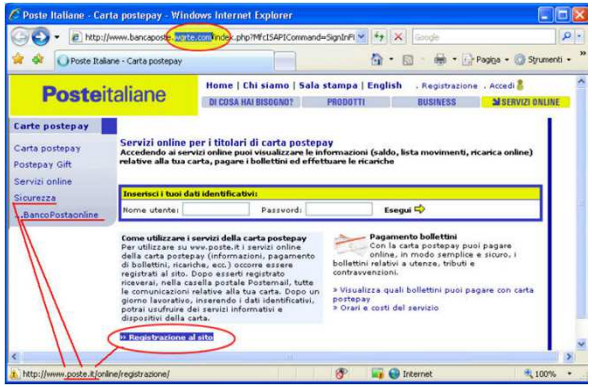
PERIZIE INFORMATICHE

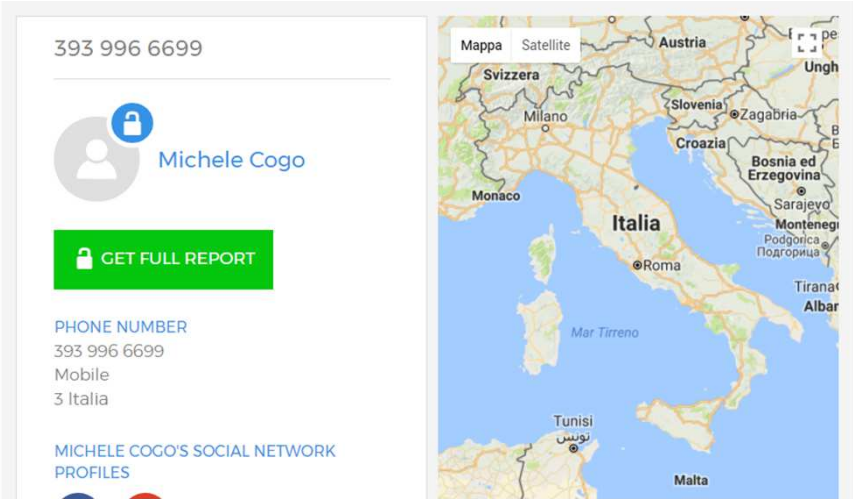
INVESTIGAZIONI/ DUE DILIGENCE

DEFENSIS


KASPERSKY
Kaspersky
ANTI-VIRUS
KASPERSKY lab
BANNED


Sarahah


Poste Italiane - Carta postepay - Windows Internet Explorer
Posteitaliane
Home | Chi siamo | Sala stampa | English
Carte postepay
Carta postepay
Postepay Gift
Servizi online
Sicurezza
BancoPostaonline
Servizi online per i titolari di carta postepay
Inserisci i tuoi dati identificativi:
Nome utente:
Password:
Esegui
Come utilizzare i servizi della carta postepay
Pagamento bollettini
Registrazione al sito


393 996 6699
Michele Cogo
GET FULL REPORT
PHONE NUMBER
393 996 6699
Mobile
3 Italia
MICHELE COGO'S SOCIAL NETWORK PROFILES
Mappa
Satellite
Austria
Svizzera
Milano
Slovenia
Zagabria
Croazia
Bosnia ed Erzegovina
Monaco
Sarajevo
Italia
Roma
Mar Tirreno
Tunisi
Malta

DEFENSIS

Inserisci la tua email per verificare se il tuo account ha subito attacchi ed é stato compromesso.

michele.cogo@gmail.com VERIFICA

Oh no! il tuo account è stato trovato!

Breach in cui sei stato coinvolto

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Dati compromessi: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Dati compromessi: Email addresses, Passwords

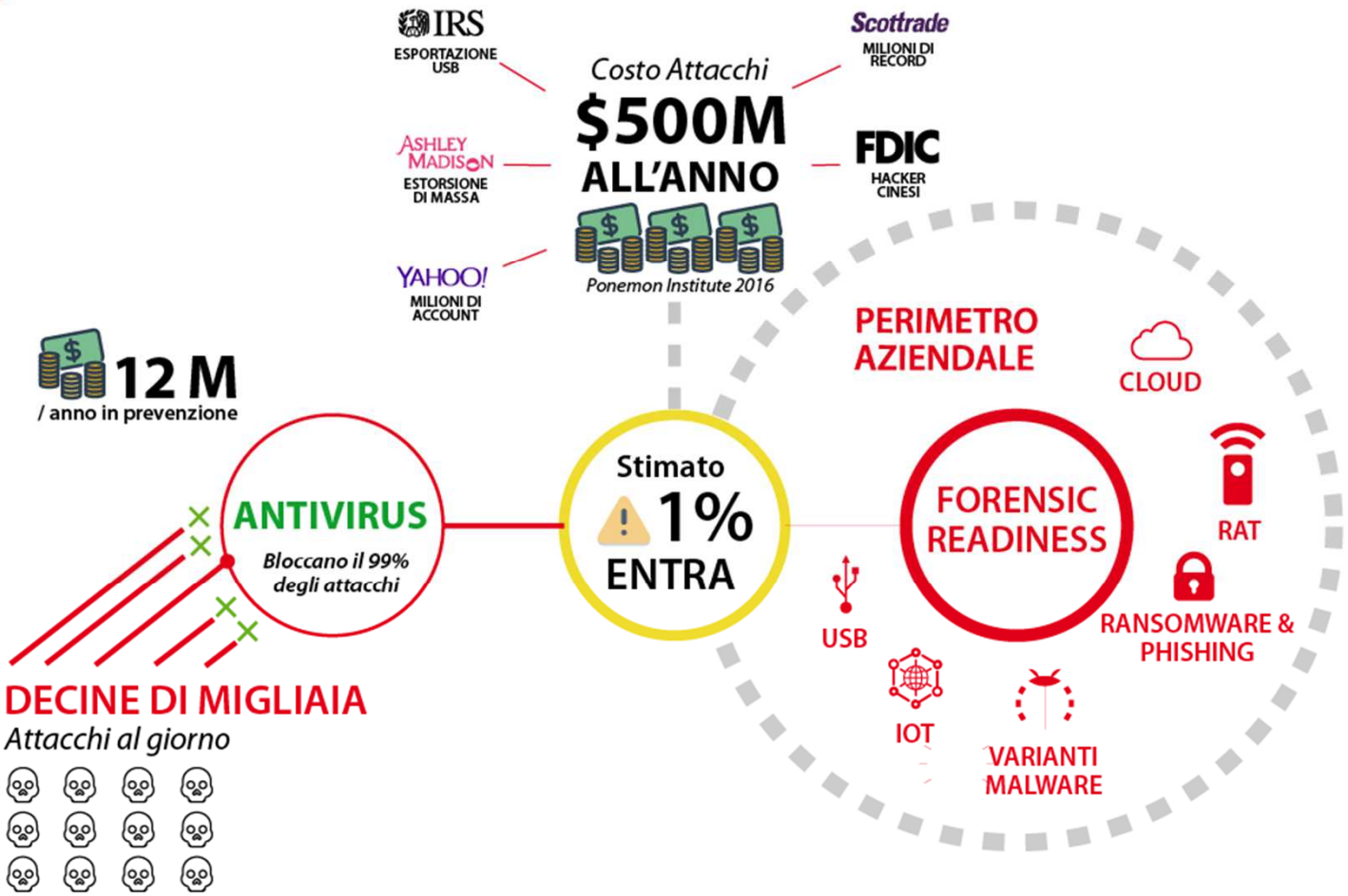
MySpace: In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Dati compromessi: Email addresses, Passwords, Usernames

DEFENSIS

DATA BREACH ITALIA 2017

DEFENSIS


IRS
ESPORTAZIONE USB
Scottrade
MILIONI DI RECORD
Costo Attacchi
$500M
ALL'ANNO
ASHLEY MADISON
ESTORSIONE DI MASSA
FDIC
HACKER CINESI
YAHOO!
MILIONI DI ACCOUNT
Ponemon Institute 2016
12 M
/ anno in prevenzione
PERIMETRO AZIENDALE
CLOUD
ANTIVIRUS
Bloccano il 99% degli attacchi
Stimato
1%
ENTRA
FORENSIC READINESS
RAT
USB
RANSOMWARE & PHISHING
IOT
VARIANTI MALWARE
DECINE DI MIGLIAIA
Attacchi al giorno

DEFENSIS

PRIVACY → **GDPR**

NUOVO ART. 4
Art. 23 D.Lgs 151/2015

Art. 6 comma F. – Legittimo Interesse
Considerando 47 – trattare dati strettamente necessari a fini di prevenzione delle frodi

Utilizzo anche ai fini del rapporto di lavoro

POLICY USO BENI AZIENDALI

AGID
Circolare 2/2017

DEFENSIS

ART. 32 – SICUREZZA DEL TRATTAMENTO

“METTERE IN ATTO MISURE TECNICHE E ORGANIZZATIVE ADEGUATE PER GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO”

DEFENSIS

ART. 33 – NOTIFICA VIOLAZIONE DATI PERSONALI

ENTRO 72 ORE:

A) DESCRIVERE NATURA E CONSEGUENZE DELLA VIOLAZIONE

B) COMUNICARE DATI REFERENTE AZIENDALE

C) DESCRIVERE LE MISURE ADOTTATE E LA REMEDIATION

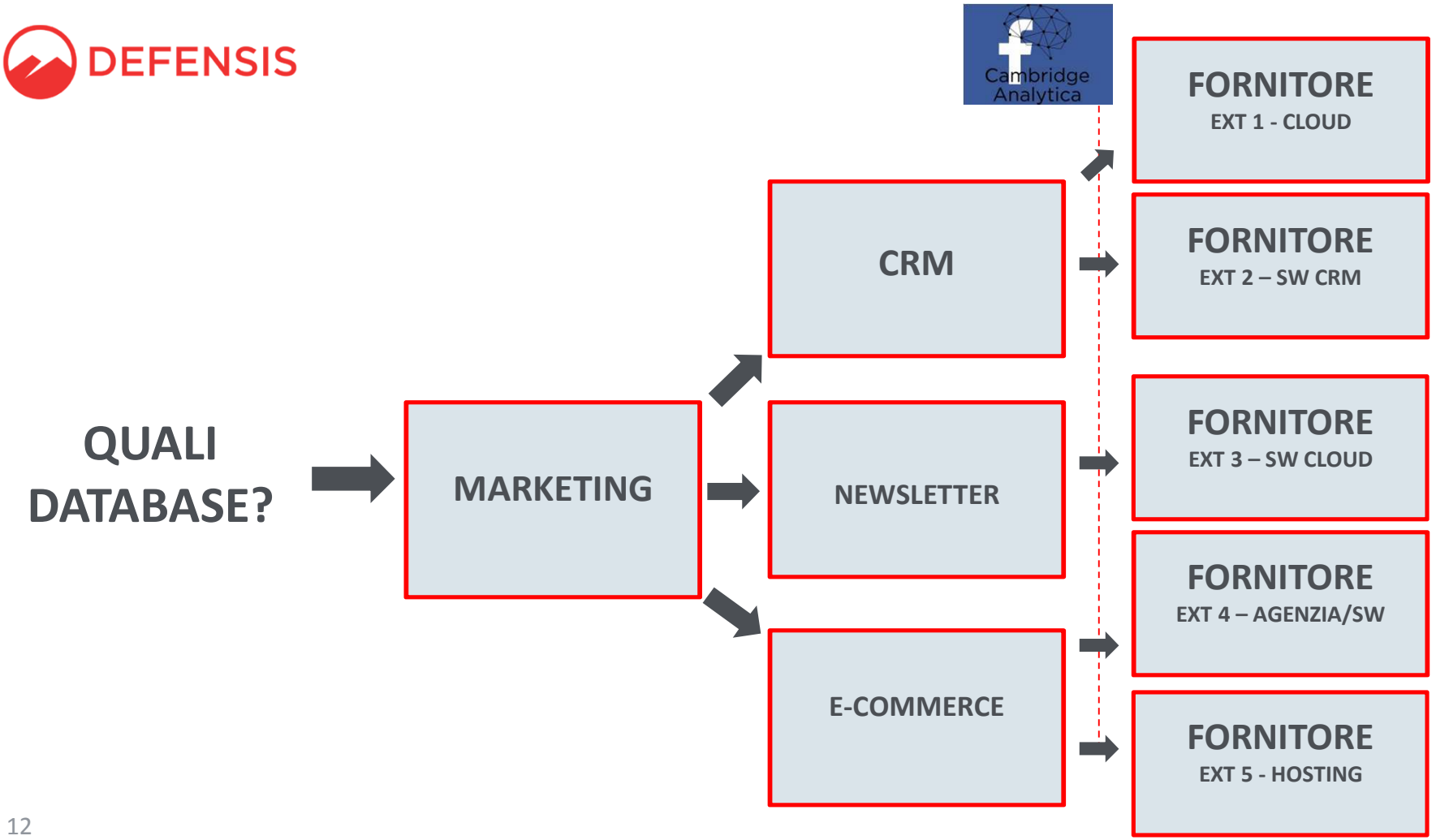
DEFENSIS

FORENSIC READINESS

*E' LA **CAPACITÀ** DI FAR FRONTE A PROBLEMATICHE INFORMATICHE, **GESTENDO** L'INCIDENTE, **RIPRISTINANDO** LE ATTIVITÀ E **RACCOGLIENDO** DATI CHE ABBIANO **VALORE PROBATORIO**.*

DEFENSIS

DEFENSIS


Cambridge Analytica
QUALI DATABASE?
MARKETING
CRM
NEWSLETTER
E-COMMERCE
FORNITORE
EXT 1 - CLOUD
FORNITORE
EXT 2 – SW CRM
FORNITORE
EXT 3 – SW CLOUD
FORNITORE
EXT 4 – AGENZIA/SW
FORNITORE
EXT 5 - HOSTING

DEFENSIS

SMALL BUSINESS

«misure tecniche e organizzative adeguate»

DEFENSIS

DEFENSIS

SMALL BUSINESS

- ***ANTIVIRUS***
- ***POLICY E LOG***
- ***TEAM DI CRISI***
- ***VA. VULNERABILITY ASSESSMENT***

DEFENSIS

LOG

- *ESPORTAZIONE DATI*
- *OPERAZIONI SU FILE*
- *PROCESSI IN ESECUZIONE*
- *…*

DEFENSIS

TEAM GESTIONE CRISI

Margine di discrezionalità molto ampio
(fare o non fare, aver adottato misure di sicurezza adeguate o meno...)

Indispensabile agire rapidamente in caso di data breach.

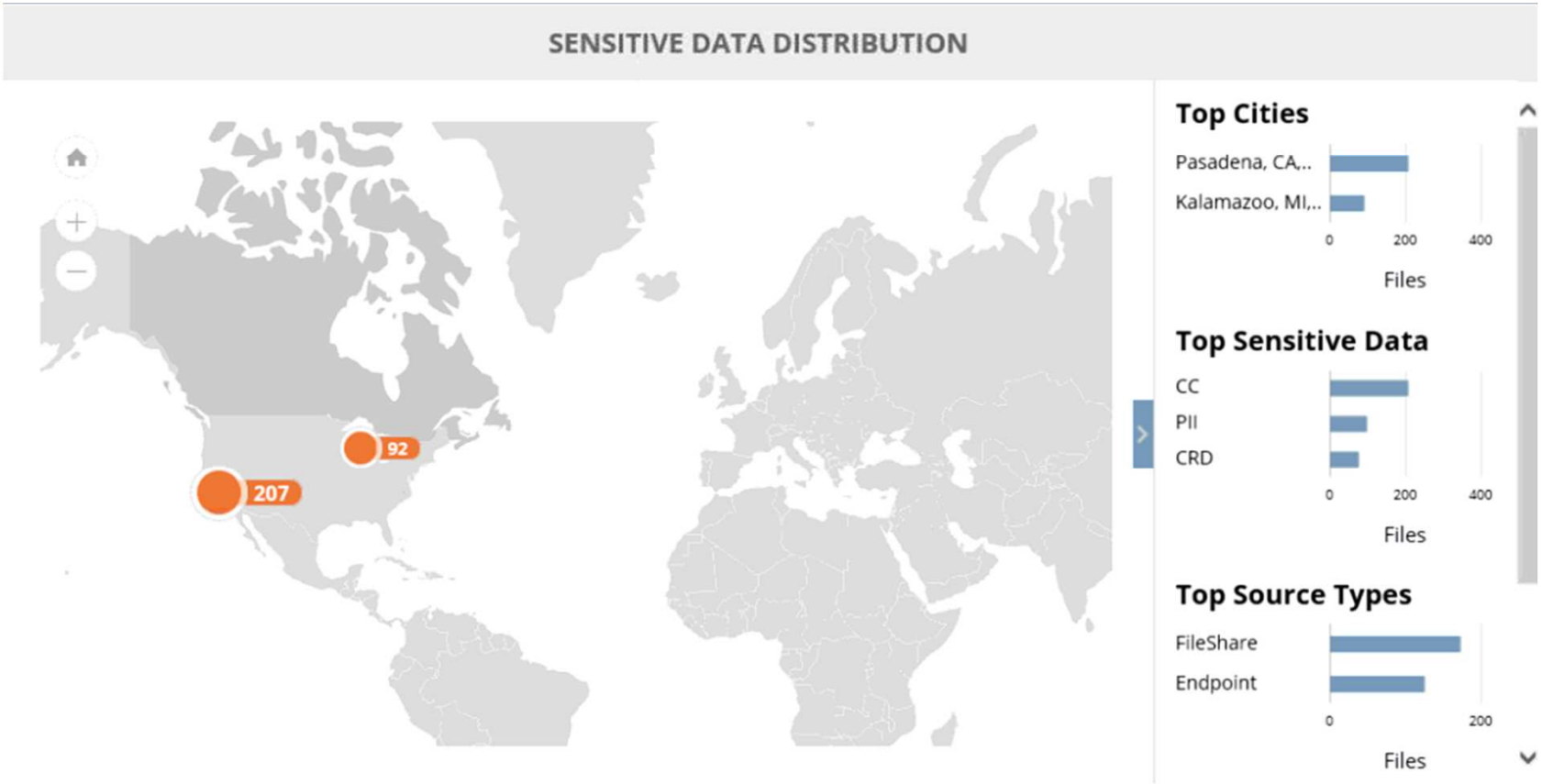
Nel vostro team di gestione crisi avete inserito anche esperti in incident response?

DEFENSIS

GRANDI AZIENDE

«misure tecniche e organizzative adeguate»

DEFENSIS


SENSITIVE DATA DISTRIBUTION
92
207
Top Cities
Pasadena, CA,..
Kalamazoo, MI,..
0
200
400
Files
Top Sensitive Data
CC
PII
CRD
0
200
400
Files
Top Source Types
FileShare
Endpoint
0
200
Files

DEFENSIS


Process '@WanaDecryptor@.exe'
vmtoolsd.exe
sidebar.exe
Skype.exe
explorer.exe
diskpart.exe
@WanaDecryptor@.exe
firefox.exe
iTunesHelper.exe
jusched.exe
SUMMARY
DLLs
CONNECTIONS
NAME @WanaDecryptor@.exe
PID 3276
PATH C:\Users\jackie.robins\AppDat...
HASH 7BF2B57F2A205768755C07F2...
THREAT SCORE 100
PARAMETERS @WanaDecryptor@.exe
HIDDEN No
CHILD PROCESSES 0
DLLS 5
CONNECTIONS 0
CLOSE

DEFENSIS

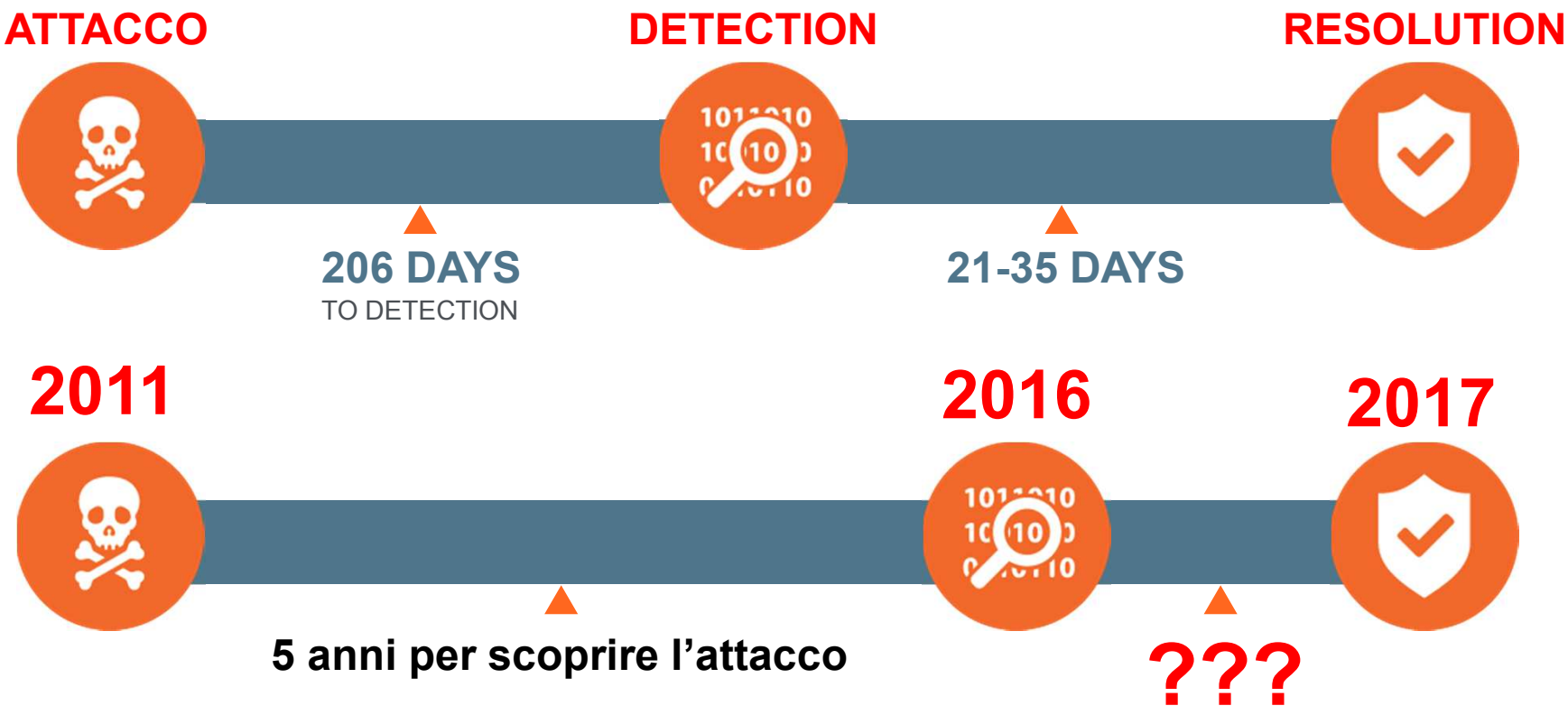
DATA RETENTION

LOG / CONTROLLI PREVISTI IN POLICY

DEFENSIS

18.327 Attaccati
1.793 Compromessi

DEFENSIS


ATTACCO
DETECTION
RESOLUTION
206 DAYS
TO DETECTION
21-35 DAYS
2011
2016
2017
5 anni per scoprire l'attacco
???

DEFENSIS

ALMENO

206

GIORNI

DEFENSIS

Potenziale statico di reazione

Distribuito e capillare

Costo Sostenibile (trascurabile)

GRAZIE

DEFENSIS

MICHELE COGO

MICHELE.COGO@DEFENSIS.IT