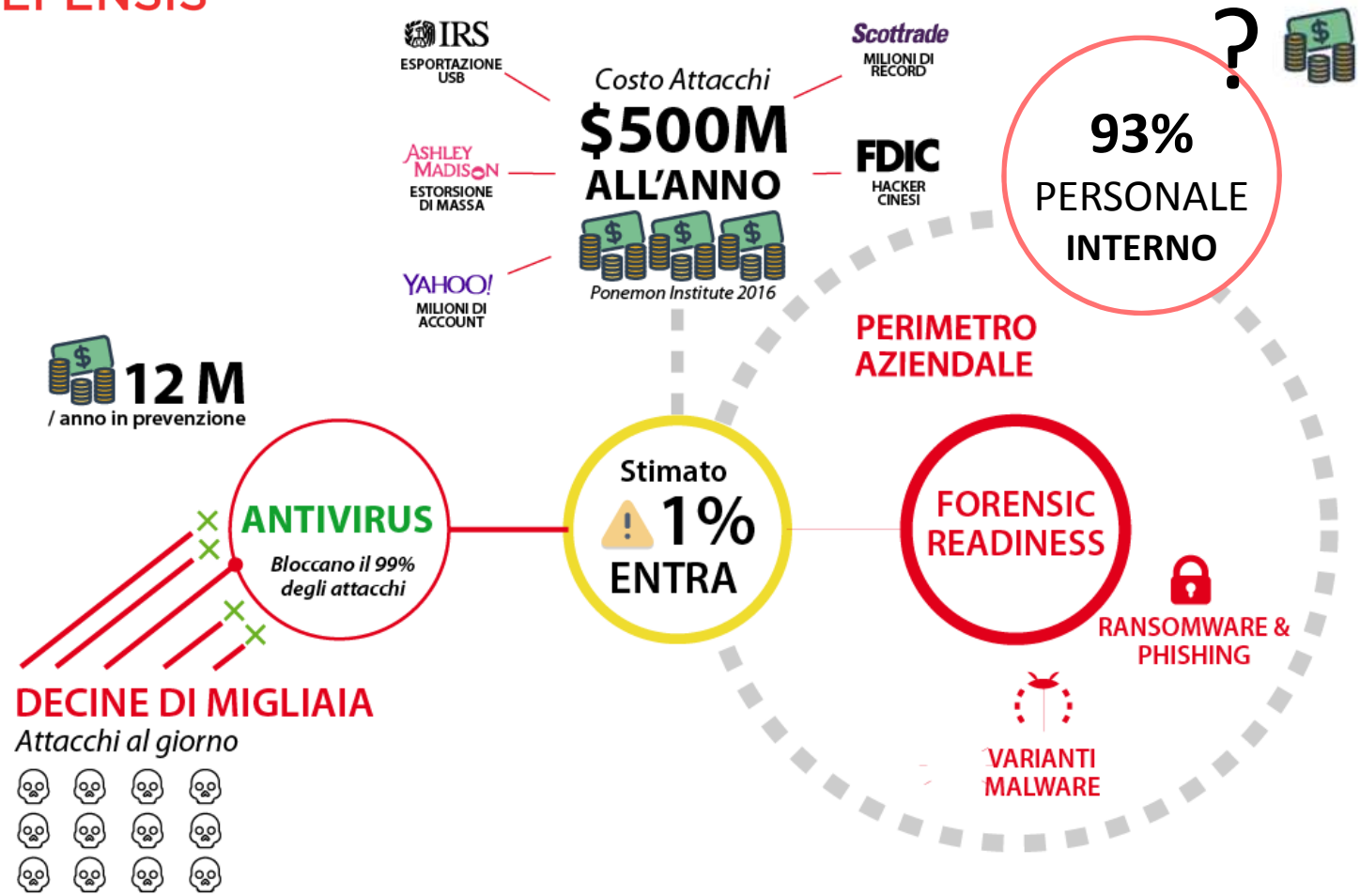
DEFENSIS

MILANO, 19 SETTEMBRE 2018

TECNOLOGIA E CONTENZIOSO

DEFENSIS


IRS
ESPORTAZIONE USB
ASHLEY MADISON
ESTORSIONE DI MASSA
YAHOO!
MILIONI DI ACCOUNT
Costo Attacchi
$500M
ALL'ANNO
Ponemon Institute 2016
Scottrade
MILIONI DI RECORD
FDIC
HACKER CINESI
?
93%
PERSONALE
INTERNO
PERIMETRO AZIENDALE
12 M
/ anno in prevenzione
ANTIVIRUS
Bloccano il 99% degli attacchi
Stimato
1%
ENTRA
FORENSIC READINESS
RANSOMWARE & PHISHING
VARIANTI MALWARE
DECINE DI MIGLIAIA
Attacchi al giorno

DEFENSIS

80 su 100 dei maggiori studi legali sono stati «hackerati» dal 2011.

Con «Panama Papers» **40 anni di informazioni sui clienti** sono state **diffuse in un singolo attacco**.

Le origini del GAP attuale

- abituati alla compliance
- Trascurata la specificità di ogni azienda.
- Si inizia solo ora a porsi il problema della cybersecurity nel design e sviluppo dei prodotti.

30% “altri IT”

DEFENSIS

Perché aumenteranno i budget in formazione/prevenzione nei prossimi 5 anni?

- *Gli attacchi cyber aumenteranno di 4 volte entro il 2020*
- *Alcuni dati, ad esempio quelli medici, restano validi per anni*
- *Perchè la normativa **abbandona le prescrizioni** minime (GDPR,NIST, AGID…)*
- ***Capacità degli hacker (interni o esterni) di mirare e aspettare***

DEFENSIS

ATTACCO HACKER, INCIDENTE, CRISI,
CONCORRENZA SLEALE, FURTO, DATA LEAK…

CONTENZIOSO

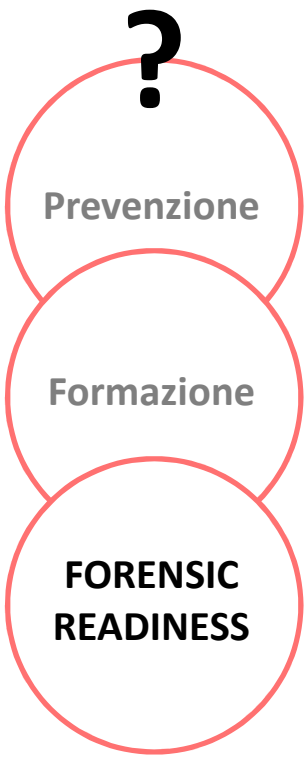
INDAGINE PENALE MANDATO INVESTIGATIVO INTERVENTO TECNICO

Ma abbiamo informazioni sufficienti?

SPESSO NO

Perché le informazioni digitali **cancellate** possono essere irrecuperabili
Perché il dispositivo su cui è transitato il dato **non c'è più**
Perché **non era previsto** che venisse raccolto quel tipo di dato

DEFENSIS



FORENSIC READINESS

*La **capacità** di far fronte a contenziosi, **gestendo** l'incidente, **ripristinando** le attività e **RACCOGLIENDO** DATI CHE ABBIANO **VALORE PROBATORIO**.*

Sia per contenziosi da voi promossi,
Sia per quelli che potreste subire.

DEFENSIS

CENSIMENTO DATI

Da 6 a 1.000 sistemi, un 30% dei dati potrebbero essere gestiti da “altri IT”

ANALISI RISCHI

Rischi IT, ma anche da frodi interne, gestione fornitori terzi, supply chain lunghissime.

IMPLEMENTAZIONE MISURE

Prendendo in considerazione I sistemi rilevati e gli attori che intervengono

- POLICY
- RED TEAM

REVISIONE ANNUALE

Ti vigili da solo... Attivitá da proceduralizzare.

DEFENSIS

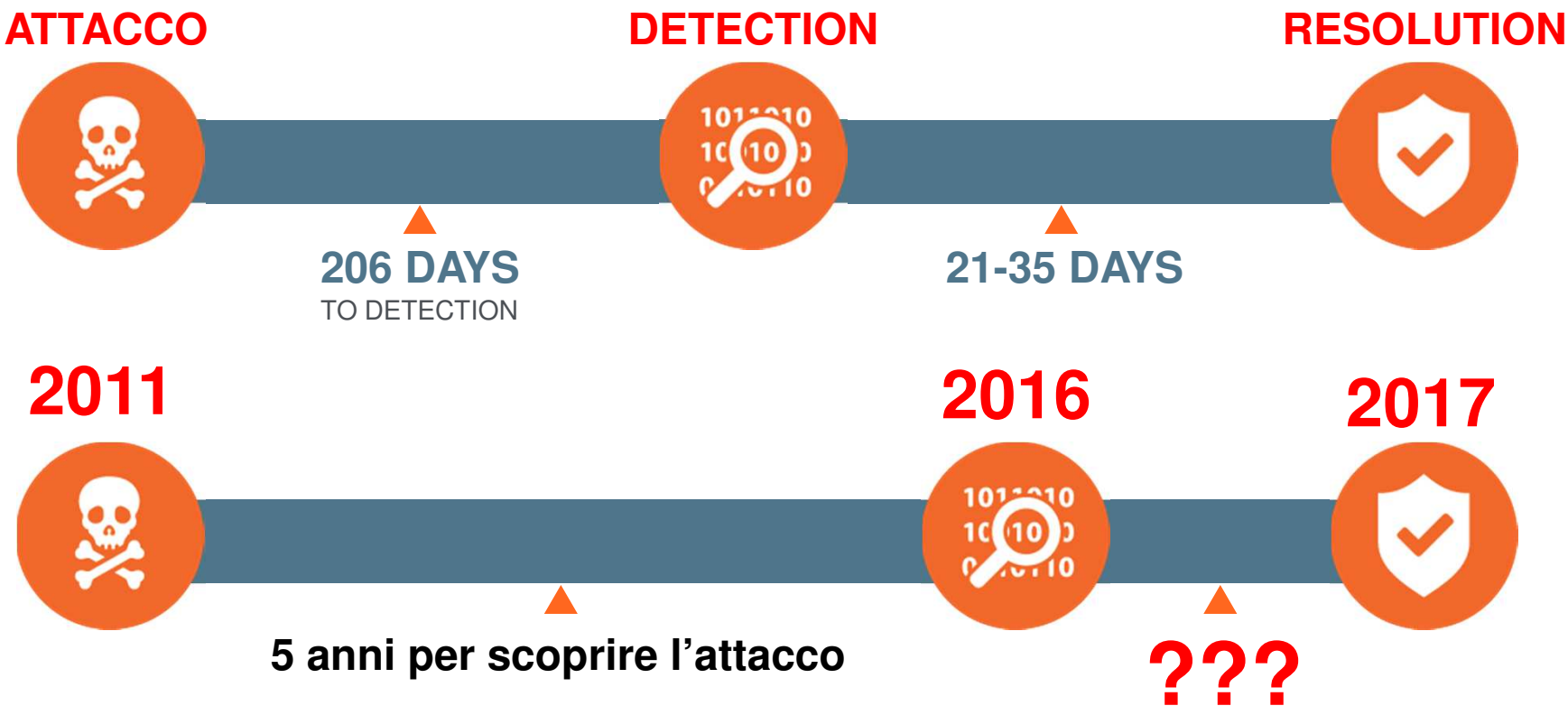
14.3 Nella gestione dei sistemi informatici aziendali, e degli strumenti di lavoro, il servizio ICT, o terzi incaricati dalla direzione, potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali: i log generati da Microsoft Windows/Android/iOS, gli accessi alla rete e ai dispositivi aziendali, la cancellazione, creazione o esportazione/trasferimento di file e informazioni, l'uso di file/software di carattere non lavorativo. I dati verranno conservati per **206 giorni** e quindi cancellati. Tali informazioni potranno essere utilizzate in caso di attacco informatico, incidente informatico e ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

DEFENSIS

DATA RETENTION

LOG / CONTROLLI PREVISTI IN POLICY

DEFENSIS


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

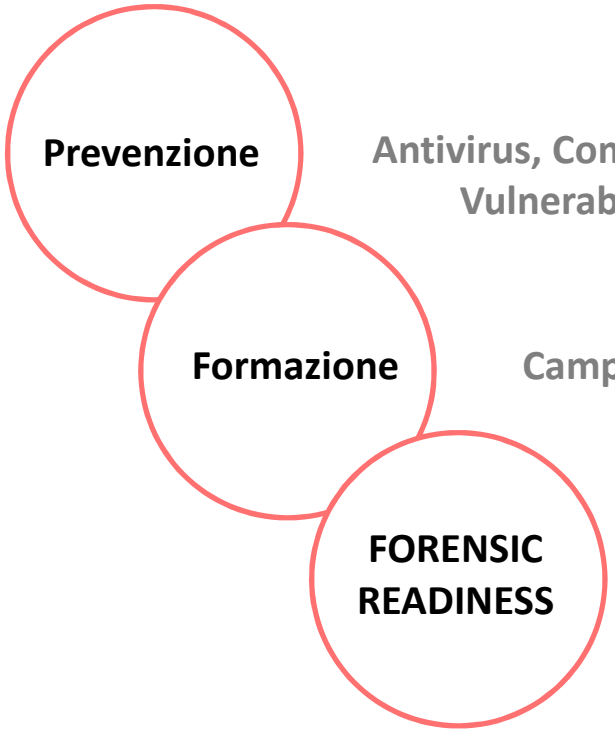
DEFENSIS

ALMENO

206

GIORNI

DEFENSIS



Antivirus, Compliance, Certificazioni, Vulnerability Assessment…

Campagne phishing, Cyber Awareness, Spiegare le policy

Analisi rischi, Raccolta LOG, **RED TEAM**

DEFENSIS

LA FRONTIERA

RED TEAM

VERIFICARE LA REALE CAPACITA' DELL'AZIENDA DI RICONOSCERE E REAGIRE AD UN ATTACCO/FRODE.

Negli Stati Uniti l'impiego è significativo dal 2003.
Si può considerare come un metodo di analisi della Corporate Security Posture alternativo.

DEFENSIS

OSINT
Ricerca di informazioni relativamente all'azienda che possono essere utilizzate per la preparazione di un attacco o che rappresentino esse stesse un rischio per il business.

INFRASTRUCTURE ATTACK
Violare la sicurezza aziendale sfruttando vulnerabilità riconducibili all'infrastruttura o, come sempre più spesso accade, presenti nelle applicazioni web.

PROCESS EVALUATION
Validare con dati oggettivi anche l'adeguatezza dei processi aziendali dal punto di vista IT, evidenziando le criticità che hanno un impatto sulla sicurezza.

HUMAN ATTACK
Il fattore umano è la prima vulnerabilità da sfruttare. Vengono svolte attività di Social Engineering, campagne di Phishing, Impersonification, Baiting.

PHYSICAL ASSESS
Verifica l'efficacia dei controlli che l'azienda ha messo in campo circa l'accesso ad aree o locali riservati, nel tentativo di esfiltrare dati.

WHITEBOARD ATTACK
«gioco di ruolo» in cui gli attaccanti (NOI) e difensori (Cliente), seduti attorno ad un tavolo, si sfidano per raggiungere i rispettivi obiettivi.

GRAZIE

DEFENSIS

MICHELE COGO

MICHELE.COGO@DEFENSIS.IT

DEFENSIS

www.defensis.it/risorse-eventi/account_check.html

DEFENSIS

Dec. 29 —medical records of 29,000 patients inappropriately accessed by an employee in its customer service call center.
Dec. 13 —$2.3 million fine data breach in 2015 that affected more than 2.2 million patient records. **Assicurazioni?**
Dec. 8 —24,000 patients their personal information is at risk after a computer was stolen **sicurezza fisica**
Dec. 7 —personal information of 11,350 people is at risk after the email of two employees were compromised in a phishing attack **formazione**
Dec. 6 —notifying 18,478 patients their personal health information was accessed or stolen when the email accounts of employees were compromised. **notifica**
Dec. 5 —warned some 3,300 patients their healthcare information is at risk after an unauthorized third party launched a ransomware attack on the clinic's systems. **Audit (davvero) dei fornitori**
Nov. 24 —notified some 6,000 people their personal identifying information is at risk after the agency accidentally sent a spreadsheet containing the data to a vendor. **nel vostro CRM?**
Nov. 22 —a $2 million settlement in a case involving allegations that the provider failed to implement **basic, reasonable safeguards** to protect patient medical information in violation of state and federal privacy laws. (medical information of more than 50,000 patients was exposed online) **ma dove erano?**
Oct 23 — A hacker group stole an undisclosed amount of data. The clinic is known for its celebrity clients, including some members of Britain's royal family. **Segmentare I dati di certi pazienti?**
Oct. 19 —employees allege they were harmed by a data breach that exposed their tax information to online thieves. **I dati dei dipendenti!**
Oct. 10 —An Amazon S3 repository belonging to XXX exposed to the public internet blood test results of an estimated 150,000 people. **Mappare dove vanno I dati che raccogliete**

DEFENSIS

Aug. 30 —notified more than 106,000 patients that their personal health information is at risk due to a data breach at third-party service **fornitori di servizi, gestire la notifica**
Aug. 28 —breaching the privacy rights of 12,000 customers in 23 states by allowing the words “filling prescriptions for XXX” to be seen in window envelopes sent to the clients. **Comunicazioni cartacee… e le email?**
Aug. 17 — San Antonio Institute for Women’s Health warned patients their personal information is at risk after it discovered a keylogger residing on its systems from June 5 to July 6. **IT Hardening**
July 18 —one of its servers and a workstation were subjected to a ransomware attack affecting 300,000 people. The group was able to continue normal operations by restoring affected data from backups. **Backup**
July 13 —personal identifying information for 547,000 customers was compromised when an employee copied and removed the data from the company’s systems. **monitoring**
July 12 —warned 5,300 patients some of their healthcare information is at risk after it was posted for two years to an unsecure application developer’s website. **Web application WA**
July 6 —notified some 15,000 patients their personal information is at risk after an employee was duped by a phishing scam. **attacchi simulati?**
July 5 —a ransomware attack affecting 500,000 people. It said there is no indication that any protected health information was accessed or acquired during the attack. **Incertezza… forensic readiness**
July 3 —patient details of any XXXalian is being sold on the Dark Net for $30 per individual. Vulnerability in the government’s systems.
June 23 —notified 500,000 people their personal health information is at risk due to unauthorized access to its infrastructure in April. **Accesso ai server?**

DEFENSIS

June 23 — more than 600 patients is at risk after xxx, a third-party vendor, accidentally sent their data to the wrong medical facilities between Feb. 13 and March 13. **anonimizzare i dati trasferiti?**
June 15 —agreed to pay $130,000 in penalties for waiting over a year to notify affected persons of a data breach that exposed 221,178 patient records. **Risposta veloce**
June 9 — notified 5,220 people their personal health information is at risk due to the insecure transfer of the data from an online form to a designated staff member. **Trasferimenti interni**
June 5 —2,000 patients was leaked online after a data breach of its systems. **Dati online**
June 1 —personal information of as many as 15,000 patients, including some celebrities, was stolen by a disgruntled employee who has posted some of the information on Snapchat, Instagram and Facebook. **Human factor**
May 26 —shut down its online patient portal after a vulnerability was discovered that exposed health records of 4.8 million customers to the public internet. **Security by design… fin dalla progettazione delle app**
May 23 —$387,200 to settle potential violations of the Health Insurance Portability and Accountability Act. **compliance**
May 16 — 3,500 patients at risk after it a volunteer enter the department without clearance to do so. **Controllo accessi**
May 5 —thousands of citizens is at risk due to a printing mistake on healthcare renewal forms mailed to residents of the province. **automazione**
April 26 — one in eight consumers have had their personal medical information stolen from technology systems.**IOT, cancellazione dati sicura?**
April 24 —agreed to pay $2.5 million to settle case arising from the theft of a laptop containing unencrypted patient data. **encryption**

DEFENSIS

April 24 —alerted an undisclosed number of people who participated a health fair from 2008 and 2012 that their demographic data is at risk due to the theft of an unencrypted flash drive. **USB**
April 22 — notified some 20,000 patients their health information is at risk after a laptop containing it was stolen from an employee's car. **Laptop+car**
April 20 — agreed to pay for storing protected health information with a third-party service provider without a Business Associate Agreement. **consenso**
March 3 —a database containing appointment information for about 80,000 patients was deleted by an intruder who demanded a ransom to restore it. **Gestione appuntamenti**
Feb. 17 — $5.5 million to settle case involving the theft of patient information by two employees **white collar crime**
Jan. 6 — California Department of Insurance found a data breach that compromised 78.8 million consumer records at health insurer Anthem was performed on behalf of a foreign government. **Infrastrutture critiche o know how**