BLUE TEAMING

& SISTEMI DI DIFESA

Simone Ravizza

Le generazioni degli attacchi

Fine anni ‘80

Attacchi Virus a PC autonomi

Inizi anni 2000

Sfruttamento vulnerabilità delle applicazioni

Intorno al 2017

Attacchi mega su larga scala e multivettoriali, utilizzando strumenti di attacco avanzati

Metà anni ‘90

Attacchi provenienti da internet

Intorno al 2010

Attacchi mirati, sconosciuti, evasive, polimorfici

Anni
‘80

GENERAZIONE 1

Hacker del seminterrato dei genitori

Personal computer utilizzati come dispositivi autonomi.
I floppy disk portatili erano utilizzati per condividere file tra utenti e PC, e metodo di proliferazione

TECNOLOGIE DI DIFESA
ANTIVIRUS

Esempio attacco Famoso

ELK CLONER

Considered the world's first computer Virus

Anni ‘90

GENERAZIONE 2

Buontemponi curiosi ed inizio Criminalità/furti

Avvento della connessione internet e diffusione dei Worm su larga scala

TECNOLOGIE DI DIFESA

FIREWALL

Esempio attacco Famoso

MORRIS WORM

1st Biggest DoS attack

Anni 2000

GENERAZIONE 3

Exploit vulnerability – Interesse a fare soldi!

Inizio dello sfruttamento delle vulnerabilità presenti in Applicazioni e Sistemi Operativi.
Un aggressore esperto poteva sfruttarle per accedere alla rete privata.
Meno interesse a notorietà, più interesse fare soldi!

TECNOLOGIE DI DIFESA

IPS

Esempio attacco Famoso

ILOVEYOU

Worm che colpì in pochi minuti decina di miglialia di macchine Windows; via mail

Anni 2010

GENERAZIONE 4

Shapeshifting – Unknown Unknows

Nuovo Attacchi di cui non si hanno signature. Miglioramento significativo della Qualità del codice dei malware e nascita dei primi Rootkit. Attacchi polimorfici che cambiano forma per evadere dal rilevamento AV.

TECNOLOGIE DI DIFESA

ANTI-BOT, SANDBOX

Esempio attacco Famoso

STUXNET

2005-10; Target SCADA System in Critical Infrastructure, including Iranian Nuclear program

Anni >2017

GENERAZIONE 5

…Gli incidenti che una volta sarebbero stati considerati straordinari stanno diventando sempre più comuni…

Attacchi multi-vettoriali, si infiltrano e proliferano silenziosamente da qualsiasi vettore: rete, cloud, branch office, endpoints, mobile, terze parti…
Mega-attacchi rapidi su scala globale, altamente sofisticati, furtivi e di successo.
Gli attaccanti, anche meno esperti e non sponsorizzati da nazioni/stati, tramite il Darkweb ora hanno accesso alla stessa potenza infrastruttura che permette attacchi su larga scala, e su più target.

TECNOLOGIE DI DIFESA

Unified, Integrated security architecture, Threat intelligence can be shared in realtime to enable fast, real-time, inline protection the first attack takes place.

Esempio attacco Famoso

WannaCry

2017; a Major Ransomware attack affecting 200.000 computers across 150 countries.

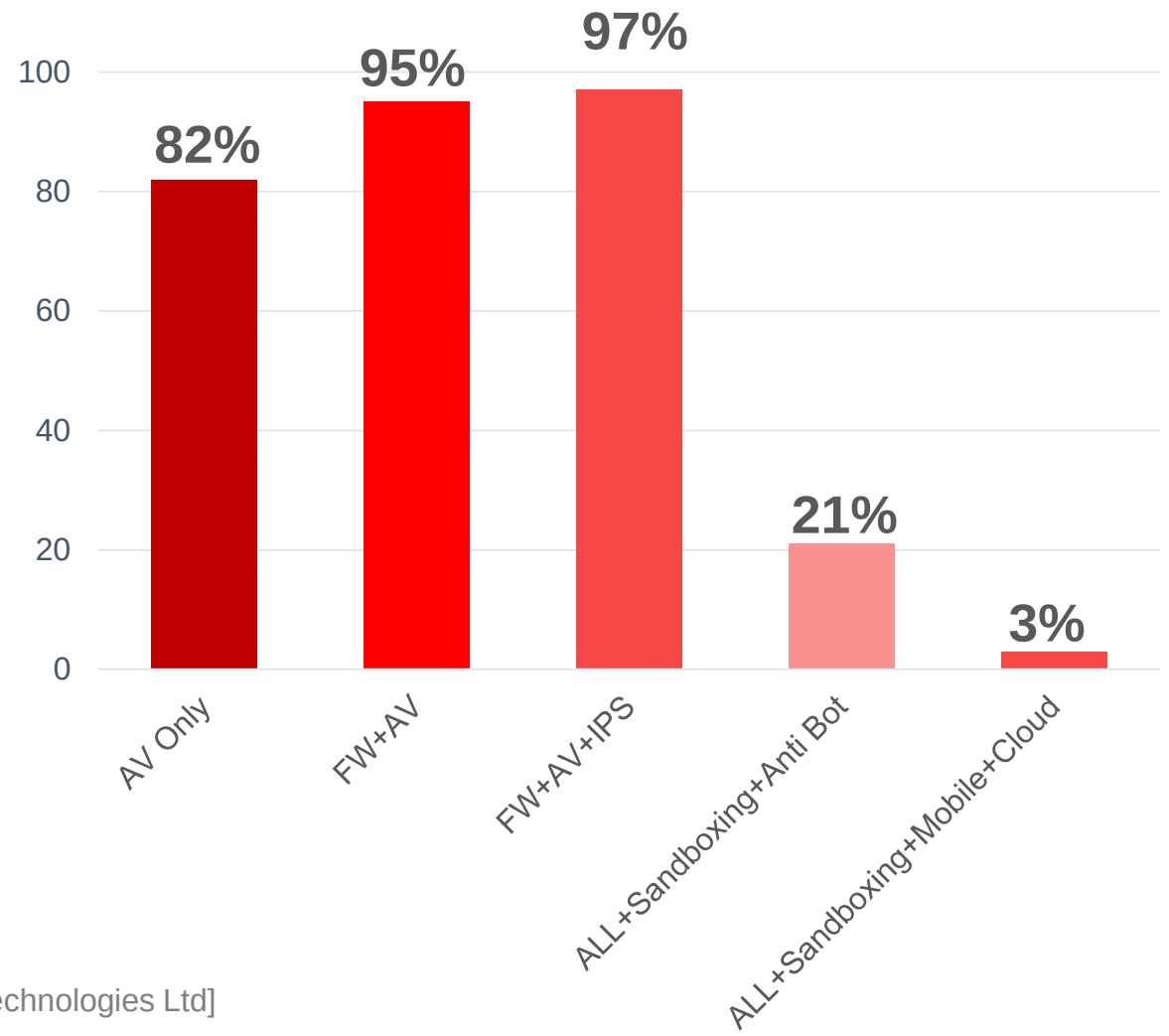
Anno 2018

CYBER SECURITY GENERATIONS ANALYSIS

Aziende Internazionali

Intervistate

443



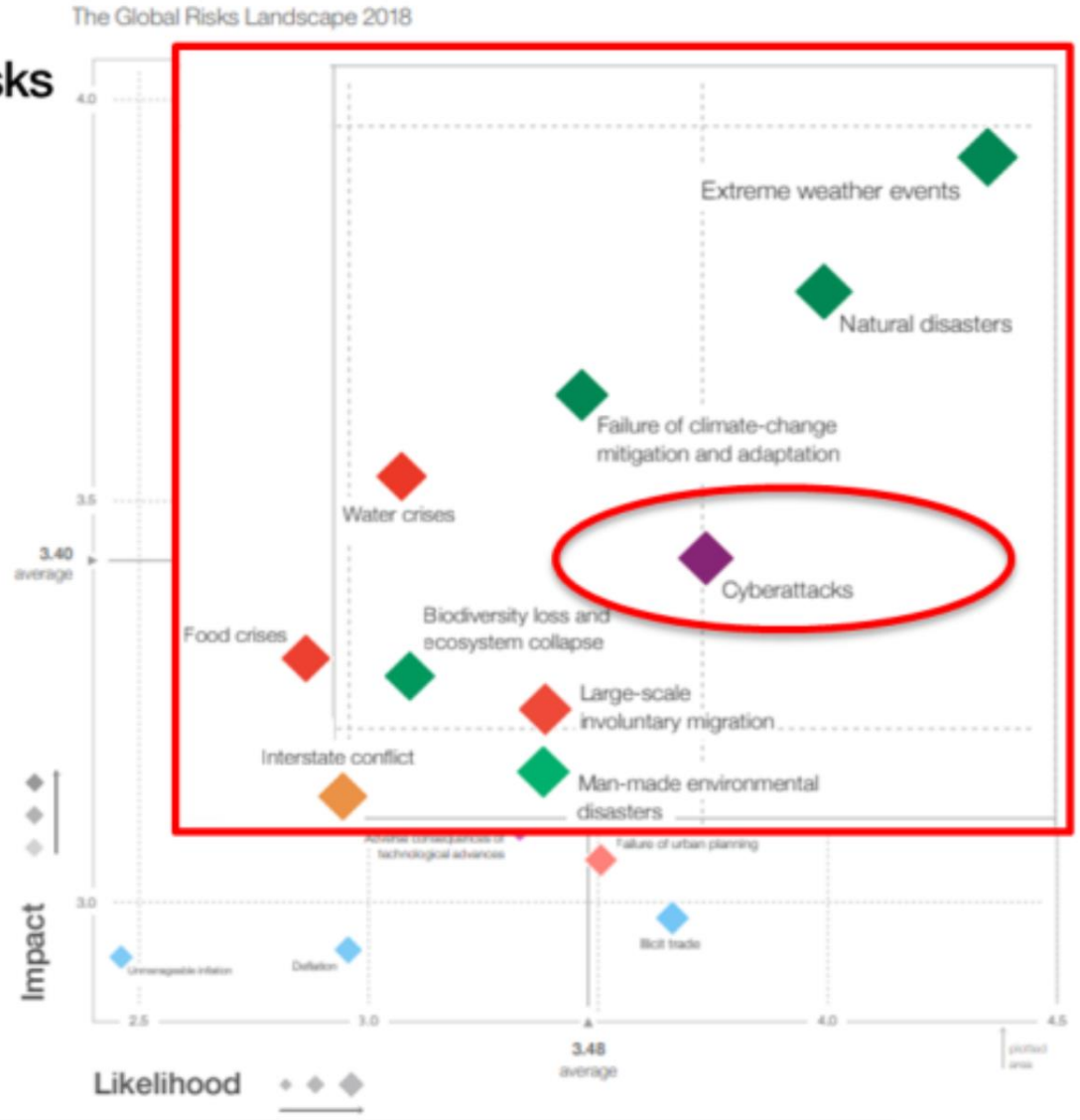
[Analisi elaborata da Check Point Software Technologies Ltd]

Anno 2018

Report Annuale sui Rischi Globali - World Economic Forum

Eventi metereologici estremi, calamità naturali, guerre, crisi del cibo, crisi dell’acqua.

> Rischio Cyber è tra i più probabili ed impattatanti




Extreme weather events
Natural disasters
Failure of climate-change mitigation and adaptation
Water crises
Cyberattacks
Biodiversity loss and ecosystem collapse
Food crises
Large-scale involuntary migration
Interstate conflict
Man-made environmental disasters
Critical information
Profound social instability
Failure of national governance
Fiscal crises
Terrorist attacks

BLUE TEAM

Analysis of information systems to ensure security

Identify security flaws

Verify the effectiveness of each security measure

Make certain all security measures will continue to be effective after implementation.

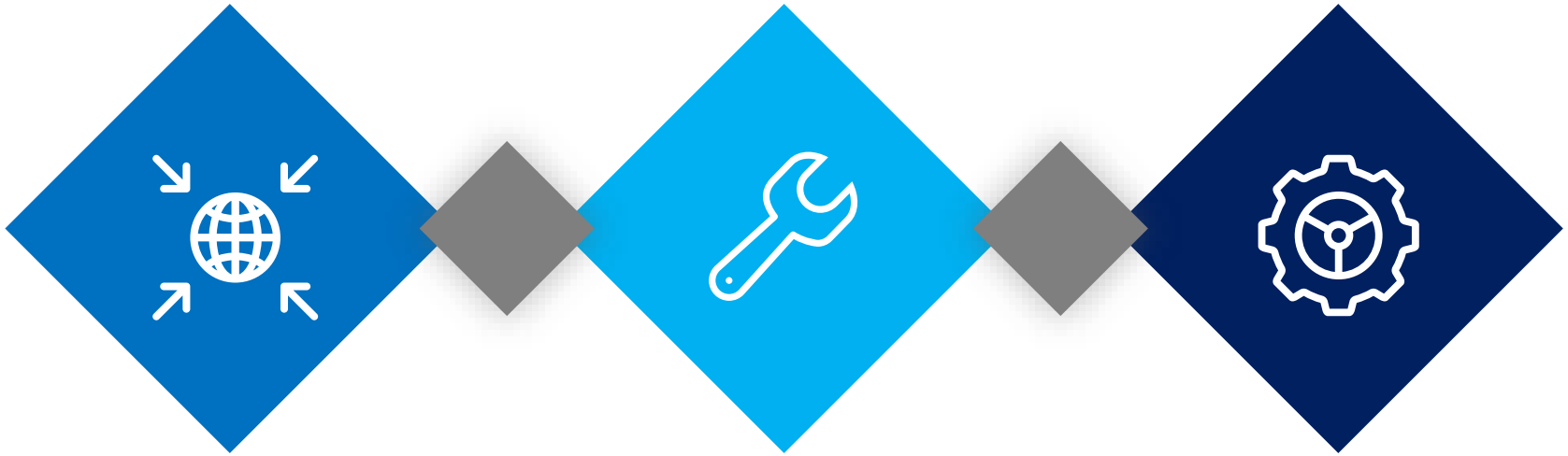
BLUE TEAM

RED TEAM VS BLUE TEAM

- OFFENSIVE - Find and exploit weaknesses in the organization's security

- Design defensive measures against such red team activities, and responding to successful breaches.

SISTEMI DI DIFESA

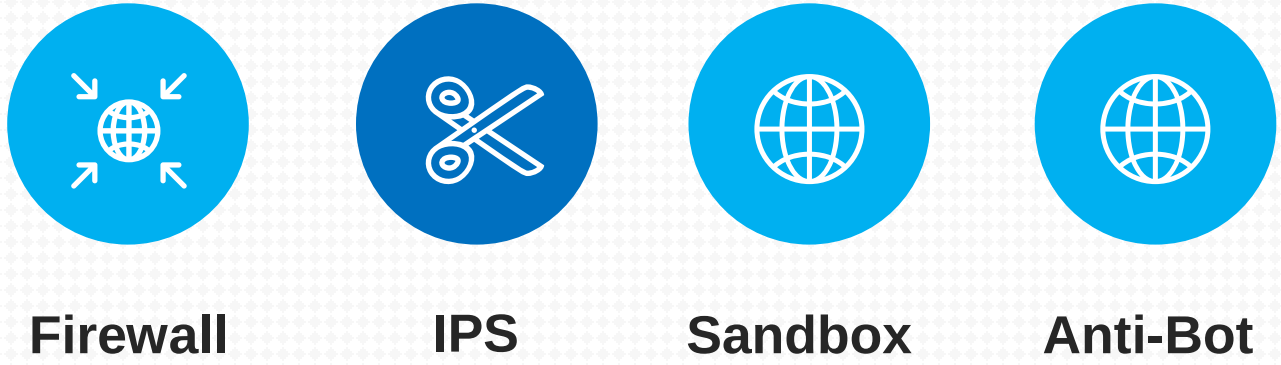


PROTEZIONE PERIMETRALE

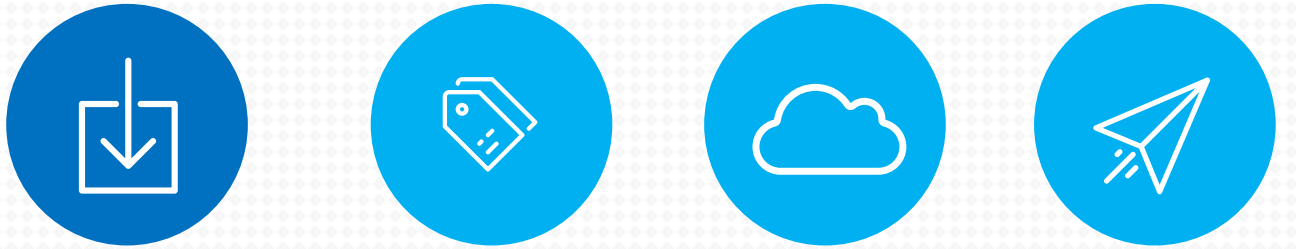
PROTEZIONE SERVER/ENDPOINT

PROCESSI DI SECURITY

PROTEZIONE PERIMETRALE

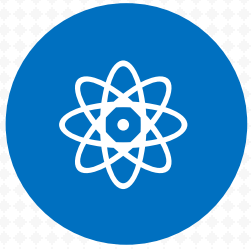


Firewall IPS Sandbox Anti-Bot

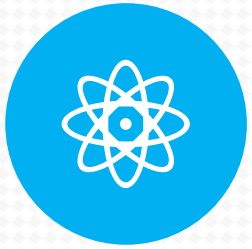


Anti-DDoS URL/Content Filtering CASB Anti-Spam

PROTEZIONE SERVER/ENDPOINT



Patch management OS



Patch management APP

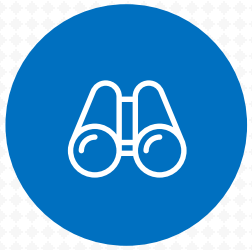
Malware Protection

Device Control

Password Policy

Device Encryption

PROCESSI DI SECURITY



Monitoraggio proattivo NOC-SOC

Vulnerabilty assessment con Remediation

Compliance GDPR

Il Fattore Umano

Aziende Internazionali Intervistate

1300

Manager **87%**

“Il personale inesperto rappresenti il rischio maggiore per i crimini informatici.”

Valutazione continua del rischio cyber che consideri le persone, i processi e la tecnologia.

[analisi elaborata da Esi ThoughtLab in collaborazione con Willis Towers Watson e altre aziende specializzate in sicurezza e gestione rischio]

“We are in a cybersecurity arms race, and the hackers are winning. Over the years, we have tested thousands of companies. There is always a way in.“

Kevin Mitnick

THANK YOU!

Simone Ravizza