E SE FOSSE UN ATTACCO MIRATO CONTRO LA TUA ORGANIZZAZIONE?

Security Summit - Roma, 5 giugno 2019

F-Secure

AGENDA

Targeted Attack

Tecniche

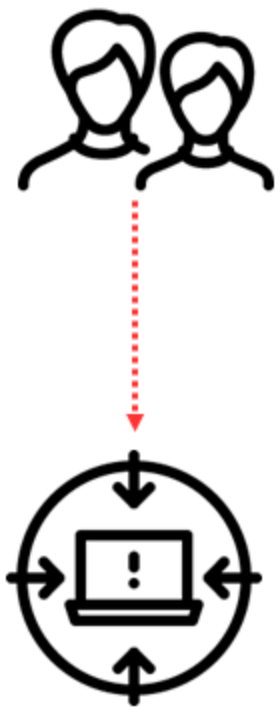
MDR

GIORGIO DI GRAZIA

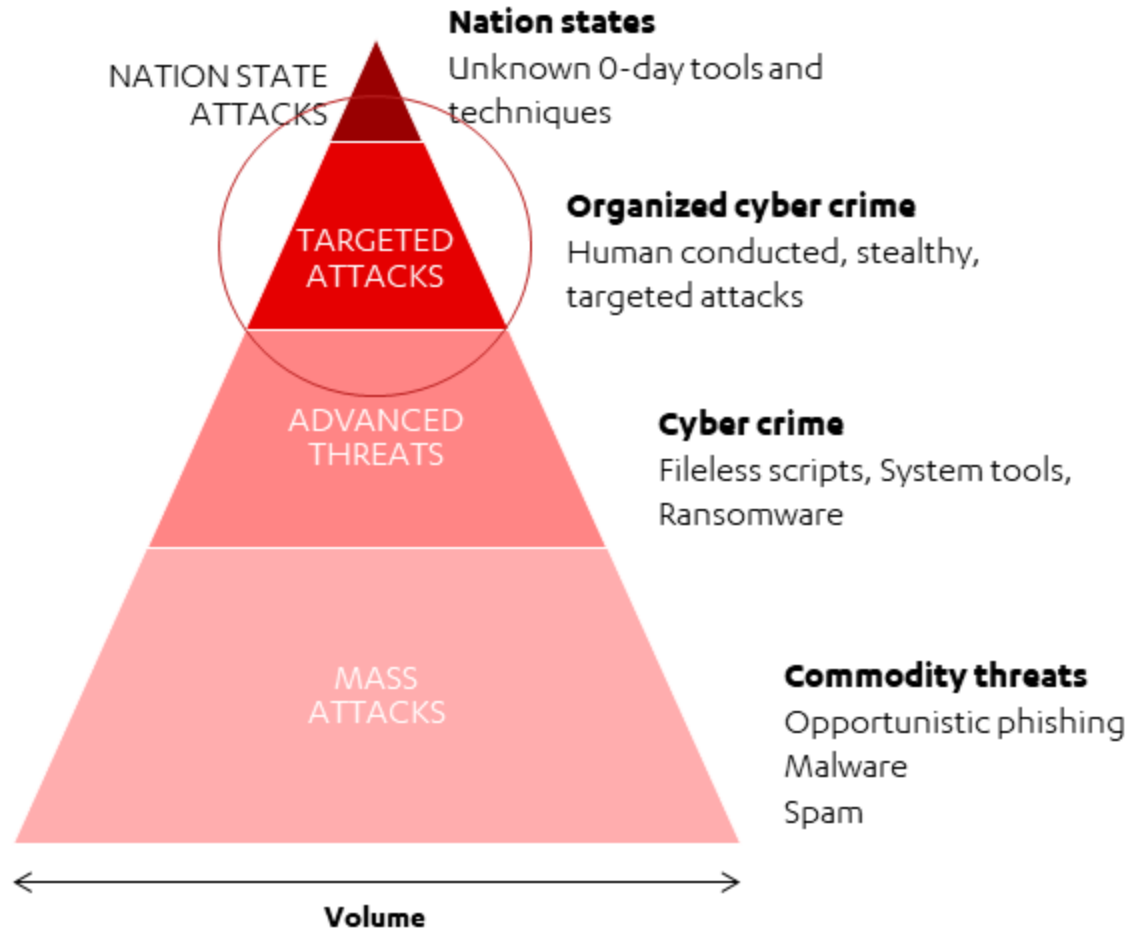
Solution Sales Engineer @ **F-Secure** (**MDR**)

TARGETED ATTACK

TARGETED ATTACK

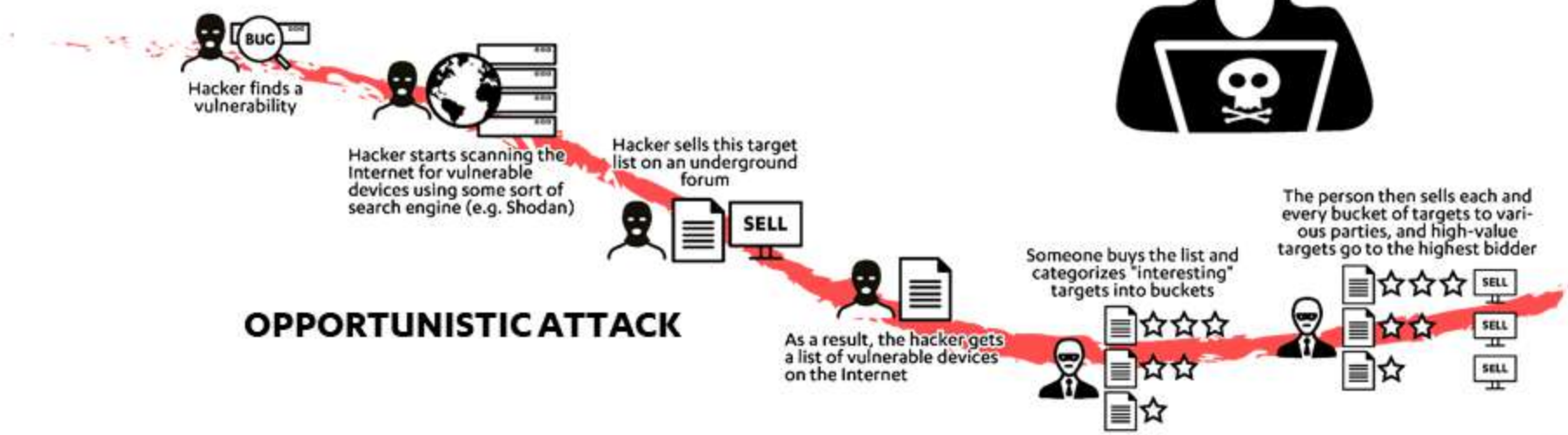


Un targeted attack è un attacco **organizzato**, con un buon livello di pianificazione, rivolto a un **obiettivo** ben definito (industria, gruppo politico), in prevalenza non automatizzato (hacking team con **capacità tecniche** evidenziabili dagli indicatori di compromissione/attacco, elasticità nell'uso degli strumenti), **silenzioso**.



TARGETED E OPPORTUNISTIC ATTACK

- **Tempistica**: tempi medio-lunghi. Lo scenario d'attacco può delinearsi con tentativi ripetuti nel tempo
- **Scopo**: profitto, furto di proprietà intellettuale, vantaggi politici ecc.
- Non è un **opportunistic attack**: non parte da una vulnerabilità per identificare un obiettivo; è vero il **contrario**



F-Secure

APT, TARGETED ATTACK, HACKTIVIST & C.

ADVANCED PERSISTENT THREAT (APT)

- Gruppi sostenuti da una nazione (**nation state actors**)
- Impiego di codice sofisticato (disponibilità finanziaria elevate), **zero-day** / **n-day**
- **Cyber espionage** (furto di segreti industriali, scientifici e tecnologici); assenza di motivazioni finanziarie immediate (furto di carte di credito, denaro)
- **PERSISTENT** significa estrema determinazione (si tratta di una **MISSIONE** che non può fallire)

TARGETED ATTACK

- **Organized Criminals**
- **Cybercriminals**
- Notevole diffusione, motivazioni economiche e politiche
- Prevalente impiego di **tool** open source (anche sofisticati), **n-day**, public **exploits**, **TTP** di nation state (per essere **persistent**)

ALTRI ATTACCHI

- **Script Kiddies**, **Hacktivists**, **Insiders**

RISCHI PER LE AZIENDE

Linea sottile: tecniche utilizzate (Tactics, Techniques, and Procedures o **TTP**) spesso comuni. **ENISA Threat Landscape** report (January 2019): *"The blurred lines between nation state actors and cyber criminals"*

ADVANCED PERSISTENT THREAT (APT)

- **RISCHI**: dipende dal settore merceologico, dalla qualità e dall'importanza dei segreti industriali

TARGETED ATTACK

- **RISCHI**: settori finanzari/retail, ma tutte le aziende sono potenziali obiettivi (attenzione alla valutazione dei rischi)

APT E IL CASO NSA

The Intercept_

INSIDE THE NSA'S SECRET EFFORTS TO HUNT AND HACK SYSTEM ADMINISTRATORS

RISK ASSESSMENT / SECURITY & HACKTIVISM

NSA hacker in residence dishes on how to "hunt" system admins

Latest Snowden docs offer lulz from NSA's internal hacker how-to board.

by Sean Gallagher - Mar 21 2014, 5:55pm EET

CYBERWAR HACKING NATIONAL SECURITY

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

BIZ & IT —

NSA hacker in "hunt" system

ZDNet CENTRAL EUROP

MUST READ: These are the 12 most

NSA targets sysa

Edward Snowden

@Snowden

Follow

Remember the "I Hunt Sysadmins" presentation by @NSAGov? Make it hard for them. Use @QubesOS.

F-Secure.

N-DAY E BLUEKEEP

Rob^beto Graham

@ErrataRob

After scanning, debugging the scanner, and rescanning, my official verdict is 950,000 machines vulnerable to BlueKeep (CVE-2019-0708) on the public Internet. blog.erratasec.com/2019/05/almost...

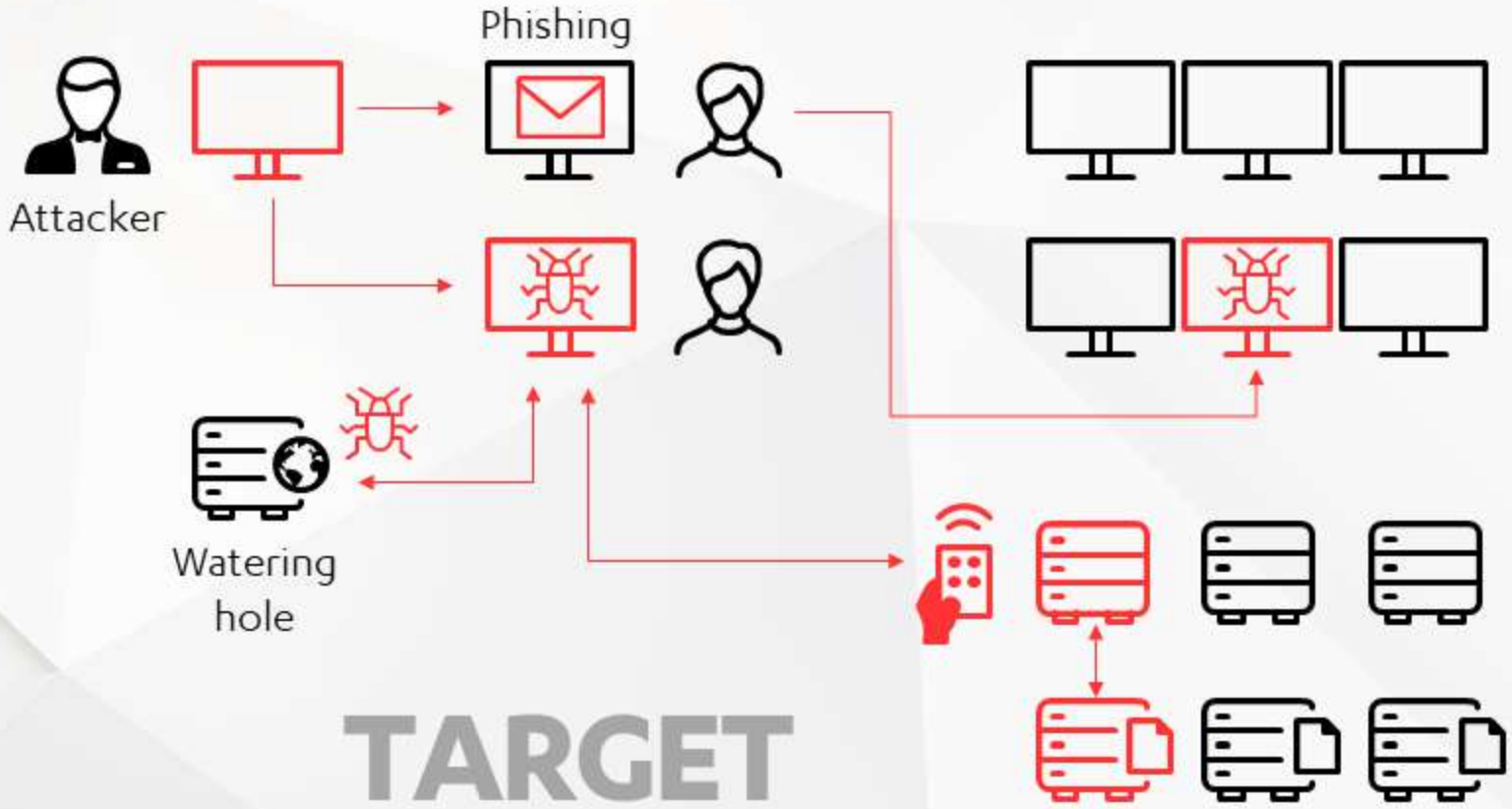
Traduci il Tweet

12:21 · 28 Mag 19 · Twitter Web Client

- Microsoft **CVE-2019-0708**: Remote Desktop Services Remote Code Execution Vulnerability, 14 maggio 2019
- Potenzialmente **wormable**, come **WannaCry**
- **Microsoft** ha rilasciato fix per Windows XP/2003 e Windows Vista (ancora tra noi)
- Robert Graham: scan con **masscan** e **rdpscan** (scanner per CVE-2019-0708)
- Risultato: **950.000** sistemi vulnerabili su Internet (28 maggio)

TARGETED ATTACK: LE FASI

- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- DATA COLLECTION
- DATA EXFILTRATION



F-Secure

TARGETED ATTACK: RECON

RECON

EXPLOITATION

COMMAND-AND-CONTROL (C2)

LATERAL MOVEMENT

DATA COLLECTION

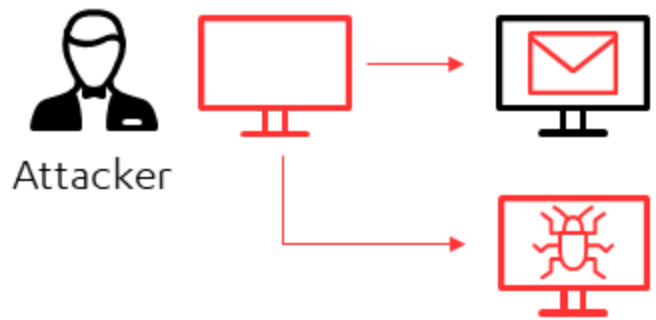
DATA EXFILTRATION

- **PRE-ATTACK**: perimetro aziendale esteso; fonti OSINT (es. Social, WWW, Search Engine quali Shodan, Censys), analisi della supply chain ecc.
- **Information gathering** (people, technology), analisi vulnerabilità, **persona development** (social engineering) ecc.

F-Secure

TARGETED ATTACK: EXPLOITATION

- RECON
- **EXPLOITATION**
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- DATA COLLECTION
- DATA EXFILTRATION



- L'uso di **0-day** (vulnerabilità ancora sconosciute) **non** è così frequente: sono costose da utilizzare, non sempre necessarie. Meglio i sistemi **non aggiornati**.
  - **Spear phishing** (link, attachment)
  - **Drive-by Compromise**
  - **Watering hole** (user community)
  - **Exploit Public-Facing Application**
  - **Removable Media**
  - **Supply Chain** Compromise
  - **Account validi** (password indovinabili, raccolte via OSINT)

F-Secure.

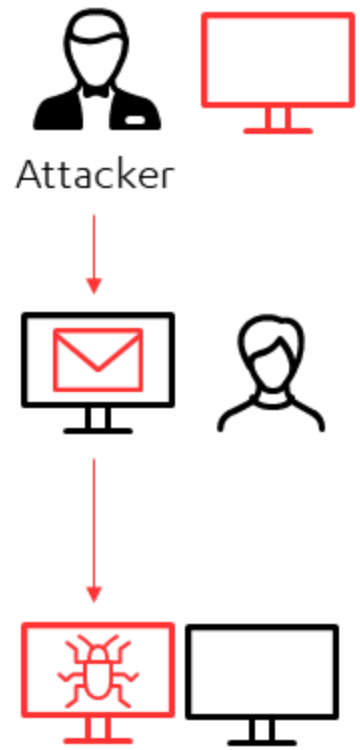
TARGETED ATTACK:
COMMAND-AND-CONTROL (C2)

- RECON
- EXPLOITATION
- **COMMAND-AND-CONTROL (C2)**
- LATERAL MOVEMENT
- DATA COLLECTION
- DATA EXFILTRATION

- **Post Exploitation**: l'attaccante è in azienda, **comunica** con i sistemi sotto controllo per proseguire l'attacco. Parola d'ordine: **basso profilo**.
  - **Porte** comunemente utilizzate (DNS, HTTP(S), SMTP, FTP)
  - **Malware** (Custom C2 Protocol)
  - **Canali legittimi** (Gmail)
  - **Remote Access Tools** (Team Viewer, Go2Assist, LogMein ecc.)
  - **Servizi Web** utilizzati per rimanere sotto copertura (social network, piattaforme cloud, Google Calendar, Twitter, Pastebin ecc.)

TARGETED ATTACK:
LATERAL MOVEMENT

- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- **LATERAL MOVEMENT**
- DATA COLLECTION
- DATA EXFILTRATION

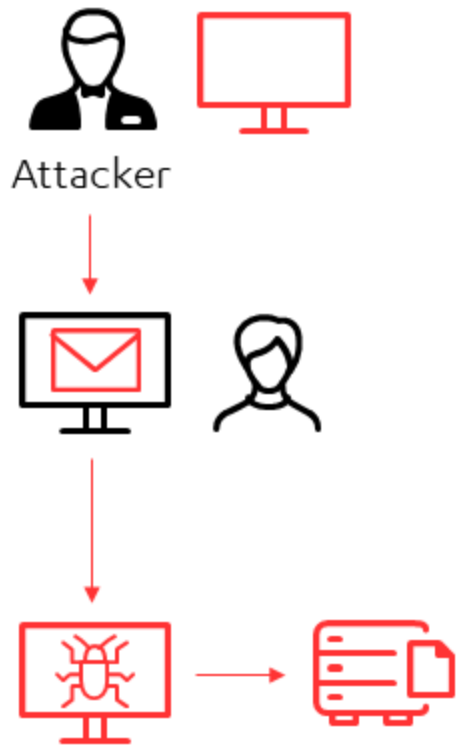


- L'attaccante tenta di spostarsi verso altri sistemi al fine di ottenere informazioni riservate.
  - **Servizi remoti**, **share di rete** (tramite account validi)
  - **Pass the hash** (PtH)
  - **Pass the ticket** (PtT)
  - **Software** di terze parti (VNC)
  - **Remote Desktop Protocol**
  - **Credential Dumping** (Mimikatz, WCE ecc.), tentativo di ottenere credenziali amministrative

F-Secure.

TARGETED ATTACK:
DATA COLLECTION

- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- **DATA COLLECTION**
- DATA EXFILTRATION

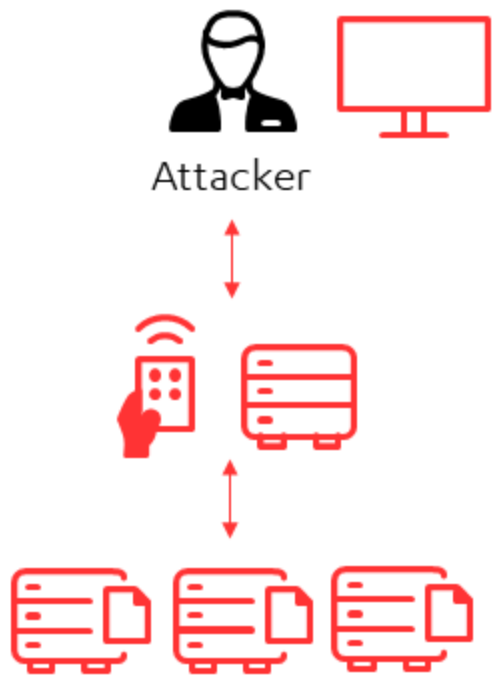


- Identificazione e raccolta dei **Critical-Value Data** (**CVD**) del target.
  - Accesso a **database/condivisioni**
  - **Script per la ricerca automatica** (file DOCX, PDF, XLSX ecc.)
  - **Screen Capture**
  - **Video Capture**
  - **Audio Capture**
  - **Email Collection** (Carbanak backdoor invia Outlook personal storage tables (PST) al proprio C2)

F-Secure.

TARGETED ATTACK:
DATA EXFILTRATION

- RECON
- EXPLOITATION
- COMMAND-AND-CONTROL (C2)
- LATERAL MOVEMENT
- DATA COLLECTION
- **DATA EXFILTRATION**



- Obiettivo **principale**. Copia dei **Critical-Value Data** (**CVD**) del target, invio alla rete dell'attaccante.
  - **Script** automatici
  - **Compressione dei dati** prima dell'invio al server C2 (7zip, RAR, ZIP)
  - **Protocolli alternativi** (FTP, WebDAV, DNS tunnel, SSH/SCP)
  - Impiego del **canale C2**
  - **Scheduled transfers**
  - **Media fisici** (USB per sistemi air-gapped)
  - **Network Medium** (Bluetooth: il toolkit Flame usava un modulo in grado di farlo, anno 2010)

F-Secure

TARGETED ATTACK:
ENISA THREAT LANDSCAPE

1. **EXPLOITATION**
2. **EXPLOIT KIT (EK)**
3. **COMMAND-AND-CONTROL (C2)**

Agenzia europea per la sicurezza delle reti e dell'informazione, gennaio 2019

Largo uso di malware open-source, **Githubification**: facilità di accesso a tool quali Mimikatz, Powersploit, Metasploit, Empire, PowerShell, PHP webshell ecc. Prevalenza tecniche **fileless attack**.

Gli EK sono ancora una minaccia, ma i cyber criminal privilegiano altri vettori d'attacco per i **payload**

L'uso di canali **C2** cifrati è in costante aumento. Abuso di canali cifrati legittimi (**Adversary OPSEC**). Scenari futuri: impiego della tecnologia **blockchain**

Fonte: ENISA Threat Landscape Report 2018 (January 2019)

DEALING WITH TARGETED ATTACKS

IN MANUFACTURING 86% OF CYBER ATTACKS ARE TARGETED

*"The target is often the **planning**, **research** and **development**"*

Fonte: Verizon 2018 Data Breach Investigations Report (DBIR)

DEALING WITH TARGETED ATTACKS

47% OF BREACHES INVOLVE THE THEFT OF INTELLECTUAL PROPERTY TO GAIN COMPETITIVE ADVANTAGE

Fonte: Verizon 2018 Data Breach Investigations Report (DBIR)

DEALING WITH TARGETED ATTACKS

66% FEATURE HACKING
ONLY 34% MALWARE

Fonte: Verizon 2018 Data Breach Investigations Report (DBIR)

DEALING WITH TARGETED ATTACKS

ERRORS WERE CAUSAL EVENTS IN 21% OF BREACHES

Fonte: Verizon 2019 Data Breach Investigations Report (DBIR)

AVERAGE TIME TO IDENTIFY THE BREACH: 197 DAYS

Ponemon Institute , "2018 Cost of a Data Breach Study"

Photo by Daniele Levis Pelusi on Unsplash

F-Secure

TECNICHE

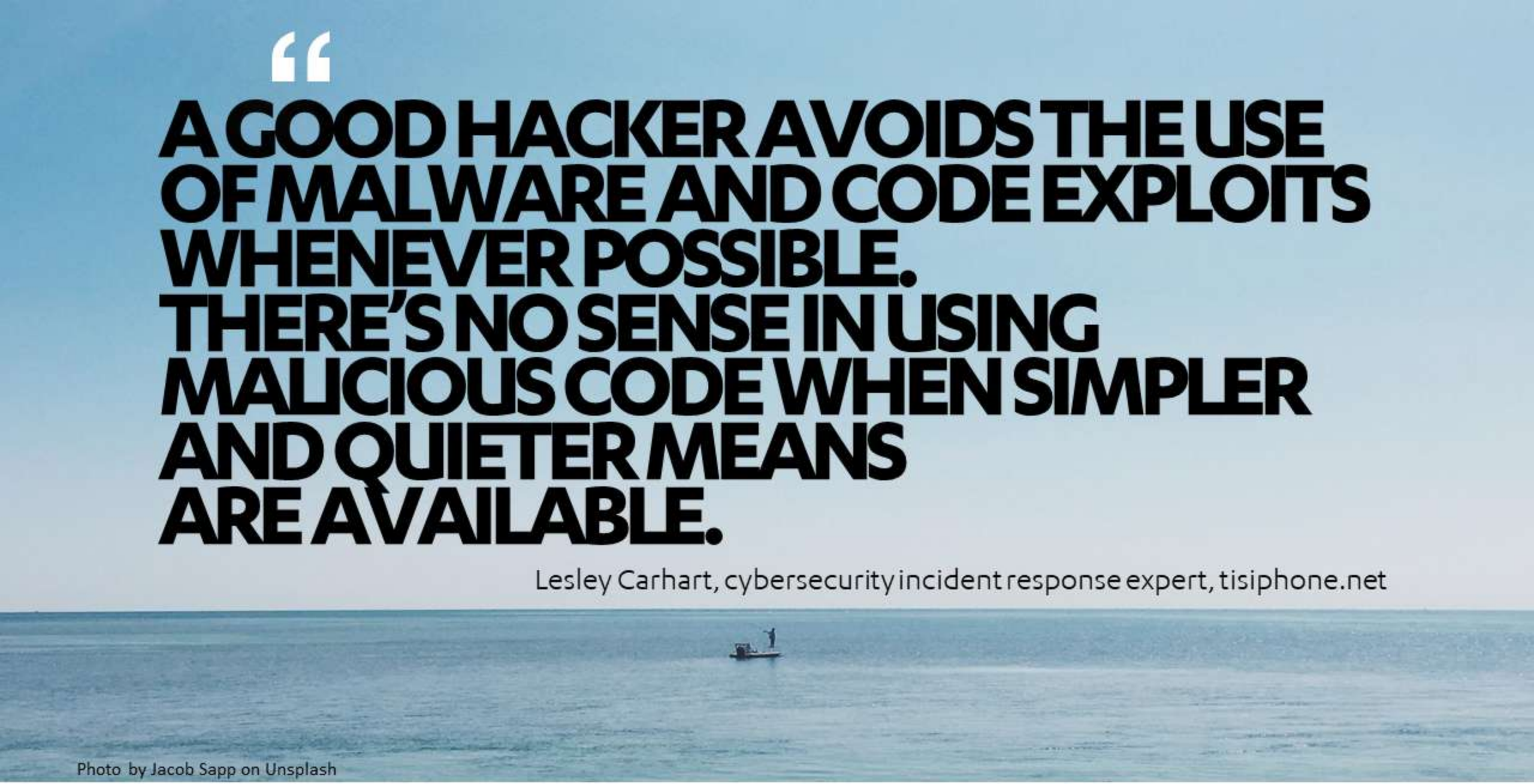


Photo by Jacob Sapp on Unsplash

F-Secure

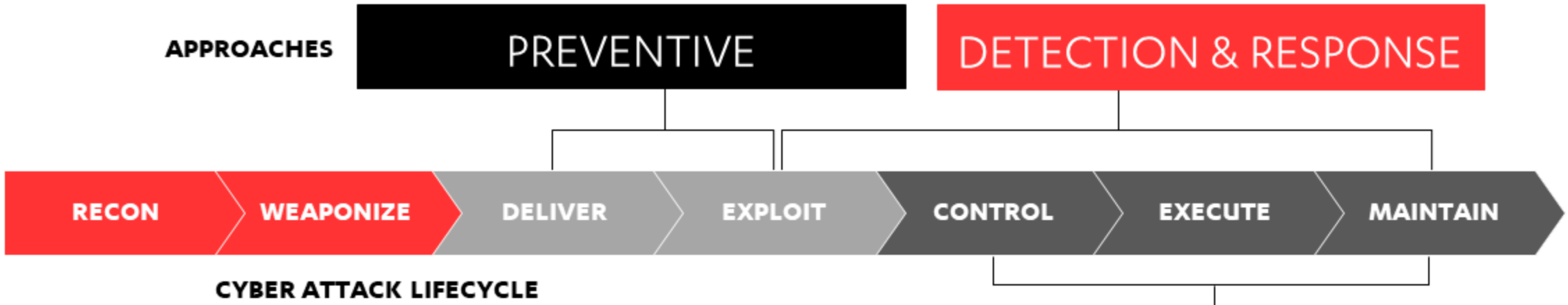
EVOLUZIONE DELLE TECNICHE

- L'evoluzione non segue una **linea temporale netta**: spesso le tecniche vengono riutilizzate
- Tendenza degli ultimi anni: **fileless** malware/attack (motivo: agire indisturbati, aggirare UAC, AV, EPP ecc.)
- **Code Red** and **SQL Slammer** erano fileless (primi anni 2000)
- **Living Off the Land**: impiego di tool e comandi già presenti nel sistema operativo, oppure dal duplice utilizzo (esempio malware: **Petya**/**NotPetya**)
- **PowerShell**: Microsoft ha introdotto nuove capacità di logging e l'Anti-Malware Scan Interface (**AMSI**); **nuove frontiere**:
  - attacchi dove l'offuscamento del codice è sempre più spinto
  - tecniche che non utilizzano PowerShell per eseguire script PowerShell (**PowerPick**), ma **.NET/C#**, agenti post-exploitation basati su **IronPython** (Python + .NET) e **C#**

MDR


“
PREVENTION IS IDEAL, BUT DETECTION IS A MUST. HOWEVER DETECTION WITHOUT RESPONSE IS USELESS.
Eric Cole, Security Expert, Chief Scientist for Lockheed Martin
Photo by Joshua Earle on Unsplash

CAPACITÀ
PREVENTIVA E REATTIVA



PRE-COMPROMISE

- Conoscenza dei rischi, prevenzione dei rischi informatici, hardening, vulnerability management, patch management, backup strategies, access control, network security ecc.
- Strumenti di difesa tradizionali: firewall, WAF, IDS/IPS, segmentazione della rete, EPP ecc.

TTP CATEGORIES

Persistence	Discovery	Exfiltration
Privilege Escalation	Lateral Movement	Command and Control
Defense Evasion	Execution	
Credential Access	Collection	

POST-COMPROMISE

- Monitoring, Detection
- Incident Response (lesson learned)

LOCKHEED MARTIN MITRE

F-Secure

MANAGED DETECTION AND RESPONSE

Incident Handling and forensics services

Managed detection and response service

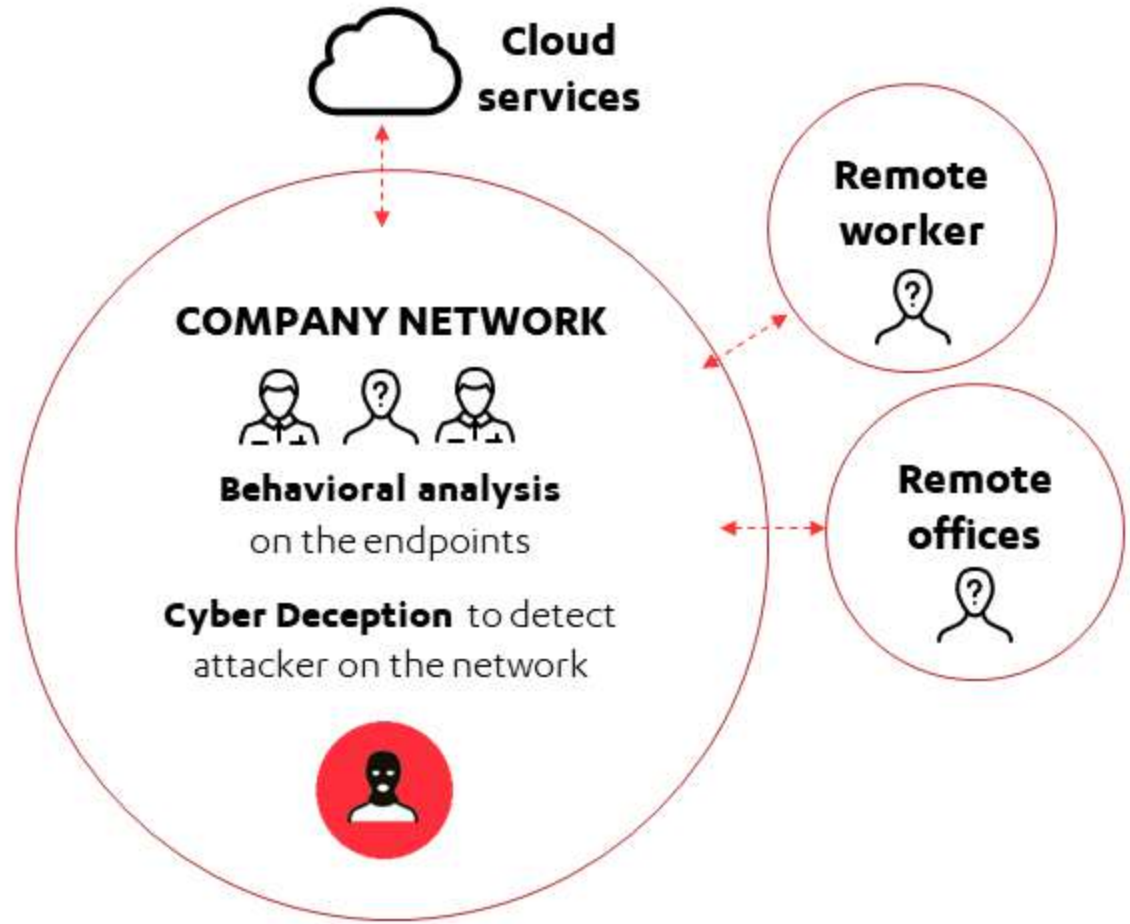
Endpoint Activity

- Servizio gestito focalizzato sulla **threat detection**
- Servizio che include un monitoraggio 24x7 da parte di analisti esperti (**SOC**)
- Servizio chiavi in mano di **Detection** e **Response**
- Utilizza la tecnologia del fornitore
- Componenti installabili presso il cliente
- Monitoraggio degli **endpoint** (e server)
- Advanced Analytics & Machine Learning (cloud)
- **Vantaggi**: team di analisti a disposizione del cliente

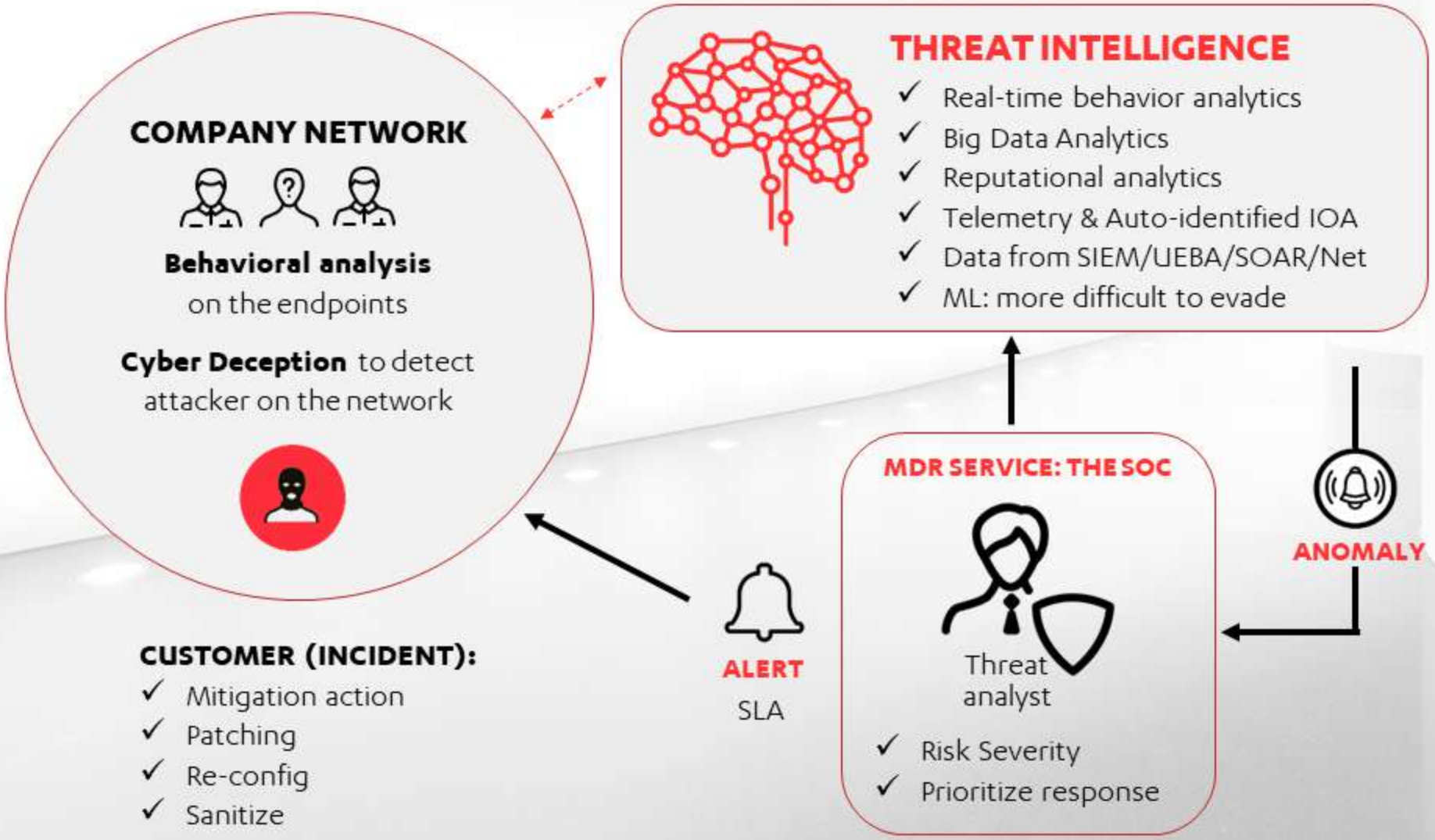
PERCHÉ IL MONITORAGGIO DEGLI ENDPOINT?

Targeted attack: un gran numero di eventi può essere identificato solo partendo dagli **endpoint**:

- ✓**Persistence**
- ✓**Defense Evasion**
- ✓**Privilege Escalation**
- ✓**Credential Access**
- ✓**Execution**
- ✓**Collection**



MDR: IL FATTORE UMANO



F-Secure

COSA ACCADE IN UN'AZIENDA DI MEDIE DIMENSIONI

Area di applicazione del **machine learning**

Organizzazione di medie dimensioni (~1300 endpoint)

F-SECURE IN SHORT

30+

We have over 30 years of experience in cyber security.

More European cyber crime investigations than any other company

We collaborate with over 70 industry actors, like Interpol.

Largest single source of security services and detection & response solutions in Europe

We work through 200+ operator and 6000+ local reseller partners.

Listed on NASDAQ OMX Helsinki Ltd. since 1999.

Leading research and development since 1988.

We operate in 100+ countries, out of 33 offices.

F-Secure®