Continuous Security Validation: misurare il rischio della tua infrastruttura di Security

Come misurare l'efficacia e il rischio della tua infrastruttura di sicurezza?

Luca Bechelli
Information & Cyber Security Advisor
Direttivo e Comitato Tecnico-Scientifico CLUSIT

Maurizio Costa
Cyber Security Services Delivery Manager
SINERGY SpA

Marco Ceccon
Advisory Practice Manager
SINERGY SpA

Dagli ultimi dati…

- un danno economico complessivo di circa 500 miliardi di dollari
- danni quintuplicati in 6 anni
- 730 attacchi gravi con danno economico, reputazionale e perdita di dati sensibili. **+31,77%** rispetto al **semestre** precedente
- La finalità cybercrime cresce del 35%, per raggiungere l'80% del totale degli attacchi

SQL Injection

-100% !!

(rispetto al II sem.2017)

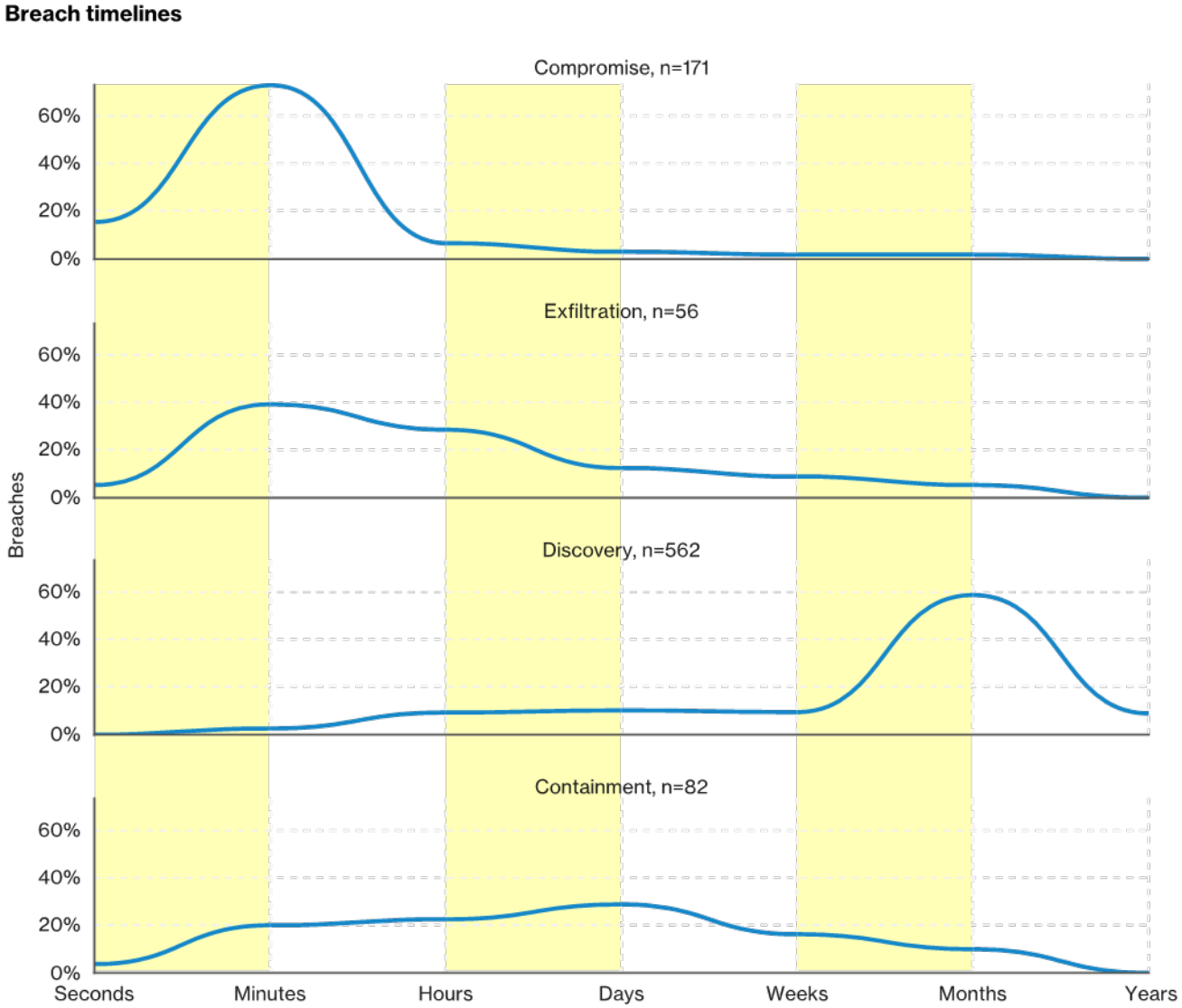
Tecniche di attacco (rispetto al II sem.2017)

+140% 0-day

+48% APT

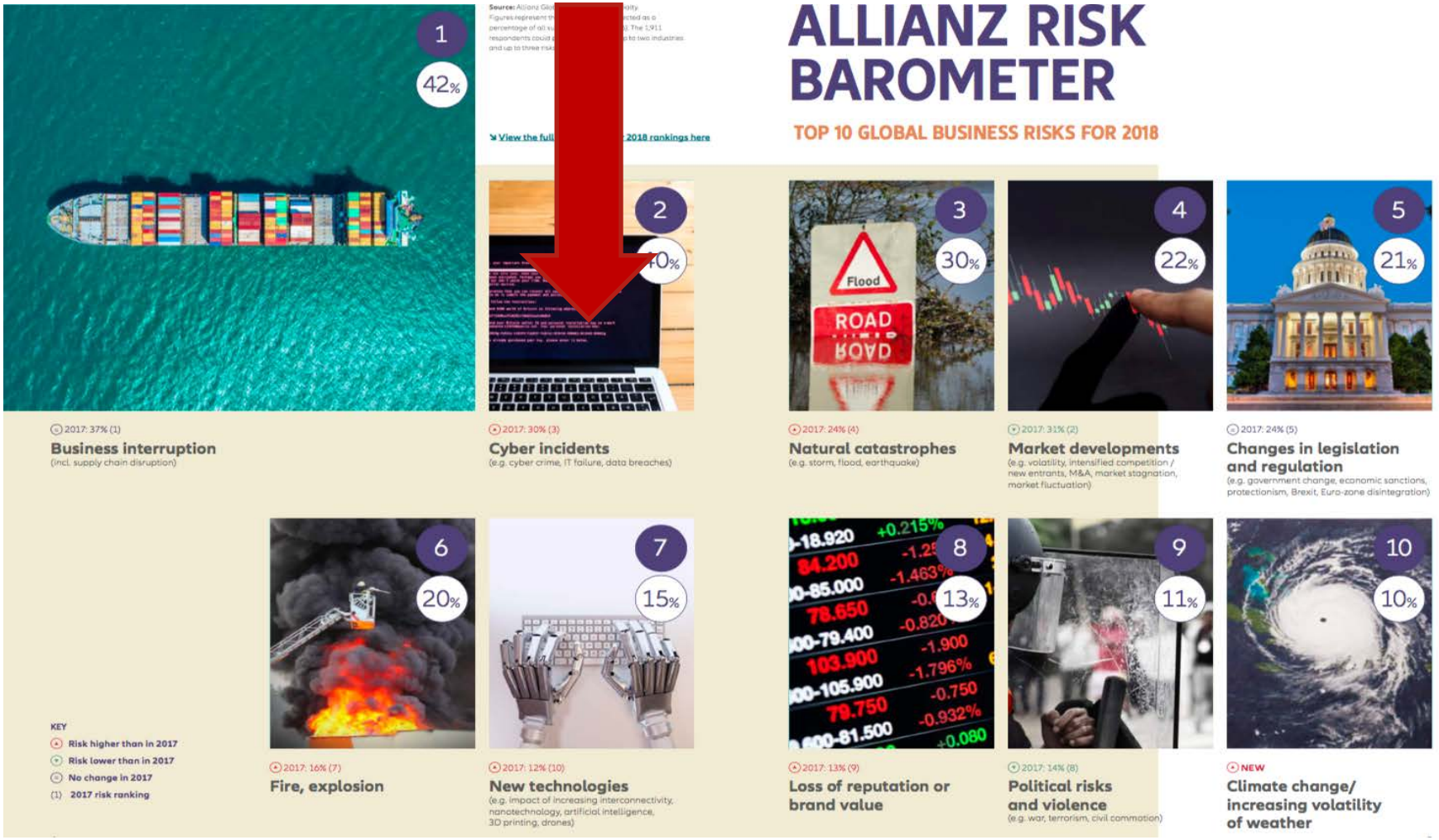
+37% Know Vulnerabilities

Una questione di velocità

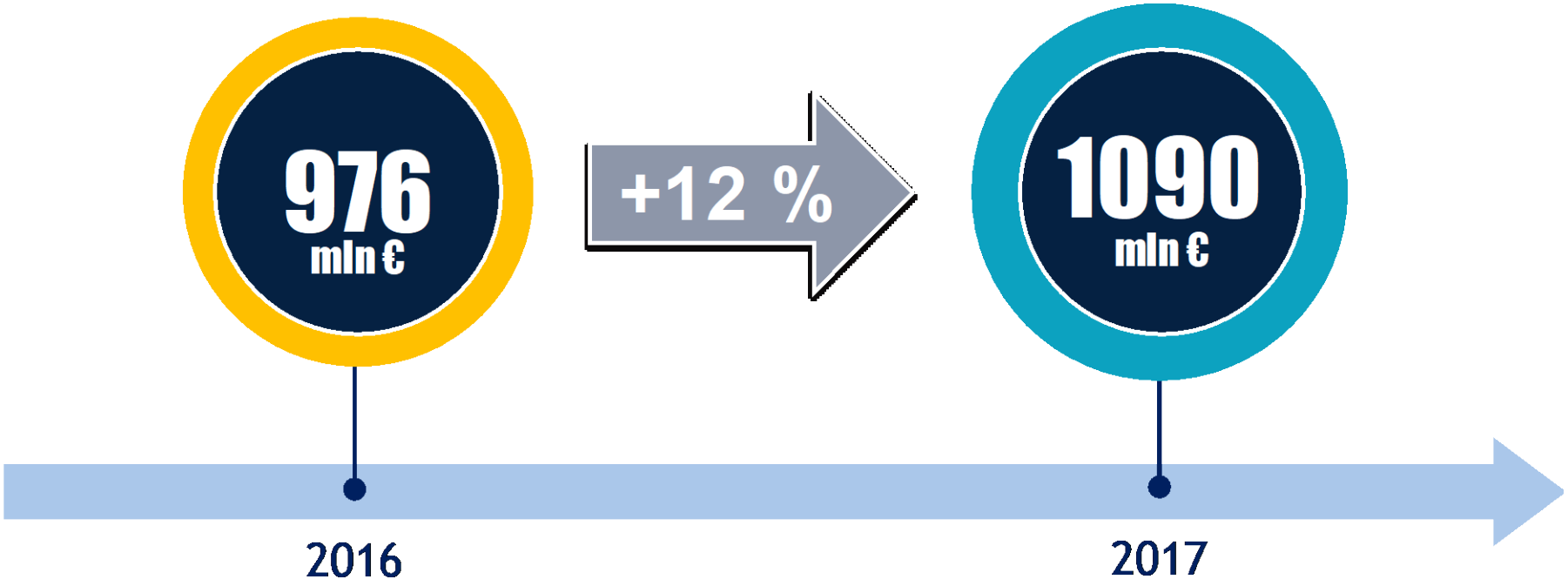


verizon

La consapevolezza cresce…



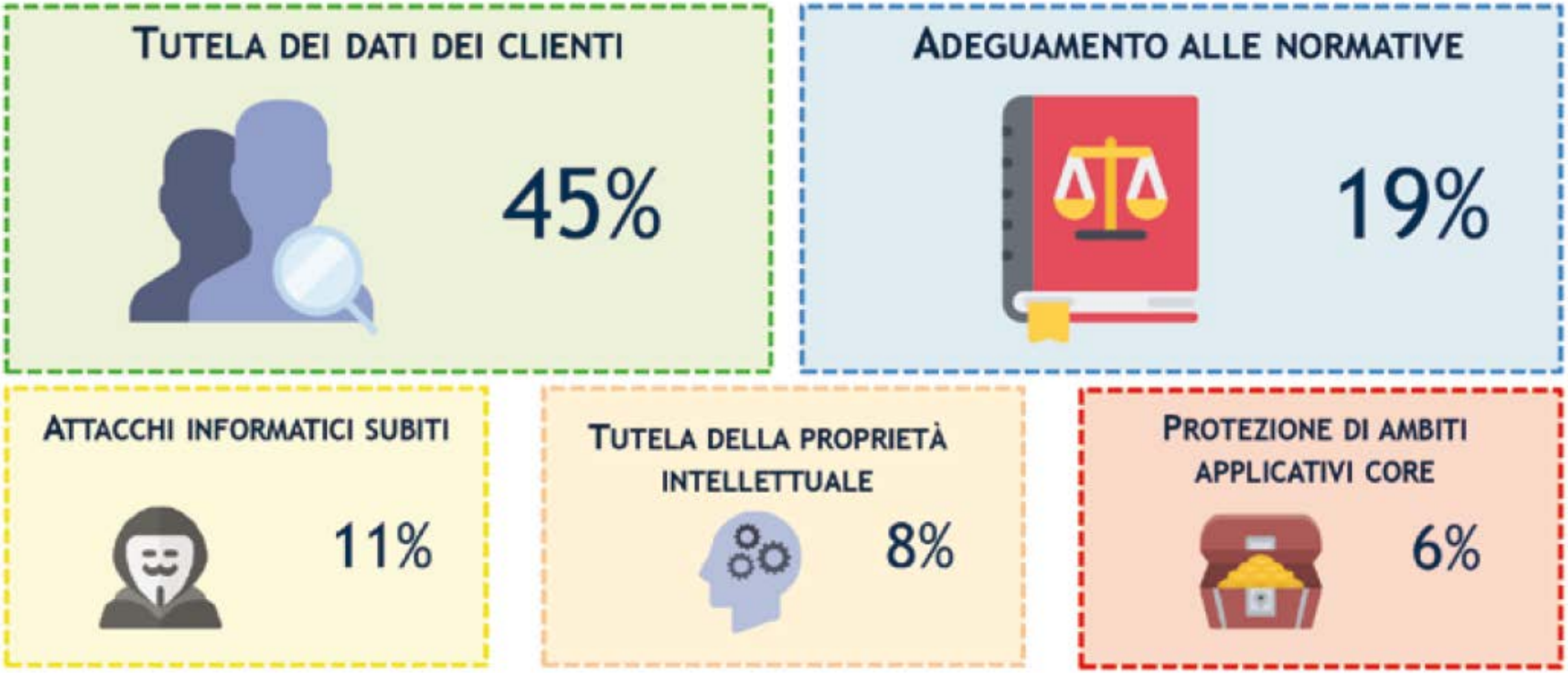
…anche in Italia



Campione: 1107 organizzazioni italiane

OSSERVATORI.NET digital innovation

Principali motivi di spesa



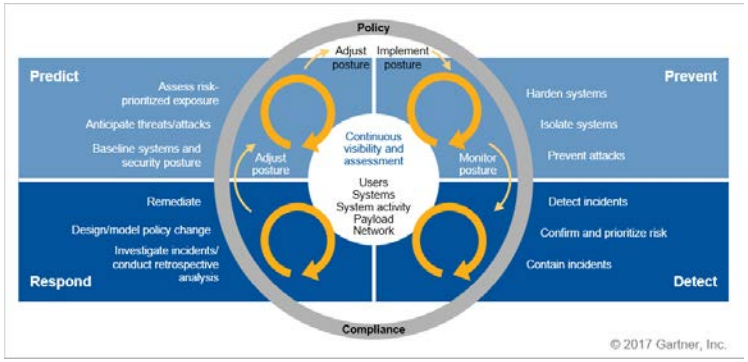
Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

OSSERVATORI.NET digital innovation

…e il GDPR?

Modelli avanzati di protezione

Sintesi dei modelli: Adaptive Security Architecture



Prevent

- **Key goal:** riduzione della superficie d'attacco
- **Challenge**:
  - o l'interfaccia non è più costituita da confini netti, tende ad ampliarsi (Cloud, IoT) e a complicarsi.
  - o Verifica **continua** delle regole di difesa

Detect

- **Key goal:** riduzione del tempo di rilevazione di un attacco
- **Challenge**: adozione di modelli di monitoraggio **continuo**

Respond

- **Key goal:** riduzione dei tempi di analisi e di rimedio
- **Challenge**: supporto **continuativo** di specialisti di sicurezza che giocano un ruolo fondamentale

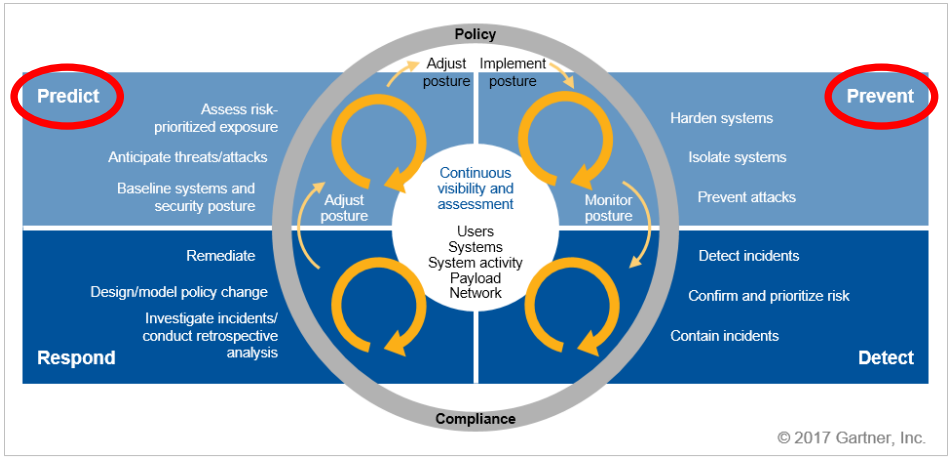
Predict

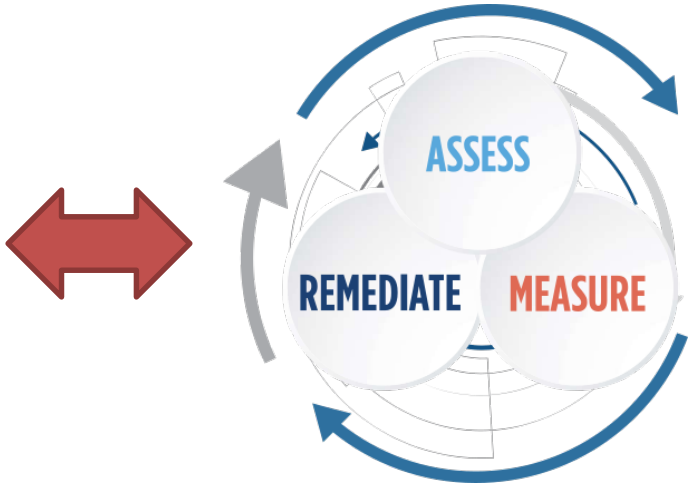
- **Key goal:** anticipare nuove metodologie e vettori di attacco
- **Challenge**: analisi **continua** del proprio stato di vulnerabilità per istruire in modo **continuativo** le fasi di prevent e detect

Adaptive Security Architecture

Continuous Security Validation (CSV)

La valutazione dell'efficacia dei presidi di sicurezza implementati nell'Organizzazione è uno degli elementi fondamentali e abilitanti l' Adaptive Security Architecture

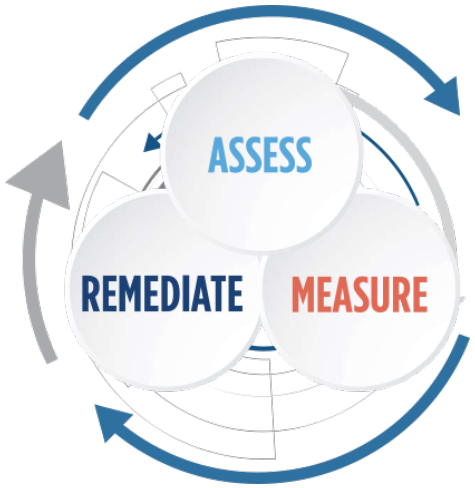




Predizione e Prevenzione: opportuni processi di Continuous Security Validation permettono alle aziende di tenere traccia di nuove emergenti minacce e di monitorare in modo continuativo la robustezza relativa dei propri sistemi di protezione, indicando eventuali priorità e modalità di intervento.

Continuous Security Validation

CyberSecurity & Compliance references



Riferimento	Controlli
ISO/IEC 27001:13	A.12.6, A.13.2, A.16.1, A.18.2
NIST SP 800-53 Rev. 4	AC-4, AC-17, AC-18, CA-2, CA-3, CA-7, CA-8, CA-9, CP-2, CP-8, PL-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, SC-7, IR-4, IR-8
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04 , BAI01.13, DSS05.02
PCI-DSS 3.2	11.2, 11.3
EU GDPR	Art. 32.1.d
AgID Misure minime di sicurezza ICT per le PA	ABSC_3, ABSC_4, ABSC_8
Banca d'Italia Circolare 285, 23° aggiornamento	Capitolo 4: Sez. IV e Sez. V

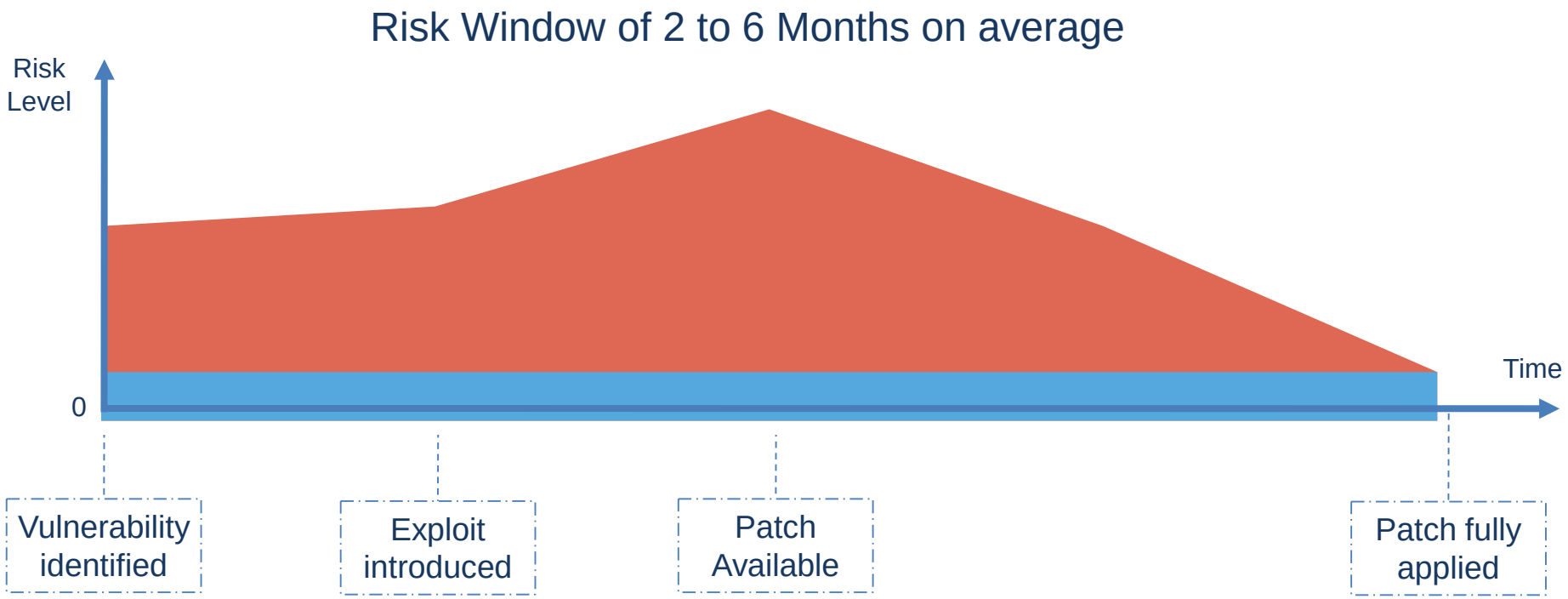
Dettagli tecnici e modelli di implementazione

CONTINUOS SECURITY VALIDATION

Incidenti diversi ma stesse modalità

- Gli attacchi Equifax, WannaCry, Petya, DragonFly e altri hanno sfruttato vulnerabilità note da mesi con patch disponibili
- Molte aziende hanno sistemi con vulnerabilità note da anni alle quali non vengono applicate le relative patch
- Se le vulnerabilità sono note e le patch sono disponibili perchè queste vengono ancora sfruttate per portare attacchi?

Il Ciclo di Patching è un processo “lungo”



Criticità dei processi di Vulnerability/Patch Management

1.000 - 100.000
too many
in numbers and types

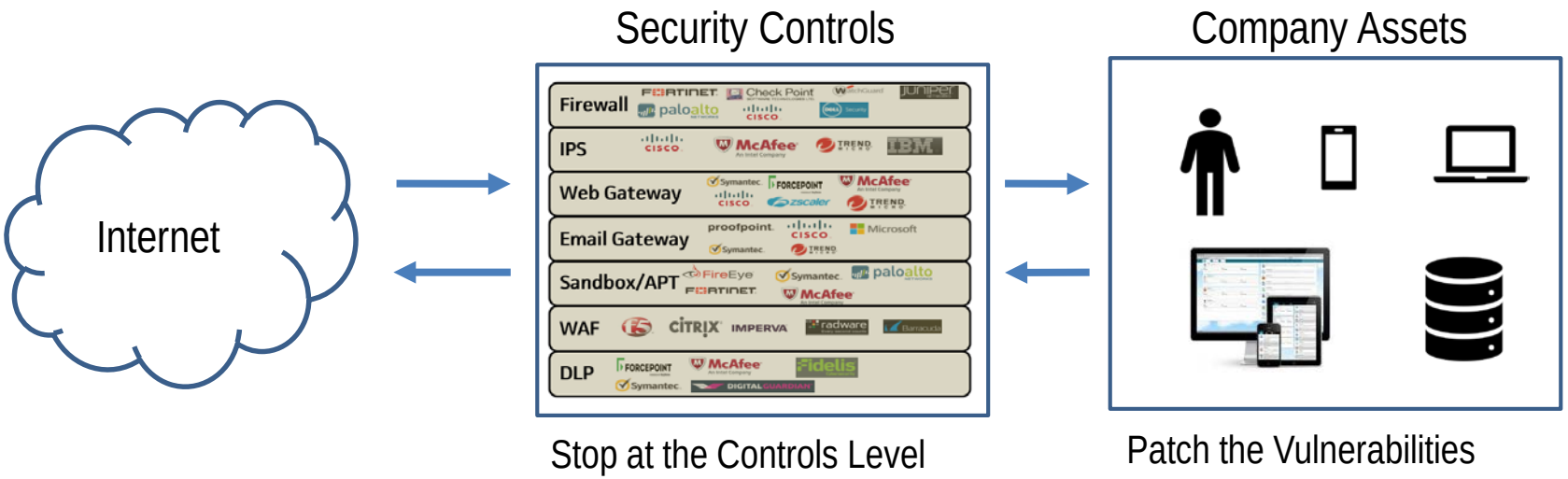
mission critical
DB and apps

3rd party
out of reach

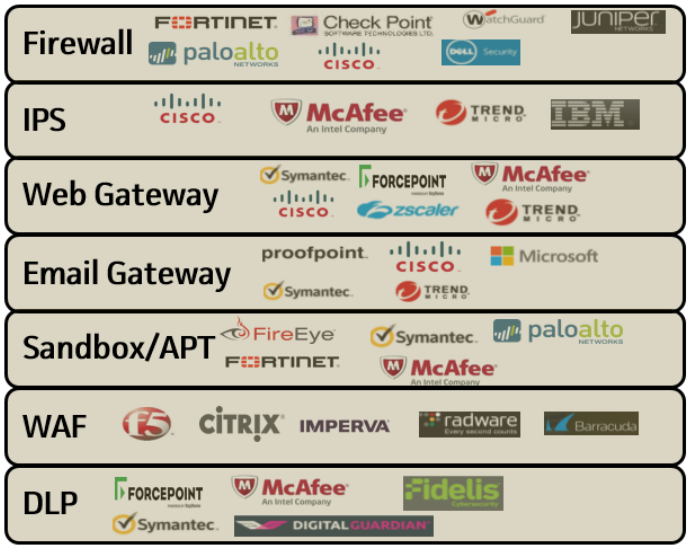
- Complessi da operare: in ambienti di grandi dimensioni, critici ed eterogenei il ciclo di patching può durare mesi
- Esistono sistemi per i quali è estremamente complesso (o quasi impossibile) applicare patch (es. ICS)
- Le infrastrutture gestite da terze parti non sono direttamente controllabili
- Definire la priorità di intervento può non essere semplice

Opzioni per Mitigare gli Attacchi

"Block it" vs "Patch Against It"

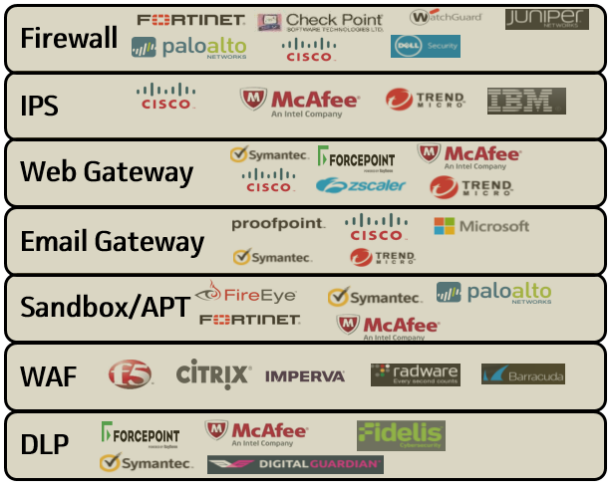


Security Controls
Riduzione del Rischio



Sfide delle Security Operations

Come è possibile verificare che i «security controls» forniscano sempre la miglior protezione possibile rispetto ai nuovi cyber-threats?



Continuous Security Validation

Automatizzare l'identificazione dei gap nei controlli di sicurezza e misurarne l'efficacia 24x7

Assess

Testare l'efficacia dei controlli di sicurezza utilizzando minace reali

Non focalizzandosi solamente sulle vulnerabilità

Reveal

Identificare i gap nella postura di sicurezza

Prima che vengano sfruttati

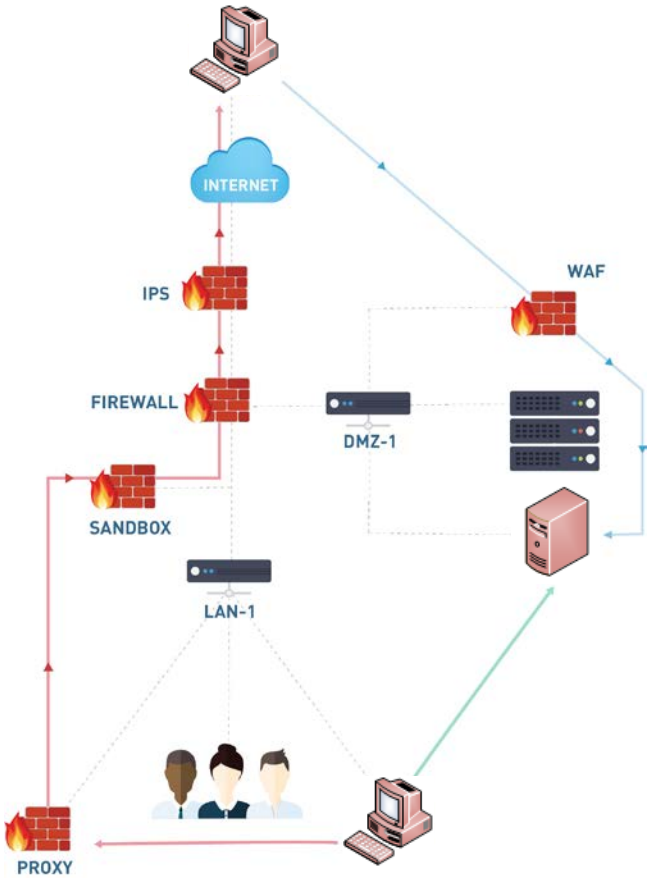
Remediate

Identificare prontamente le soluzioni per correggere i gap ed applicarle con le giuste priorità

Non convivere con il rischio finché le vulnerabilità sono eliminate

Come funziona?

- I sistemi vengono posizionati nei segmenti di interesse della rete
- Vengono definiti gli scenari di attacco tra i sistemi (es. client side, server side, data exfiltration, ecc.)
- Gli scenari di attacco, sono eseguiti andando a testare i controlli di sicurezza attraverso un insieme di minacce costantemente aggiornate
- Viene eseguita una misurazione continua degli attacchi andati a buon fine e non rivelando l'efficacia dei controlli implementati
- Vengono indicate remediation per i gli attacchi andati a buon fine



Cyber-Threat Database

- **Malicious Code**

  Adware, APT, Backdoor, Banking Malware, Botnet, Exploit Kit, Infostealer, Keylogger, Linux Malware, Loader, macOS Malware, Malicious File Download, Malware Downloader, Malware Dropper, Office Exploit Payload, Ransomware, RAT, Rootkit, Spyware, Stealer, Trojan, Trojan Downloader, Virus, Worm and more…

- **Web App Attacks**

  Backdoor, Code Execution, Code Injection, Command Injection, Evasion, File Inclusion, Hack Tools, Injection, Path Traversal, Protocol Anomaly, Protocol Violation, Reflected File Download, Security Misconfiguration, Sensitive Data Exposure, SQL Injection, Unvalidated Redirect, XSS and more…

- **Vulnerability Exploitation**

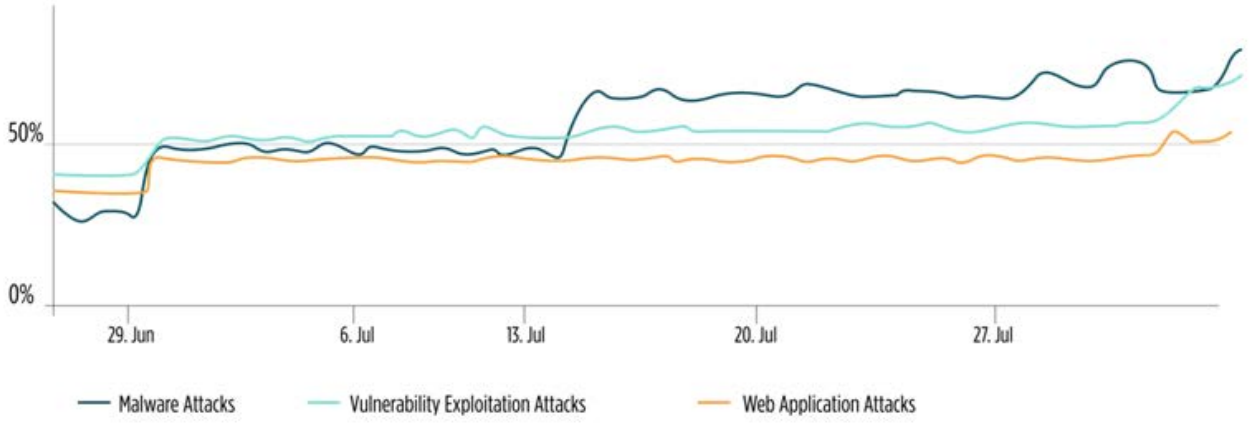
  Backdoor, Buffer Overflow, Code Execution, Denial of Service, File Disclosure, Information Disclosure, Input Manipulation, Memory Corruption, Privilege Escalation and more…

- **Data Exfiltration**

  Administrative Data, Critical OS Info, Payment Card Industry, PCI and PII, Personally Identifiable Information, Source Code and more…

Use Cases

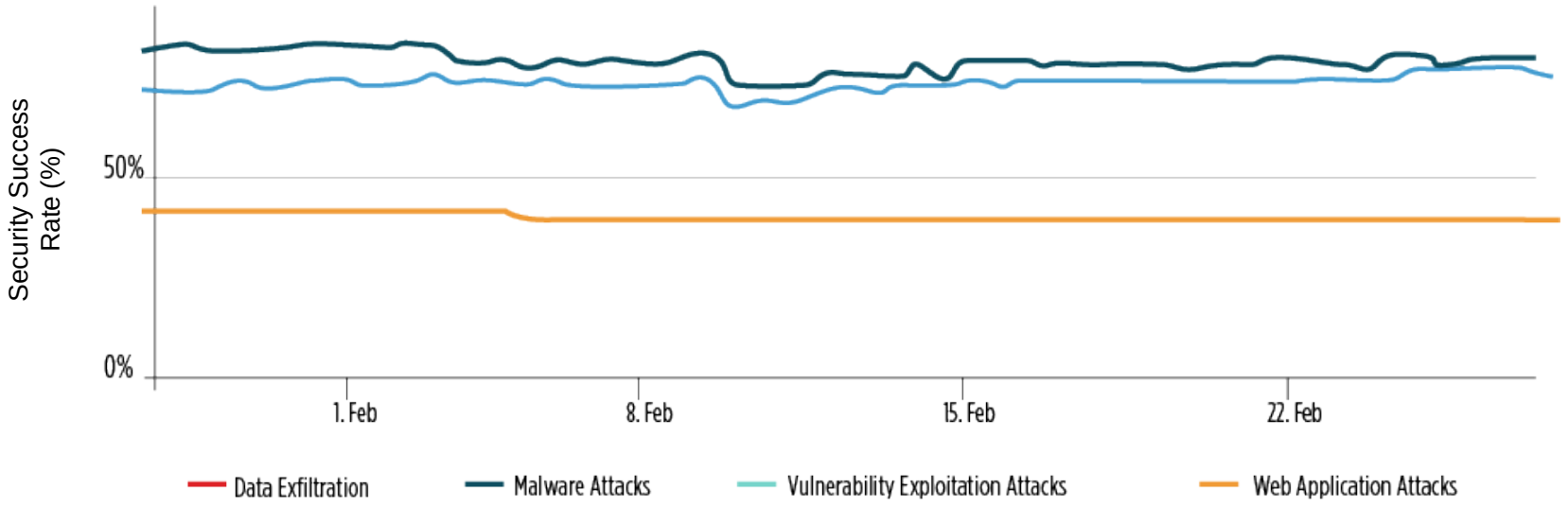
Aumentare l’efficienza delle soluzioni di sicurezza



Check Point 80% 2234/2799	BIG-IP 84% 466/554	FORTINET 77% 1174/1521
paloalto 84% 1998/2391	FORTINET 73% 367/506	modsecurity 84% 297/352
FORTINET 80% 234/291	McAfee 86% 2238/2616	SOURCEfire 85% 1946/2280
79% 201/254		

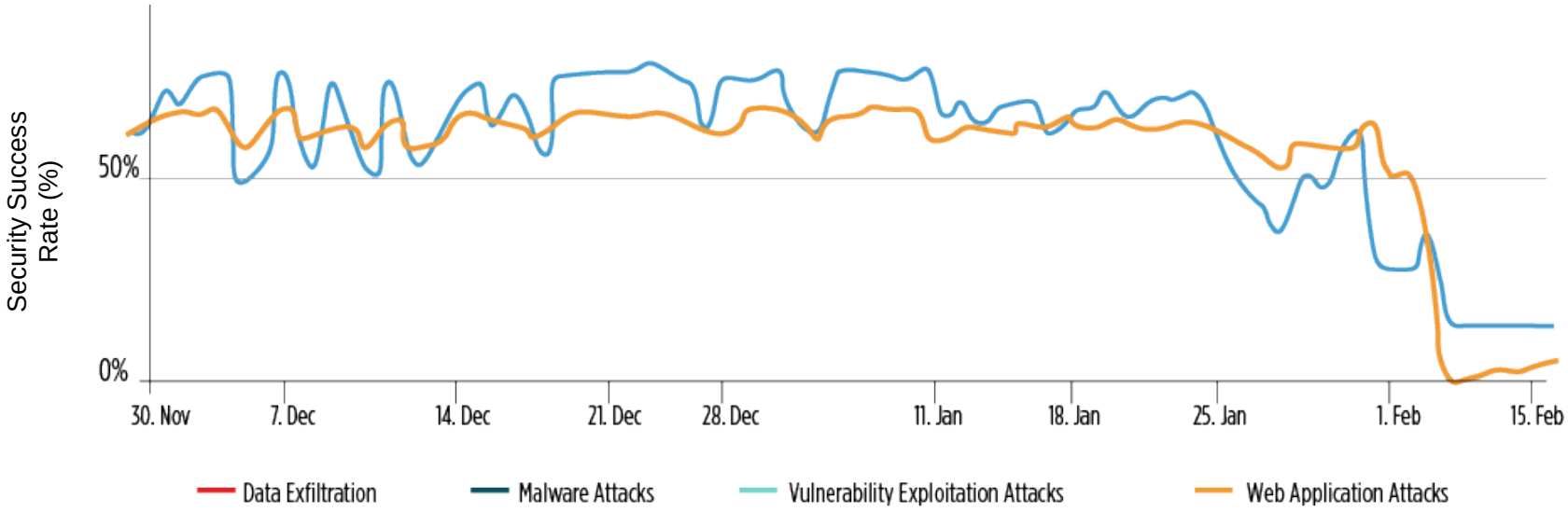
Use Cases

Conoscere le proprie «capabilities» di sicurezza per indirizzare gli investimenti



Use Cases

Identificare problemi di stabilità e performance delle soluzioni implementate



Continuous Security Validation

Key Benefits

Utilizzo efficiente degli investimenti in sicurezza

Ottenere il massimo ROI dalle soluzioni di sicurezza attualmente implementate

Essere preparati nei confronti di minacce emergenti

Rimediare velocemente ai gap rilevati mediante azioni specifiche per i Vendor o mediante regole open-source

Conoscere la propria situazione in tempo reale

Misurare i livelli di efficacia dei propri presidi di sicurezza nei confronti delle varie fasi di un attacco (Kill-chain)

Facilitare le decisioni su nuovi investimenti

Rivelare le soluzioni di sicurezza adeguate da quelle meno efficienti.

Aiutare le Organizzazioni a scegliere in modo opportune le prossime tecnologie di difesa su cui investire

Verificare i livelli di servizio

Valutare la qualità dei servizi di sicurezza garantiti da Vendor e consulenti

Aumentare l'efficienza operativa

Automatizzare l'analisi dei gap e velocizzare le fasi di rimedio

Analisi degli incidenti

Mettere a disposizione degli analisti i sample di attacco per analisi specifiche durante e dopo un incidente

Grazie dell’attenzione

Per approfondimenti

m.costa@sinergy.it

m.ceccon@sinergy.it