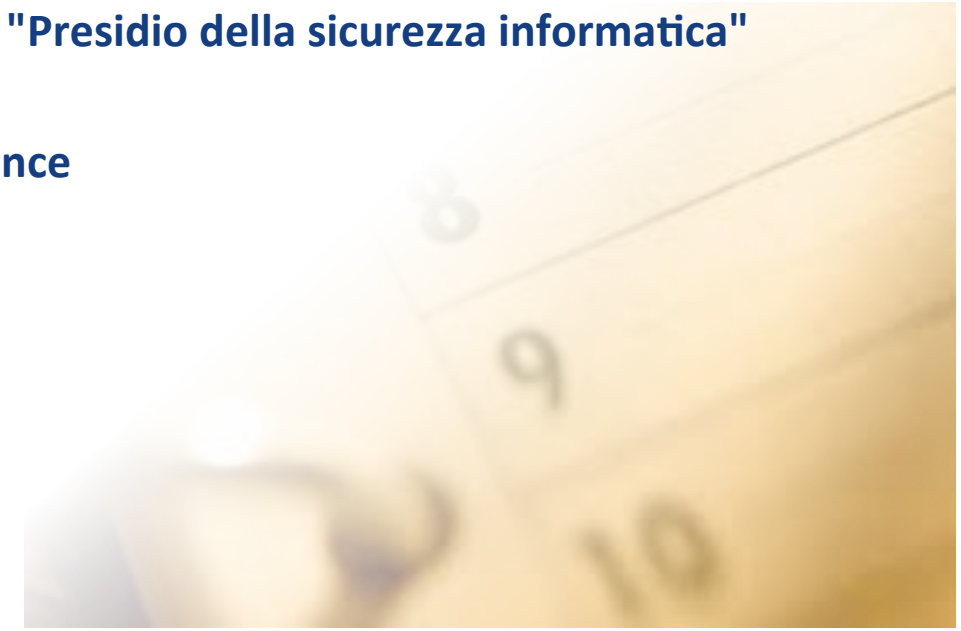
INTESA SANPAOLO
GROUP SERVICES

Rafforzamento dei presidi di Sicurezza all'interno del Gruppo Intesa Sanpaolo

Flavio Paolinelli
Infrastructure Security

Agenda

- Gli obiettivi di presidio della sicurezza informatica del Gruppo Intesa Sanpaolo
  - Il presidio della sicurezza informatica nell'anno 2014
  - Il presidio della sicurezza informatica nell'anno 2015
- L'evoluzione del concetto "Perimetro da proteggere"
- La conseguente evoluzione del concetto di "Presidio della sicurezza informatica"
- L'affermazione di nuovi modelli di Intelligence
- L'istituzione della funzione ISP-CERT
- Le prossime sfide



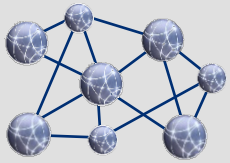
Gli obiettivi di presidio della sicurezza informatica del Gruppo Intesa Sanpaolo

Che cosa significa "Presidiare la sicurezza informatica del Gruppo Intesa Sanpaolo?"

Avere ben chiaro il perimetro da proteggere

Conoscere le minacce da cui difendersi

Disporre di processi e contromisure adeguate



Rete complessa di sistemi:

- Mainframe
- Midrange
- Client-server
- Web-based
- PdL
- PC Clienti

Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malware	↑	→
2. Web based attacks	↑	→
3. Web application attacks	↑	→
4. Botnets	↓	→
5. Denial of service	↑	→
6. Physical damage/theft/loss	⊃	↑
7. Insider threat (malicious, accidental)	↑	↑
8. Phishing	⊃	↓
9. Spam	↓	↓
10. Exploit kits	↑	↓
11. Data breaches	⊃	↓
12. Identity theft	⊃	↑
13. Information leakage	↑	↓
14. Ransomware	↑	↑
15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

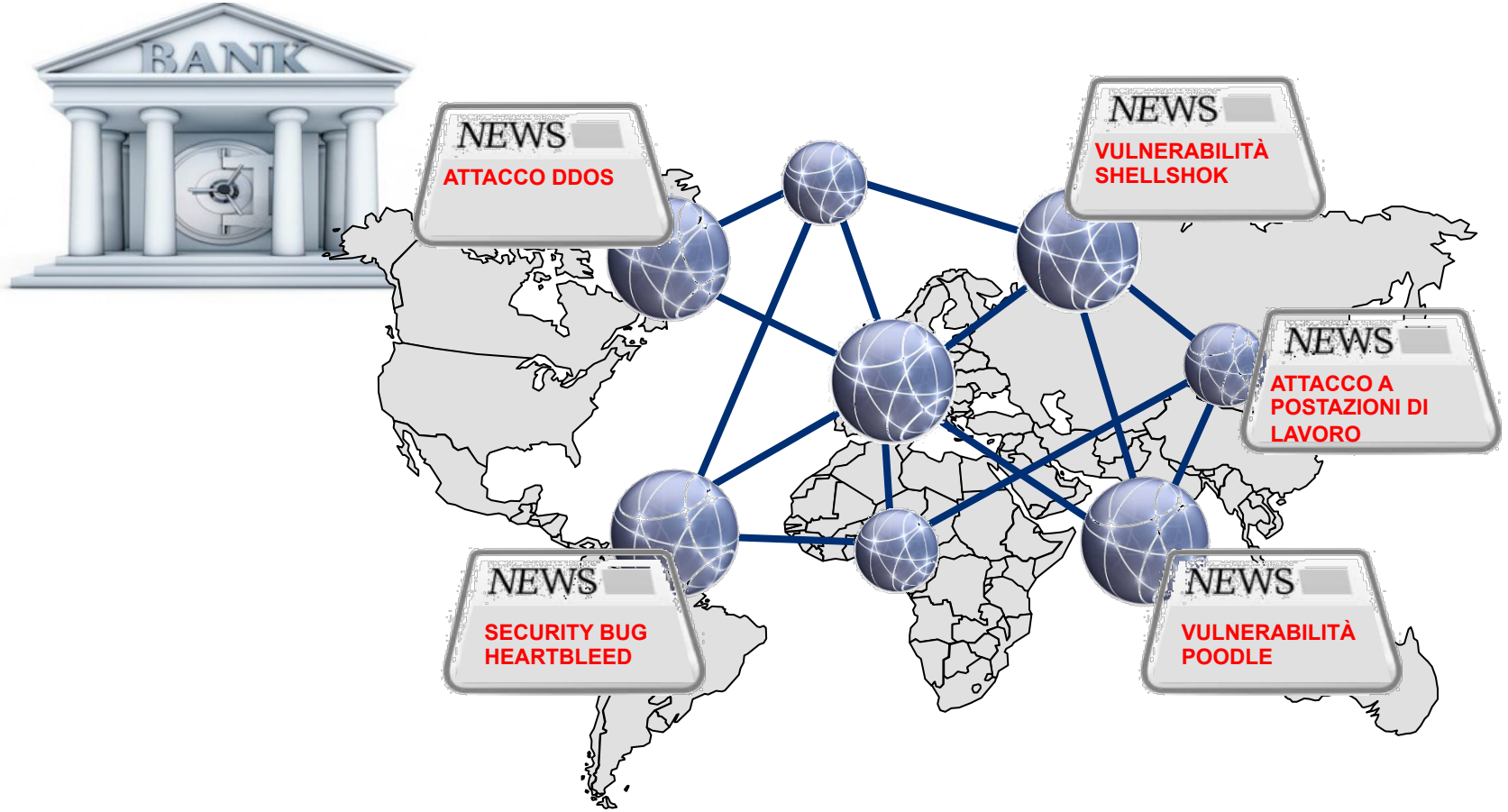
enisa

ENISA Threat Landscape 2015 | January 2016

- Adozione di soluzioni e strumenti di protezione leader di mercato (anti-DDOS, antiphishing, antimalware, anti APT, IAM, firewalling, …)
- Allestimento di un SOC 24x7
- Aderenza a Best Practices di settore (certificazione ISO-27001 dei servizi core)
- Adeguamento nel tempo del quadro normativo di Sicurezza Informatica di Gruppo
- Simulazioni di attacco ed effettuazione periodica di vulnerability assessment e penetration test
- Adozione metodologie e modelli di analisi del rischio di sic. informatica integrate nel modello di presidio dei rischi aziendale
- Pianificazione iniziative formative e di awareness destinate a dipendenti e clienti del Gruppo
- …

Il presidio della sicurezza informatica nell'anno 2014

Quali sono state le principali minacce del 2014?

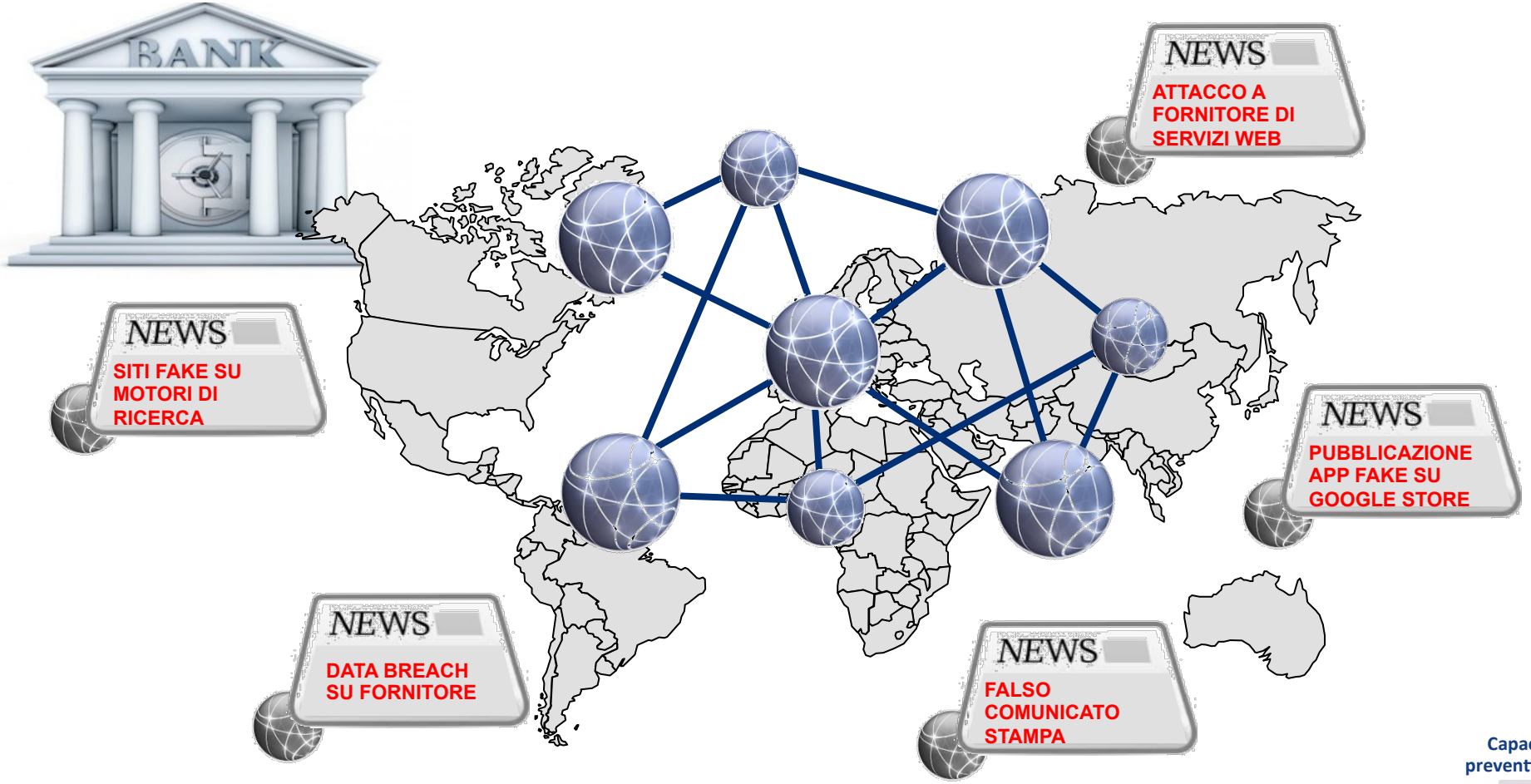


Le misure di protezione del sistema informativo aziendale (contromisure in esercizio, livelli di presidio dell'IT aziendale, processi di controllo interno) **hanno consentito nella totalità dei casi di contenere sul nascere gli impatti dell'incidente di sicurezza**

Capacità di contrasto preventivo e/o immediato

Il presidio della sicurezza informatica nell'anno 2015

Quali sono state le principali minacce del 2015?



Capacità di contrasto preventivo e/o immediato

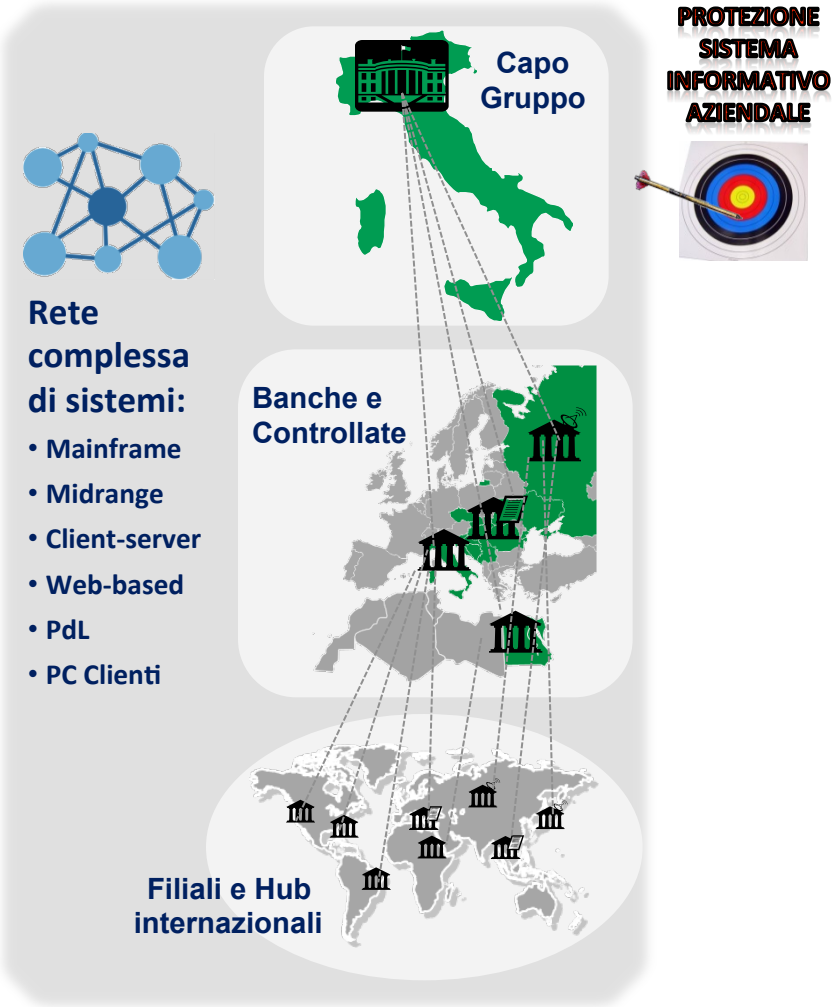
Le misure di protezione del sistema informativo aziendale (contromisure in esercizio, livelli di presidio dell'IT aziendale, processi di controllo interno) **NON hanno consentito nella totalità dei casi di contenere SUL NASCERE gli impatti dell'incidente di sicurezza.**

IL SISTEMA INFORMATIVO AZIENDALE NON È MAI STATO INTERESSATO DALL'ATTACCO

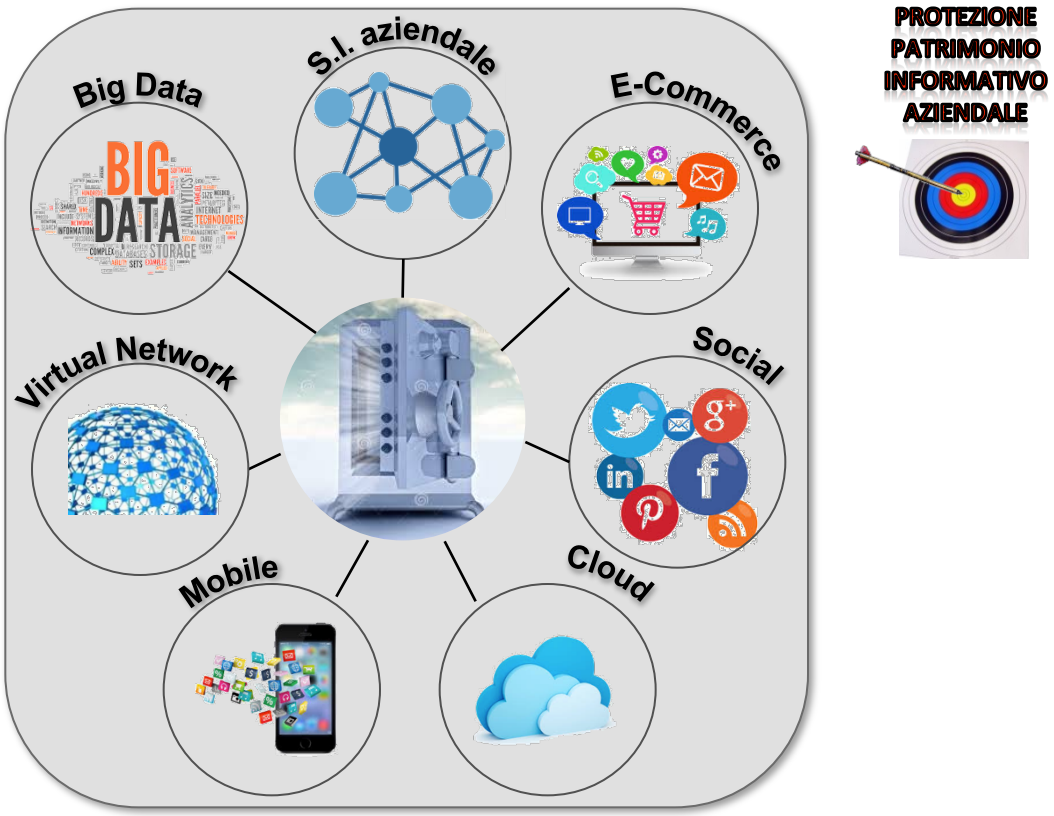
L'evoluzione del concetto "Perimetro da proteggere"

Ha ancora senso parlare di *Protezione del sistema informativo aziendale*?

Il "perimetro da proteggere" non coincide più con il solo sistema informativo aziendale



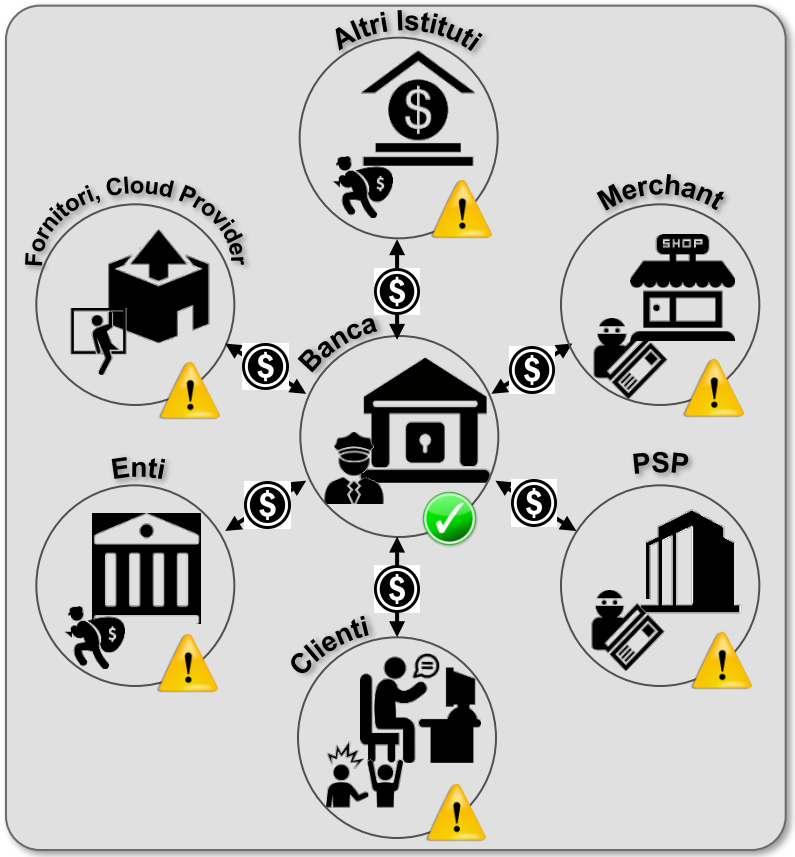
Oggi la banca è un sistema "aperto" che opera su diversi canali, gestiti da una pluralità di attori tra loro differenti.
Il perimetro è sempre più l'**intero patrimonio informativo aziendale**

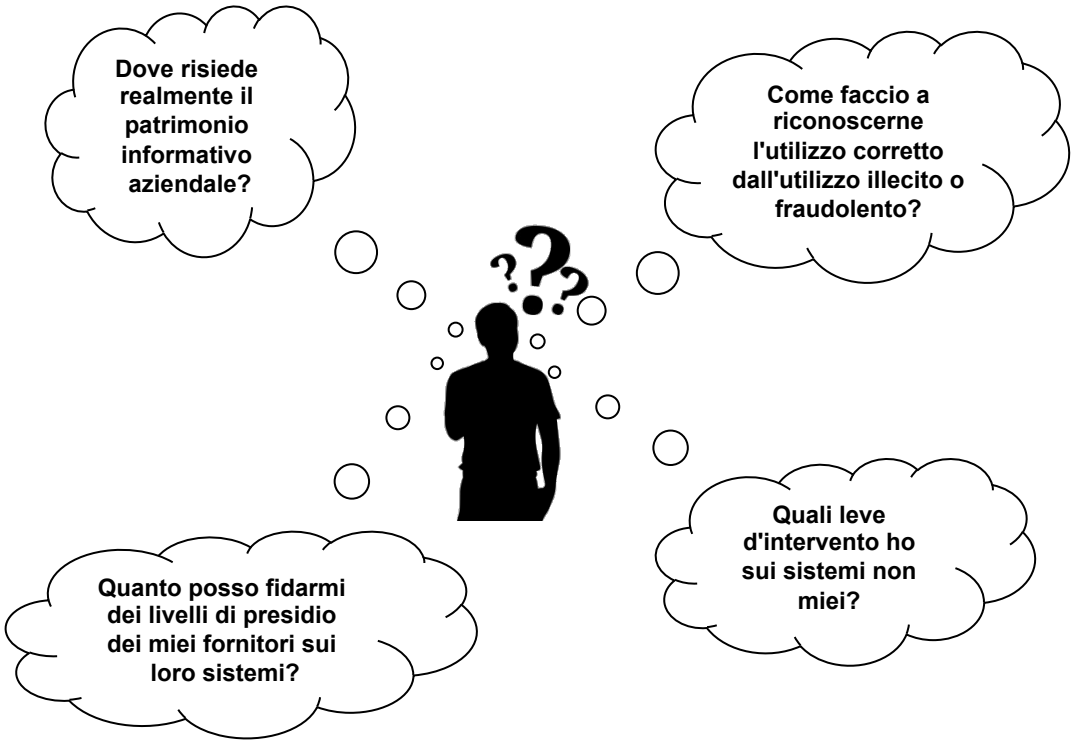


La conseguente evoluzione del concetto di "Presidio della sicurezza informatica"

Quali sono le nuove "Big Question" imposte dalla rivisitazione del perimetro ?

- L'adozione di adeguate misure di sicurezza **all'interno della Banca** non è più sufficiente a garantire la protezione dalle minacce di cybercrime.
- Il perimetro ICT in cui è possibile trovare informazioni aziendali **spesso estremamente sensibili** si estende oltre i confini della banca.
- La Banca è infatti interconnessa con terze parti con cui scambia dati ed effettua transazioni, le quali potrebbero adottare standard di sicurezza non adeguati.





L'affermazione di nuovi modelli di Intelligence

L'evoluzione delle logiche di presidio della Sicurezza Informatica richiede la definizione di nuovi modelli di intelligence che si vadano ad affiancare a quelli tradizionali che devono essere rigorosamente mantenuti.

COSA
- Analisi eventi interni al sistema aziendale (SIEM, IPS/IDS, accessi non autorizzati, …)
- Presidio esterno di vulnerabilità e minacce tramite "armi convenzionali" (Vulnerabilità, Spam, Botnet, clonazione siti ISP, DDOS, campagne phishing, …)

COME
- Specializzazione personale interno
- Utilizzo soluzioni leader di mercato

Security Intelligence

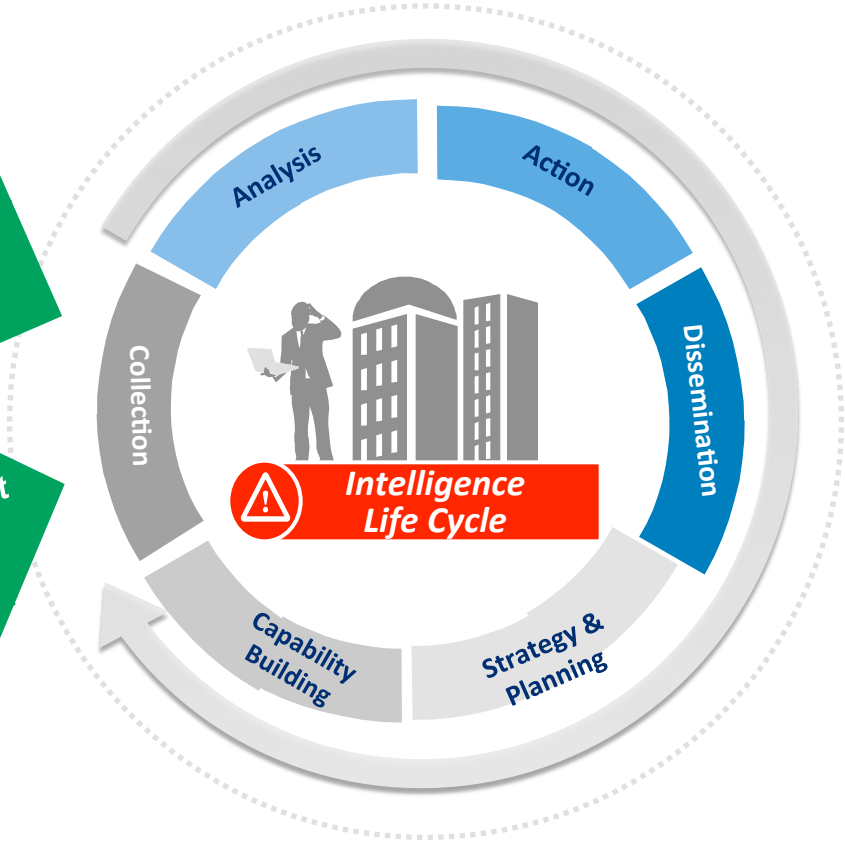
- **RICERCA IoC NOTI SU PERIMETRO INTERNO / ESTERNO**
- **INCIDENT RESPONSE PROCEDURALIZZATO**

COSA
- Ricerca di nuovi trend di attacco (hacktivism, criminalità organizzata, spionaggio commerciale, infedeltà collaboratori, …)
- Presidio esterno di minacce tramite "armi non convenzionali" (informazioni aziendali su fonti OSINT, deep web, black market, …)

COME
- Specializzazione personale interno
- Utilizzo soluzioni emergenti di Intelligence
- Collaborazioni con enti governativi, istituzionali e di altri settori dell'industria

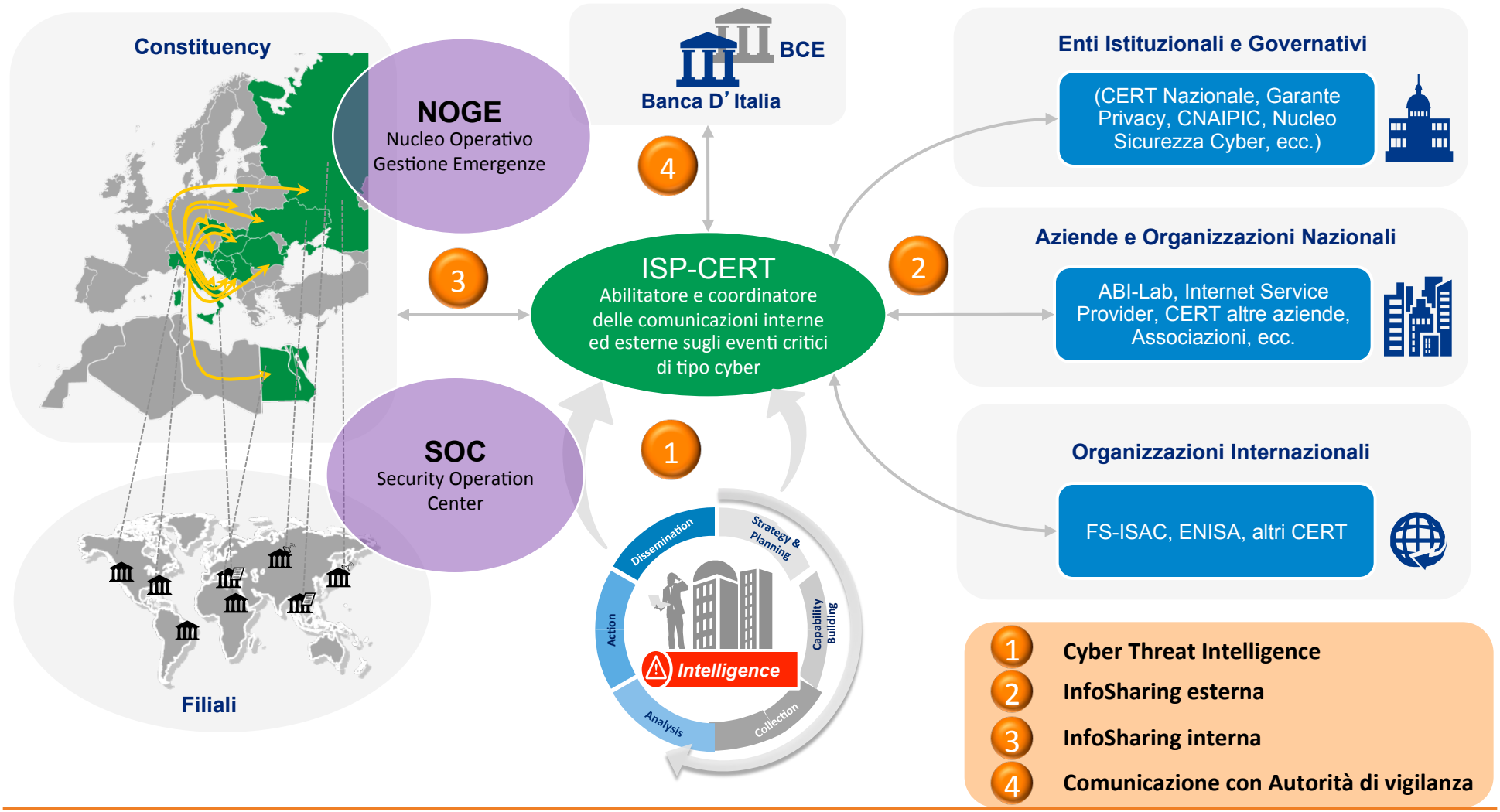
Cyber Threat Intelligence

- **RICERCA IoC NON NOTI SU PERIMETRO INTERNO / ESTERNO**
- **FILTRO DELLE INFORMAZIONI DI INTERESSE**
- **INCIDENT RESPONSE SPECIALISTICO**



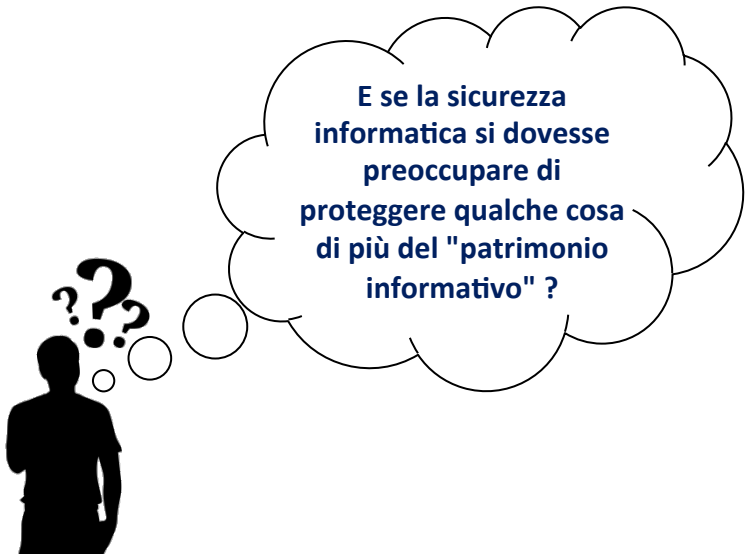
L'istituzione della funzione ISP-CERT

- ISP-CERT costituisce l'interfaccia operativa per gli eventi critici cyber nei confronti degli stakeholder esterni garantendo :
  - la gestione ed il coordinamento della comunicazione in ingresso ed in uscita
  - il coordinamento con Crisis Management e SOC di CapoGruppo



Le prossime sfide

Sarà davvero sufficiente estendere il presidio alle minacce "tradizionali" su un perimetro "allargato" ?



IoT

Le tecnologie IoT, permettendo la convergenza di applicazioni, piattaforme e dispositivi fisici e consentendone la gestione da remoto, espongono a nuove potenziali criticità non sempre riconducibili al solo "patrimonio informativo" di un'azienda.

CPS

L'utilizzo dei Cyber Physical System consente di controllare da remoto sistemi fisici per mezzo di componenti software. In tale contesto assume particolare criticità l'integrità del software di controllo e dei comandi trasmessi alle componenti fisiche gestite.

Realtà Virtuale nelle aziende

Sempre più spesso si parla di realtà virtuale / aumentata e dei potenziali nuovi scenari di applicazione anche in ambito aziendale con particolare riferimento alla ridefinizione delle proposizioni commerciali, di marketing e di comunicazione nei confronti della clientela.

Di questo avremo modo di parlarne a "Banche e Sicurezza 2017" …

Grazie per l'attenzione

Flavio Paolinelli (flavio.paolinelli@intesasanpaolo.com)
Enterprise Security
Responsabile Infrastructure Security