Solo insieme si vince

Verso un’ecosistema unificato di soluzioni per la sicurezza

Francesco Palmieri

Dipartimento di Informatica

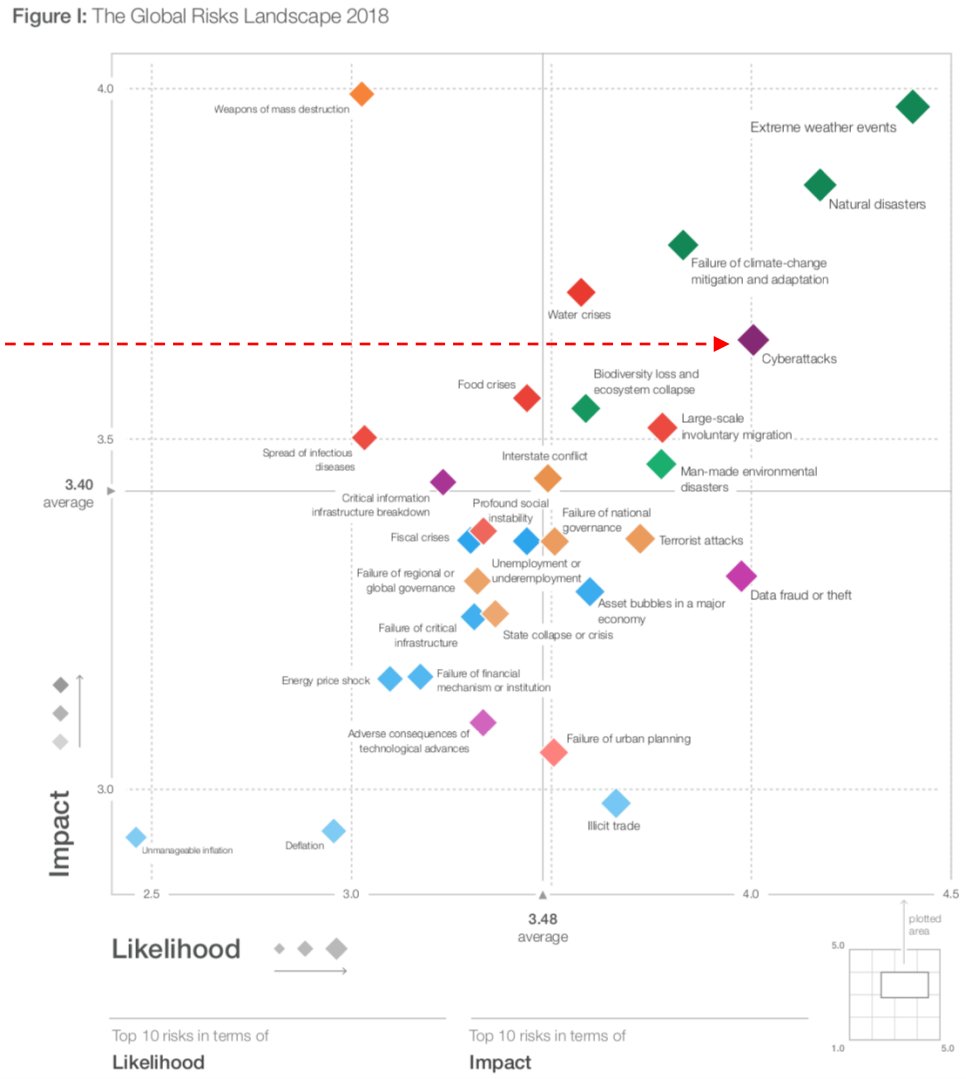
Università degli Studi di Salerno

Il rischio Cybersecurity

Rischio di Attacchi cyber

Superato solo da:

- Armi di distruzione di massa
- Eventi meteorologici estremi
- Disastri naturali
- Cambiamento climatico
- Mancanza d'acqua



- Fonte: world Economic Forum (Davos 2018): The Global Risks Report 2018 13th Edition

Valore a rischio ed impatto economico

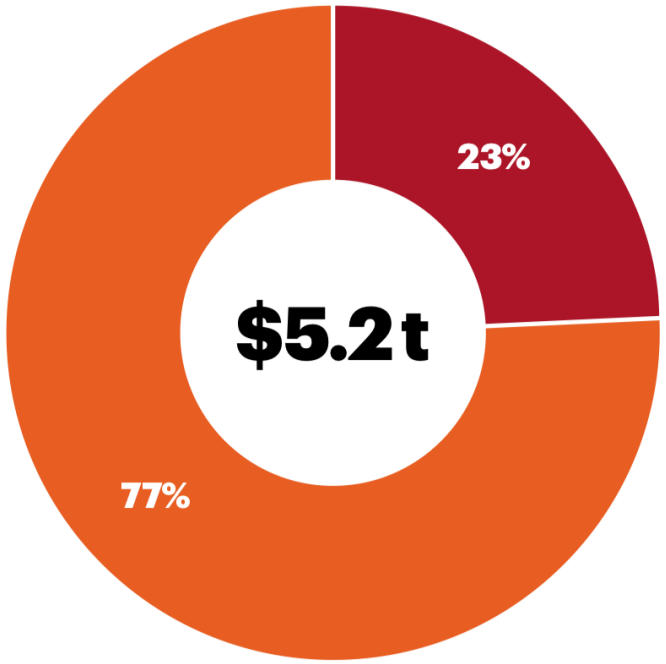
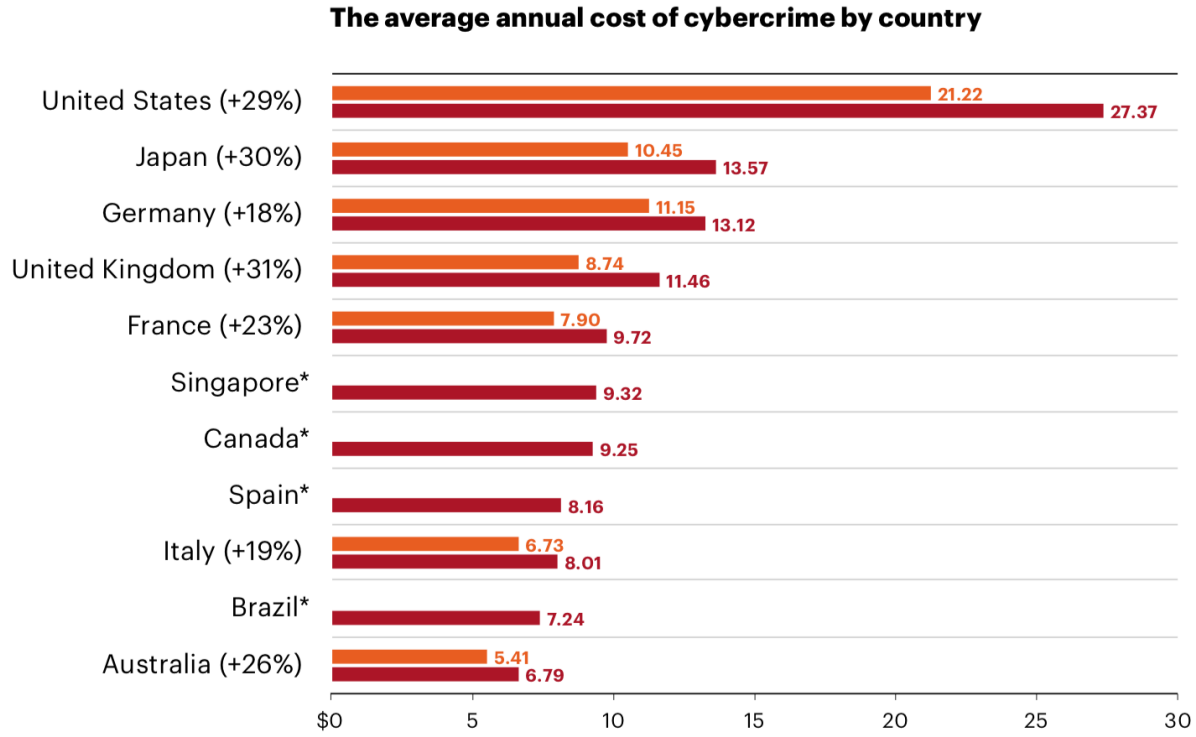


FIGURE 5
Value at risk globally from direct and indirect cyberattacks (Cumulative 2019 to 2023)

Legend
- Value at risk from direct attacks
- Value at risk from indirect attacks



Fonte: Accenture - ANNUAL COST OF CYBERCRIME STUDY

Radar delle minacce

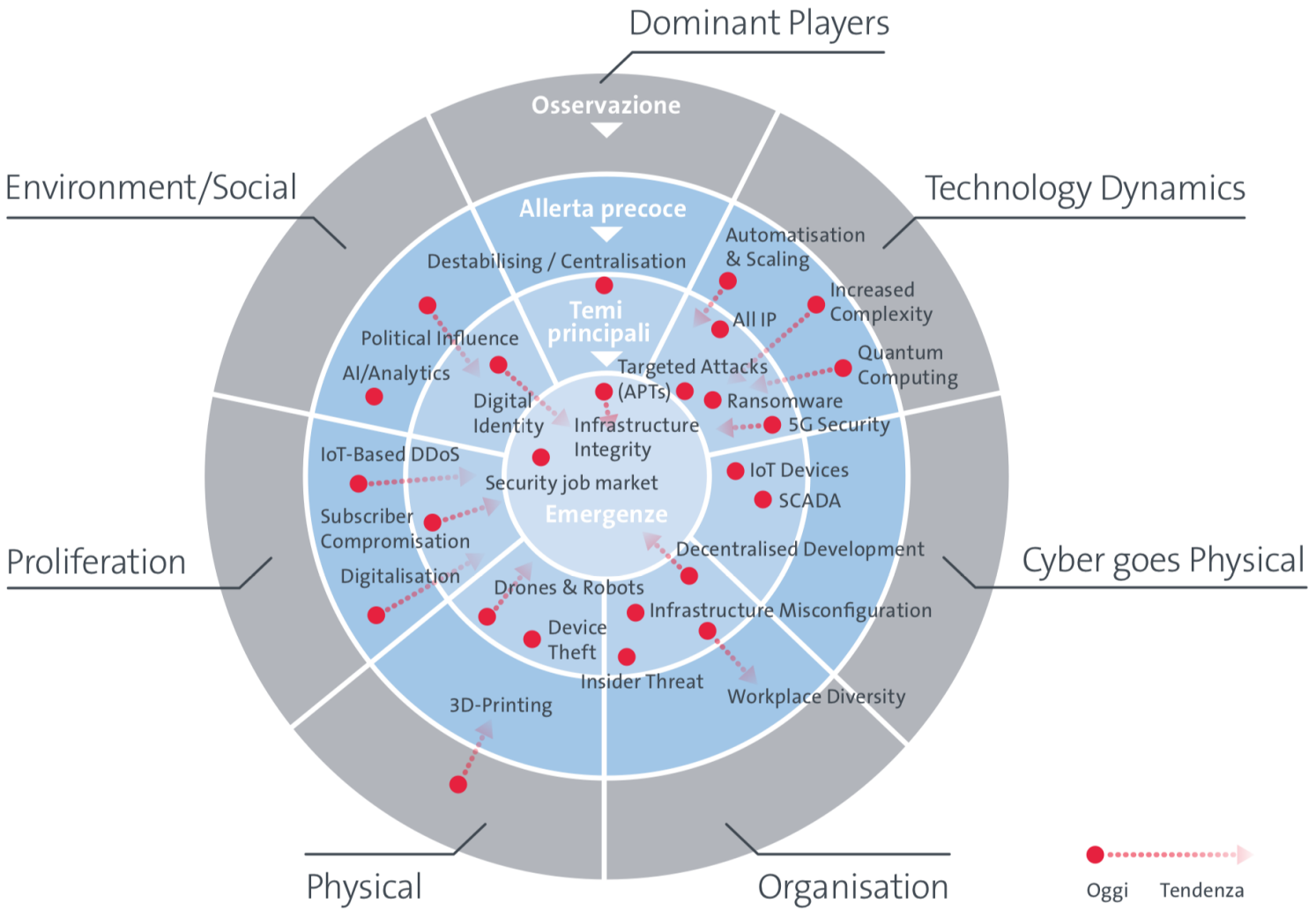
Il radar delle minacce è diviso in sette segmenti che delimitano i diversi domini delle minacce.

I cerchi indicano:

- l'attualità della minaccia
- l'approssimazione della sua valutazione

Più la minaccia è vicina al centro

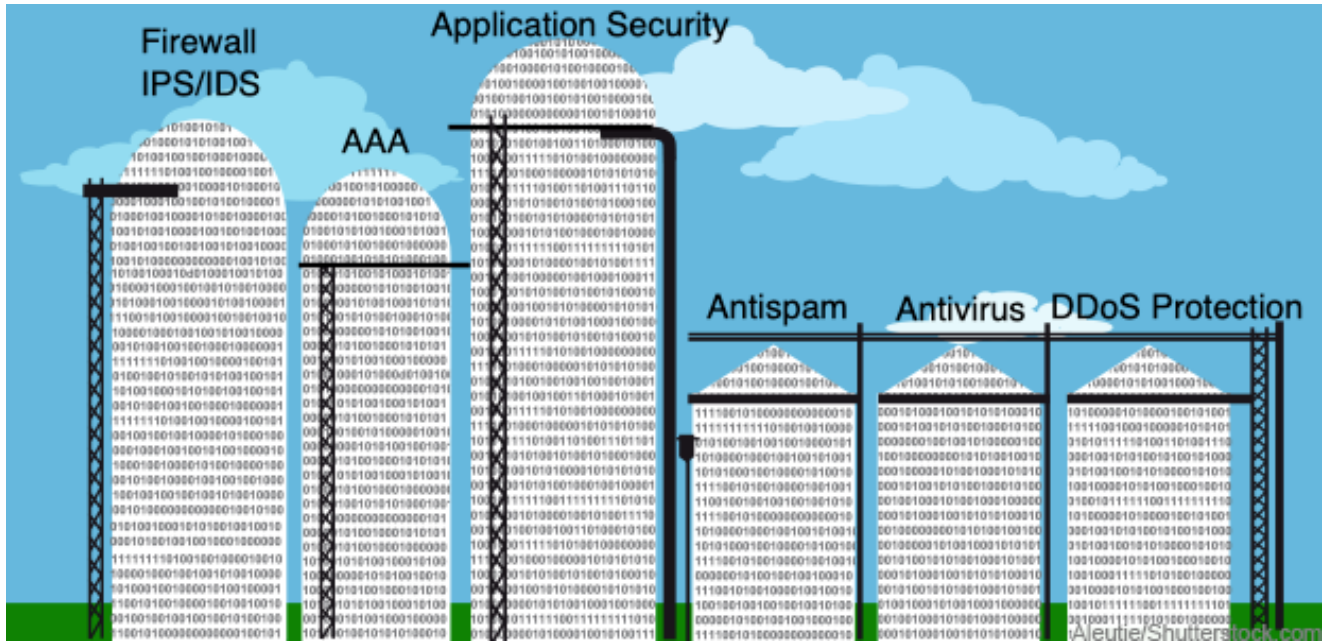
- più è concreta
- più strategiche sono le contromisure necessarie.



Fonte: Swisscom: cyber Security Report

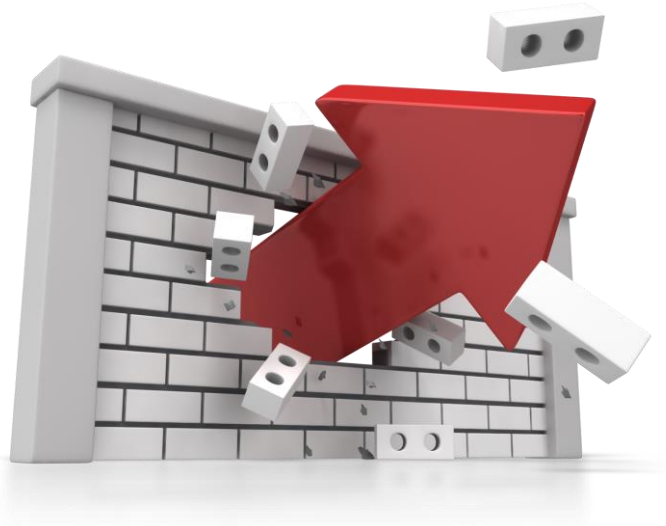
Il problema: Siloed Security

- Nelle attuali organizzazioni coesiste un'eterogenità di sistemi e prodotti (spesso anche ridondati) e approcci diversi alla sicurezza
  - Security Endpoints, Antivirus, antispyware,
  - Firewall, honeypot, Intrusion Detection System, Intrusion Prevention System, sistemi crittografici, sistemi di autenticazione
  - Soluzioni di backup o per resilienza/affidabilità
- Responsabilità differenziate
  - ognuno gestisce un pezzo di sicurezza
- Soluzioni integrate in tempi diversi
- Obiettivi di gestione diversi:
  - funzionamento delle reti e dei server
  - controllo accessi
  - operatività applicazioni etc.
- Limitata Interoperabilità
  - Soluzioni/interfacce legacy
  - Mancanza di standard



Cambiare Vision e Approccio

- Bisogna partire da una nuova visione architetturale:
  - perimetro liquido
    - fine concetto sicurezza perimetrale
  - utenti mobili
  - connettività ubiqua e erogata da soggetti multipli
    - Scomparsa reti proprietarie
    - Combinazione di fornitori accesso (e.g. 5G)
  - dati e applicazioni delocalizzati in cloud
    - Problemi di soveregnity
    - Limitazioni capacità di intervento

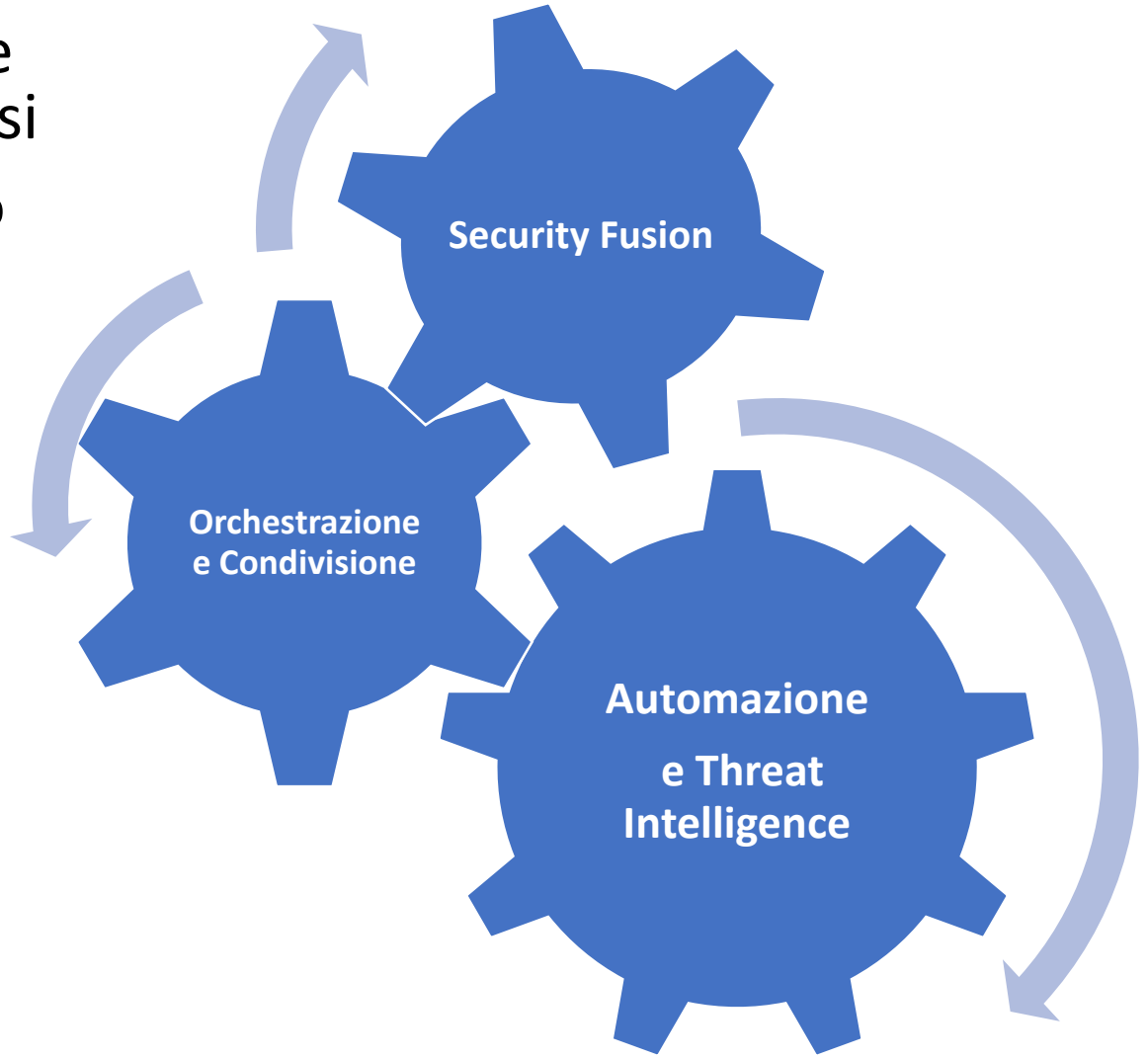


- Approccio **olistico** e **collaborativo** alla sicurezza
  - **Consapevolezza** dei rischi e minacce
  - **Integrazione** fra sistemi di sicurezza
  - **Condivisione** informazioni per migliorare la visione
  - **Cooperazione** per un azione coordinata più efficace

Security by Design

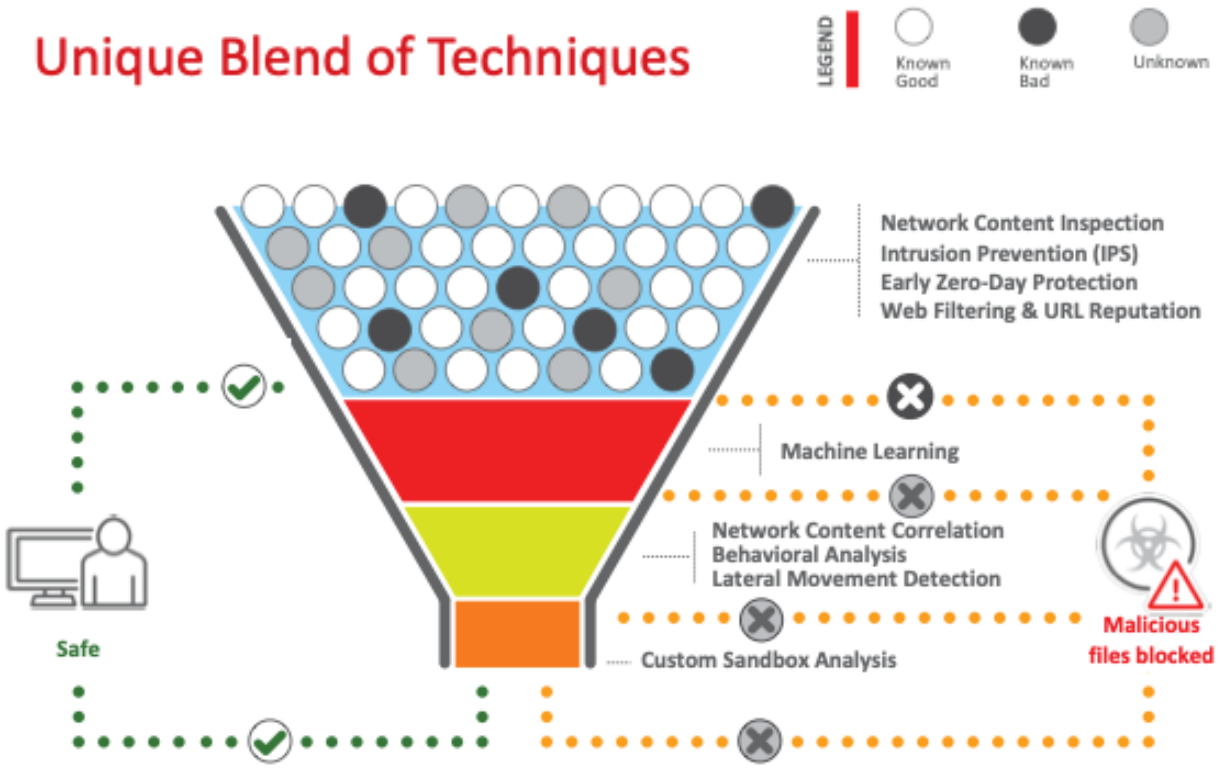
- Concetto di sicurezza nativa, partendo dalle infrastrutture di rete e dagli oggetti connessi
  - Architetture e applicazioni vanno progettate ab inizio per offrire garanzie di sicurezza
  - Servono standard e interfacce comuni per garantire l'interoperabilità fra sistemi
  - L'integrazione fra prodotti deve avvenire attraverso l'utilizzo di API open
  - Va migliorata capacità di reazione attraverso principi di coalizione quali condivisione e correlazione di conoscenza

- **Security Fusion**
- **Orchestrazione** e **Condivisione**
- **Automazione e Threat Intelligence**



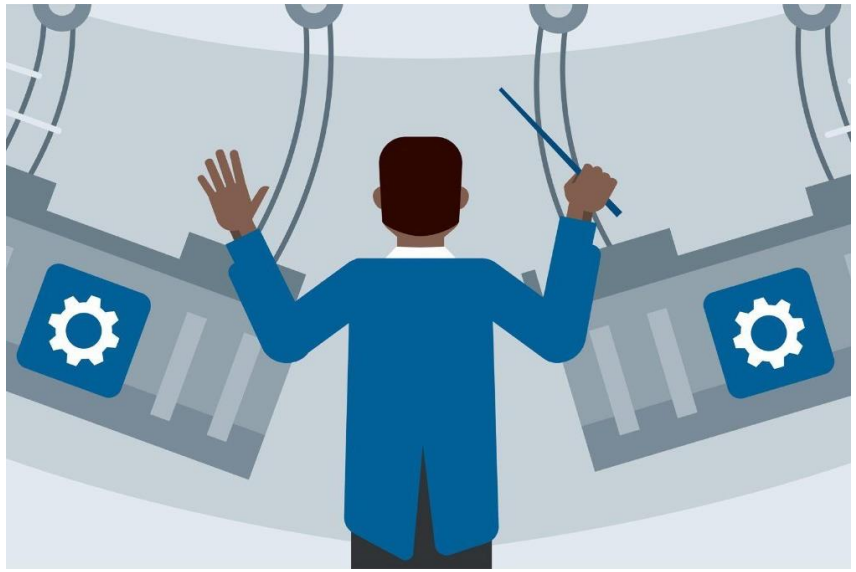
Security Fusion

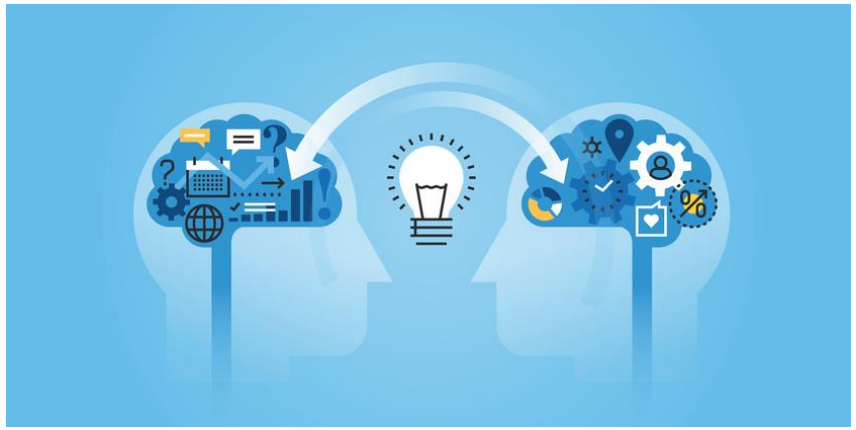
- Consolidamento di multipli componenti funzioni in **una singola entità decisionale** del punto di vista di gestione della sicurezza
  - Operazioni più coordinate ed efficienti
  - Tempi di reazione più veloci
  - Ogni computer, applicazione, agent, dispositivo, diventa un sensore connesso in grado di fornire informazioni utili alla sicurezza
- Integrazione funzioni gestionali e gruppi di lavoro
  - SoC,
  - NoC,
  - Application Security,
  - Developers



Orchestrazione e Condivisione

- **Ecosistema di protezione** in grado di incrementare le difese in ottica di:
  - **Prevenzione**: bloccare attacchi prima che raggiungano gli asset vulnerabili
  - **identificazione delle minacce**: per bloccare attacchi prima che raggiungano gli asset vulnerabili
  - **Dinamicità e adattatività**: aggiornamenti in tempo reale delle contromisure e policy
- La **correlazione** di eventi rende possibile decisioni orientate da **context awareness**
  - visibilità centralizzata e integrata su tutti gli strati di sicurezza fornisce una vista più completa del problema
- Le decisioni nascono da **conoscenza collettiva** e **condivisa**
  - condividere le informazioni accelera i tempi di risposta
  - le informazioni condivise tra tutti i prodotti e gli ambienti consente una risposta cooperativa





Ecosistema di Protezione

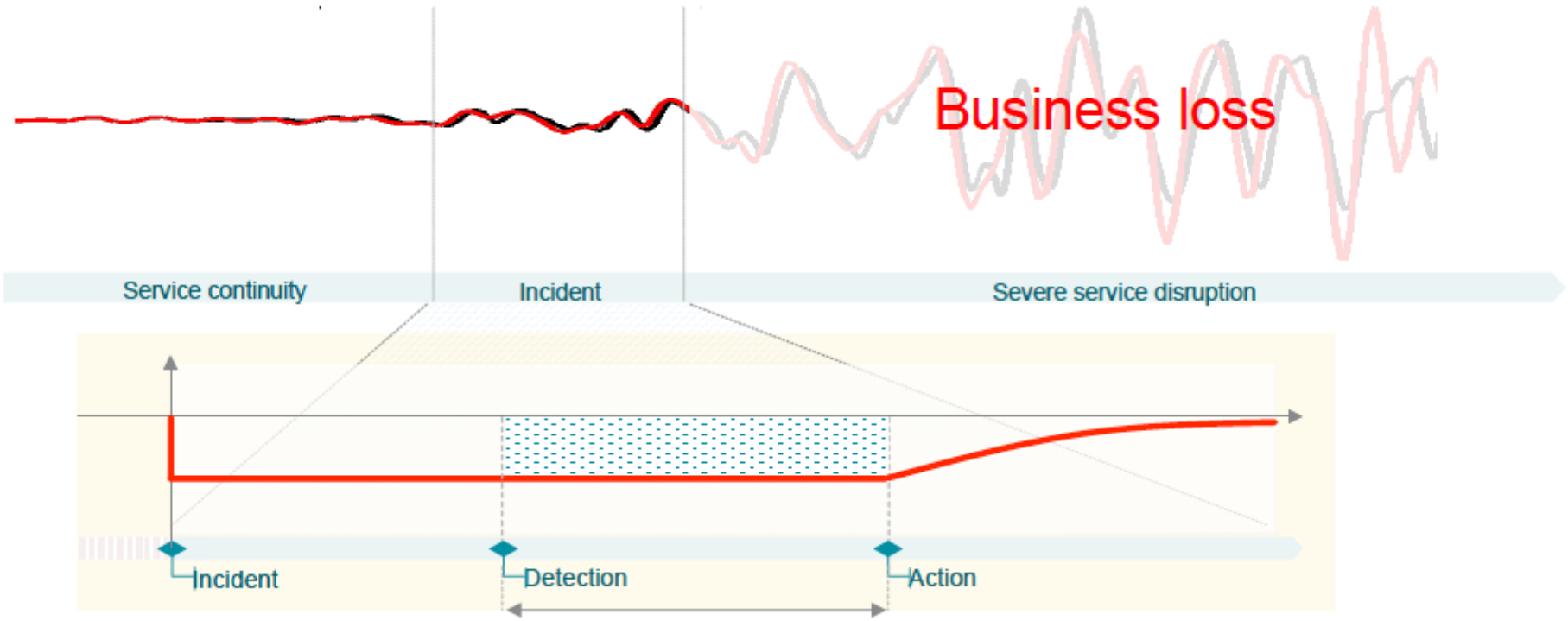
- **Firewall:** gestione centralizzata dei criteri/politiche di protezione
  - Implementazione politiche controllo accessi
  - Ispezione bidirezionale per filtraggio granulare del traffico
  - tracciamento e logging
- **Intrusion Detection/Prevention:** difesa da vulnerabilità note o zero day
  - Web App Protection e protezione applicazioni legacy
  - Ispezione del traffico per individuazione attacchi o violazione delle policy
  - Copertura vulnerabilità/exploit via Virtual Patching
  - Sandboxing per analisi cooperativa nuove minacce
- **Content filtering & Web Reputation**:
  - Blocco accesso a URL dannosi o contentuti non consentiti
- **Integrity Monitoring**: individuazione in tempo reale di cambiamenti sospetti
  - Monitoraggio sistemi e applicazioni critiche
  - Variazione a policy di sicurezza e controllo accesi
- **Log inspection**: automatizzare l'analisi dei Log e di generazione alert.
  - Ottimizzazione e generazione dinamica regole di filtraggio
  - Interfaccia con i sistemi SIEM
- **Antimalware**: protezione in tempo reale dispositivi e applicazioni
  - Real Time Scan
  - Remediation
- **Application Control**: gestione e controllo applicazioni
  - monitoraggio dell'esecuzione di software sui sistemi controllati
  - Controllo accessi e autorizzazioni via API

Automazione e Threat Intelligence

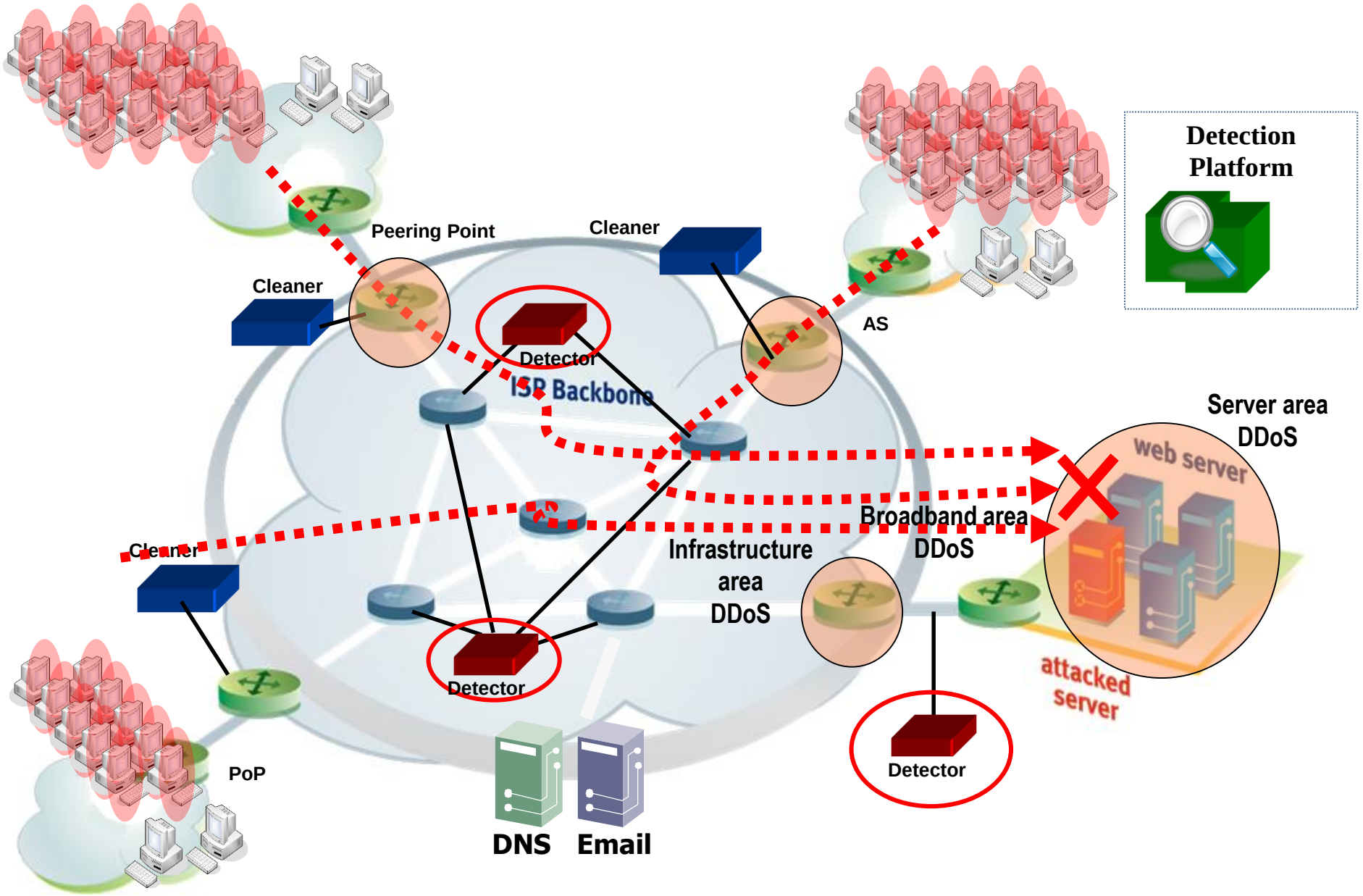
- Piattaforme automatizzate che includono anche componenti di intelligenza artificiale per il supporto alle decisioni
  - Machine learning
  - Nuovi modelli di DSS
  - Sentiment Analysis
  - Anomaly Detection
  - Agenti intelligenti e reazione autonoma
- Introduzione threat intelligence
  - Gestione e reporting degli incidenti
  - Security data Analytics
  - Assessment del rischio
  - Elaborazione modelli predittivi di attacco
  - Definizione strategie e tattiche di sicurezza

Obiettivi

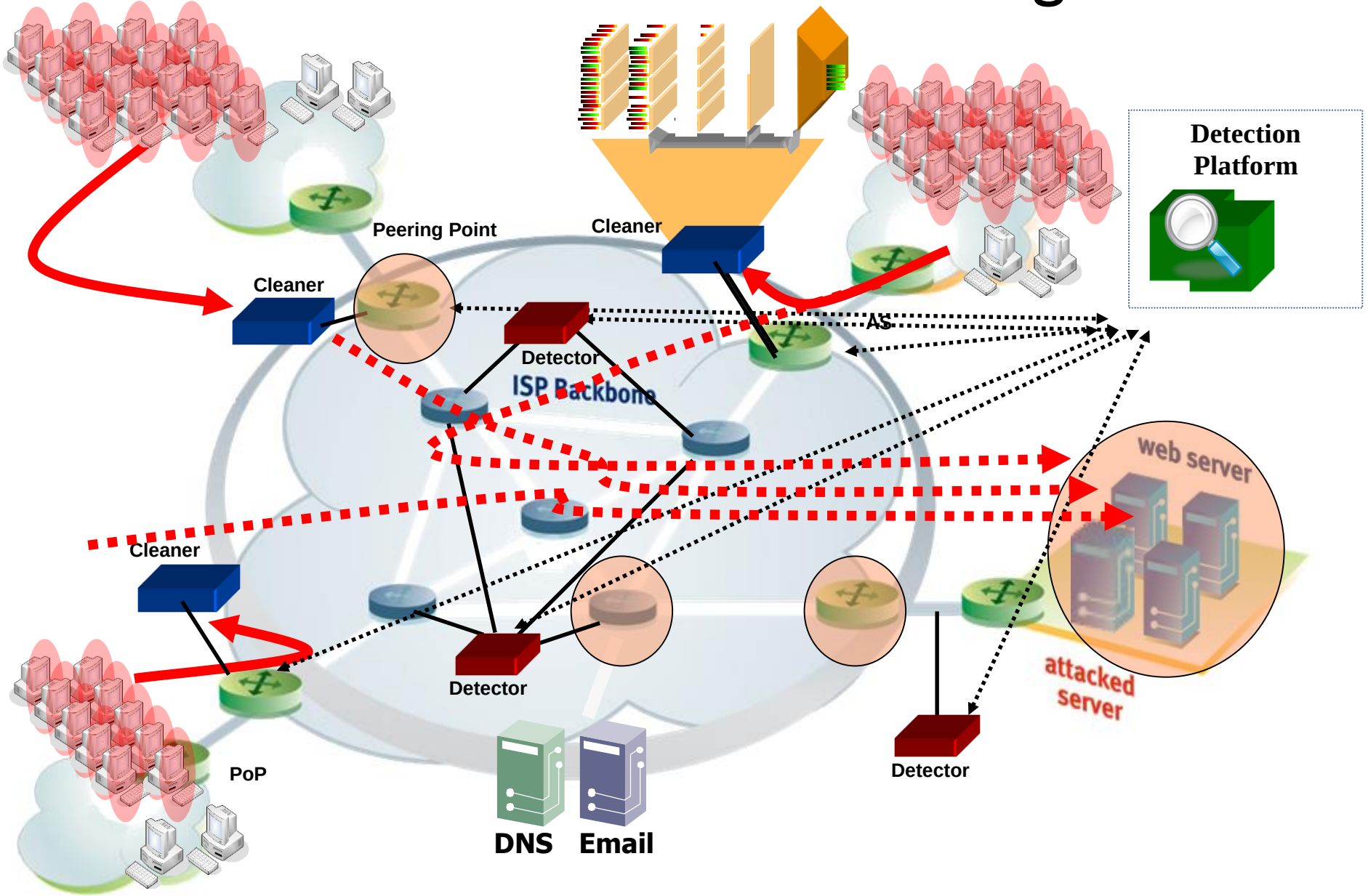
- Allerta rapida attraverso sistemi di early warning
- **Compressione della timeline per ridurre discontinuità**
- **Reazione coordinate a grandi attacchi**



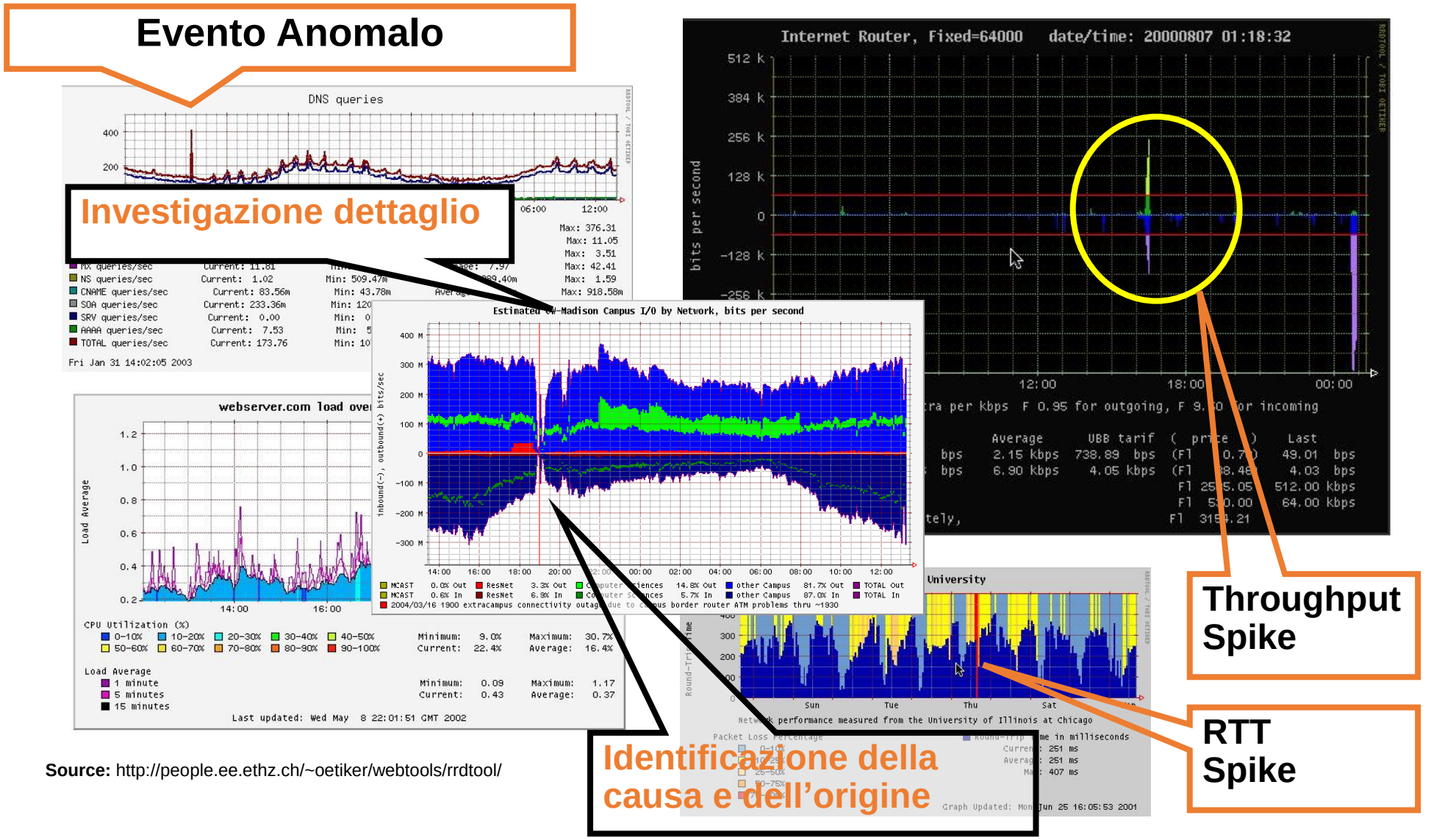
Reazione coordinata: Detection



Reazione coordinata: Cleaning



Centri comuni di controllo e monitoraggio



Source: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

Q & A?

Grazie per l’attenzione…