MCIPLab.it

ROMA TRE UNIVERSITÀ DEGLI STUDI

EVENT MANAGEMENT COME CONTRIBUTO ALLA CYBERSECURITY IN AMBITO INDUSTRIALE

RICCARDO COLELLI

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

EMAIL: RICCARDO.COLELLI@UNIROMA3.IT

EVENTO: GESTIONE DEL RISCHIO IN SISTEMI INTERDIPENDENTI: LA PROBLEMATICA CYBER-FISICA

DATA: 29 OTTOBRE 2019

SOMMARIO

- Introduzione alle minacce cyber
- Strategie di detection
- Soluzioni industriali
- Smart Extension
- Conclusioni

IT

Confidentiality

Confidentiality
Integrity
Availability

OT

Availability

Availability
Integrity
Confidentiality

Internet of Things

SISTEMI CYBER-FISICI

- Combinare il processo fisico con le risorse computazionali in un framework interconnesso
- Espone i sistemi di controllo a nuove vulnerabilita e minacce legate alla interdipendenze tra il mondo cyber e quello fisico
- Necessità di un rilevamento e identificazione appropriati

ALCUNI ESEMPI

- Distribuzione acqua e gas
- Generazione e distribuzione di energia elettrica
- Rete di trasporto

ATTACCO CYBER

Un attacco cyber è una qualsiasi azione offensiava per mezzo di singoli individui o di organizzazioni che prende di mira reti di calcolatori, infrastrutture e/o dispositivi personali.

- Attacchi attivi
  - Denial-of-service (DoS)
  - Man-In-The-Middle (MITM)
- Malware
  - Virus
  - Worm
  - Trojan
  - Ransomware

CATEGORIE DI ATTORI MALEVOLI

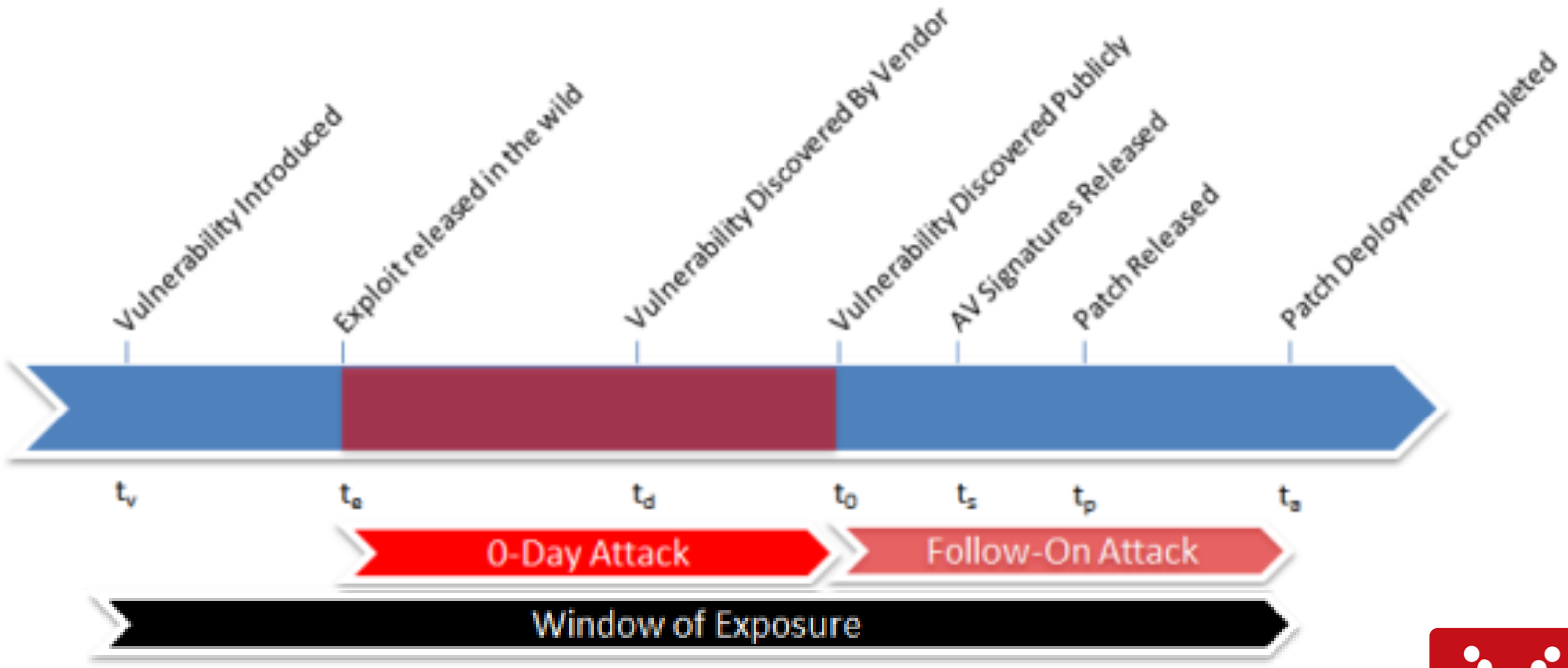
Script kiddie: un individuo con poche skills che usa script o programmi sviluppati da altri al fine di attaccare computer o una rete. Il loro obiettivo è quello di ottenere i privilegi di amministratore. La loro conoscenza del software implementato è bassa. Possono diventare pericolosi se agiscono in gruppi

Crackers: un individuo che tenta di forzare i blocchi imposti da un software per ottenere profitto. Questo individuo possiede una elevata conoscenza dell'informatica.

Insider: sono dipendenti o ex-dipendenti con intenti malevoli. Sono motivati da ragioni personali, sono molto preparati. Hanno piena conoscenza della struttura e del sistema.

ZERO-DAY ATTACKS

Una vulnerabilità Zero-Day si verifica quando un attaccante identifica una falla nella sicurezza. Nel giorno zero, i programmi di sicurezza non hanno ancora identificato una regola che potrebbe essere utilizzata per prevenire tale attacco.



ATTACCHI AI SISTEMI SCADA

Maroochy Water System (2000): un attacco causato da un ex-dipendente

Davis-besse centrale nucleare (2003): un attacco basato su uno Slammer worm che ha penetrato un computer privato all'interno della rete. Il monitoraggio di sicurezza è stato disabilitato per diverse ore.

Stuxnet (2010): malware creato per sabotare una centrale nucleare in Iran

ATTACCHI AI SISTEMI SCADA

Ukraine power grid (2015): considerato il primo attacco cyber su una rete elettrica, ha causato differenti blackout in Ucraina.

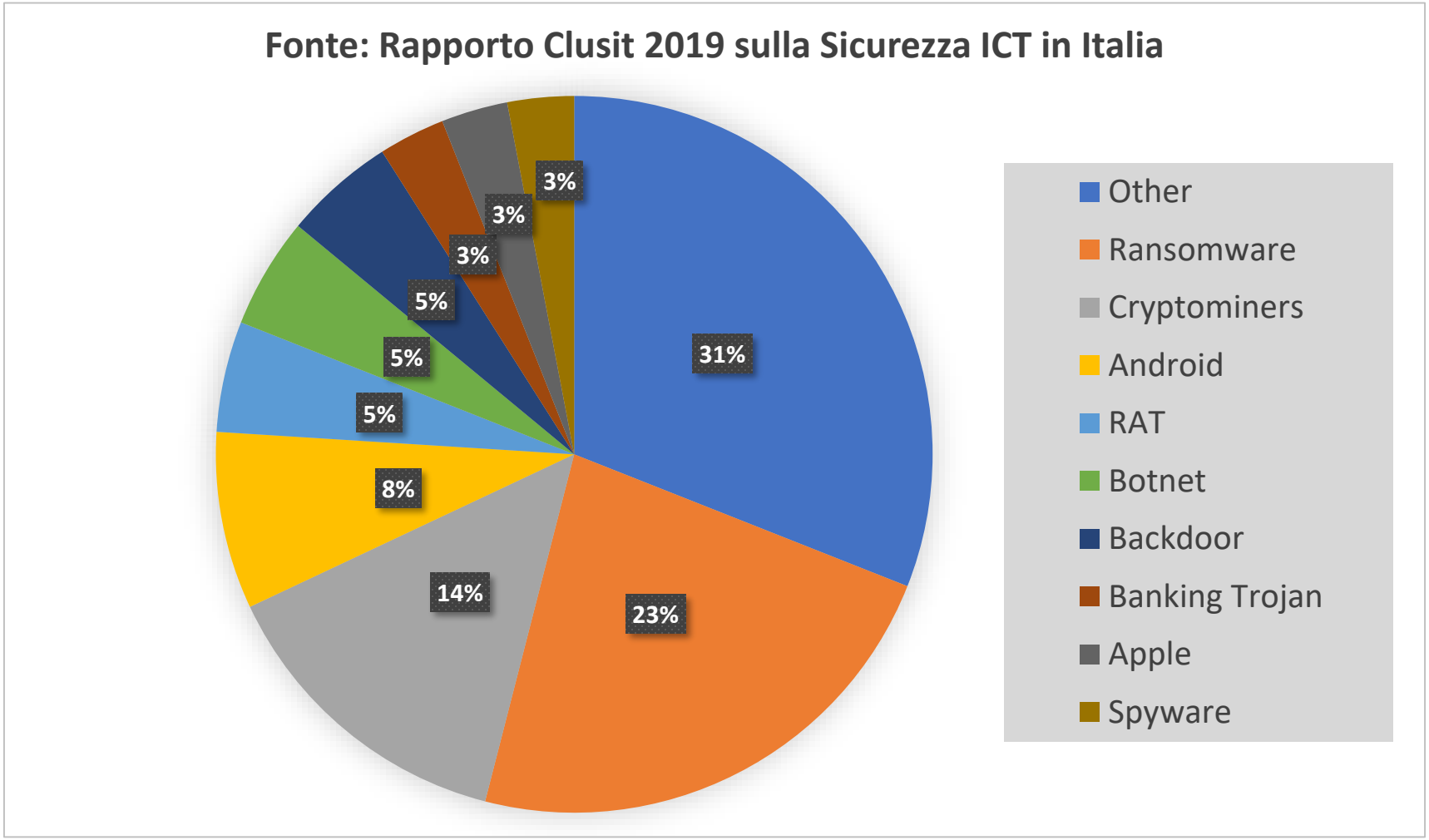
Trisis (2017): malware che prende di mira i controllori Schneider Electric's **Tri**conex **S**afety **I**nstrumented **S**ystem. Il malware è in grado di comunicare con il SIS, riprogrammandolo con istruzioni definite dall'attaccante o inviandogli specifici comandi per interromperne il funzionamento o leggere il contenuto della memoria.

L'EVOLUZIONE DEL CRYPTOJACKING

L'uso di malware per aumentare i profitti in cripto-valute degli aggressori

- **Norsk Hydro (2019):**Le celle per il monitoraggio dell'alluminio sono state impostate alla modalità manuale, arresto forzato di alcuni impanti, estrusori di metallo chiusi, computer inaccesssibili. Fortunatamente nessun incidente di sicurezza.

TIPOLOGIA E DISTRIBUZIONE MALWARE



STRATEGIE DI DETECTION

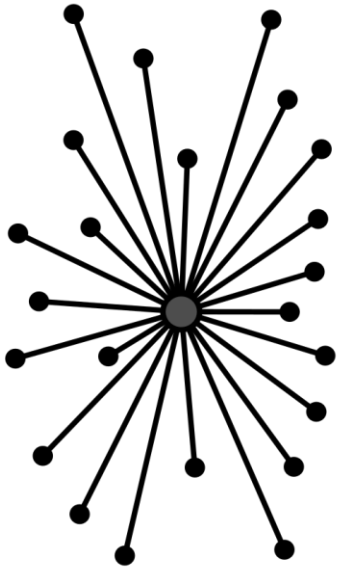
- **Advance detection**
  - Sistemi distribuiti implementati con NFV (Network Function Virtualization) e SDN (Software Defined Networking).
- **Configuration management**
  - Una risorsa in grado di notificare in caso di modifiche non autorizzate e in grado di ripristinare una modalità di sicurezza.
- **Continua identificazione delle vulnerabilità**
  - Detection di configurazioni sbagliate o pericolose.

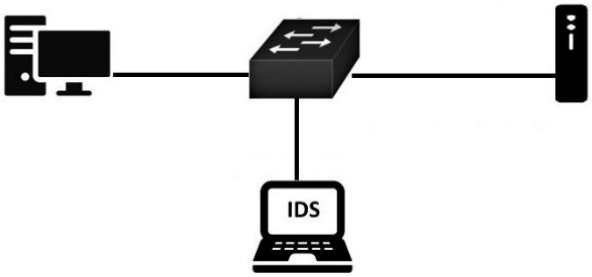
INTRUSION DETECTION SYSTEM (IDS)

Gli **IDS** sono strumenti passivi di una rete capaci di ispezionare il traffico sulla rete. In caso di anomalia, sono in grado di notificare un'allerta all'operatore.

- **Signature-Based**: una serie di regole di attacchi noti viene usata per gestire il traffico sulla rete.
- **Anomaly-Based**: il normale comportamento della rete è creato per delineare un profilo. Quando il comportamento si discosta da questo profilo si presenta una anomalia.

IDS NETWORK-BASED





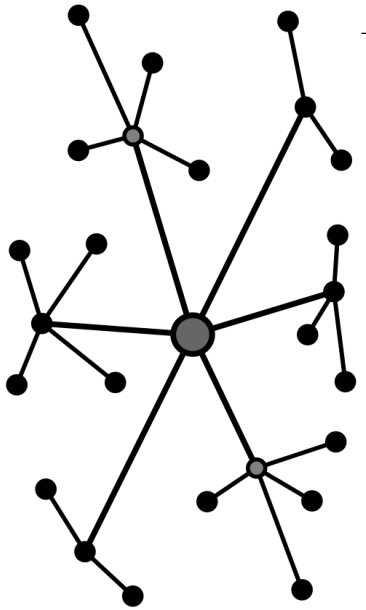
Pros

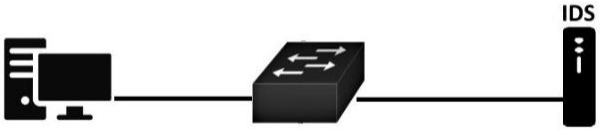
- monitoraggio di tutti I dispositivi
- non influenza le performance dei dispositivi sulla rete

Cons

- analizza un grande traffico
- porta di monitoraggio

IDS NETWORK-BASED





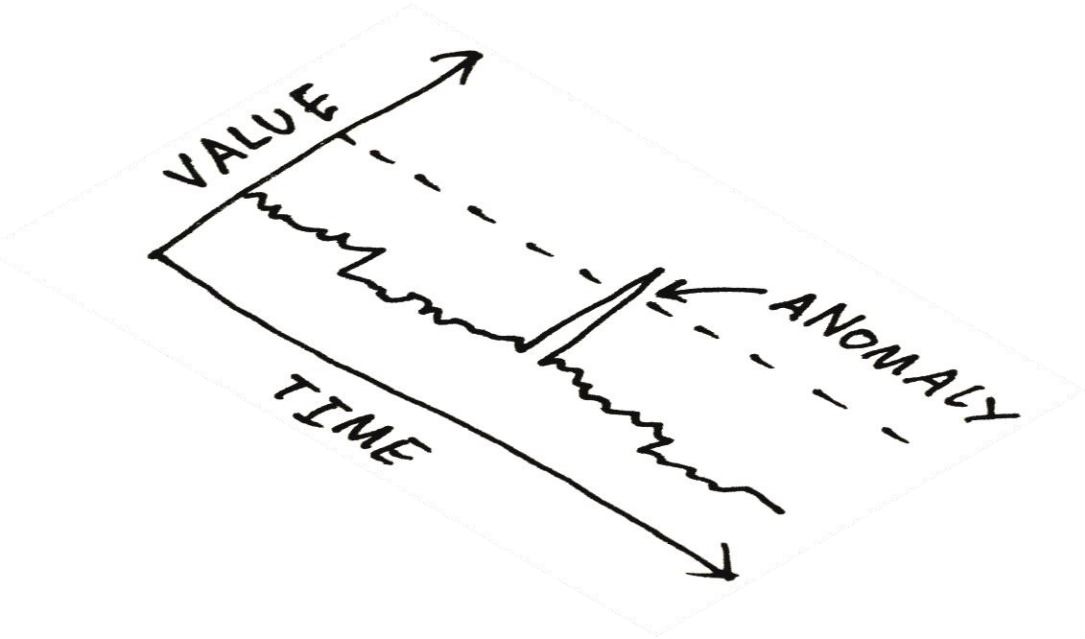
Pros

- ambiente criptato
- scalabile sulla rete

Cons

- mancanza della visione globale
- vulnerabilità legata al dispositivo (HW/SW)

COMPORTAMENTO ANOMALO DELLA RETE



- Identificare il comportamento anomalo è una soluzione contro gli attacchi zero-day.
- Quando un Network Behaviour Anomaly Detection (NBAD) software rileva un'anomalia, invia una allerta all'amministratore della rete.

- ✓ Payload Anomaly Detection
- ✓ Protocol Anomaly: MAC Spoofing
- ✓ Protocol Anomaly: IP Spoofing
- ✓ Protocol Anomaly: Duplicate IP
- ✓ Protocol Anomaly: Duplicate MAC
- ✓ Virus Detection
- ✓ Bandwidth Anomaly Detection
- ✓ Connection Rate Detection

SECURITY INFORMATION AND EVENT MANAGEMENT

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- **Raccolta dati**: invia i dati contenuti all'interno dei file di log al server

- **Parsing e normalizzazione**: provvede ad uniformare i dati raccolti, catalogandoli per tipo di dato.

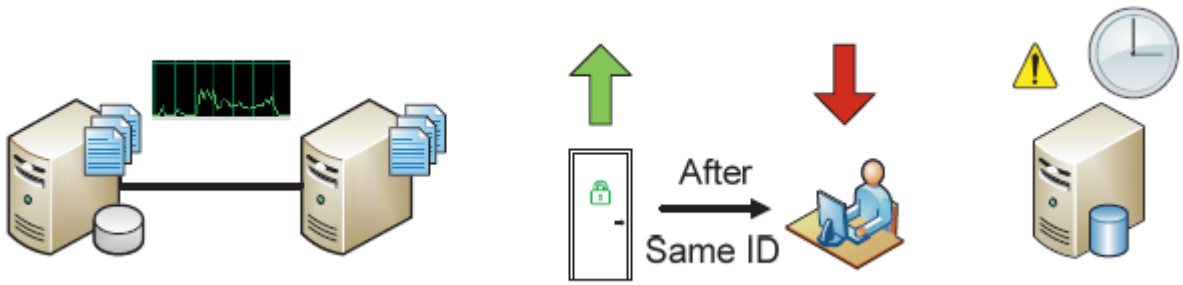
- **Correlazione**: basandosi sulla correlazione tra gli eventi di sicurezza e i dati sulle vulnerabilità presenti nel sistema è possibile attribuire una priorità ad un evento.

- **Reporting**: l'archiviazione dei dati a lungo termine unita alla possibilità di sfruttare query personalizzate per l'estrazione dei dati a scopo di audit o di analisi forense.

- **Dashboard**: forniscono una rappresentazione dei dati sotto forma di diagrammi o altri modelli.

- **Notifiche**: le segnalazioni posso avvenire tramite dashboard o utilizzando servizi come la posta elettronica o gli SMS.

ESEMPIO SIEM



1. Il badge di un dipendente è stato registrato dal sistema di controllo degli accessi in quanto la persona ha lasciato l'azienda.

2. Dopo 30 minuti, avviene un'azione di accesso al sistema con username/password che appartengono allo stesso dipendente

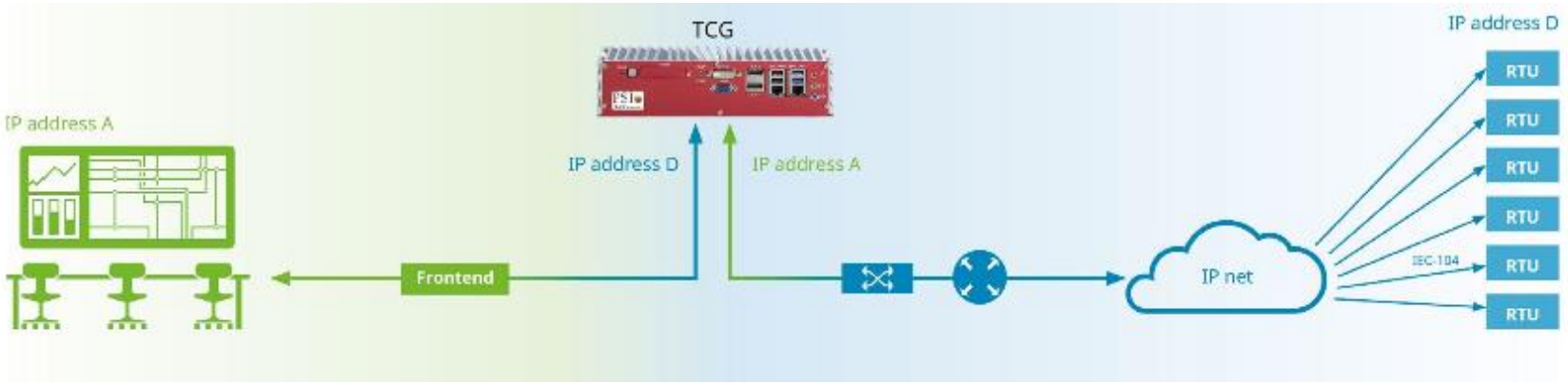
Ciascuna delle due azione è in linea con i relativi controlli di sicurezza.

DISPOSITIVI COMMERCIALI PER LA SICUREZZA INDUSTRIALE

- Prevenzione/individuazione di attacchi cyber in OT;
- Monitoraggio dei processi;
- Conforme ai protocolli industriali.

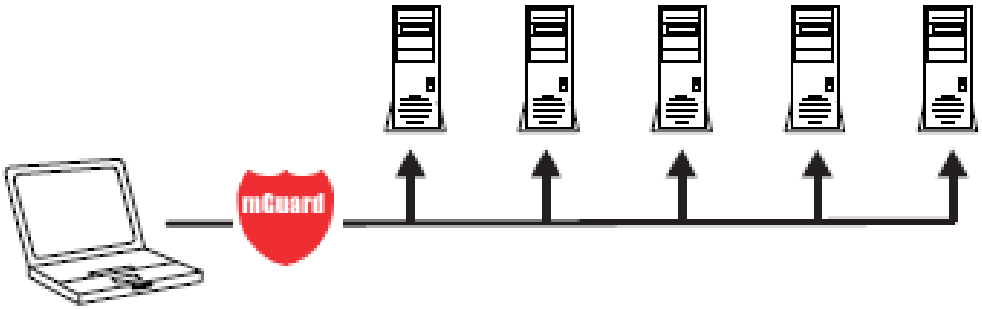
RTU 104 Security Proxy – PSI Nentec

- Installazione trasparente nell'ambiente già esistente senza riconfigurazione;
- Modalità di ascolto per più sistemi di controllo;
- filtraggio protocollo IEC 104;
- Proxy server.



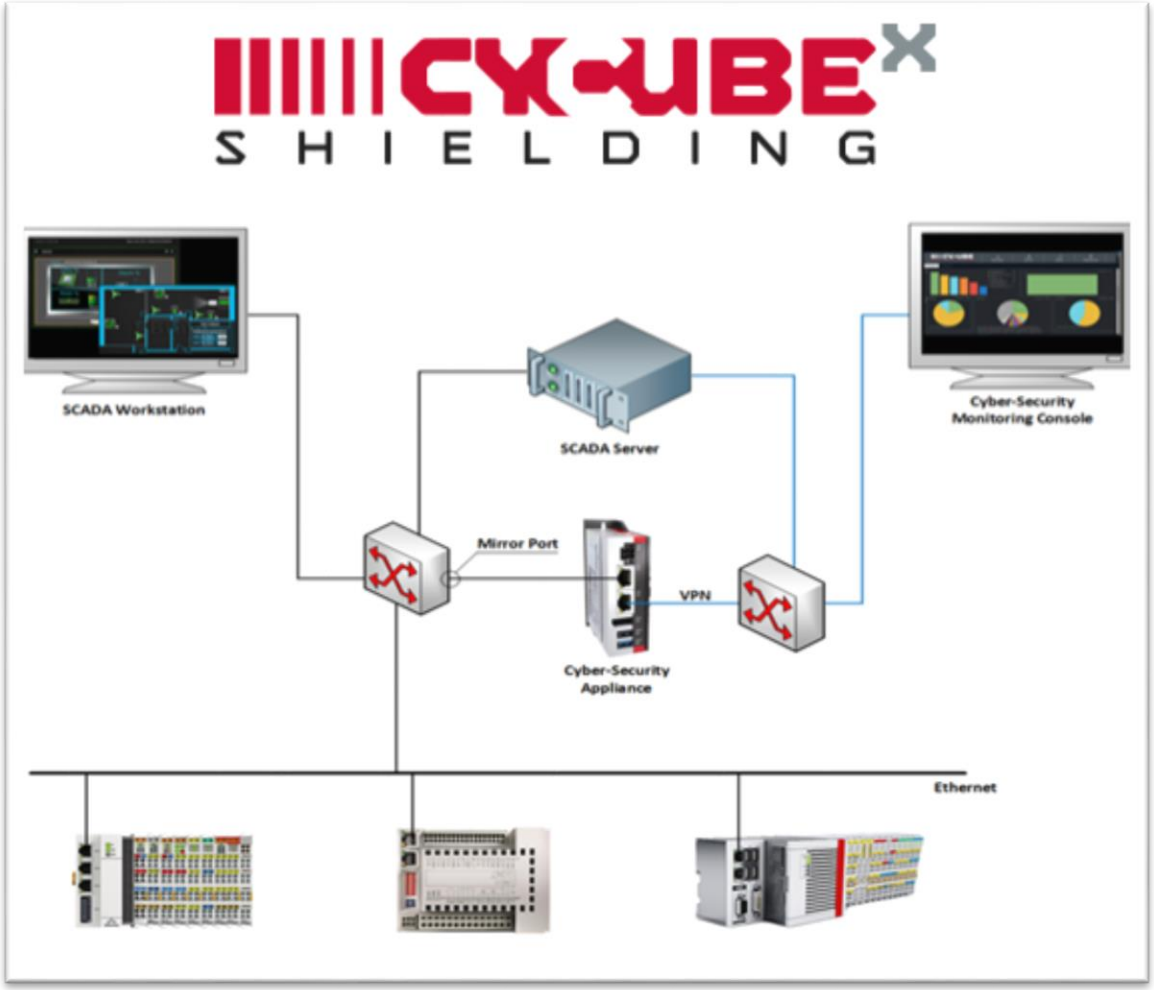
MGUARD – PHOENIX CONTACT

- Stealth mode (Plug-n-Protect)
- Network router
- DMZ (demilitarized zone)
- VPN gateway
- WLAN via VPN tunnel
- Resolving network conflicts



CYCUBEx – VITROCISET

- Analisi del traffico attraverso IDS/IPS per rilevare o prevenire attacchi nella rete,
- Controllo della comunicazione tra due o più dispositive attraverso firewall,
- Registrazione del traffico

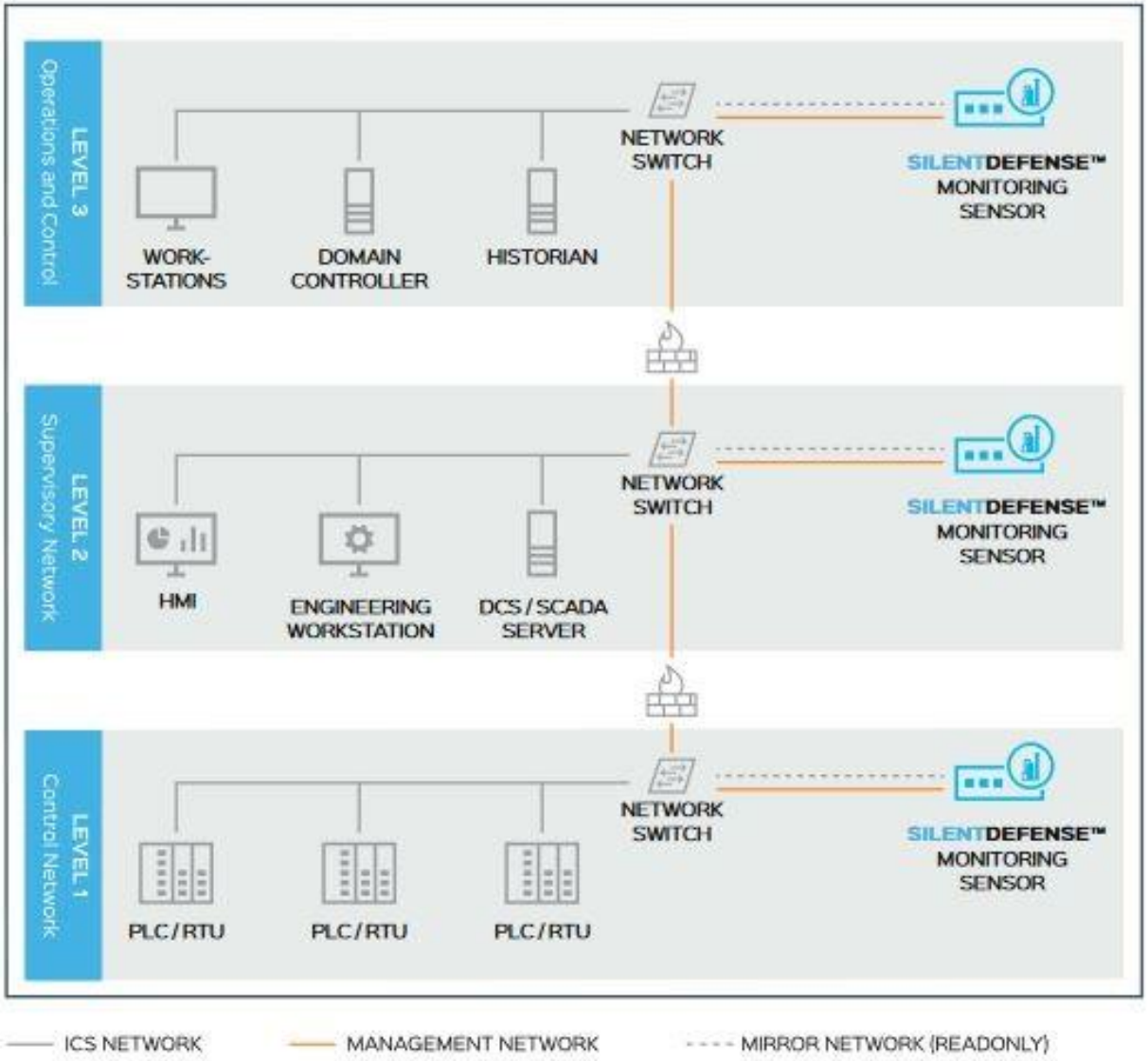


SCADAGUARDIAN – NOZOMI NETWORKS

- Identificazione degli asset, visualizzazione della rete e monitoraggio;
- Scalabilità dovuta alla Central Management Console;

- Integrazione e condivisione di informazioni di sicurezza nella infrastruttura IT/OT;
- compatibilità con tutti I prodotti NOZOMI.

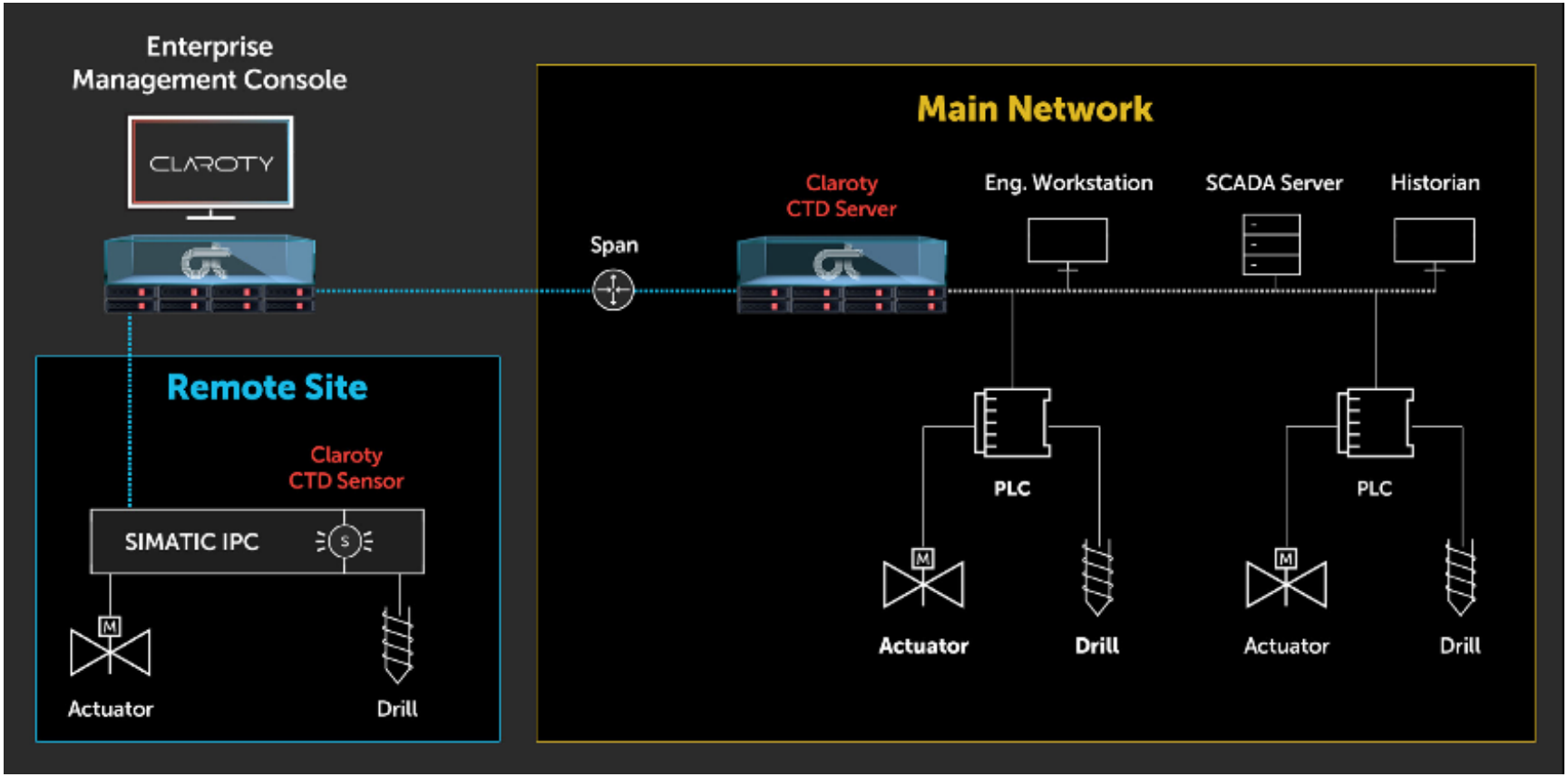
SILENTDEFENSE – SECURITY MATTERS



Analizza passivamente la rete industrial, fornisce informazioni riguardo **alerts** e **assets** in **real-time** per ogni minaccia.

Controllo dell'andamento di ogni singolo device.

SIEMENS AND CLAROTY



SIEMENS

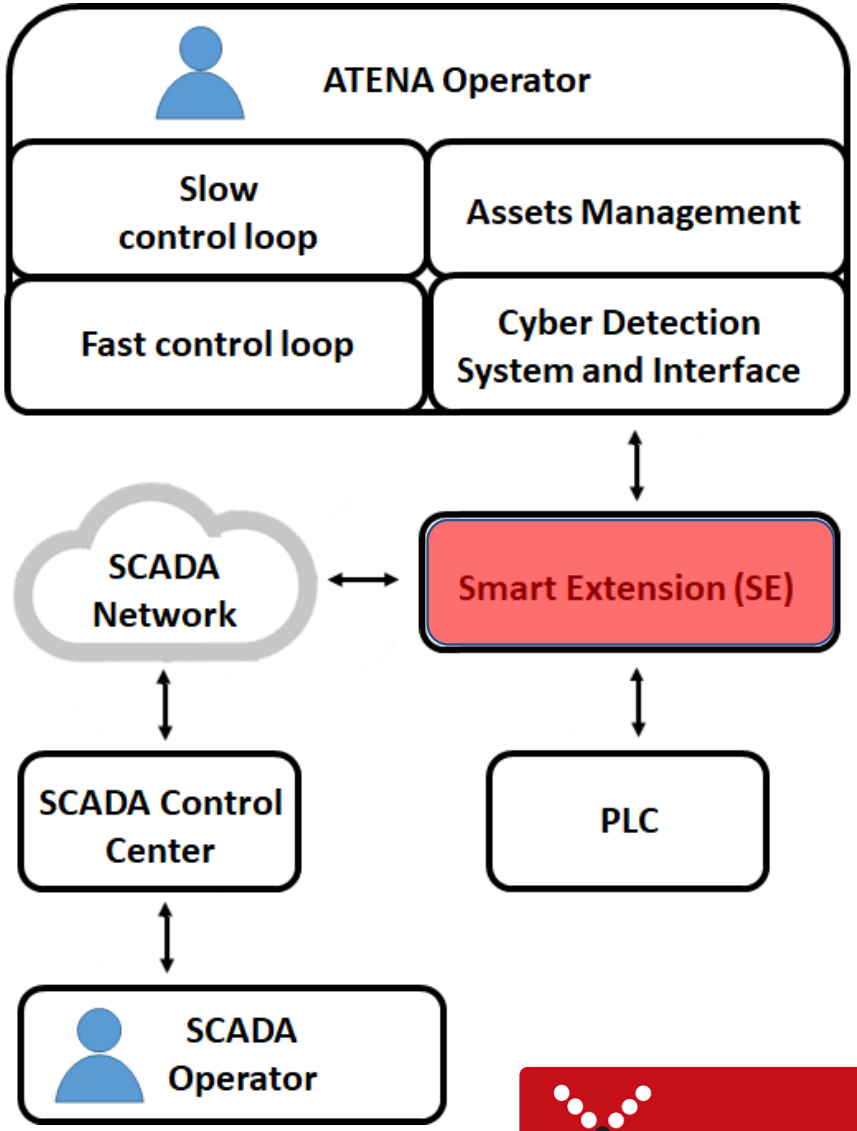
CLAROTY
Clarity for OT Networks

IL PROGETTO ATENA

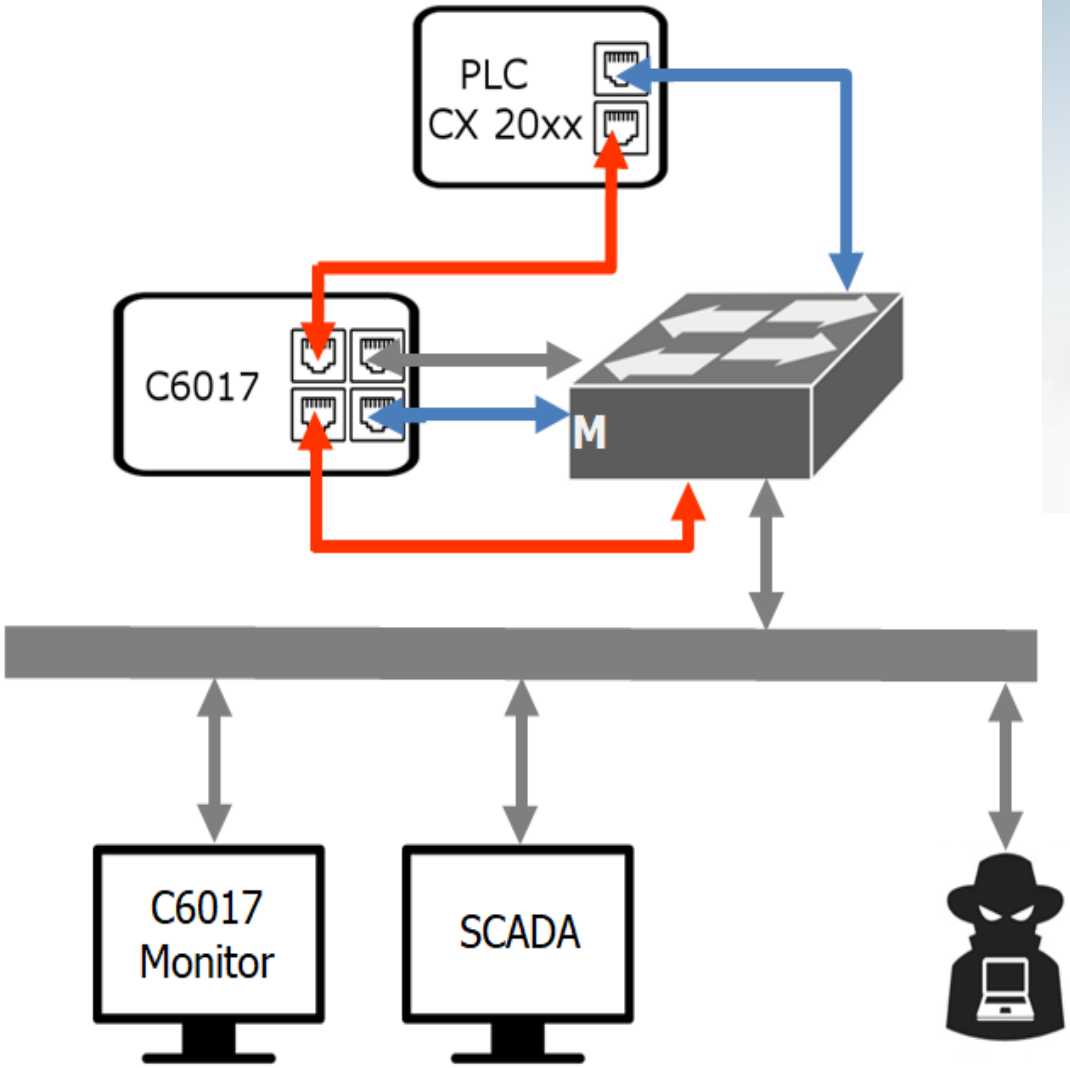
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

ATENA

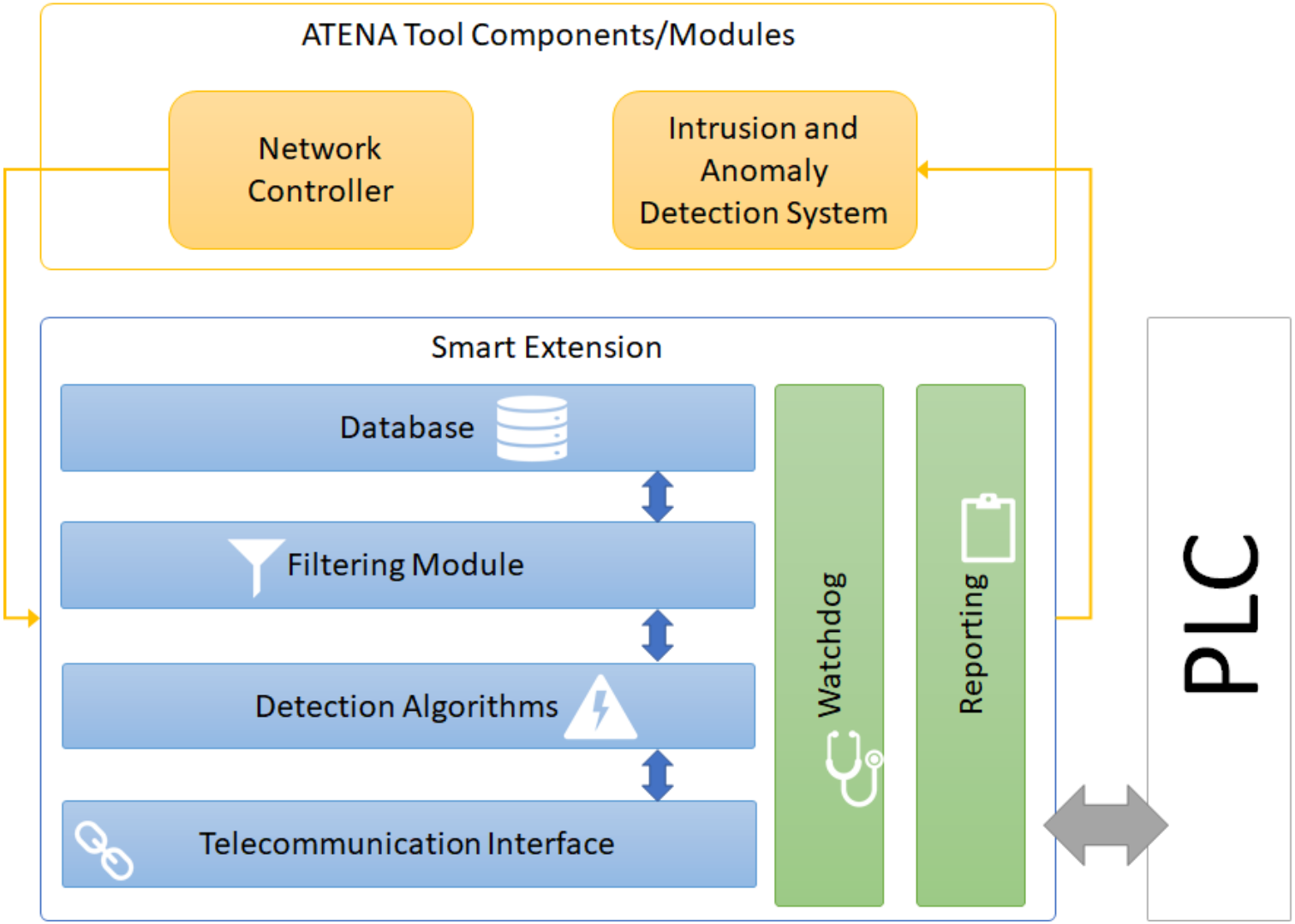
- **Duration**: 3 years for 899 person months
- **Budget**: 8.11 Mio€ funded by the European Commission at 6.9 Mio€
- **Consortium**: 7 countries, 3 Universities, 3 Research Centres, 5 International Cie and 2 SME



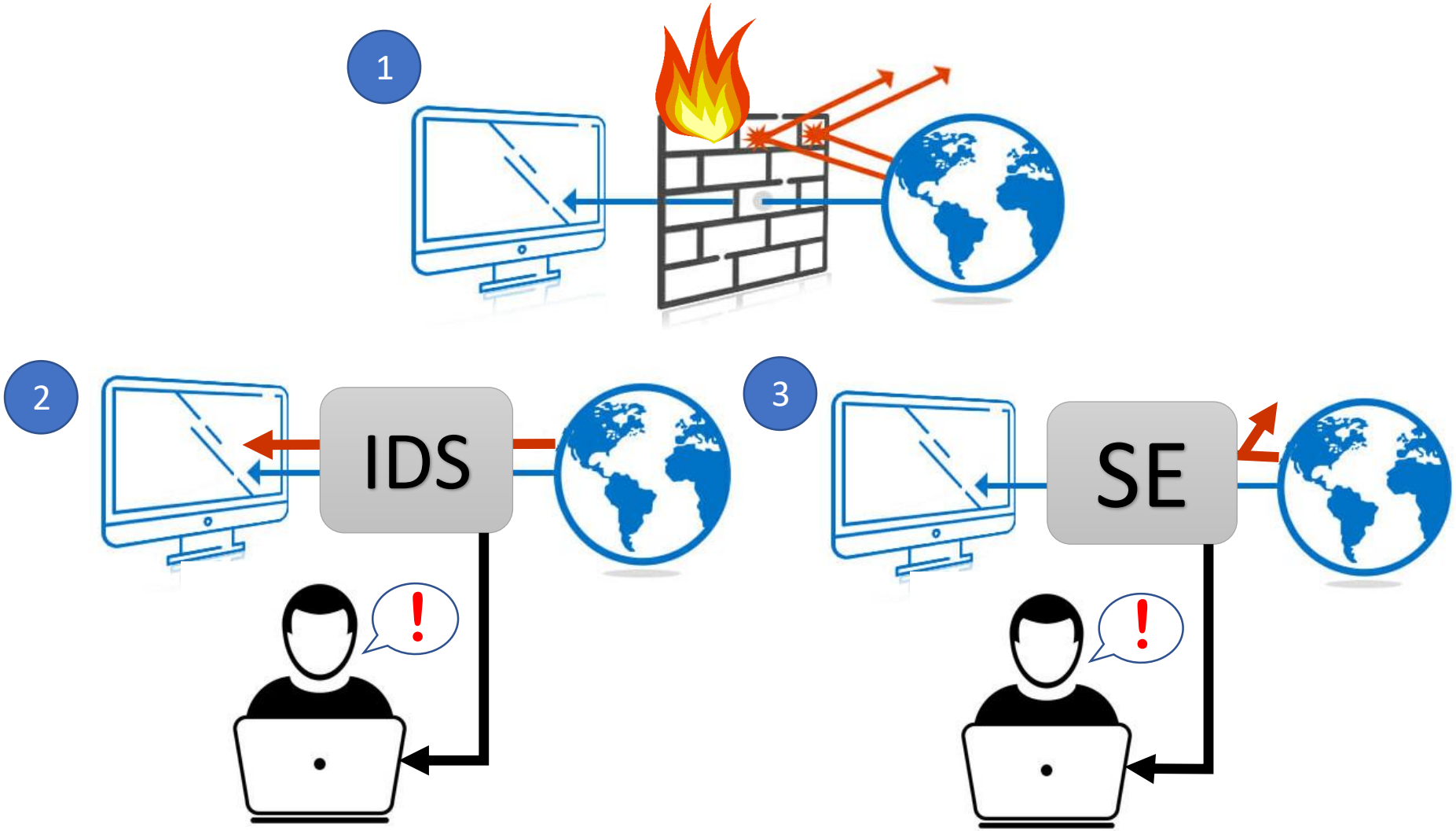
SMART EXTENSION



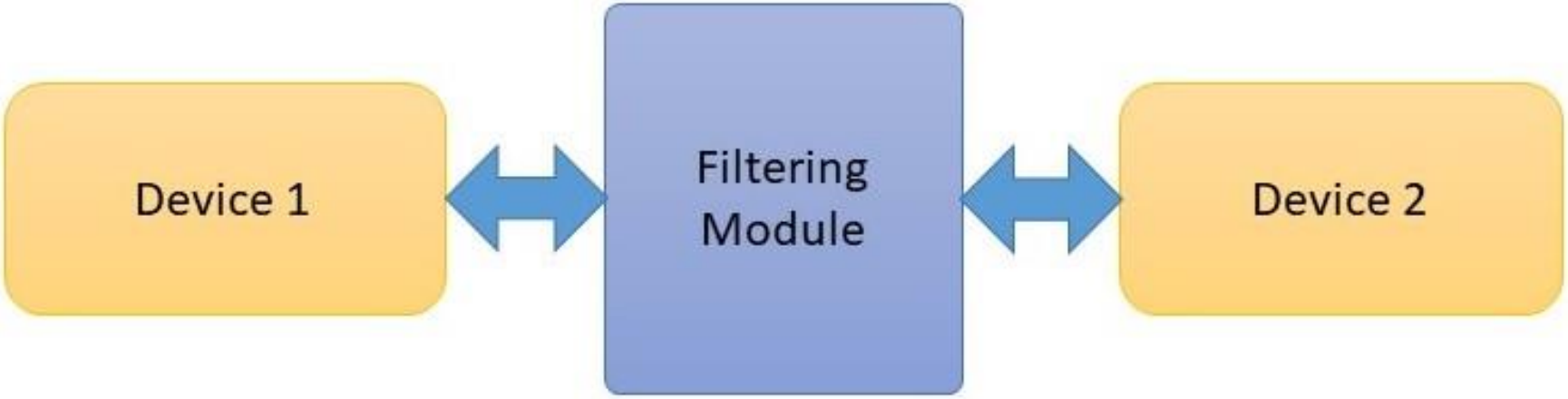
SE ARCHITETTURA



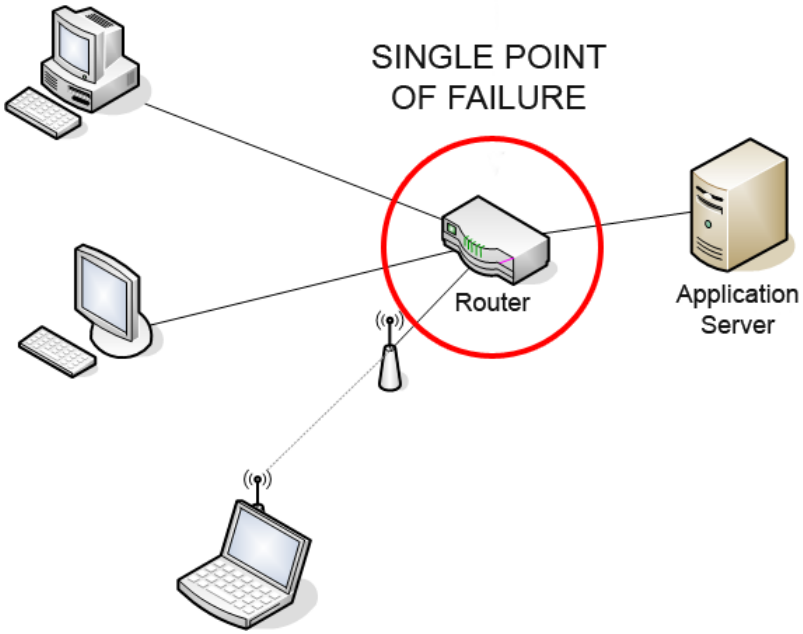
SMART FILTERING

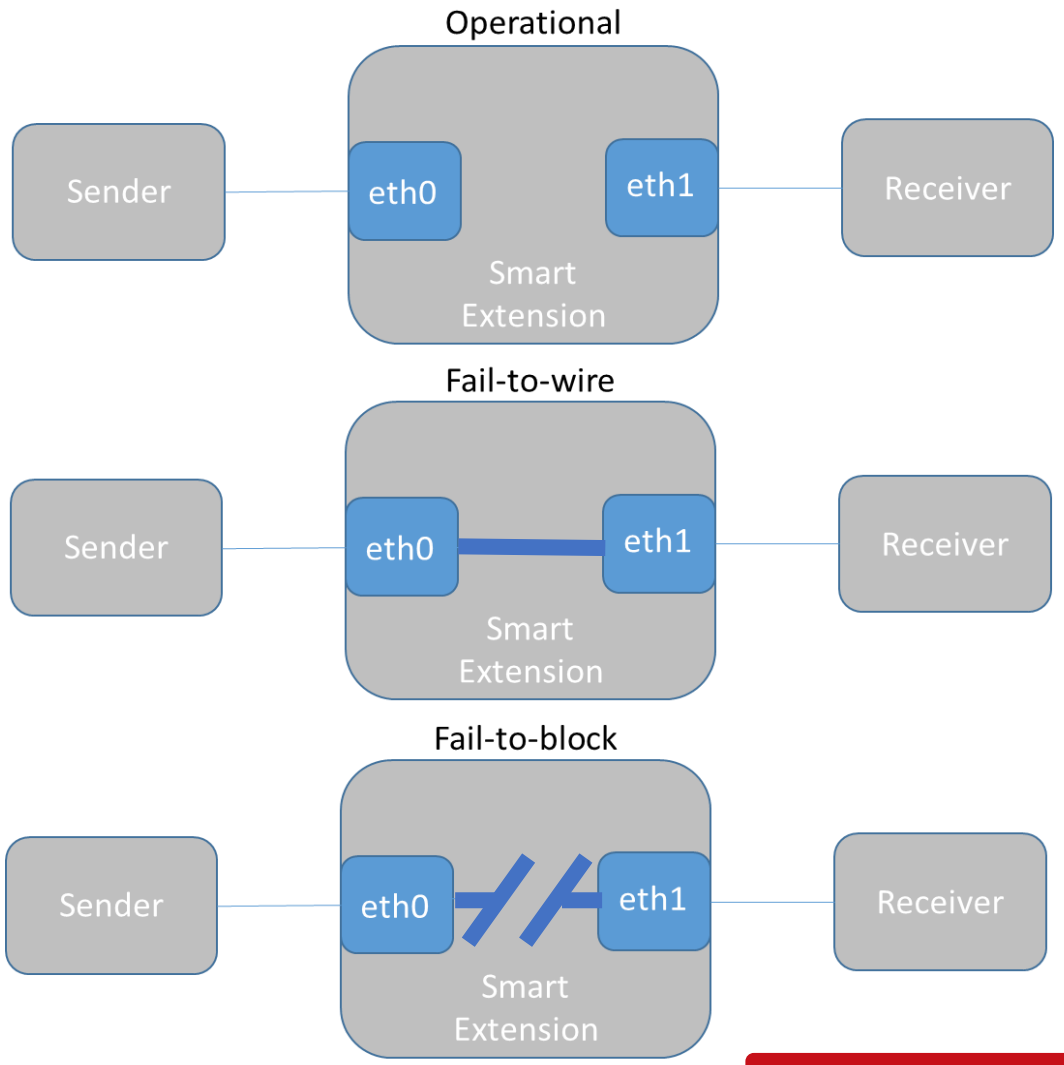


FILTERING MODULE

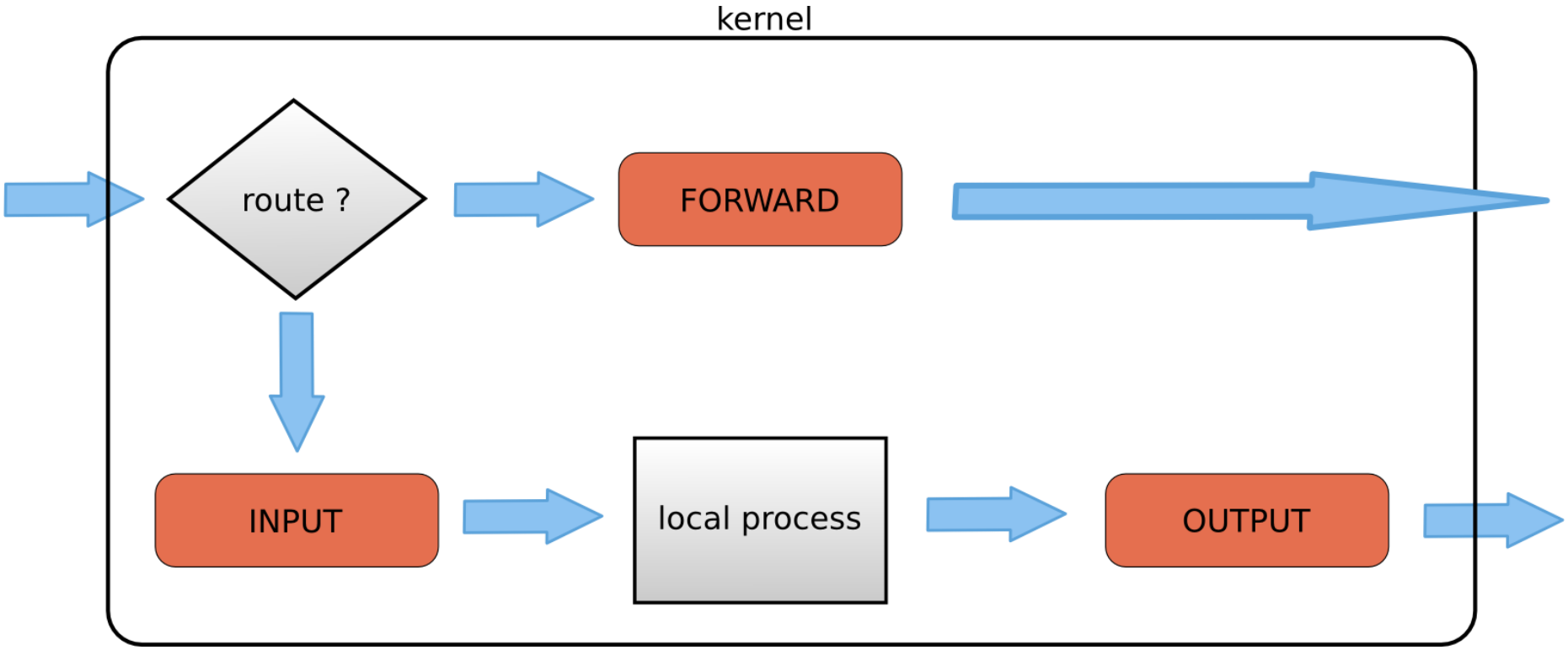


SINGLE-POINT-OF-FAILURE





IPTABLES



FALSE DATA INJECTION

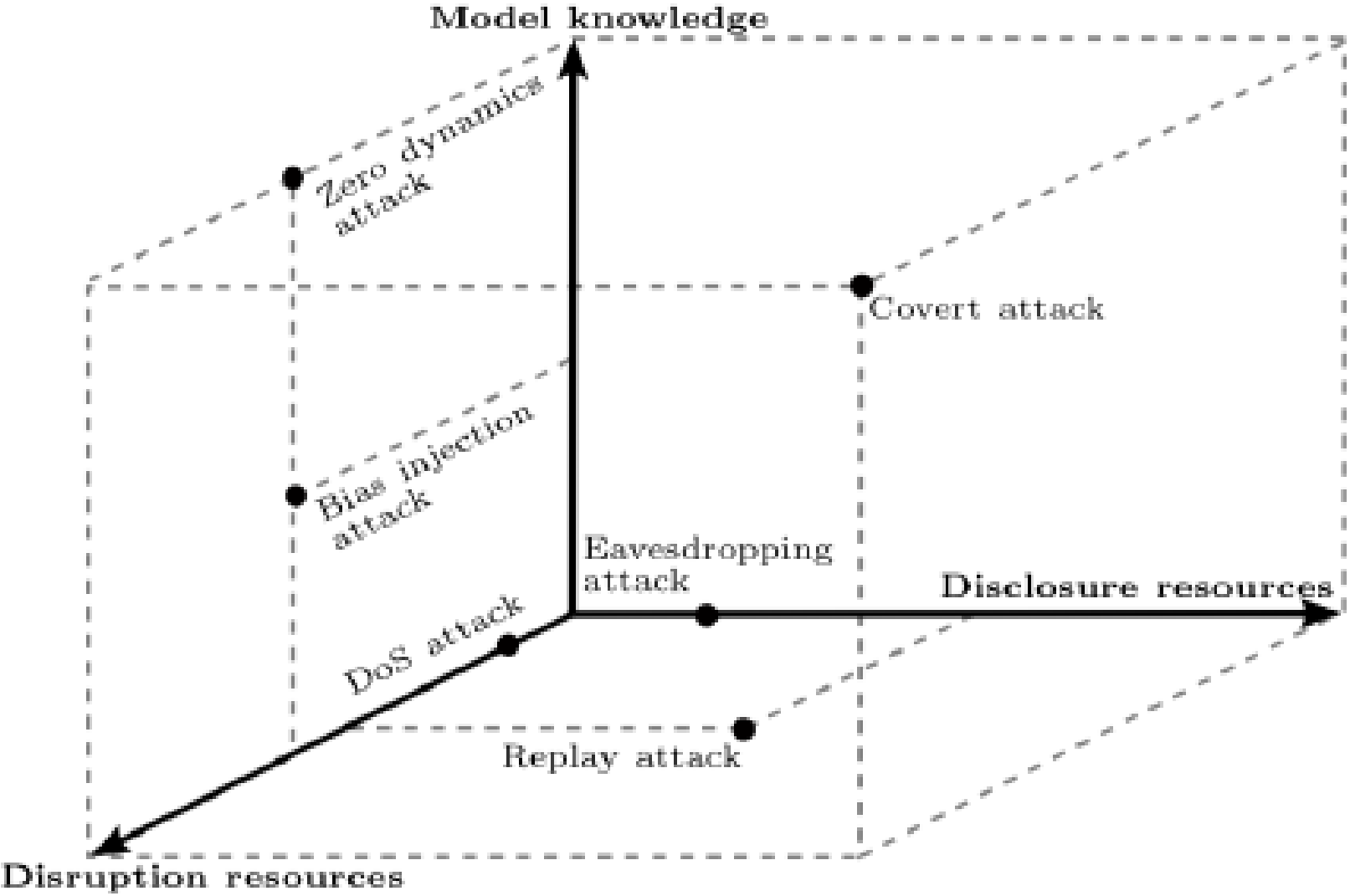
7998	85.086513	192.168.0.101	192.168.0.100	AMS	104 ADS Read Response
7999	85.098342	192.168.0.100	192.168.0.101	AMS	105 ADS Write Request
8000	85.102513	192.168.0.101	192.168.0.100	AMS	96 ADS Write Response
8001	85.118328	192.168.0.100	192.168.0.101	AMS	124 ADS Write Request
8002	85.122511	192.168.0.101	192.168.0.100	AMS	96 ADS Write Response

```
InvokeId: 0x000004fd
ADS Write Request
    IndexGroup: 0x0000f005
    IndexOffset: 0x8e00000f
    CbLength: 1
    Data
```

```
0000  00 01 05 25 a8 99 54 42  49 57 72 98 08 00 45 00   ···%··TB IWr···E·
0010  00 5b 3d e9 40 00 80 06  3a 9a c0 a8 00 64 c0 a8   ·[=·@··· :····d··
0020  00 65 bf 02 c0 18 e3 3c  02 c3 99 31 dc 27 50 18   ·e·····< ···1·'P·
0030  00 fe a4 89 00 00 00 00  2d 00 00 00 05 25 a8 98   ........ -····%··
0040  01 01 53 03 c0 a8 00 0f  01 01 95 85 03 00 04 00   ··S····· ........
0050  0d 00 00 00 00 00 00 00  fd 04 00 00 05 f0 00 00   ........ ........
0060  0f 00 00 8e 01 00 00 00  00                        ........ ·
```

01

ATTACK SPACE



DEFENSE-IN-DEPTH

STRATEGIE DI DIFESA

- Usare sensori per misurare lo sato della rete;
- Applicare un controllo resiliente per non interrompere il servizio;
- Implementare soluzioni security-by-design (topologia e protocolli di comunicazione)

Grazie

riccardo.colelli@uniroma3.it