SECURITY
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

2015

**Danilo Benedetti**

# Aspetti di sicurezza di sistemi SCADA e Smart Metering

# Sistemi ICS e SCADA

# Il ruolo dei sistemi di controllo industriale

I sistemi automatici di controllo industriale permettono a numerosi settori di operare con adeguati livelli di affidabilità e sicurezza

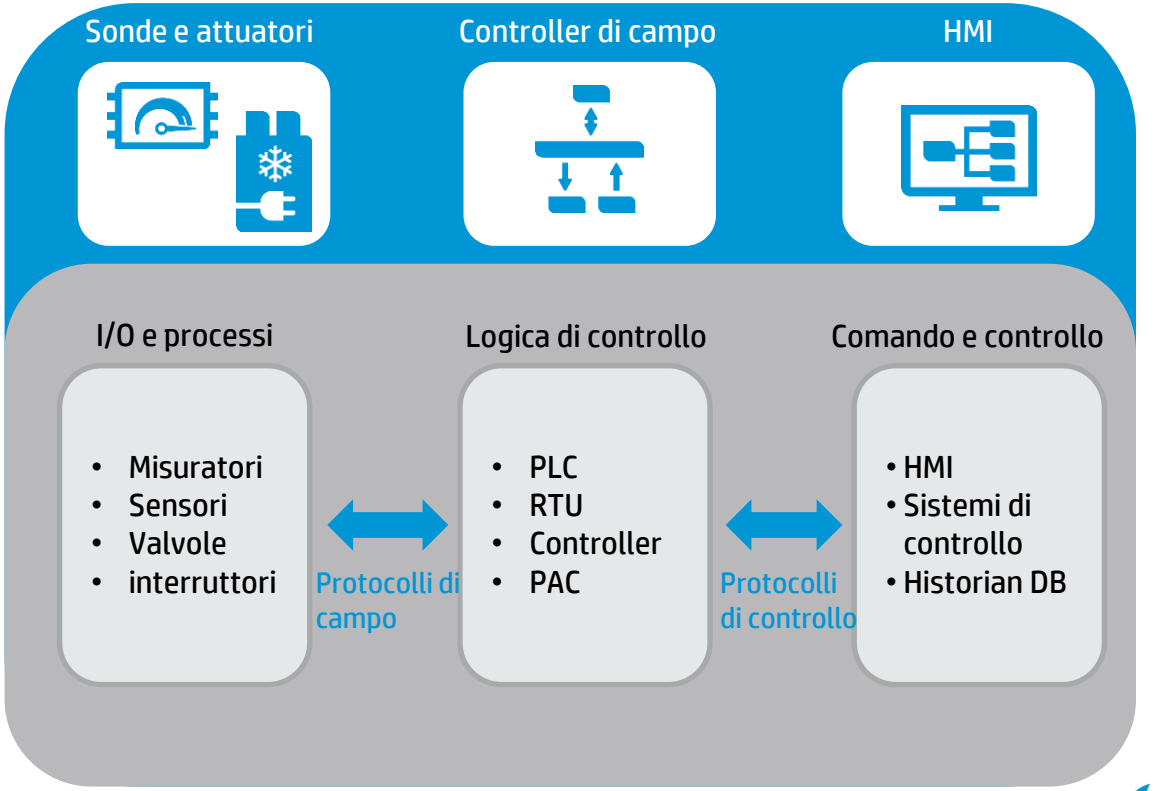
- Chimica
- Commercio e distribuzione
- Manifattura
- Energia
- Pharma

- Acquedotti
- Trattamento rifiuti
- Telecomunicazioni
- Trasporti
- Poste e spedizioni

# Architettura e caratteristiche di reti ICS/SCADA

I sistemi di controllo industriale (ICS – Indstrial Control System) fa riferimento a differenti sistemi, fra i quali:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety instrumented system)



# Le Principali Criticità in ambito ICS

Storicamente la rete SCADA è stata «isolata» e quindi anche «sicura». Oggi questo isolamento è svanito a più livelli: tecnologico, organizzativo, di interconnessione, creando delle criticità nella sicurezza

**Policy di Sicurezza IT su SCADA insufficienti, scarso training sulla Cyber Security**

- Limitata copertura delle best practices relative alla cyber security
- Competenze limitate circa i rischi inerenti la sicurezza informatica

**Limitata presenza di controlli/sistemi di sicurezza sugli host**

- Servizi di OS non utilizzati e mantenuti comunque attivi
- Gestione carente delle utenze: password deboli, utenze condivise, password “eterne”
- Limitata o assente gestione dei permessi nel filesystem

**Protocolli non protetti rendono i sistemi vulnerabili**

- Non testati specificamente sulla sicurezza
- Protocolli privi di procedure di autenticazione
- Basati su standard ASN.1 (DNP, ICCP)

**Vulnerabilità ad attacchi «tradizonali»**

- DOS e DDOS su sistemi di accesso per il telecontrollo
- Worm e Malware sulle reti di processo
- Phishing
- DNS Poisoning / redirection

**Molte componenti utlizzano OS standard**

- Patching limitato o assente su sitemi in produzione
- Spesso vulnerabilità identificata anni prima sono ancora presenti nelle reti SCADA
- Utenze di default non disattivate

**Una insufficiente segmentazione delle reti non isola sufficientemente gli ambienti SCADA**

- La comunicazione è considerata affidabile e non criptata
- Possibilità di di attacco verso e da la rete SCADA
- Necessità di identificare correttamente il perimetro (modem…)

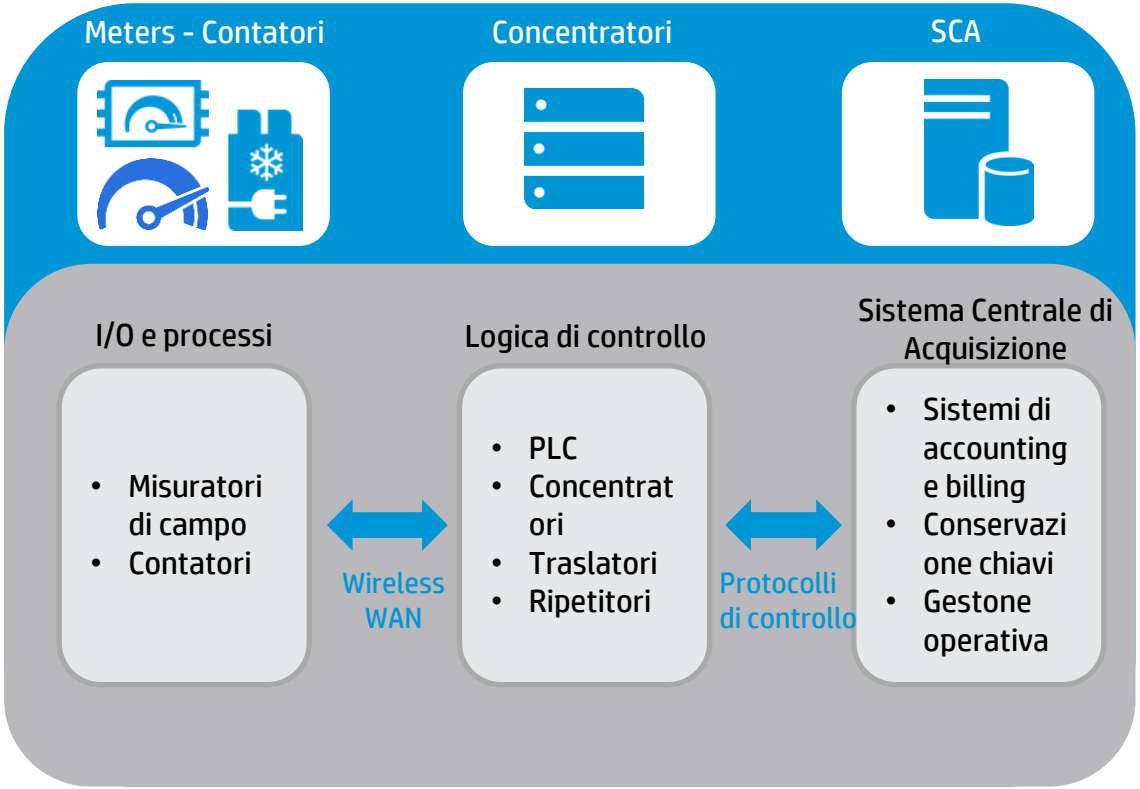
# Sicurezza in ambienti ICS

## A causa delle differenti finalità di sistemi ICS e Metering, rispetto ai sistemi IT, l'approccio alla sicurezza deve essere adattato

| Elemento | IT standard | Sistemi di controllo industrial |
|---|---|---|
| **Protezioni degli endpoint** | Ampiamente utilizzato | Impiego limitato, e con cautele |
| **Tempo di vita dei sistemi** | 3-5 anni | Fino a 20 anni, ed oltre |
| **Outsourcing** | Pratica accettata | Uso limitato |
| **Patching** | Regolare | Lento – può richiedere la preventiva approvazione e testing del fornitore tecnologico |
| **Change management** | Regolare | Richiede tempi lunghi |
| **Ritardi elaborativi** | Possono spesso essere tollerati | Possono avere impatti anche gravi |
| **Security Skills & Awareness** | Buona | Limitata fra gli operatori del telecontrollo |
| **Security Testing** | Ampiamente diffuso | Impiego limitato, e con cautele |
| **Physical Security** | Presidiata | Buona, ma possono esistere sistemi non presidiati |

# Smart Metering

# Architettura di sistemi smart metering




I contatori intelligenti sono dispositivi elettronici che registrano il consumo di energia, gas o acqua e comunicano le informazioni almeno giornalmente ai sistemi di monitoraggio e fatturazione.

I più diffusi protocolli sono:

- ANSI C12-18 (US)
- IEC 61107
- ETSI OSGP
- TCP/IP (?)

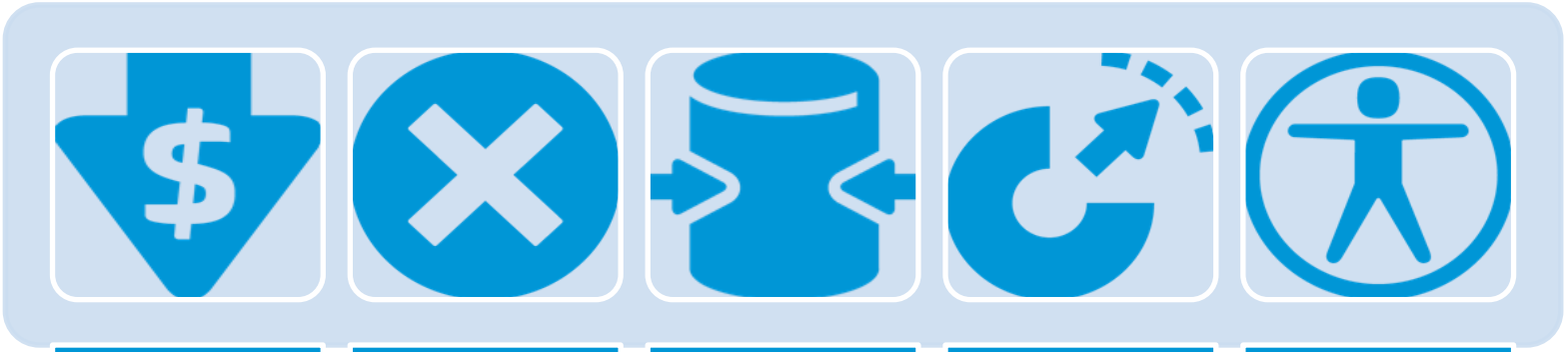
# Esplosione degli Smart Meter

La Comunità Europea prevede la sostituzione dell'80% dei misuratori esistenti con smart meter entro il 2020, con l'obiettivo di ridurre del 3% il consumo energetico.


Numero totale di letture annuali di un singolo misuratore, assumendo 4 letture al giorno.

# Le Principali Criticità dello smart metering

Il profilo di rischio dello smart metering è più legato a logiche IT tradizionali, almeno finché non se ne considera la connessione con i sistemi di produzione



**Frodi / Sabotaggi**

Rischio di frodi/sabotaggi ai danni dell'azienda

**Indisponibilità del servizio**

Mancata disponibilità di servizi con impatti sull'operatività di risorse, utenti business e di alta direzione o su un numero significativo di clienti

**Alterazione / Perdita di dati**

Alterazione/perdita di dati di business sulla clientela

**Non conformità**

Complessità della normativa

Mancanza di uno schema di certificazione

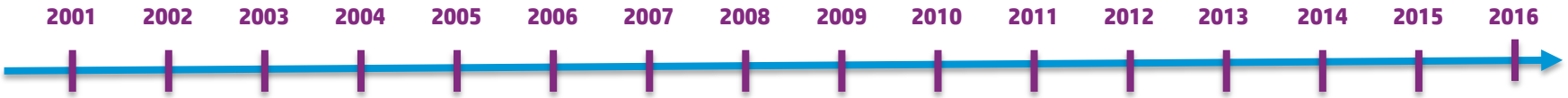
Produttori di Meter ancora non pienamente allineati alla norma Confidenzialità dei dati

**Reputazione**

Impatti su dati e servizi visibili alla opinione pubblica o che compromettono la reputazione dell'azienda e il grado di fiducia della clientela

# Profili di rischio per ICS/SCADA

# SCADA: un obiettivo strategico?




2001 – Porto di Houston. System crash

2003 – Slammer Worm. Controllo di volo, ATM, 911, Sistema di monitoraggio centrale nucleare

2003 - 2004 – Titan Rain. Attacchi contro Installazioni militari

2007 – Tehama Canal Auth. Ex dipendente installa SW non autorizzatosu un computer per il controllo idirico

2009 – Attacco alla rete di distribuzione elettrica USA. Attacco individuato dall'FBI

2009 – 2010 – Operazione aurora. Furto di proprietà intellettuale. Fra i target, aziende di sicurezza

2010 – **Stuxnet**

2011 – Nitro. Attacco contro industrie chimiche, utilizzando un trojan acquistabile sul mercato nero

2012 – Shamon. Malware disabilita centinaia di computer di Saudi Aramco

2012 – Flame. Attacco contro sistemi Iraniani per raccogliere informazioni sul programma nucleare

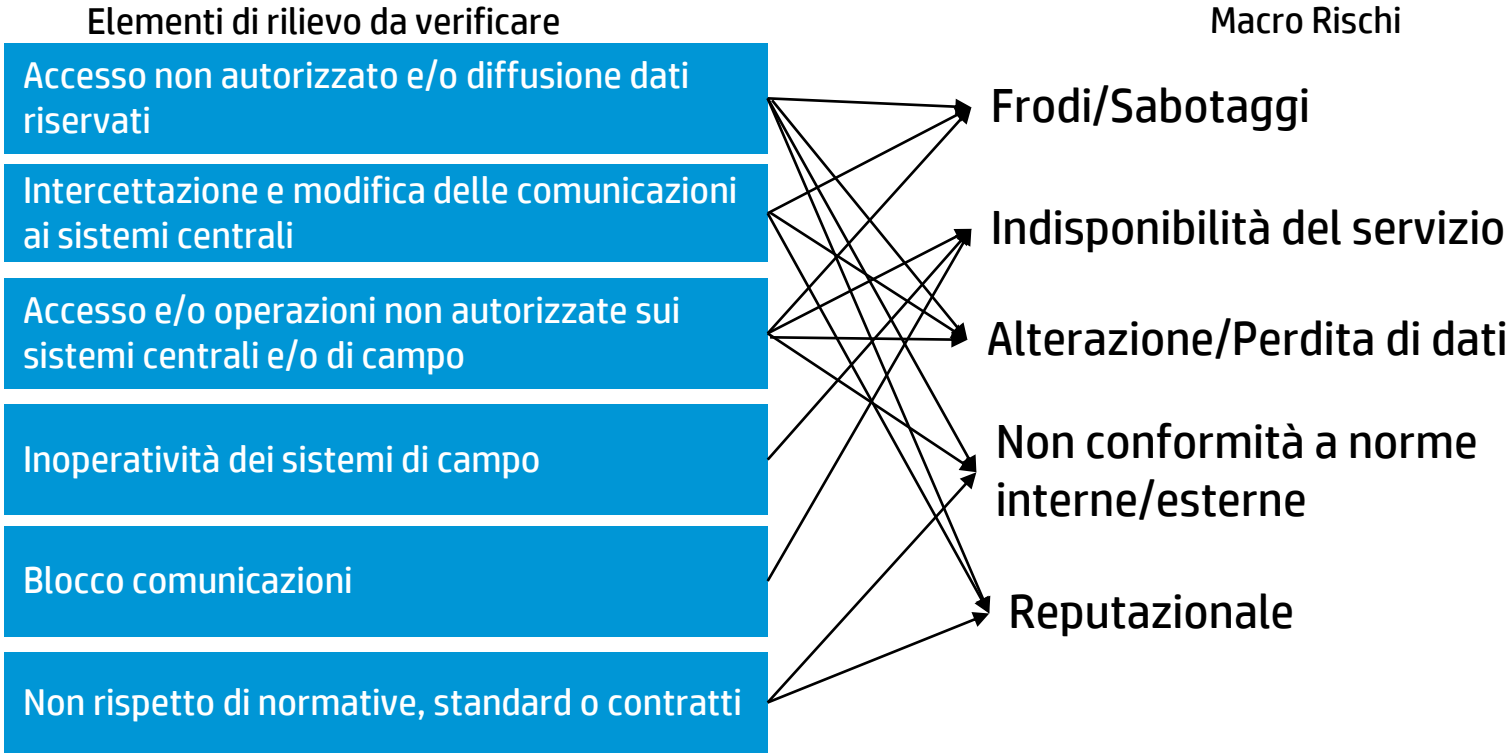
2012 – Attacco contro le reti di utilities mirante al furto di credenziali. Identificato da ICS-CERT

2013 – US ICS-CERT riporta oltre 200 attacchi ad infrastrutture critiche (53% energy)

2013 – NATO lancia una massiccia esercitazione di cyberdefence: Cyber coalition 2013

2014 – Havex. Trojan capace di infettare sistemi ICS di 3 vendor. Campagna di malware contro obiettivi ICS

# Scenari di rischio SCADA



# Il quadro normativo

# Pressione regolamentare - ICS

Il settore delle infrastrutture critiche è oggetto di una forte attenzione regolamentare

### Stati Uniti

- **NIST** Framework for Improving Critical Infrastructure Cybersecurity
- **NERC** Critical Infrastructure Protection (CIP) v5
- **ES-C2M2** – Electricity Subsector Cybersecurity Capability Maturity Model

### Comunità Europea

- **ENISA** - Protecting Industrial Control Systems - Recommendations for Europe and Member States
- **EU Cybersecurity Strategy**
- **EU 2008/114/EC Directive** - Identification and designation of European critical infrastructures
- **EU Proposed NIS Directive** - Network and Information Security

### Global Best Practices

- **ISO 27019** - Information Security for the Energy Utility Industry
- **ISA/IEC 62443** – Security for industrial automation and control systems
- **IEC 61513** - Nuclear power plants. Instrumentation and control important to safety.

# NIST - Framework for Improving Critical Infrastructure Cybersecurity

| ID Funzione | Funzione | Categoria |
|---|---|---|
| ID | Identify | Asset management<br>Business environment<br>Governance<br>Risk assessment<br>Risk management strategy |
| PR | Protect | Access Control<br>Awareness and training<br>Data security<br>Information protection processes and procedures<br>Manutenzione<br>Tecnologia a protezione |

| ID Funzione | Funzione | Categoria |
|---|---|---|
| DE | Detect | Anomalie ed eventi<br>Monitoraggio della sicurezza<br>Processo di identificazone |
| RS | Respond | Pianificazione delle risposte<br>Comunicazioni<br>Analisi<br>Mitigazione<br>Miglioramento |
| RC | Recover | Recovery planning<br>Miglioramento<br>Comunicazioni |

# NERC CIP

## 8 standard, 42 requisiti – Obbligo di comformità per i centri di produzione elettrica

| Critical cyber assets | Security management | Personnel security | Electronic secure perimeter | Physical & environment security | Systems & information integrity | Incident response | Contingency planning |
|---|---|---|---|---|---|---|---|
| •Metodi per l'identificazione degli asset critici<br>•Asset critici<br>•Verifica annuale<br>•Approvazione annuale | •Poicy di sicurezza<br>•Leadership<br>•Eccezioni<br>•Protezione delle informazioni<br>•Controllo degli accessi<br>•Change control e gestione configurazio-ni | •Training<br>•Verifica dei rischi legati al personale<br>•Accesso | •Perimetro di sicurezza<br>•Gestione identità e accessi digitali<br>•Monitoraggio degli accessi<br>•Vulnerability assessment<br>•Gestione della documentazione | •Piano della sicurezza fisica<br>•Controllo accessi fisici<br>•Protezione dei sistemi di controllo accessi<br>•Monitoraggio degli accessi fisici | •Procedure di test<br>•Porte e servizi<br>•Patching<br>•Prevenzione virus e malware<br>•Monitoraggio di sicurezza<br>•Terminazione sicura degli asset<br>•Vulnerability assessment | •Piano di risposta agli incidenti di sicurezza cyber<br>•Documentazione | •Piano di recupero<br>•Esercitazoni<br>•Backup & restore<br>•Test dei backup |

Se l'obiettivo è strategico, la sola protezione preventiva non è sufficiente: è necessario poter pianificare la risposta e il recupero dagli attacchi

# Regolamentazione Smart Metering

## Il caso Gas, riferibile anche ad un'ottica multiservizio

Il principale riferimento normativo per la sicurezza dei gas meter è costituito dalle specifiche tecniche dell'Authority contenute nella norma **UNI/TS 11291 parte 10** (Febbraio 2013) e **11291 parte 11**, con use case di dettaglio per GdM residenziali.
Elementi chiave della Norma sono:

- Protezione da manomissioni fisiche dei sistemi (GdM, Concentratori, Ripetitori, Traslatori)
- Protezione del software (hashing)
- Protezione delle chiavi di cifratura
- Gestione dei casi di perdita o degrado della fonte energetica (batteria, alimentazione primaria)
- Protezione dei canali di comunicazione applicativa
- Gestione chiavi di rete

# Evoluzione della protezione

# Obbiettivo prioritario: conoscere

E’ necessaria una campagna di verifiche è per identificare e mitigare i rischi nei sistemi di controllo industriale. L’attività dovrebbe coprire almeno:

- Analisi dell’architettura di rete
- Analisi dei controlli di sicurezza, sia tecnici sia procedurali
- Revisione delle policy
- Test delle vulnerablilità degli applicativi
- Valutazione della sicurezza fisica
- Wireless security assessment
- Analisi non intrusiva (mirrored) del traffico
- Revisione delle procedure di aggiornamento dei sistemi

# Attività di verifica della sicurezza SCADA

**Assessment della sicurezza**

- Verifica della configurazione dei sistemi perimetrali
- Analisi delle procedure operative e di sicurezza
- Revisione delle policy

**Analisi e verifica della infrastruttura**

- Revisione delle Network Security Zone
- Revisione dell'architettura di sicurezza rete
- Analisi della rete SCADA e identificazione di potenziali criticità
- Verifica ella sicurezza Wireless
- Verifica della sicurezza fisica

**Vulnerability Assessment**

- Network Vulnerability Testing
- Application Vulnerability Testing
- Modem Testing and War Dialing

# Evoluzione verso 5G SOC

## Priorità

Migliorare i controlli di compliance e le capacità di Risk Management

Ottimizzare l'impegno di risorse, minimizzando quelle manuali a vantaggio di controlli automatici gestiti dal SIEM anche mediante algortimi di analisi comportamentale

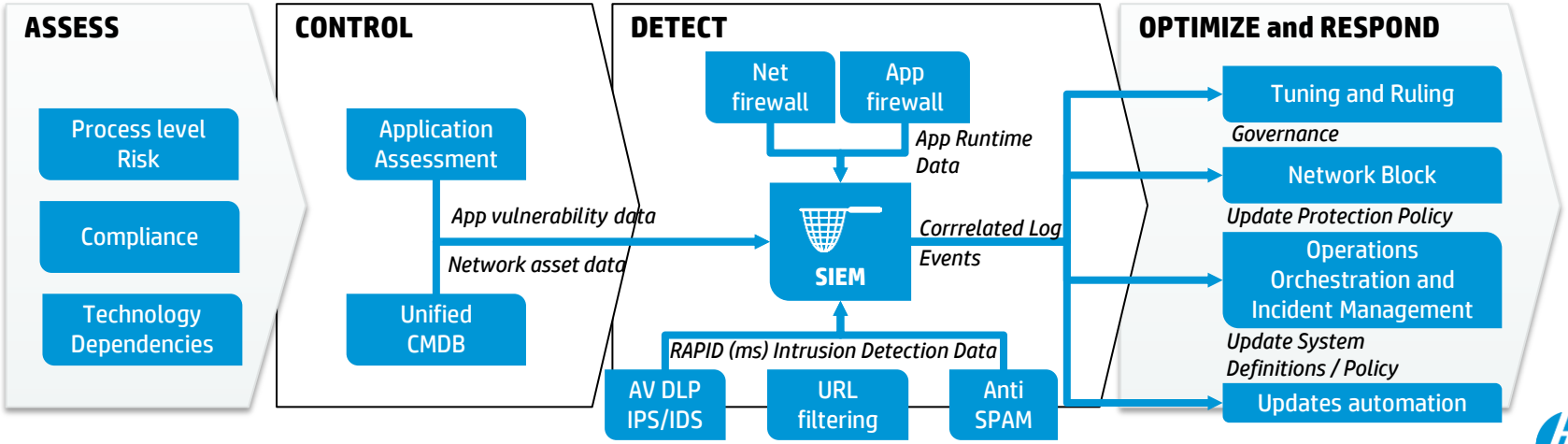
Mitigare gli impatti con un approccio proattivo

## Percorso

Valutazione delle applicazioni che supportano i processi critici (in base a tutti i parametri di sicurezza)

Espansione degli eventi gestiti dal SIEM

Visualizzazione e reportistica coerente con gli obiettivi istituzionali



# Grazie per l’attenzione