

# Sicurezza nelle grandi organizzazioni

Fabio Vernacotola, Simone Patonico

3/12/2020



# Sezione 1

Progetti di sicurezza, perché...

# Iniziative di sicurezza delle informazioni

## Obiettivi

E' la motivazione fondamentale dell'iniziativa (driver). Strategica, di gestione del rischio, o di conformità alle leggi

Strategy

Risk Management

Compliance

## Asset

Identifica il «bene» oggetto di protezione. In generale è una informazione ma può essere anche una identità digitale, una capacità operativa (Application) o una informazione chiave.

Identity

Application

Information

## Ambito

Identifica il contesto tecnologico e/o organizzativo di applicazione dell'iniziativa

Mobile

Processes

Cloud

On  
Premise

Organ.

Workplace

# Obiettivi strategici

- Direttamente correlati al core business dell'organizzazione
- Forniscono all'organizzazione un vantaggio competitivo

## Esempi:

- Fornitore di servizi che offre servizi «sicuri» ai propri utenti (Marketing)
- Organizzazione che certifica ISO27001 i propri processi produttivi per poter accedere a gare pubbliche

# Risk Management

...evitare gli incidenti ovvero l'impatto economico relativo alla perdita di:

- Riservatezza;
- Integrità
- Disponibilità



What we do About us Media Careers Contacts

Home / About Us / Notice On Cyber Attack



## Notice on cyber attack

18 November 2020

Over half of the applications - deactivated to preserve their integrity - have been put back into operation and are now safely available to RINA personnel, customers and partners.

The analysis and safety of the terminals owned by the company also continues. The data analysis is ongoing and will take a few days to get to a sufficient level.

16 November 2020

RINA informs that it has recently been hit by a cyber-attack which has been blocked. Presently, customers' data does not appear to have been exposed to the risk of disclosure. If access to such data is ascertained, those concerned will be promptly informed.

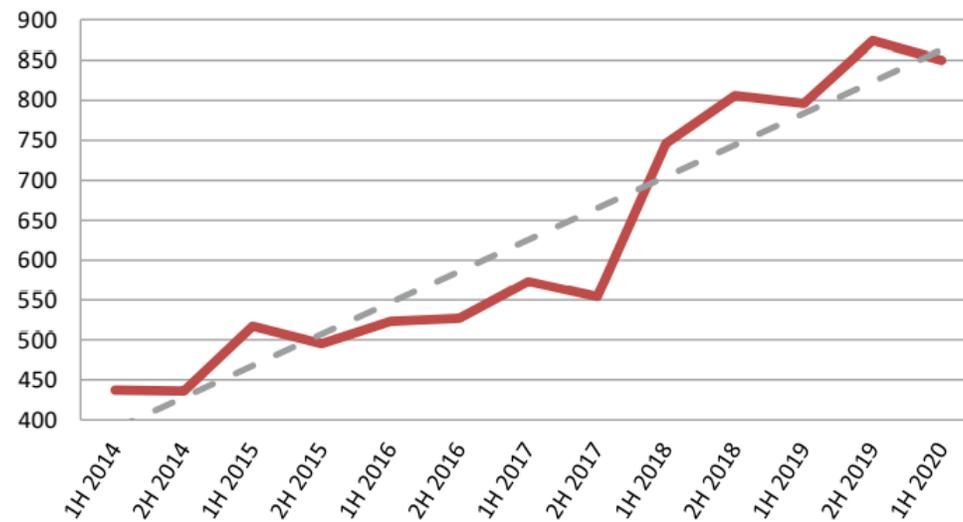
RINA's IT department managed to repel subsequent attacks and immediately took the necessary countermeasures to contain their effects. For this reason, the restoration of the full operation of the systems is taking place, with the support of a team of cybersecurity experts, gradually and based on the utmost prudence and security.

The company immediately made the communications required by law.

Further developments will be promptly announced on this page.

## Rapporto Clusit 2020

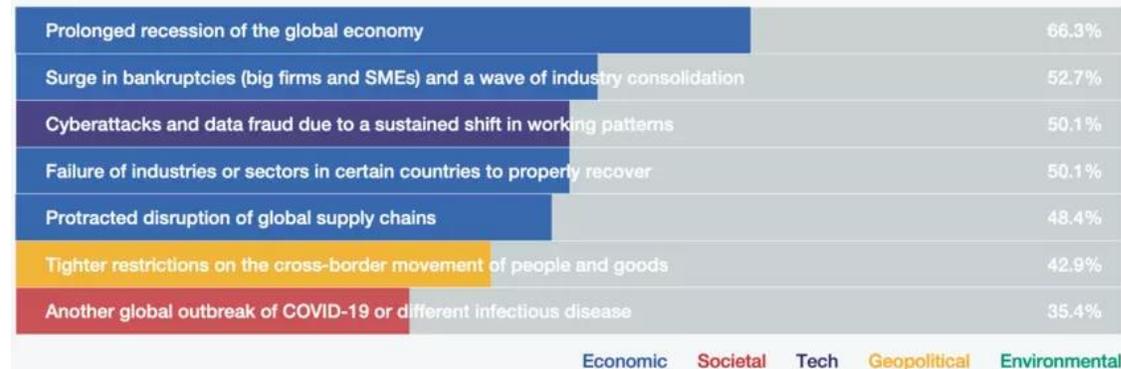
Numero di attacchi gravi per semestre (2014 1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

## World Economic Forum

### Most worrisome for your company



# Risk management

- $\text{Rischio} = \text{Frequenza di un incidente} * \text{impatto del singolo incidente}$

L'obiettivo dell'organizzazione è quello di:

- limitare l'impatto;
- limitare la frequenza;

I rischi di sicurezza possono raggiungere valori economici molto significativi. Il costo medio di un mega data breach, ad esempio, è stato calcolato nel 2018 in 3,86 M\$ \*

# Esempio: infezione ransomware su un server

- Impatto per:

- Costo per indisponibilità delle applicazioni che utilizzano il server;
- Costo di ripristino;
- Costo di inoperatività del personale;

## Mitigazione dell'impatto:

- ridondanza dei server;
- immagini virtuali ripristinabili in minor tempo possibile;

# Esempio: infezione ransomware su un server

Ridurre la frequenza

Implementare contromisure come:

- Istruire i dipendenti (Security awareness);
- Limitare l'esecuzione di programmi sui server;
- Limitare l'uso di utenze privilegiate;
  
- In generale interrompere la *kill chain* tipica degli attacchi ransom



# Compliance – Conformità alla norme

E' un obiettivo dettato da obblighi di legge:

- Es. Conformità al Regolamento Europeo per la protezione dei dati personali 679/2016 (GDPR)
- Misure minime di sicurezza ICT per le pubblica amministrazioni emanate dall'AgID
- Direttiva NIS

O da accordi/contratti di servizio:

- PCI DSS (Payment Card Industry Data Security Standard)

# Sezione 2

Approccio Framework Based per la gestione del sistema di sicurezza aziendale

# Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Secondo la ISO27000:

*Un SGSI consiste nelle policy, procedure, linee guida e risorse ed attività associate gestate collettivamente dall'organizzazione allo scopo di proteggere gli asset informativi.*

*Un SGSI è un approccio sistematico per stabilire, realizzare, condurre, monitorare, rivedere, mantenere e migliorare la sicurezza delle informazioni aziendali al fine di supportare gli obiettivi di business.*

# Framework di riferimento

- Insieme di «controlli», variamente organizzati, che definiscono cosa una organizzazione deve fare per poter gestire la propria sicurezza informatica.
- I framework rappresentano la formalizzazione di una «best practice» ma possono essere anche di derivazione normativa.
- I framework:
  - consentono una valutazione del proprio livello di sicurezza;
  - semplificano le attività di conduzione del proprio Sistema di Gestione della Sicurezza delle Informazioni;
  - forniscono una base per le attività di audit interno.

# Esempio ISO27001

Dominio

Obiettivo di controllo

Controlli

## A.5 Politiche per la sicurezza delle informazioni

### A.5.1 Indirizzi della direzione per la sicurezza delle informazioni

Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.

A.5.1.1	Politiche per la sicurezza delle informazioni	<i>Controllo</i> Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	<i>Controllo</i> Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

## A.13 Sicurezza delle comunicazioni

### A.13.1 Gestione della sicurezza della rete

Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.

A.13.1.1	Controlli di rete	<i>Controllo</i> Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	<i>Controllo</i> I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	<i>Controllo</i> Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

# SANS TOP 20

The **SANS Institute** is a private U.S. company that specializes in internet security training. It was founded in 1989 and provides computer security training, professional certification through Global Information Assurance Certification (GIAC), and a research archive - the SANS Reading Room.

1. Inventario dei device autorizzati e vietati;
2. Inventario dei software autorizzati e vietati;
3. Configurazione sicura per Hardware e Software su device mobili, portatili, workstation e server;
4. Vulnerability assessment continuo e relativa remediation;
5. Difesa dai Malware;
6. Sicurezza Applicativa;
7. Controllo dei device wireless;
8. Data recovery;
9. Security skill assessment a training appropriato;
10. Configurazione sicura dei device di rete;

11. Limitazione e controllo di porte, protocolli e servizi;
12. Uso controllato dei privilegi amministrativi;
13. Difesa "perimetrale";
14. Manutenzione, monitoraggio ed analisi dei log;
15. Controllo di accesso in ottemperanza al need to know;
16. Monitoraggio e controllo degli account;
17. Data Loss Prevention;
18. Incident Response and Management;
19. Ingegneria di rete sicura;
20. Penetration Test e addestramento;

# CIS Security Controls

Il Center for Internet Security è un'organizzazione non profit, fondata nell'ottobre 2000. La sua missione è "identificare, sviluppare, convalidare, promuovere e sostenere le migliori pratiche di difesa informatica e costruire e guidare le comunità per creare un ambiente di fiducia in cyberspazio"

## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

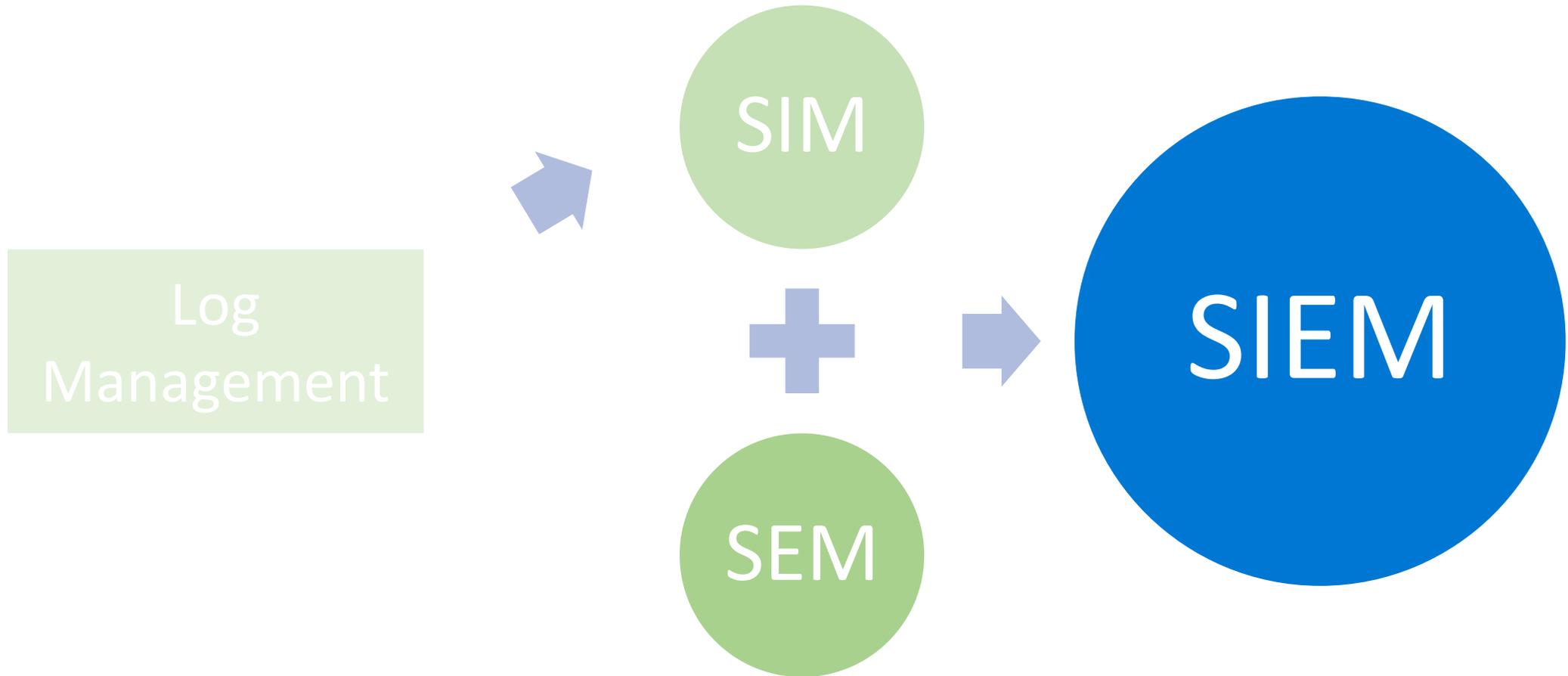
### CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
-------------	------------	-------------------	---------------	----------------------

# Sezione 3

Tecniche di attuazione dei controlli: i Sistemi SIEM

# Ma che cos'è un SIEM?



# SIM vs SEM vs SIEM

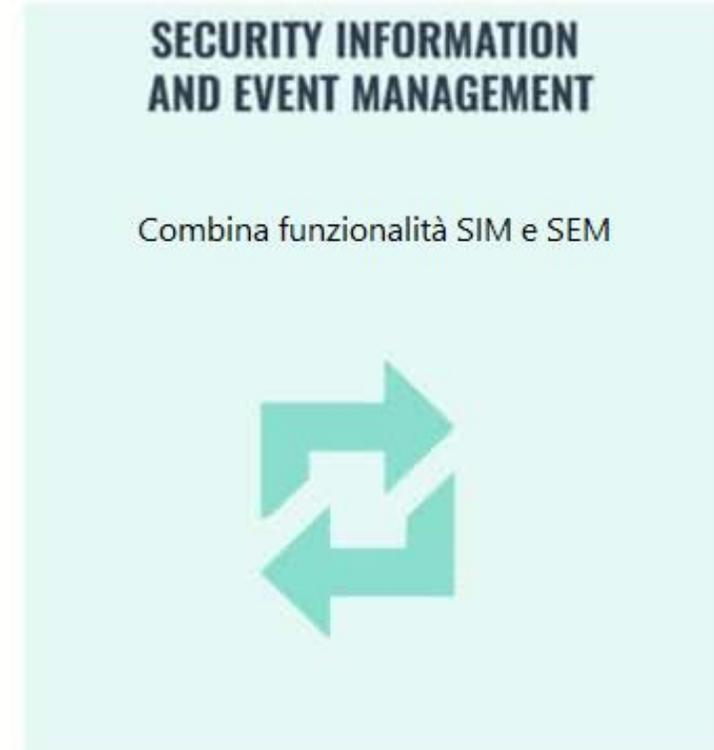
## SIM



## SEM



## SIEM



# Mapping sui framework di controlli

- CIS Security Controls
  - CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

A.12.4 Raccolta di log e monitoraggio		
Obiettivo: Registrare eventi e generare evidenze.		
A.12.4.1	Raccolta di log degli eventi	<i>Controllo</i> La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.
A.12.4.2	Protezione delle informazioni di log	<i>Controllo</i> Le strutture per la raccolta dei log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati.
A.12.4.3	Log di amministratori e operatori	<i>Controllo</i> Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.
A.12.4.4	Sincronizzazione degli orologi	<i>Controllo</i> Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento.

- ISO/IEC 27001:2013
  - A12 Sicurezza delle attività operative

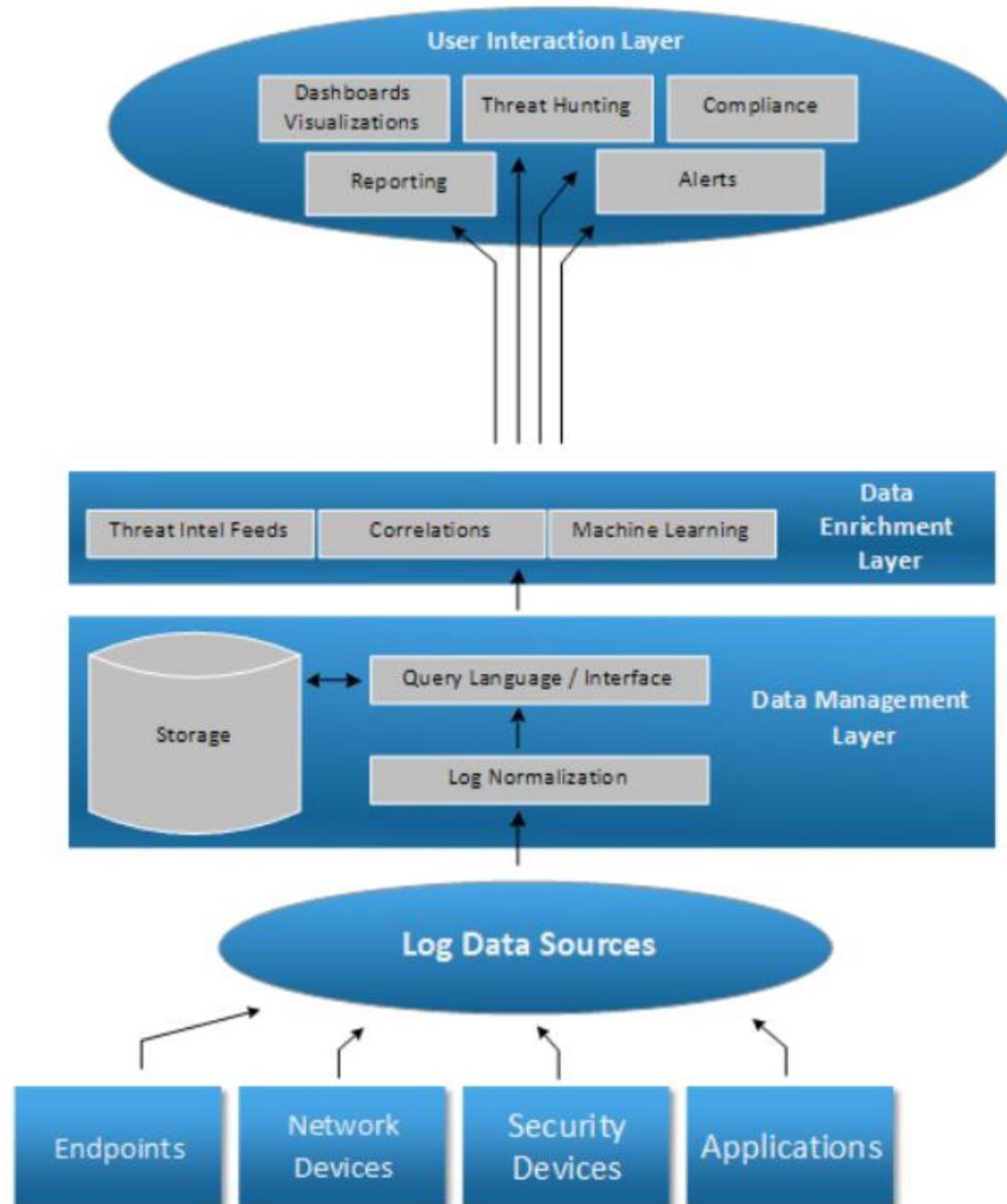
## 6 CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

*Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.*

### CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
6.4	Network	Detect	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.
6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.

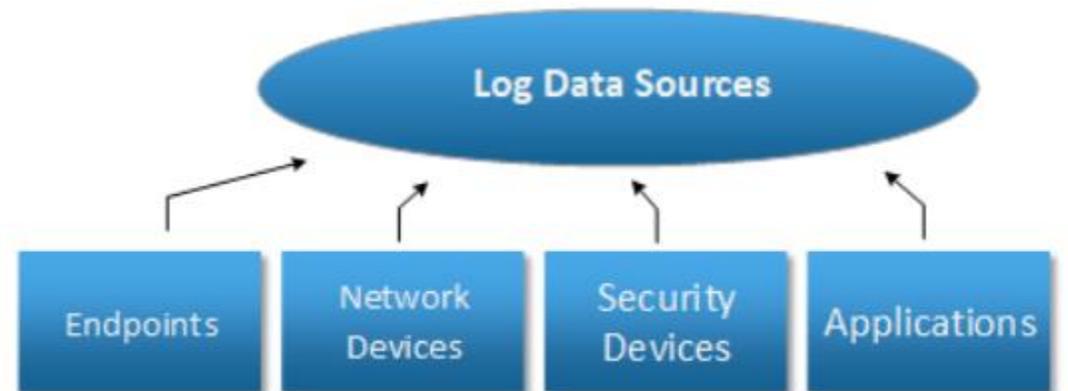
# SIEM tradizionale



# Log and Event Collection

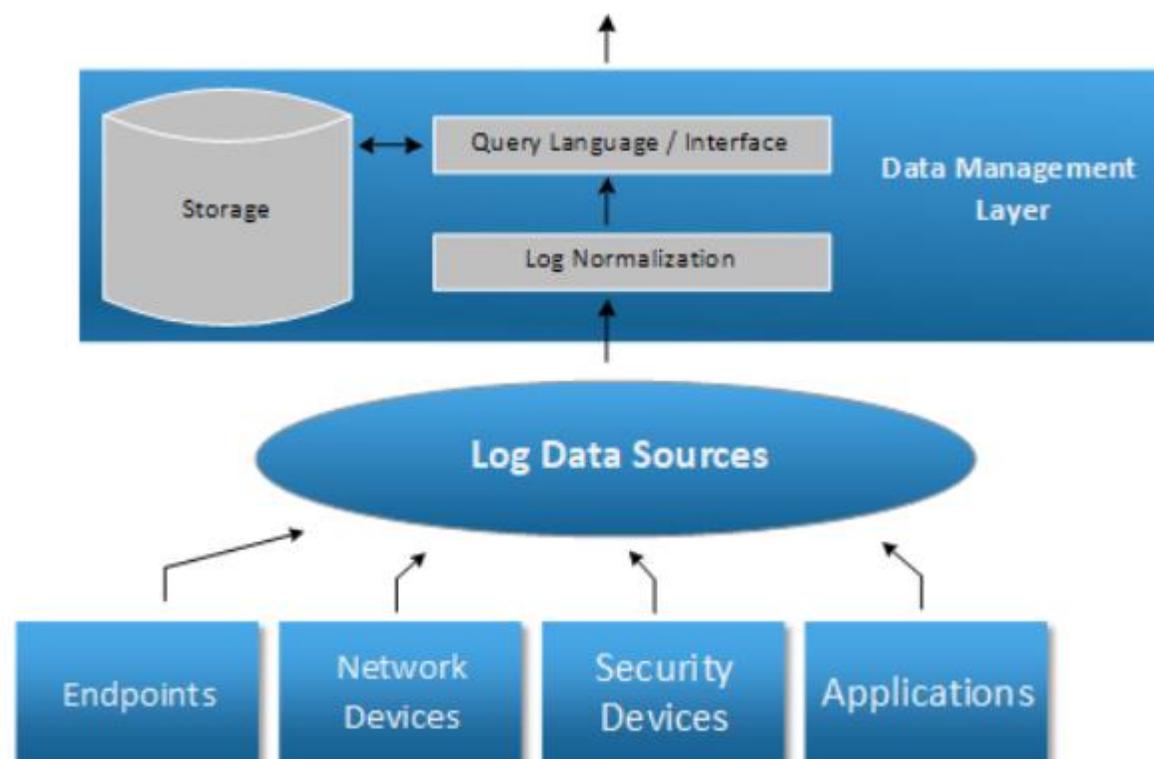
Un SIEM colleziona dati da varie sorgenti:

- Windows/Linux Servers e Workstations
- Dispositivi di rete (switches, routers, load balancers)
- Dispositivi di sicurezza (firewalls, IPS/IDS, VPN, URL filtering)
- Applicazioni web
- Database (MSSQL Server, Oracle DB)



# Data Management Layer

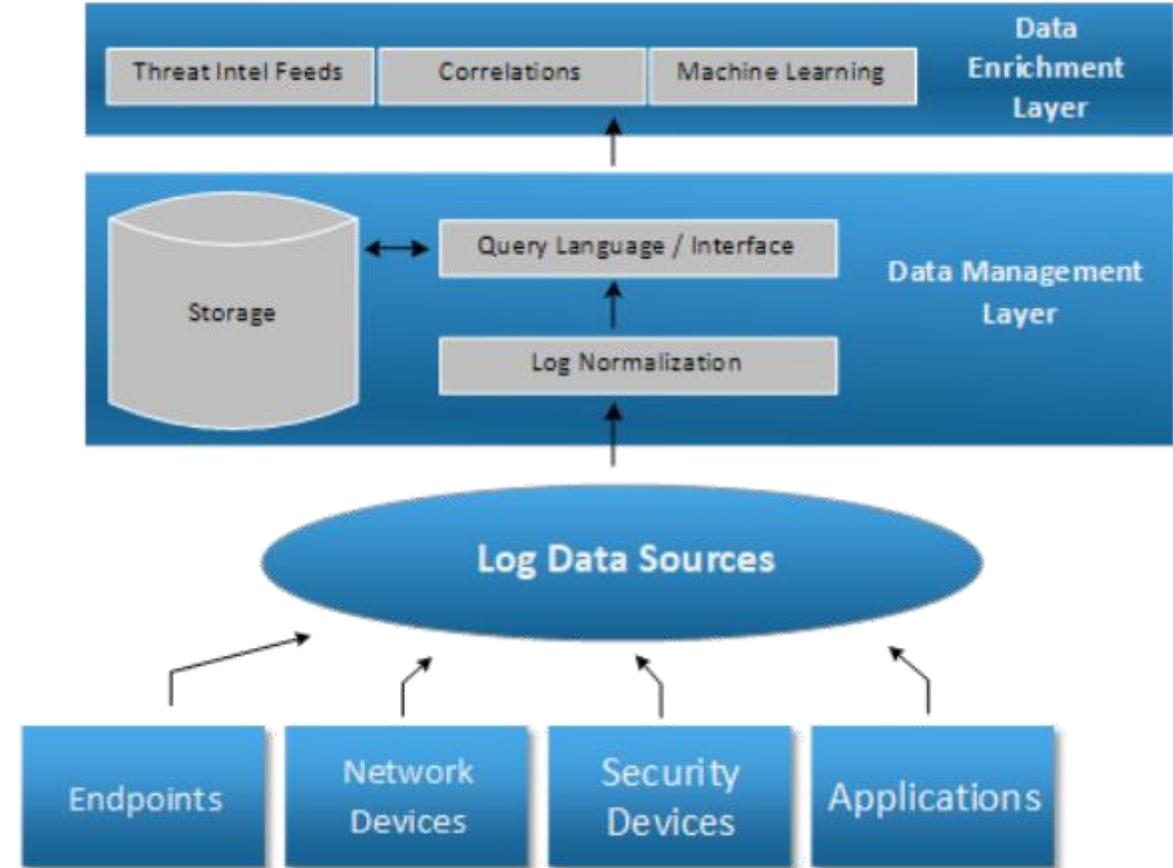
- Immagazzinamento e mantenimento dei log raccolti in accordo alle policy di mantenimento aziendali e legali.
- Normalizzazione dei log
  - Rimozione dei duplicati
  - Miglioramento dell'efficienza delle query
- Filtraggio ed aggregazione dei dati mediante query



# Data Enrichment Layer

Dopo l'estrazione dei dati tramite query, il data enrichment layer offre funzionalità:

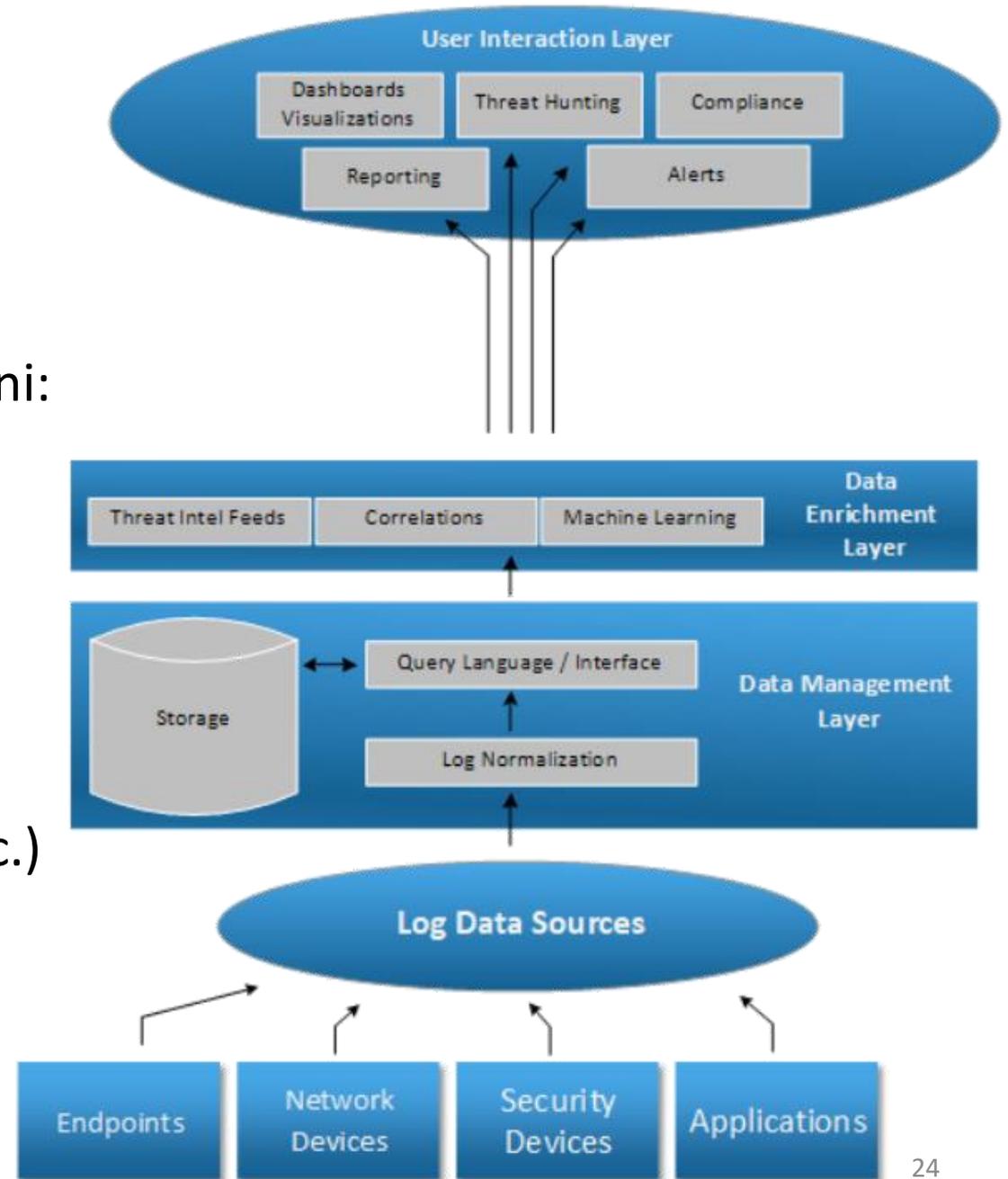
- Arricchimento dei dati con informazioni aggiuntive (es: posizione geografica)
- Correlazione dei log delle diverse sorgenti di sicurezza
- Correlazione con Threat Intelligence da fonti esterne
- Correlazione con informazioni aggiuntive fornite dagli algoritmi di machine learning



# User Interaction Layer

Fornisce visibilità dei dati estratti dallo storage ed arricchiti con ulteriori informazioni:

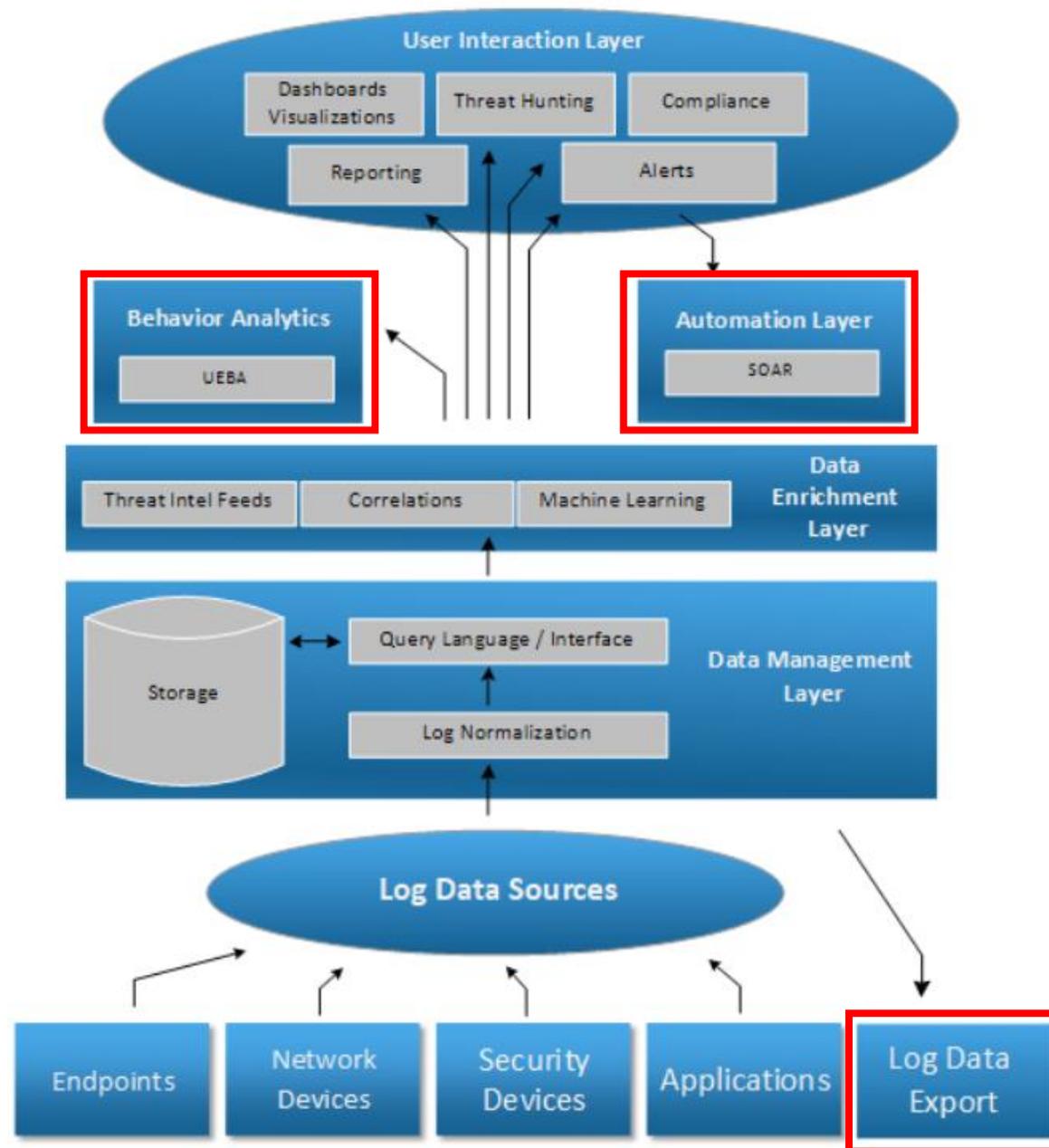
- Dashboards
- Report periodici su specifici utenti
- Threat Hunting per la ricerca di specifici eventi / attacchi
- Compliance per la generazione di report soddisfacenti norme legali (PCI, GDPR, etc.)
- Alerts
  - Notifica specifici utenti/amministratori



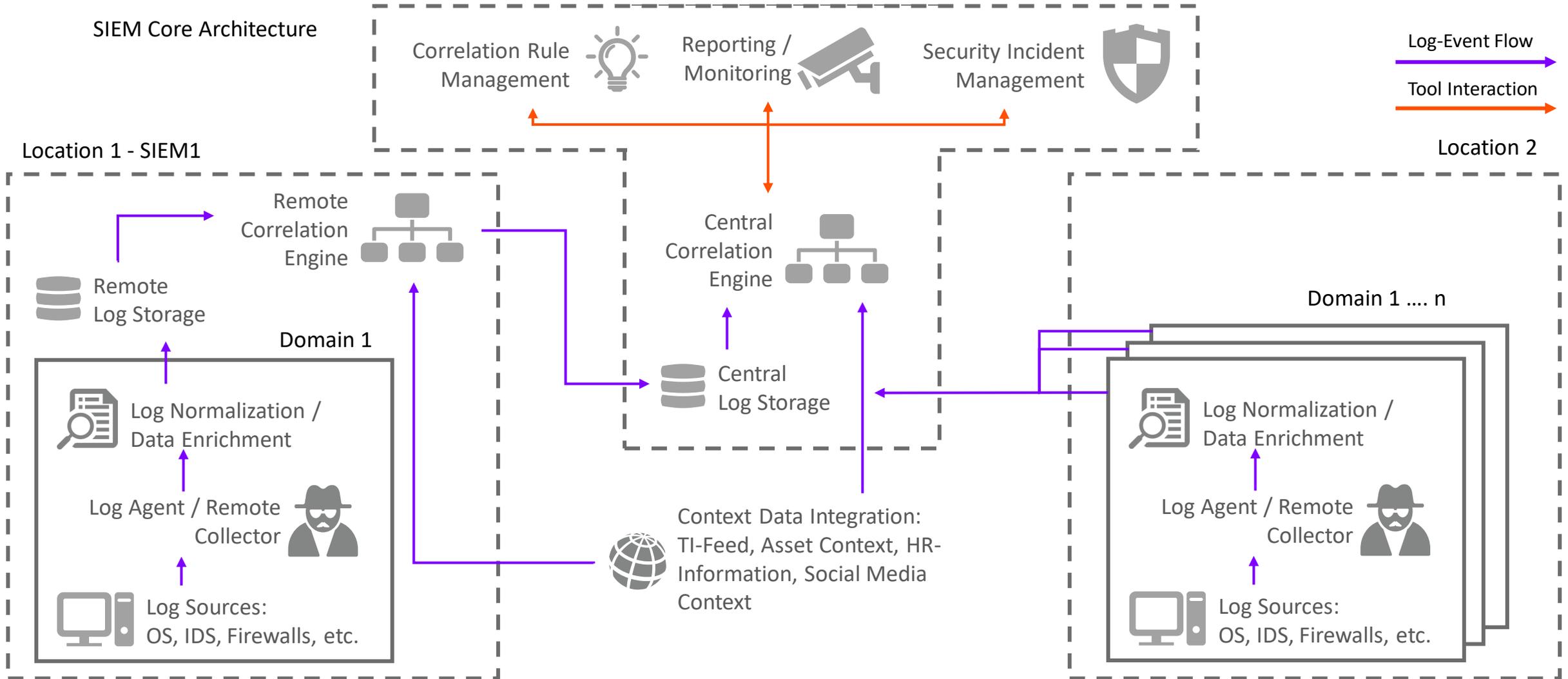
# SIEM moderno

Un SIEM moderno aggiunge 3 funzionalità:

- **Automation Layer.** Funzionalità SOAR per la risposta automatica ad incidenti (Playbooks)
- **Behavior Analytics.** Funzionalità UEBA per l'identificazione di comportamenti anomali
- **Log Data Export.** Esportazione dei dati su software di terze parti



# SIEM Deployment Architecture - Example

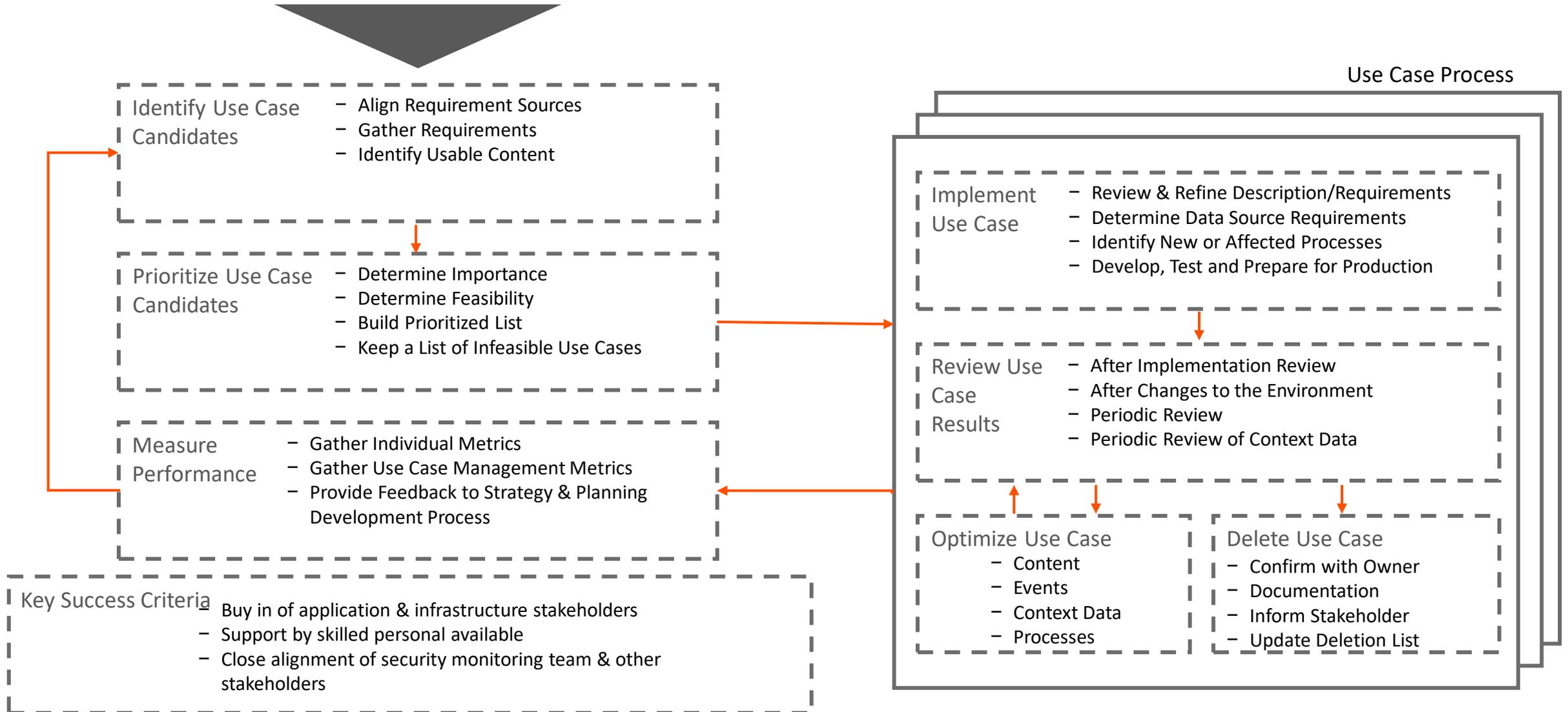


# Razionali per la scelta architettonica

Fattori da considerare:

- **Origine degli eventi:** se gli eventi sono generati in cloud portarli *on premise* determina maggiori costi ed inefficienza che mantenerli in cloud. Se sono generati on premise vale l'opposto.
- **Single pane of glass:** è vantaggioso disporre di una console unica di monitoraggio in termini di *skill* e della possibilità di centralizzare i processi di gestione degli allarmi.
- **Complessità organizzativa:** un modello gerarchico può consentire la giusta indipendenza e visibilità sugli eventi generati in organizzazioni cooperanti, mantenendo la centralità di alcune funzioni aziendali come il SOC o la *Compliance*.
- **Modello di licenza:** può influenzare fortemente i costi. E' necessaria una analisi del flusso di generazione degli eventi e della quantità complessiva di log da analizzare/conservare nonché il tempo di archiviazione per decidere se adottare un modello di licenza unificato o diversificato quando possibile.

# SIEM Use Case Management Framework – Life Cycle

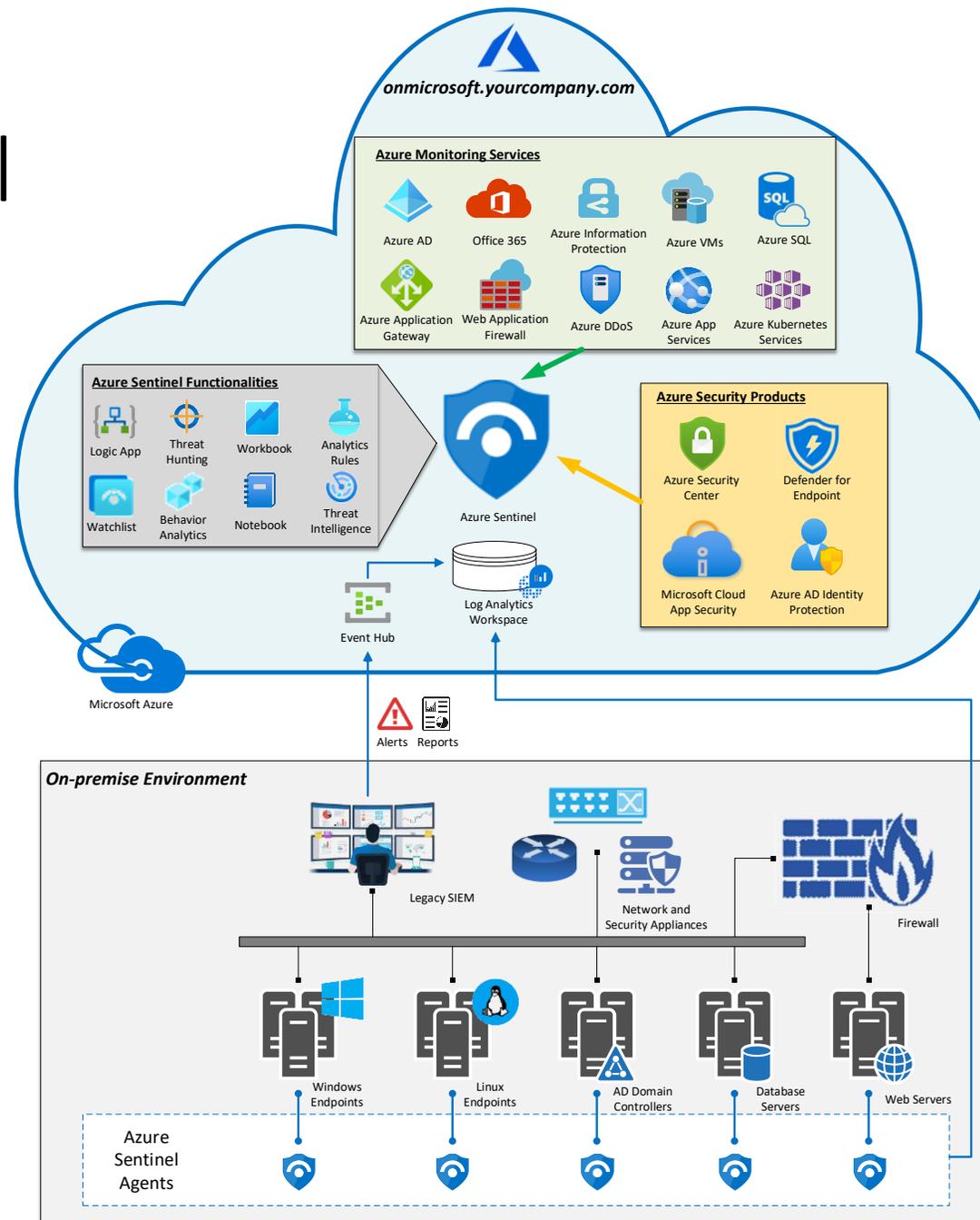


# Esempio di SIEM moderno su Cloud

Azure Sentinel (MSFT)

# Azure Sentinel

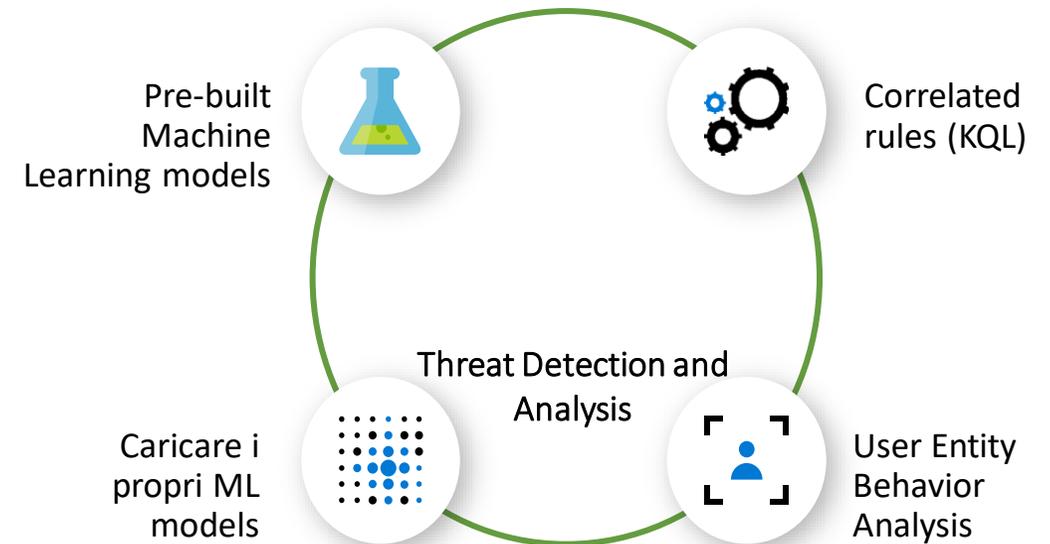
SIEM nativo su Cloud



# Vantaggi di un SIEM moderno nativo su Cloud

I vantaggi di un SIEM moderno nativo su Cloud rispetto a un SIEM tradizionale sono i seguenti:

- Nessuna necessità di installare e mantenere l'infrastruttura usata dal SIEM
- Nessun investimento iniziale, pagamento al consumo
- Capacità di scalare le risorse in modo automatico e assenza di limitazioni di calcolo o storage
- Capacità di estensione di sorgenti e apprendimento di nuove minacce più rapido (real-time threat detection)

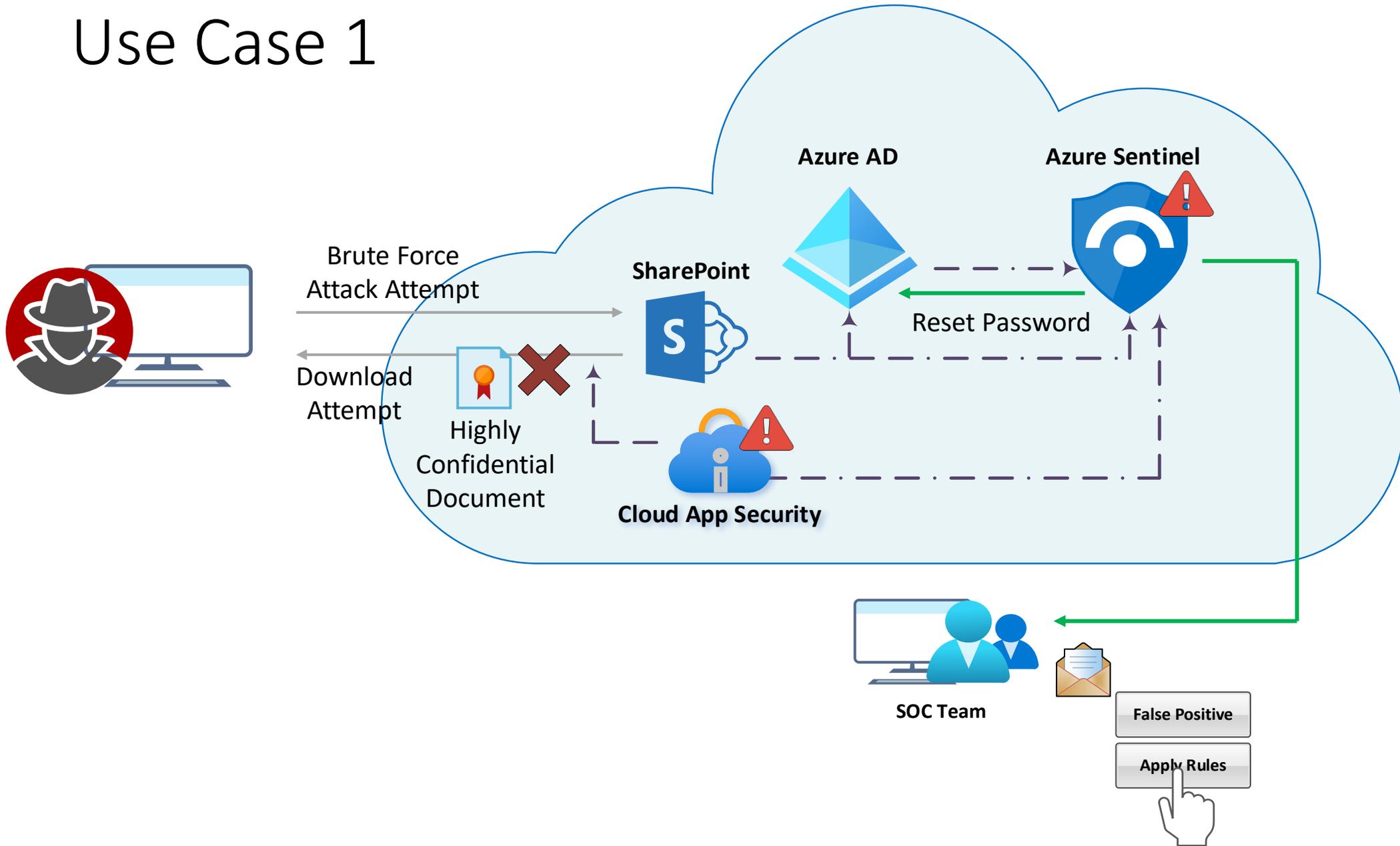


# Possibili use case e live Demo

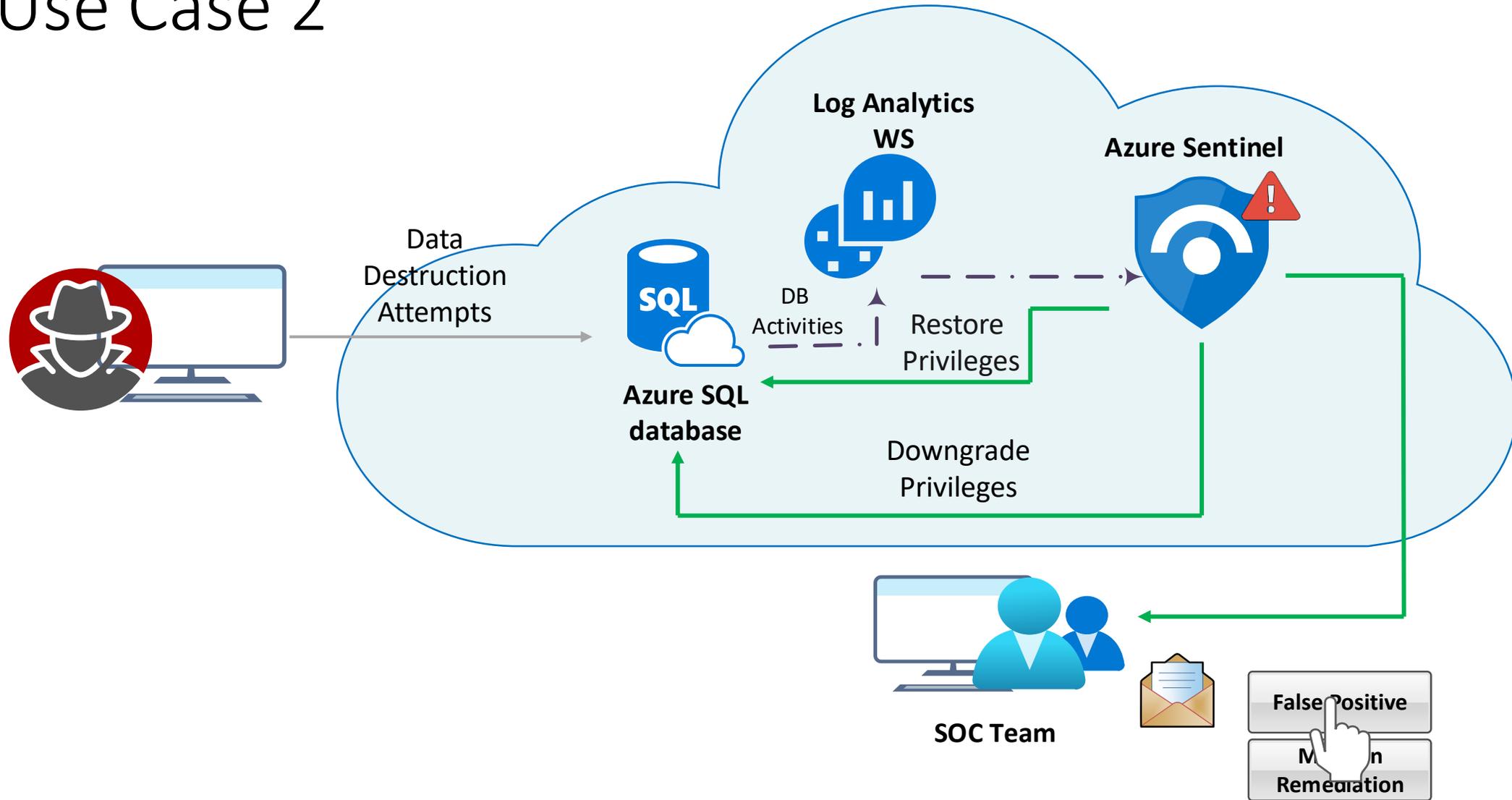
Esempi di possibili use cases

- 1. Brute force su sharepoint e tentativo di download di file confidenziali**
2. Brute force su utenza di dominio
- 3. Cancellazione massiva di dati**
4. Attività anomale su risorse Azure
5. Rilevazione di Malware
6. Attivazione di regole di email forwarding a seguito di login sospetti
7. Attacchi di SQL Injection su applicazione web

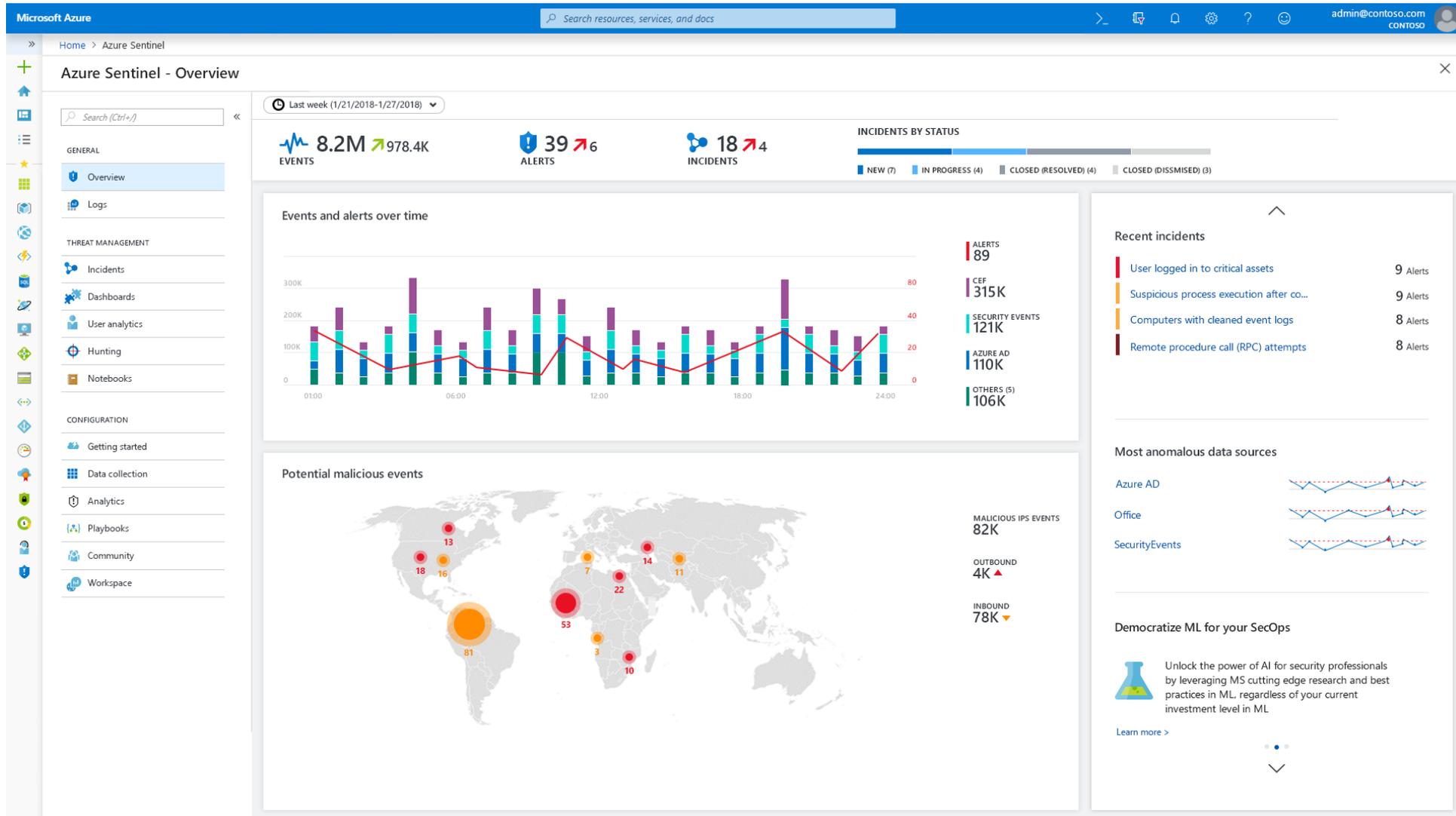
# Use Case 1



# Use Case 2



# Overview Interfaccia





# Logic Apps Design – Playbook

Dashboard > Azure Sentinel workspaces > Azure Sentinel - Playbooks > BlockIP\_PaloAlto\_BlockUserAAD\_ServiceNow > Logic Apps Designer

### Logic Apps Designer

Save Discard Run Designer Code view Templates Connectors Help

```
graph TD; A[When a response to an Azure Sentinel alert is triggered (Preview)] --> B[Open incident in ServiceNow (Preview)]; B --> C[Post a message to SOC channel (Preview)]; C --> D[Send approval email]; D --> E[Condition]; E --> F[If true]; E --> G[If false]; F --> H[Block user in Azure AD]; H --> I[Block IP in Palo Alto]; G --> J[Close incident in ServiceNow (Preview)];
```

Condition: And - Selected... x is equal to Block user and IP

If true: Block user in Azure AD, Block IP in Palo Alto

If false: Close incident in ServiceNow (Preview)

100%

SOAR



Fabio Vernacotola  
Avanade Security Practice Lead Italia  
Rome Area, Italy

Add profile section ▾ More...

- Avanade
- Coventry University
- See contact info
- See connections (286)

Fabio.Vernacotola@Avanade.com

S.Patonico@Avanade.com



Add profile section ▾ More...

Simone Patonico  
Security Analyst at Avanade  
Milano, Lombardy, Italy · 66 connections · Contact info

- Avanade
- Università Politecnica delle Marche