Sicurezza nelle grandi organizzazioni

Fabio Vernacotola, Simone Patonico

17/12/2019

Sezione 1

Progetti di sicurezza, perché…

Iniziative di sicurezza delle informazioni

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

SAIPEM ENGINEERING ENERGY

SAIPEM ANNIVERSARY

Saipem: aggiornamento sull'attacco informatico subìto

San Donato Milanese (MI), 12 dicembre 2018 - In riferimento al comunicato del 10 dicembre 2018, Saipem comunica che l'attacco informatico ha colpito i server basati nel Middle East, India, Aberdeen e, in modo limitato, l'Italia attraverso una variante del malware Shamoon.

L'attacco ha comportato la cancellazione di dati e di infrastrutture, effetti tipici del malware.

Le attività di ripristino, in modalità graduale e controllata, sono in corso attraverso le infrastrutture di back-up e, quando completate, consentiranno la piena operatività dei siti impattati.

Saipem mantiene costanti contatti con le autorità competenti per ogni opportuna azione.

Saipem è uno dei leader mondiali nei servizi di perforazione, ingegneria, approvvigionamento, costruzione e installazione di condotte e grandi impianti nel settore oil&gas a mare e a terra, con un forte orientamento verso attività in ambienti difficili, aree remote e in acque profonde. Saipem fornisce una gamma completa di servizi con contratti su base "EPC" e/o "EPCI" ('chiavi in mano') e dispone di capacità distintive ed asset ad alto contenuto tecnologico.

CNN Money Markets Economy Companies Tech Autos India Video International

British Airways' latest tech problem is a major credit card hack

Yet another technical meltdown is plaguing British Airways. This time, hackers stole the payment card details of 380,000 customers.

The company said the data thieves made off with the names, addresses, emails and credit card details including the card number, expiration date and security code belonging to travelers who booked flights on British Airways' website and app between August 21 and September 5. No passport or travel details were taken.

Risk management

- Rischio = Probabilità di un evento avverso * impatto dell'evento avverso

L'obiettivo dell'organizzazione è quello di:

- limitare l'impatto;
- limitare la probabilità;

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$ *

* fonte Ponemon Institute 2018

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;

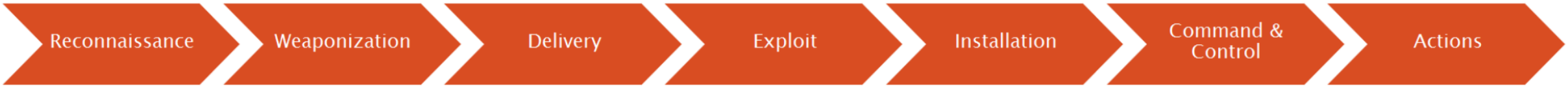
Esempio: infezione ransomware su un server

Ridurre la probabilità

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 obbiettivo 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

Cos’è un SGSI

Secondo la ISO27000:

Un SGSI consiste nelle policy, procedure, linee guida e risorse ed attvità associate gestate collettivamente dall’organizzazione allo scopo di porteggere 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	*Controllo* 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	*Controllo* 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	*Controllo* 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	*Controllo* 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	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

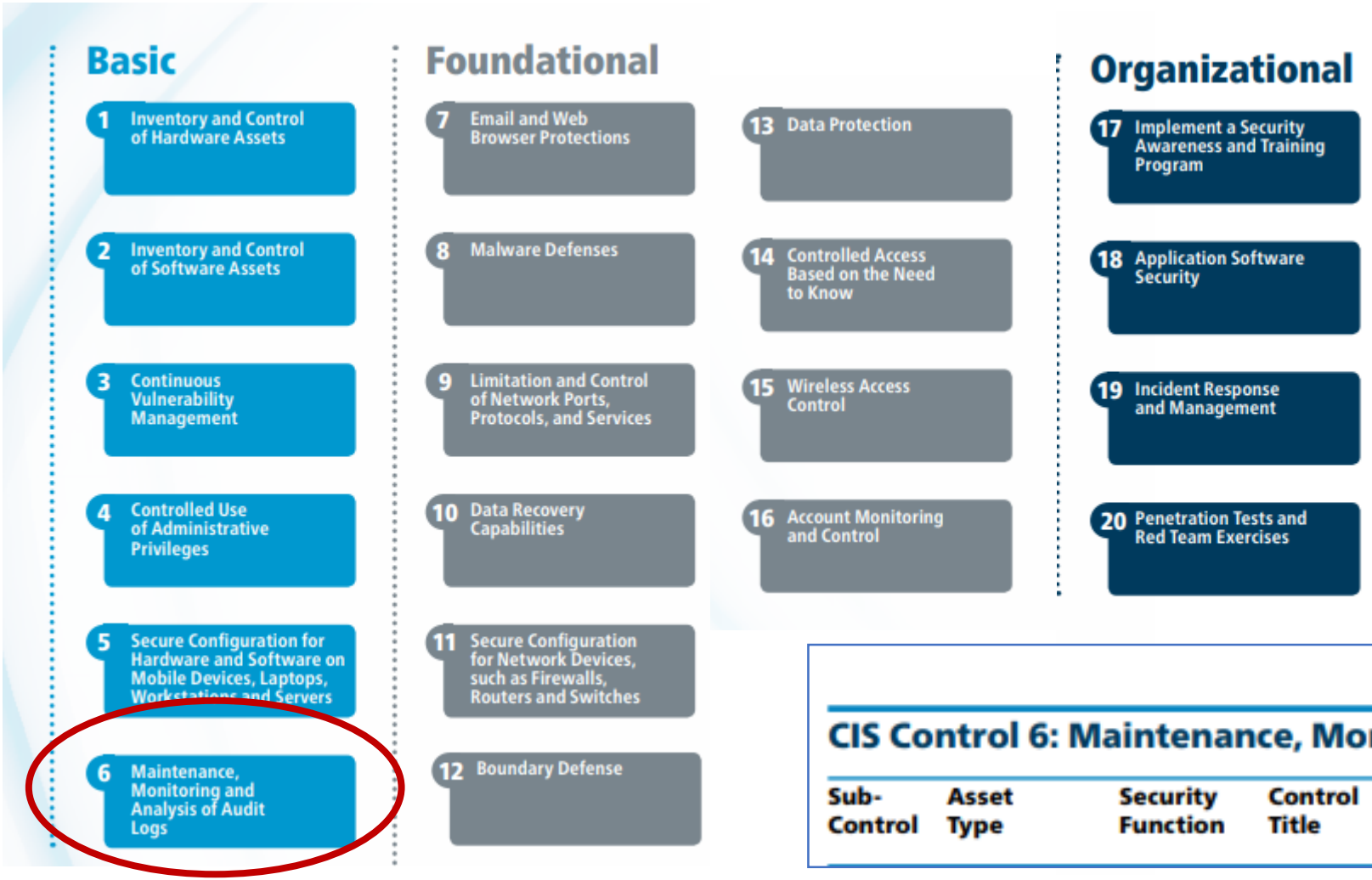
SANS TOP 20

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"



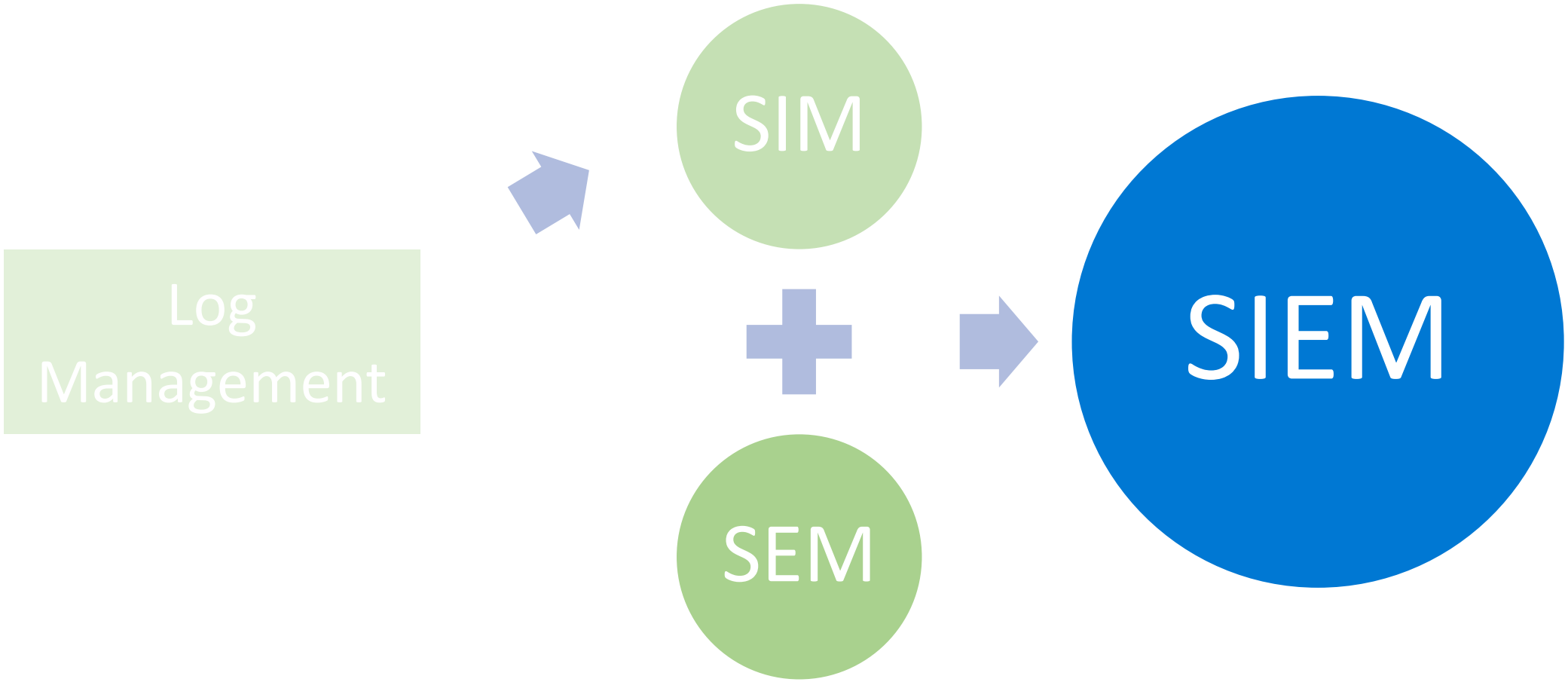
CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

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?

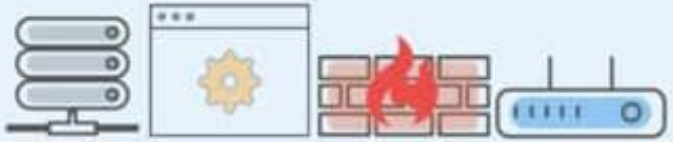


SIM vs SEM vs SIEM

SIM

SECURITY INFORMATION MANAGEMENT

Software che automatizza la raccolta dei log



Dati generati da numerose fonti

Forti capacità di gestione dei log

SEM

SECURITY EVENT MANAGEMENT

Gestione avanzata degli eventi, analisi delle minacce in tempo reale, visualizzazione, ticketing, risposta agli incidenti e security operations

Database

Dati generati dal database

Scarse capacità di gestione dei log

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

Combina funzionalità SIM e SEM

Mapping sui framework di controlli

A.12.4 Raccolta di log e monitoraggio		
Obiettivo: Registrare eventi e generare evidenze.		
A.12.4.1	Raccolta di log degli eventi	*Controllo* 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	*Controllo* 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	*Controllo* 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	*Controllo* 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

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

6

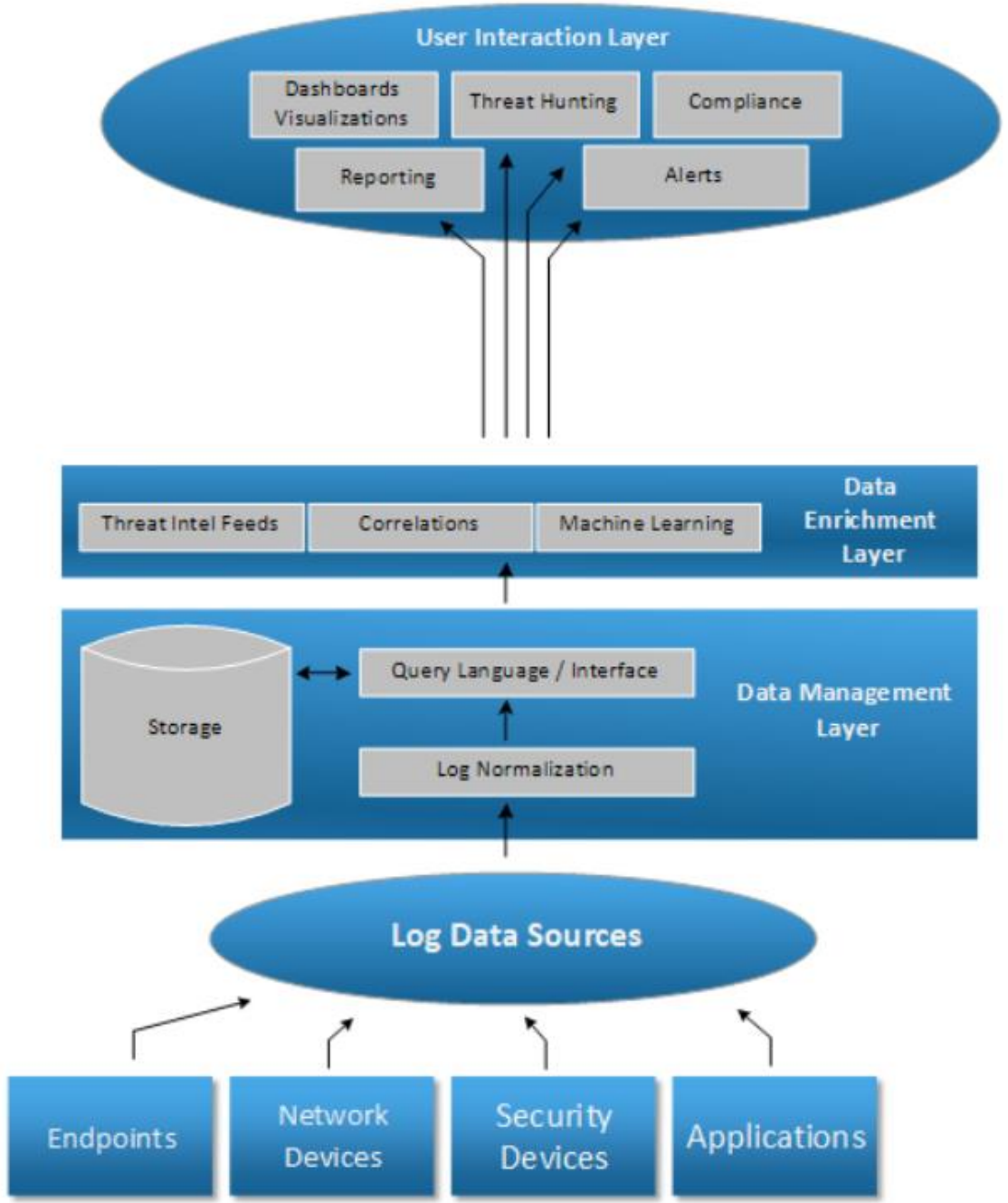
CIS Control 6:
Maintenance, Monitoring and Analysis of Audit Logs

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

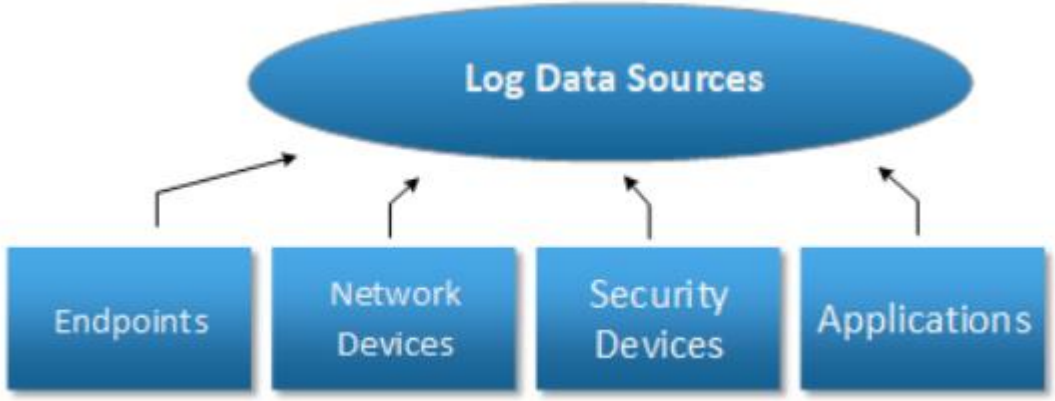


https://www.managedsentinel.com/2019/06/26/siem-traditional-vs-cloud/

Log and Event Collection

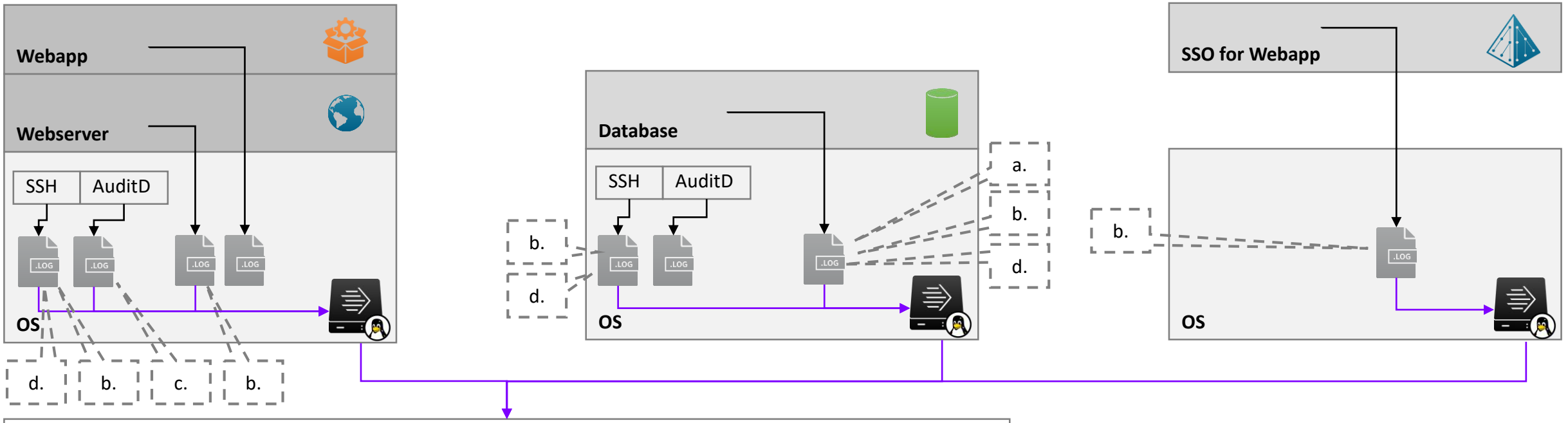
Un SIEM colleziona dati da varie sorgenti:

- 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)



Central Log Management – Onboarding Example

Schematic sample view on core onboarding components



Requisiti:

a. Monitorare l'accesso non autorizzato al database applicativo
b. Monitorare l'eccessivo numero di login falliti da account tecnici, utenti e amministratori
c. Monitorare modifiche non autorizzate a file di configurazione rilevanti a una o più applicazioni
d. Monitorare e rilevare la creazione di account locali

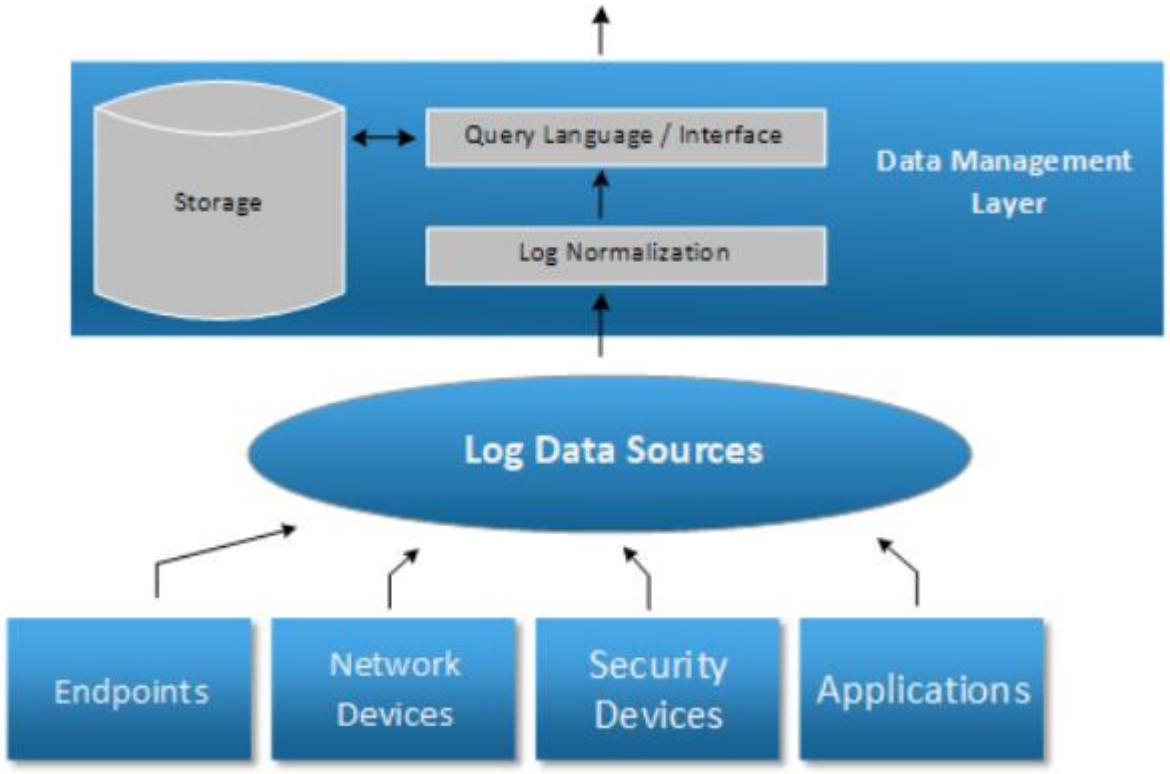
- Il Log Management per un'applicazione coinvolge sempre diverse componenti
- Una chiara visione architetturale dell'applicazione permette di identificare facilmente i rischi e le vulnerabilità
- Definire il dettaglio dei log per componenti standard come sistemi operativi, database server, etc. Può ridurre significatamente la quantità di lavoro

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

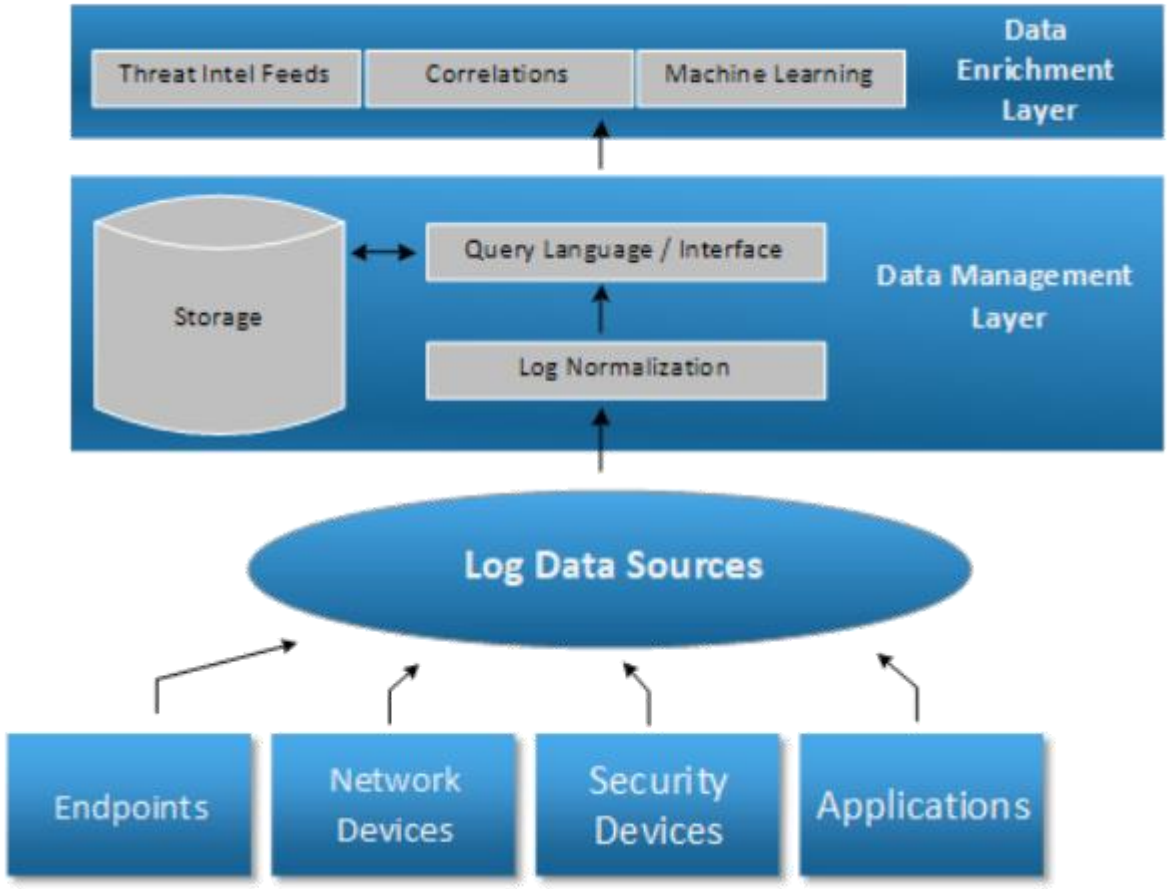
- Filtraggio ed aggregazione dei dati mediante query



Data Enrichment Layer

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

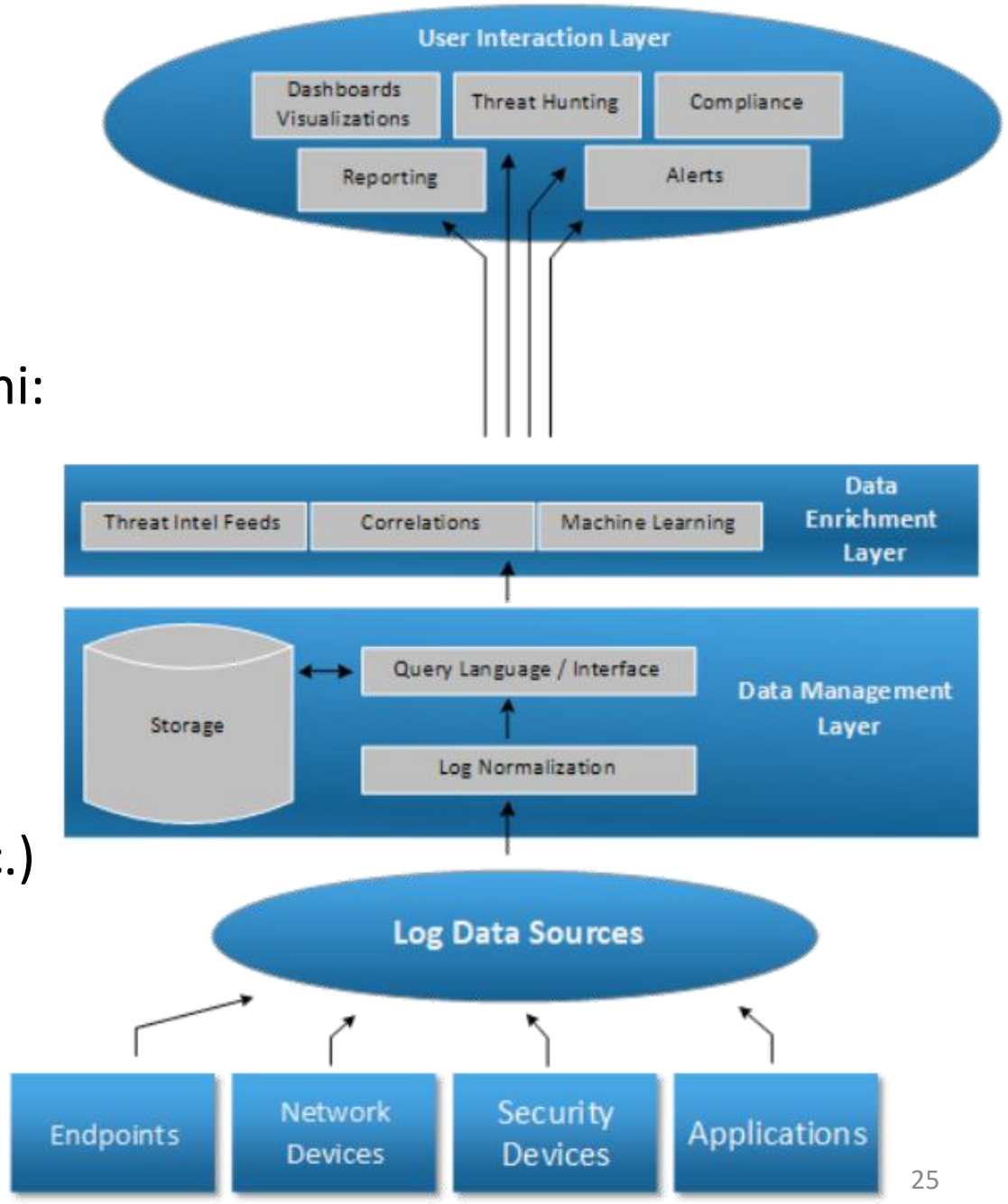
- Arricchimento dei dati con informazioni aggiuntive (es: posizione geografica)
- Correlazione dei log delle diverse sorgenti di sicurezza
- Correlazione con Threat Intelligence da fonti esterne
- Correlazione con informazioni aggiuntive fornite dagli algoritmi di machine learning



User Interaction Layer

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

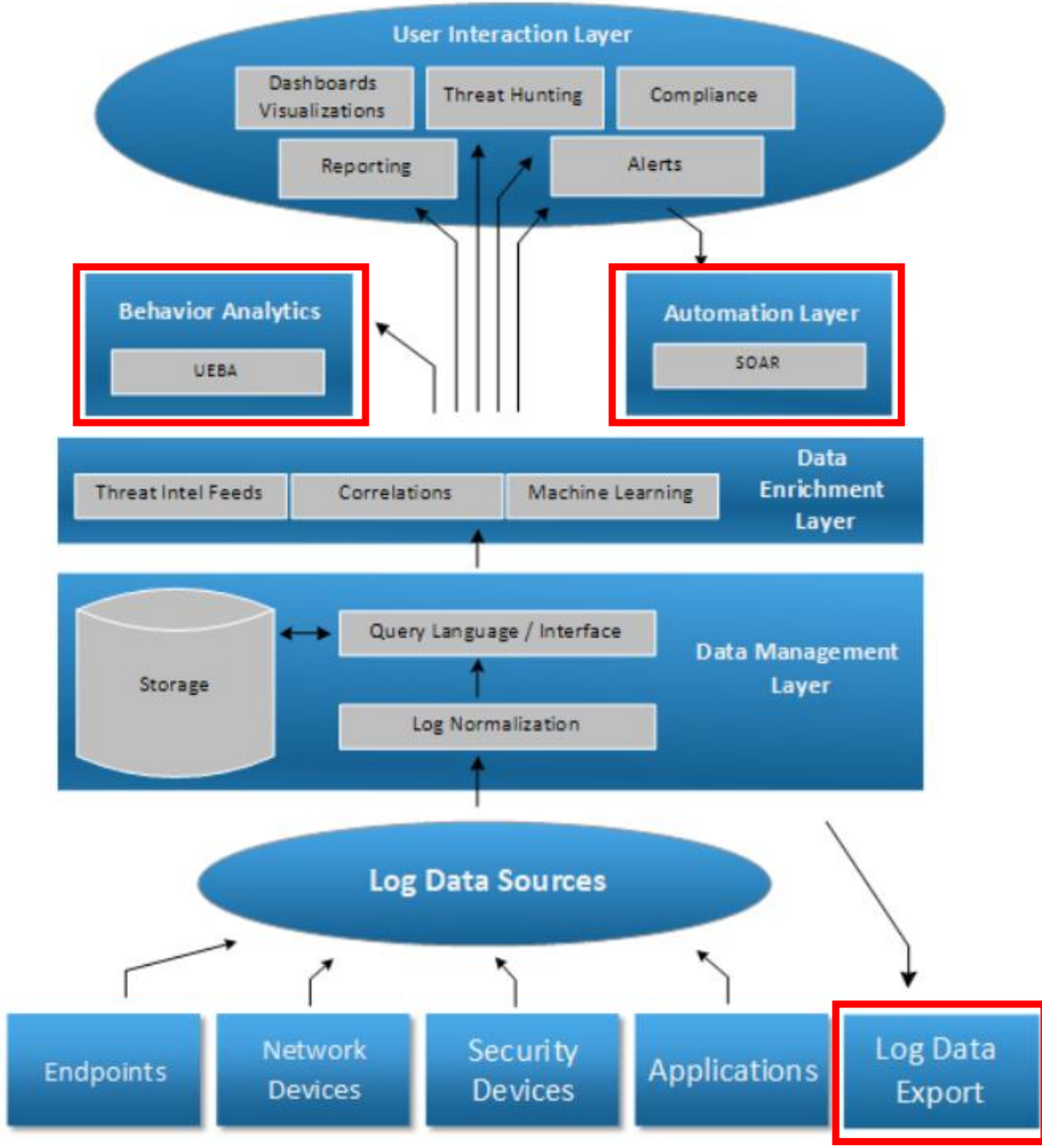
- Dashboards
- Report periodici su specifici utenti
- Threat Hunting per la ricerca di specifici eventi / attacchi
- Compliance per la generazione di report soddisfacenti norme legali (PCI, GDPR, etc.)
- Alerts
  - Notifica specifici utenti/amministratori



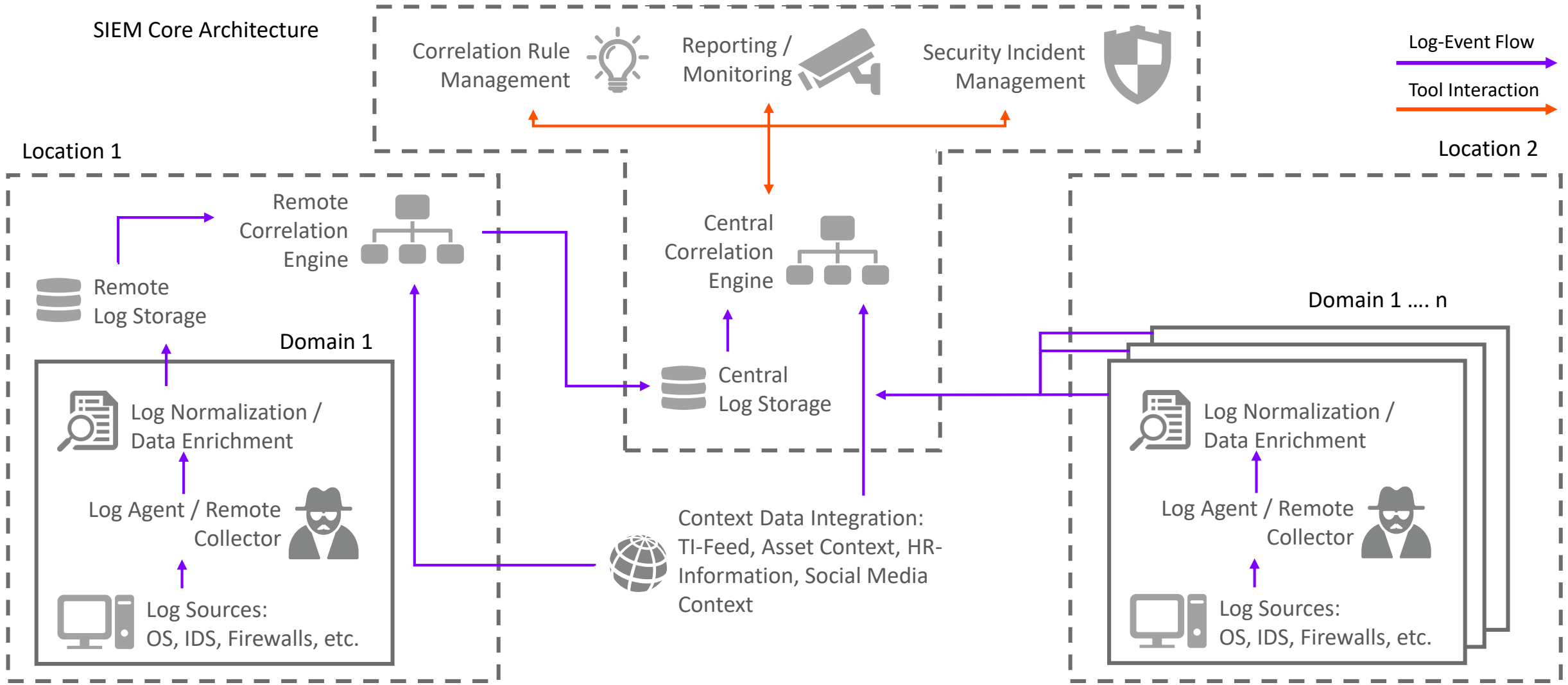
SIEM moderno

Un SIEM moderno aggiunge 3 funzionalità:

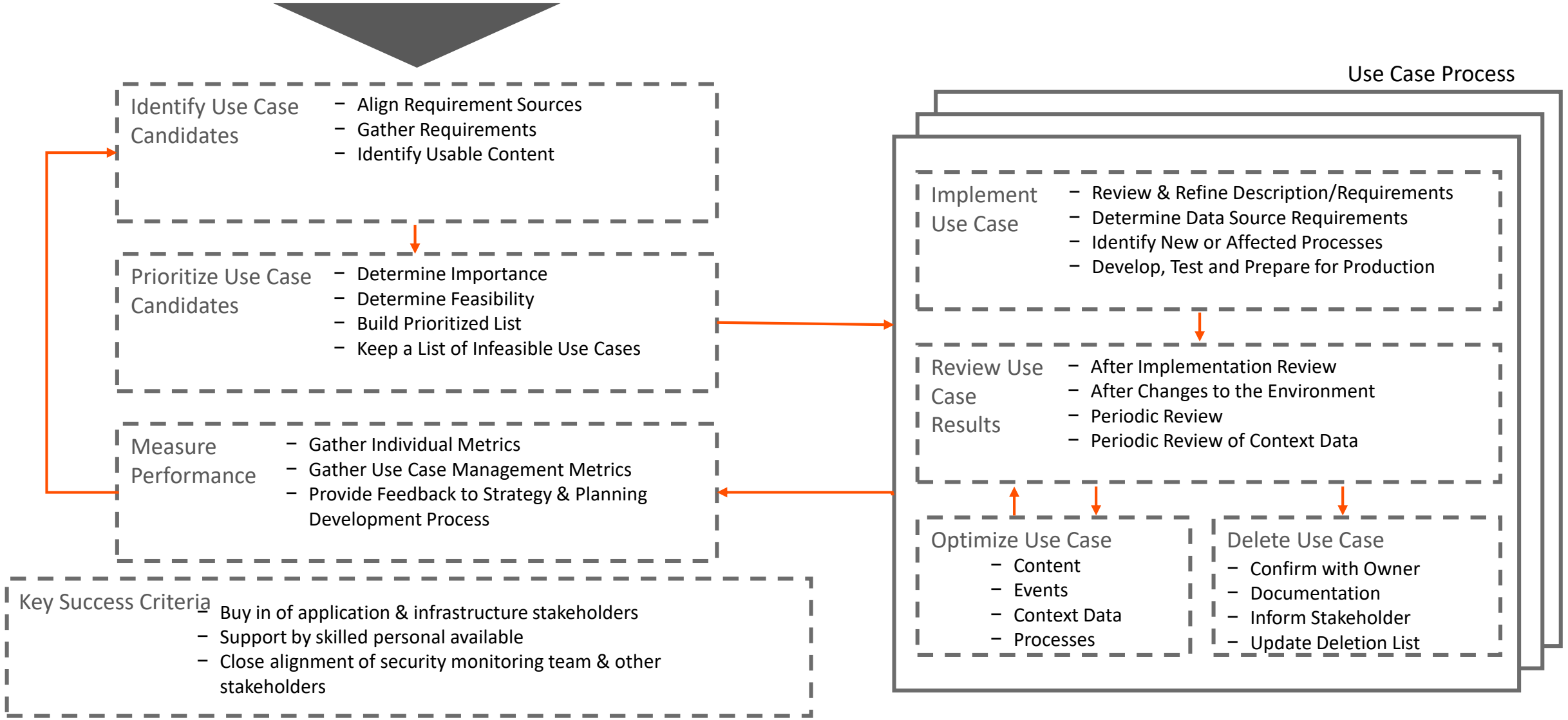
- **Automation Layer**. Funzionalità SOAR per la risposta automatica ad incidenti (Playbooks)
- **Behavior Analytics**. Funzionalità UEBA per l'identificazione di comportamenti anomali
- **Log Data Export**. Esportazione dei dati su software di terze parti



SIEM Deployment Architecture - Example



SIEM Use Case Management Framework – Life Cycle

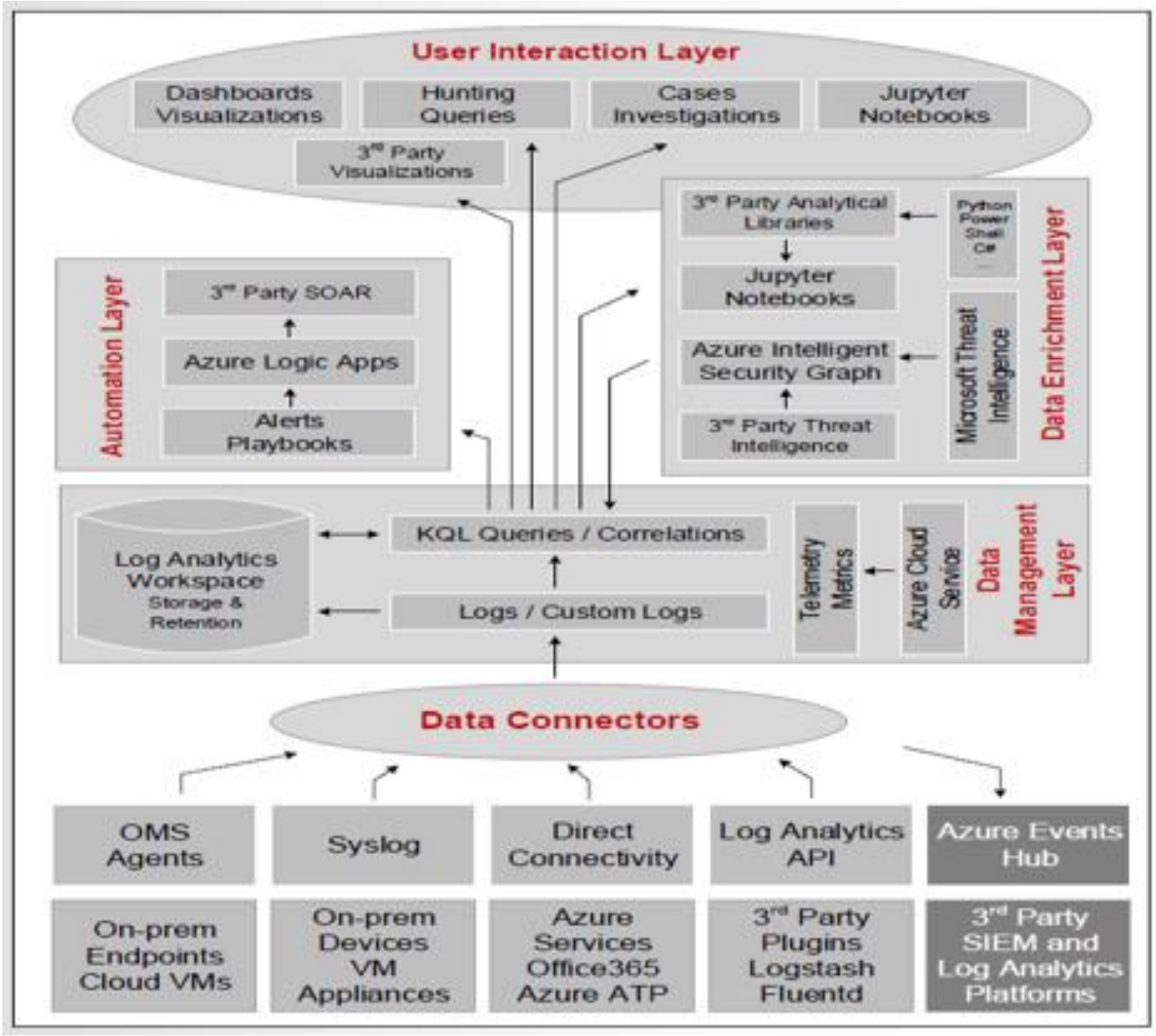


Esempio di SIEM moderno su Cloud

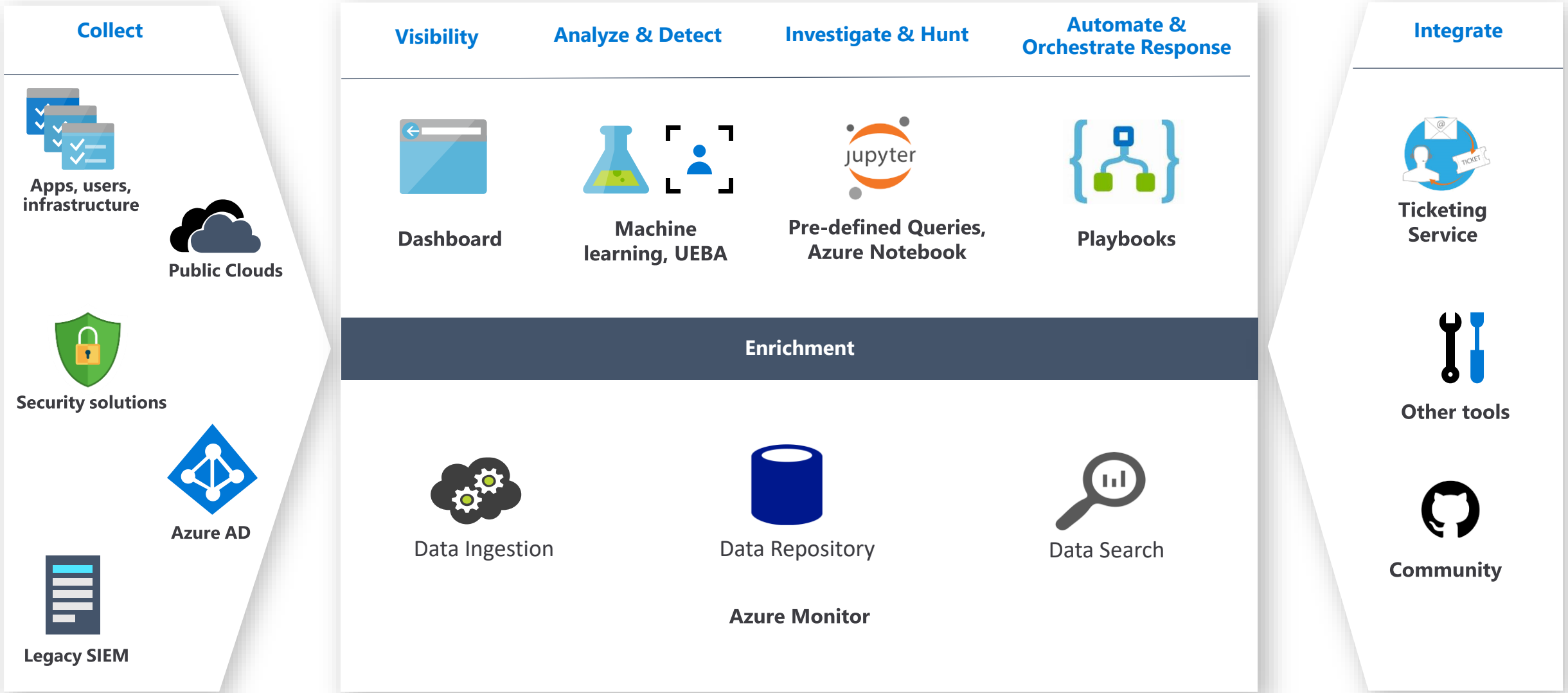
Azure Sentinel (MSFT)

Azure Sentinel

SIEM nativo su Cloud



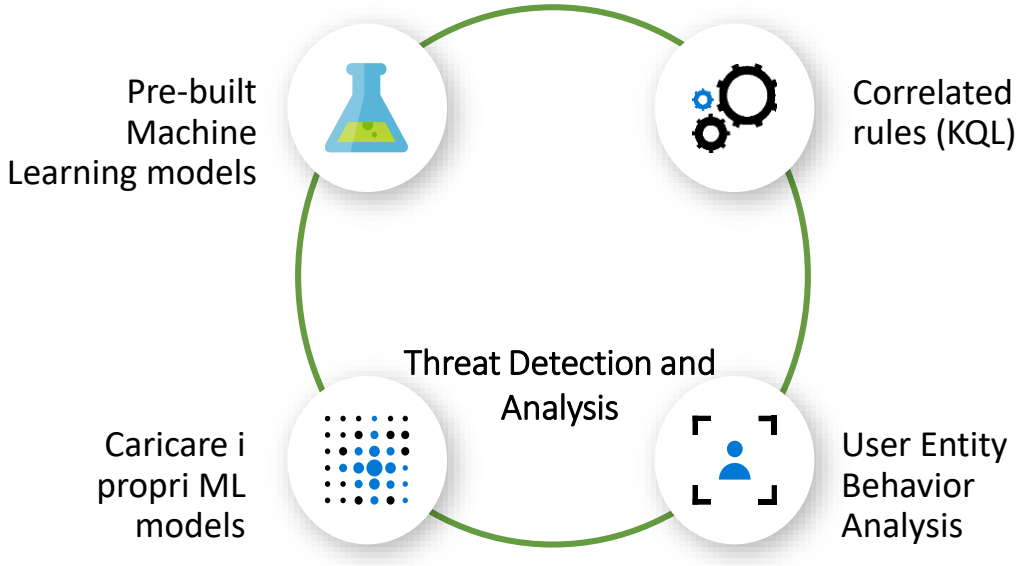
Ovierview funzionalità di Azure Sentinel



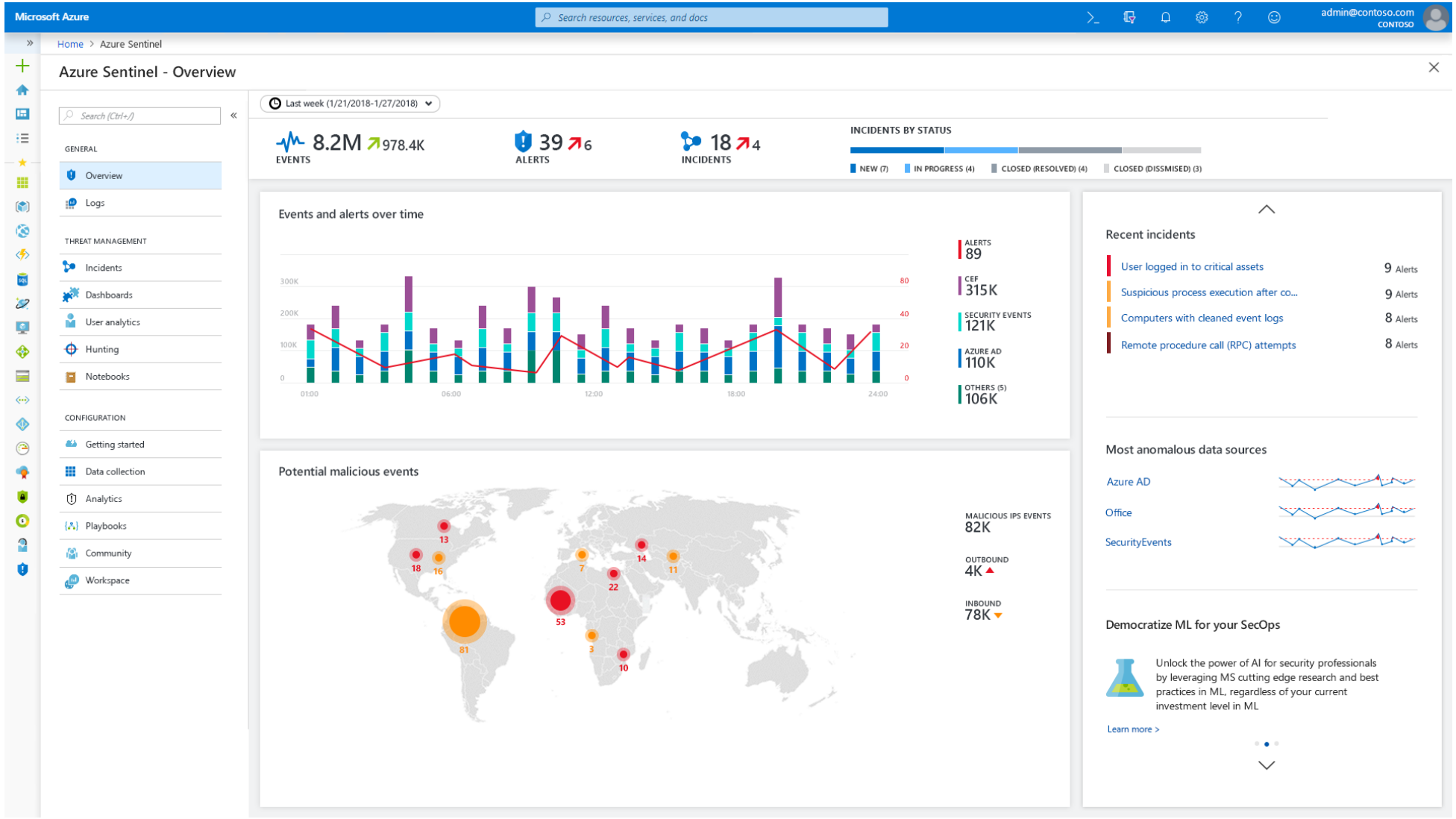
Vantaggi di un SIEM moderno nativo su Cloud

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

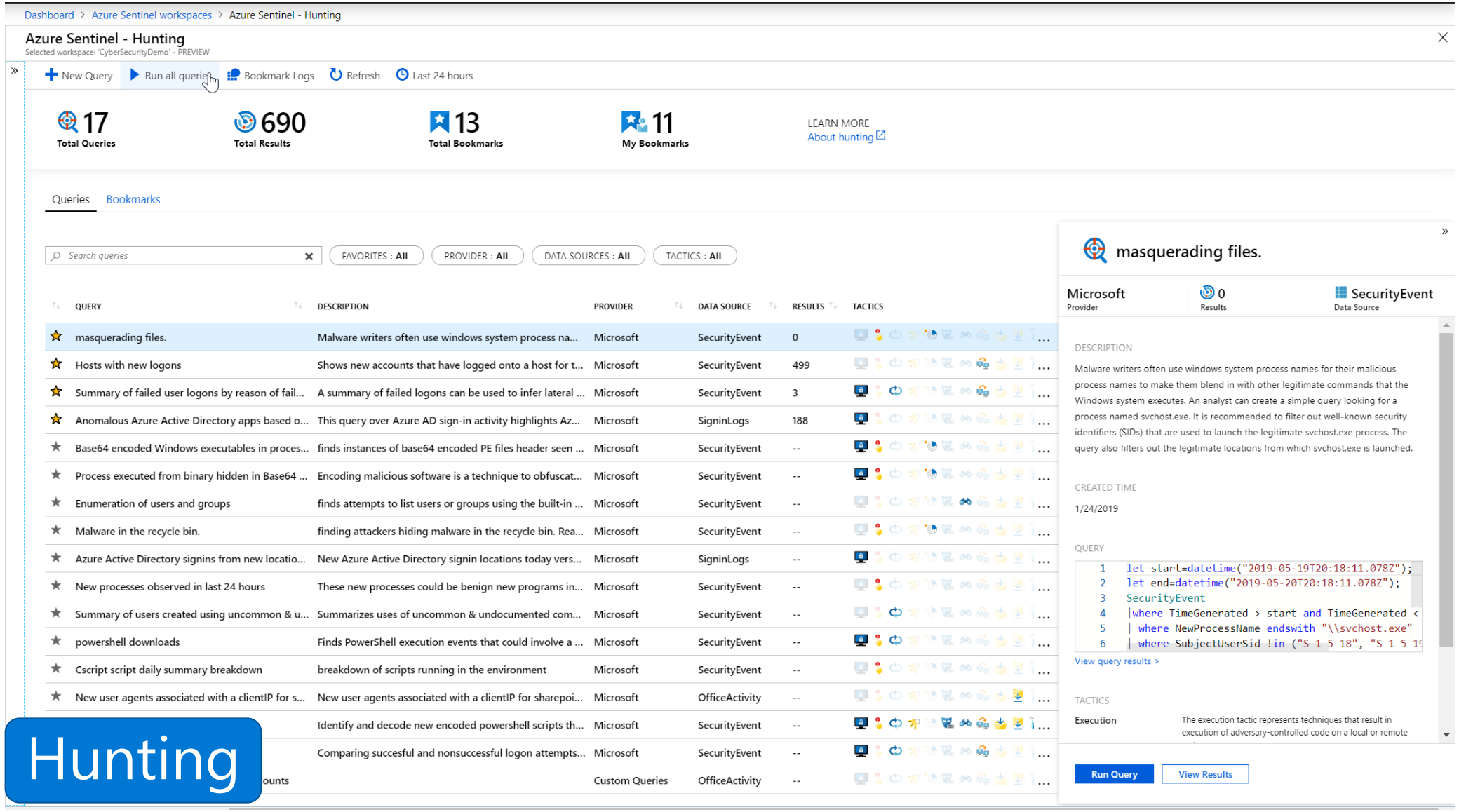
- Nessuna necessità di installare e mantenere l'infrastruttura usata dal SIEM
- Nessun investimento iniziale, pagamento al consumo
- Capacità di scalare le risorse in modo automatico e assenza di limitazioni di calcolo o storage
- Capacità di estensione di sorgenti e apprendimento di nuove minacce pù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



Overview Interfaccia

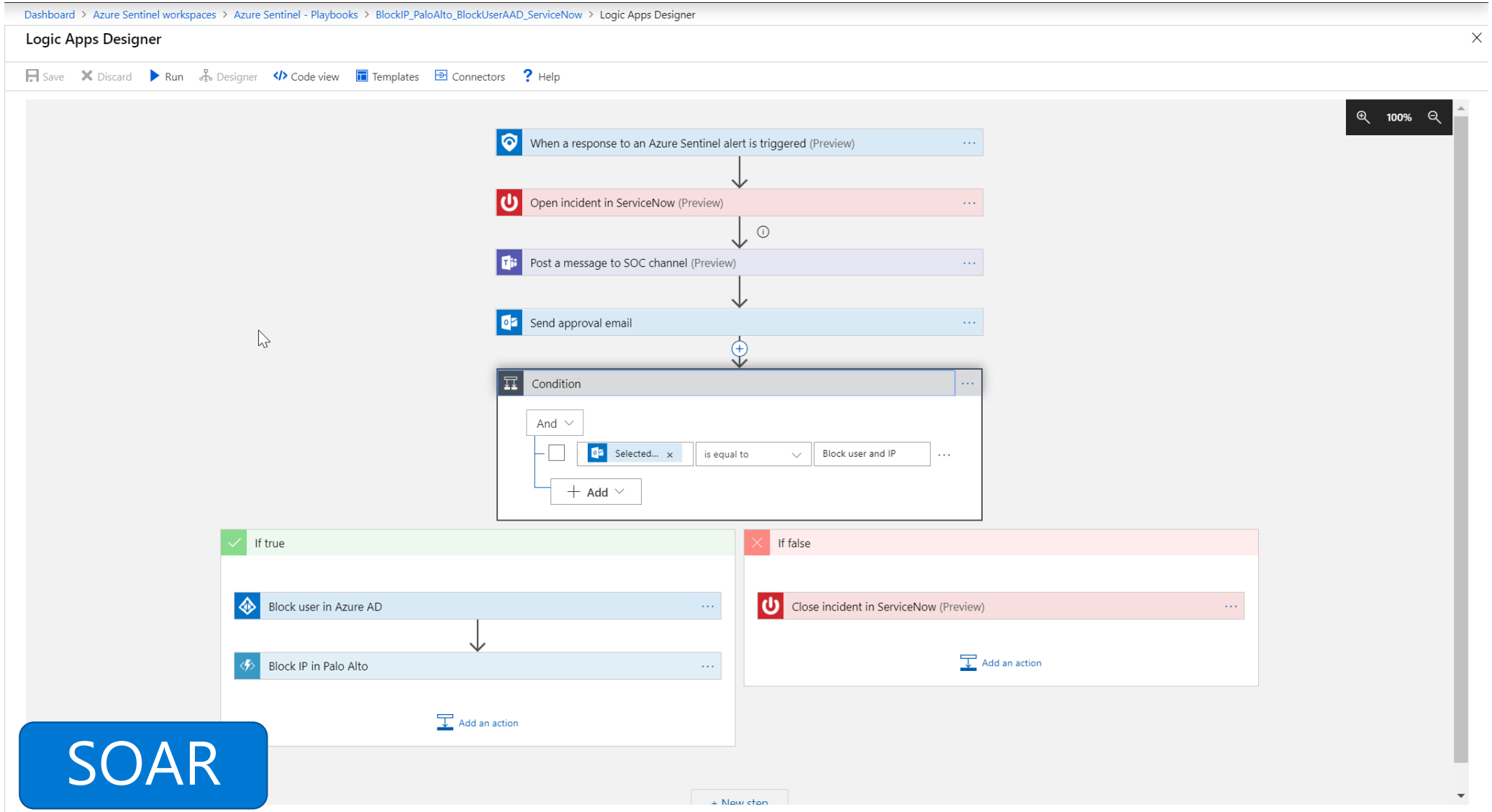


Hunting – linguaggio di query KQL



Hunting

Logic Apps Design – Playbook



SOAR