

# SIEM (Security Information & Event Management)

## La soluzione

Il servizio **SIEM** (*Security Information & Event Management*). La caratteristica principale di questa tecnologia è quella di raccogliere i dati da tutte le risorse critiche che risiedono sulla rete e di presentare tali dati come informazioni utilizzabili tramite un'unica interfaccia. SIEM consente al Security Team di ottenere una comprensione completa dello stato di sicurezza delle risorse, assegnare priorità agli incidenti e di dimostrare la conformità alle normative in modo efficiente.

## A chi è rivolto?

Per la sua natura e per le normative vigenti tutti gli enti ed istituzioni dovrebbero dotarsi di uno strumento SIEM. La soluzione è funzionale alla sicurezza informatica per quelle aziende che hanno un gran numero di dispositivi e prodotti diversi e su cui risulta difficile effettuare analisi forensi o azioni di controllo.

Il SIEM consente anche di velocizzare le attività di audit funzionale alle "compliance" vigenti e di produrre strumenti di sintesi e report per il monitoraggio di quanto avviene nell'infrastruttura ICT.

Uno strumento SIEM moderno è anche utile per tutte le aziende che hanno necessità di migliorare la propria postura in termini di sicurezza operativa e che intendono dotarsi di una struttura di Cyber Security.



## Come erogiamo il servizio

Cybertech offre due tipi di Servizi:

1. Servizio di installazione, configurazione e messa in opera della piattaforma e successiva gestione in modalità SaaS (Software as a Service) o On Premise.
2. Servizio di gestione della piattaforma esistente del cliente, mettendo a disposizione le nostre competenze attraverso gli servizi erogati dalla **Control Room Cybertech** o il supporto dei nostri esperti On Premise (presso le strutture del cliente).



## Punti di forza

- Capacità di raccogliere i dati di sicurezza da tutte le risorse critiche che risiedono sulla rete;
- Presentare tali dati come informazioni utilizzabili tramite un'unica interfaccia.



## Perché SIEM

- Per rilevare e risponde alle minacce e alle violazioni di sicurezza IT;
- Per ridurre il rischio;
- Per garantire la conformità.



## Vantaggi

- Soluzione chiavi in mano (SaaS);
- Gestione remota della piattaforma;
- Disponibilità del centro di competenze Cybertech.



Opzioni del servizio	Bronze	Silver	Gold
<b>Metriche della fornitura (Ambiente di Produzione)</b>			
Eventi al secondo	Fino a 1000	Fino a 2500	Fino a 5000
Flussi al minuto	Fino a 25 mila	Fino a 100 mila	Fino a 200 mila
Tipologie di sorgenti log	Fino a 15	Fino a 30	Fino a 45
Sorgenti log	Fino a 200	Fino a 500	Fino a 1000
<b>Features</b>			
1 Ambiente di Produzione	✓	✓	✓
Log source integration	✓	✓	✓
Modifica o creazione dashboard	✓ (n°1)	✓ (n°3)	✓ (n°5)
Modifica o creazione report	✓ (n°3)	✓ (n°5)	✓ (n°10)
Network hierarchy onboarding	✓	✓	✓
Retention configuration	✓ (n°1)	✓ (n°2)	✓ (n°5)
Daily configuration backup	✓	✓	✓
Weekly data backup	✓	✓	✓
Restore in case of failure to latest valid backup (1 backup every 24 hours – maintaining 3 days of configuration backup and 2 weeks of data backups)	✓	✓	✓
<b>Corrective Maintenance (1 year starting from production delivery)</b>			
Support on delivered features	✓	✓	✓
Platform Monitoring	✓	✓	✓
Tickets per year	25	60	120



# IBM QRADAR

Con **IBM QRADAR** ottieni

- *Insight concretamente utilizzabili;*
- *Rilevazione rapida delle minacce informatiche;*
- *Consolidamento degli avvisi per una chiara identificazione dei rischi.*



## Osserva tutto

**QRadar** permette una visibilità completa dei dati aziendali in ambienti on-premise e basati su cloud da un'unica schermata.



## Automatizza l'intelligence

**QRadar** rileva le minacce conosciute e sconosciute, va oltre i singoli avvisi per identificare e dare priorità ai potenziali incidenti e applica l'AI per accelerare i processi di indagine del 50%.



## Diventa proattivo

**QRadar** permette di ottenere un feedback continuo e costante e utilizza il tempo risparmiato per individuare proattivamente le minacce e automatizzare i processi di contenimento.



**Per saperne di più visita il sito**  
[www.cybertech.eu](http://www.cybertech.eu)

