

# **CYBERPACK: Security Information and Event Management**

**SOLUZIONI CYBERTECH**

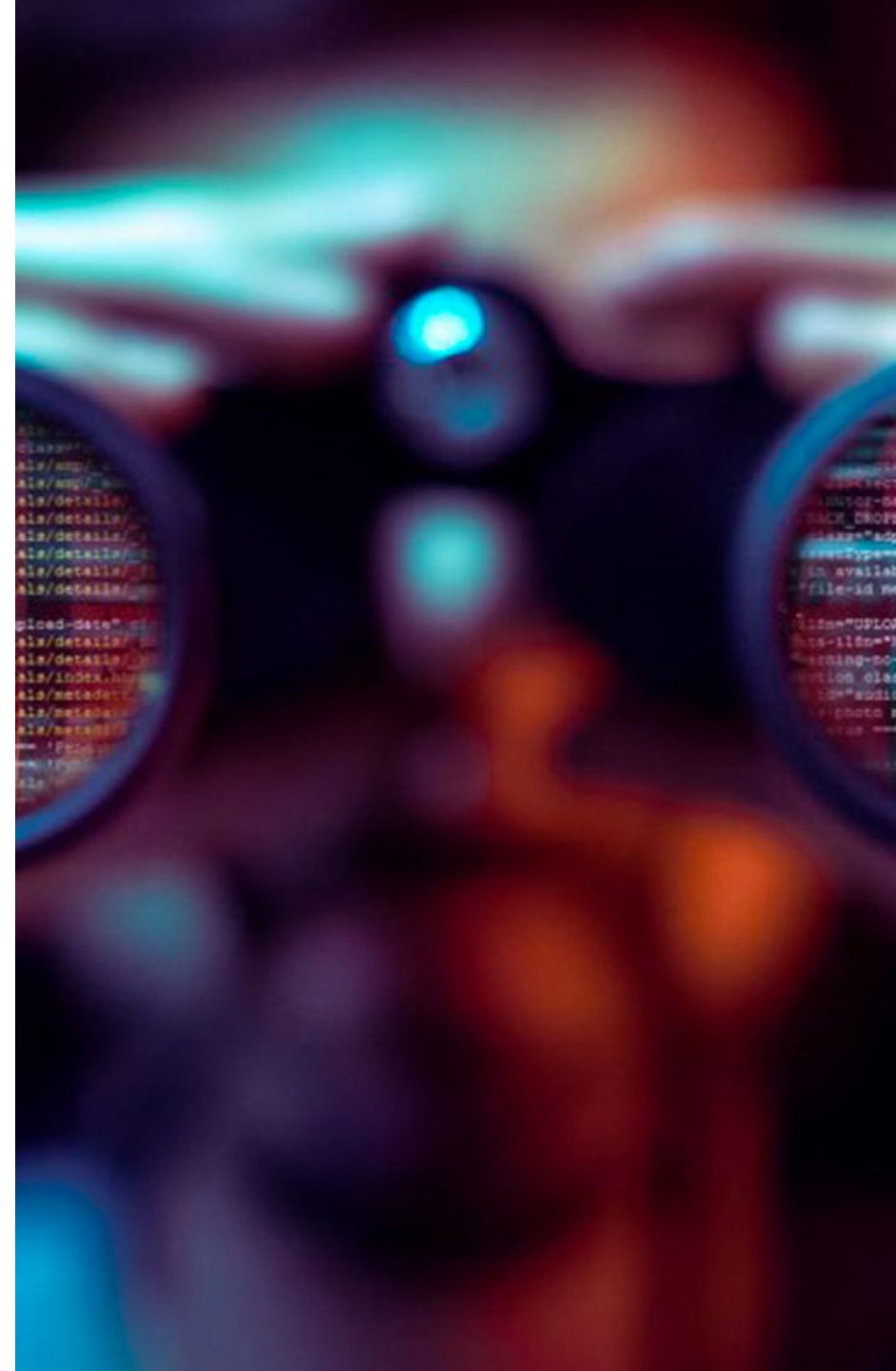


# Il contesto

**Gli attacchi cyber sono in costante crescita ed evolvono velocemente.**

- Si infiltrano nei sistemi aziendali
- Eliminano le proprie tracce
- Avanzano in cerca di dati sensibili

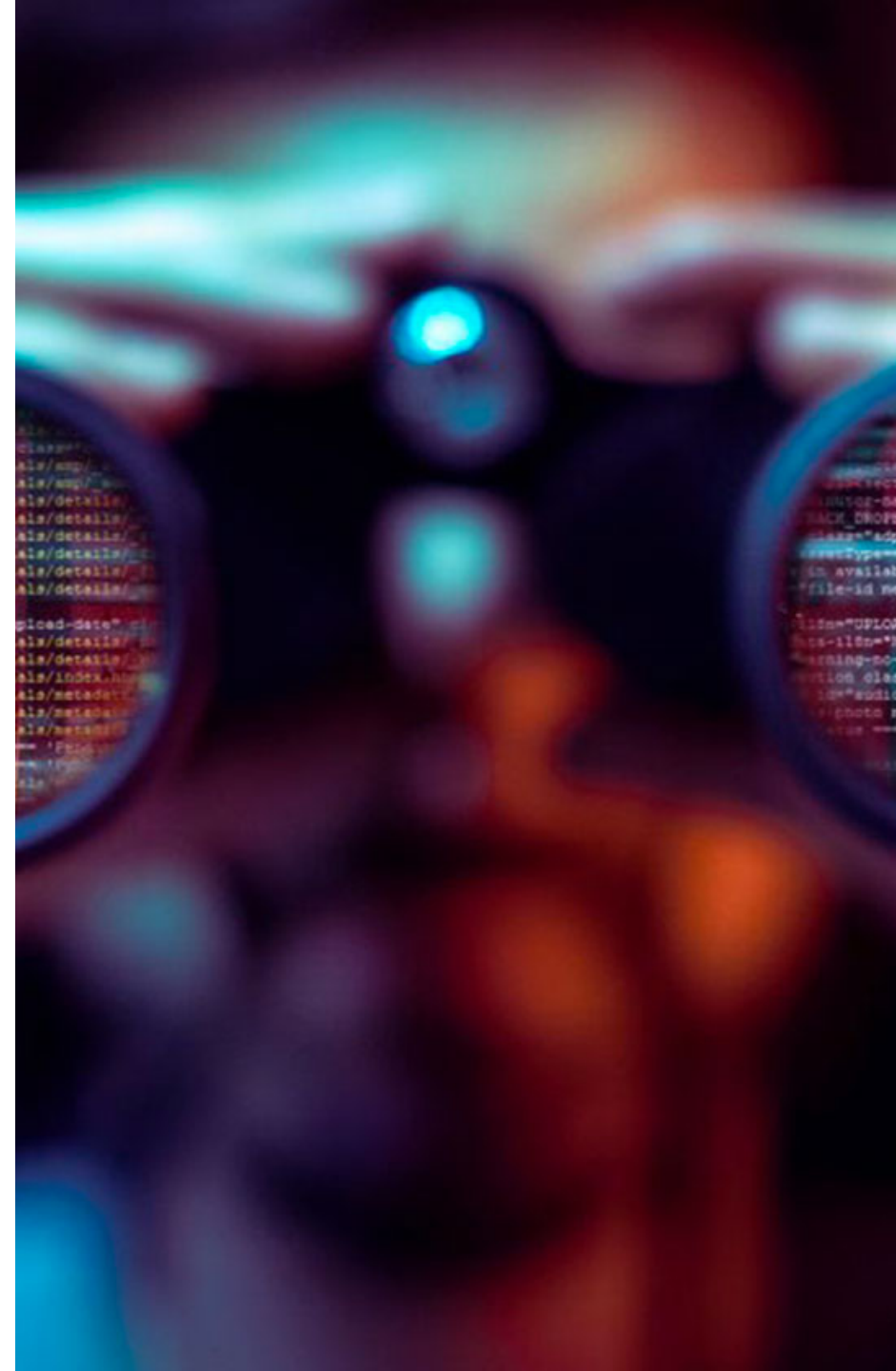
**Per rilevare e contenere un attacco, le aziende impiegano in media più di 8 mesi.**



# Esigenze

**Per proteggere i dati Aziende e Istituzioni hanno bisogno di:**

- una visione completa del potenziale rischio
- saper riconoscere l'evento effettivamente malevolo
- reagire rapidamente, sia prima che dopo aver subito un attacco



# La soluzione

## Security Information and Event Management

### 1. SIM - Security Information Management

Analisi e riproduzione di report per aderire a norme di compliance.

### 2. SEM - Security Event Management

Monitoraggio degli eventi in real time.



# Benefici

## La soluzione consente:

- Controllo in tempo reale dei fenomeni
- Monitoraggio dell'attività degli utenti e delle applicazioni
- Correlazione dei dati (intelligenza del sistema)
- Effettuare query e report di compliance
- Analisi sistematica degli eventi

# Benefici

**Con le soluzioni SIEM è possibile prevenire gli attacchi interni ed esterni:**

- Rilevando possibili attacchi interni
- Tenendo traccia dei sistemi infetti
- Creando alert (sistema compromesso da Malware o Data Breach)
- Effettuando un replay di eventi passati per l'analisi
- Generare report provenienti dal log ai fini di Incident Response e Compliance

# Opzioni del servizio

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





# 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.

**I tuoi dati  
in mani sicure**

