CYBER SECURIT



DIGINETICA IT WORKS

La Cybersecurity per proteggere il tuo business

- Next Gen Firewall
- Endpoint Protection
- E-Mail Protection
- Identity Protection
- Data Protection/Backup
- Vulnerability Assessment
- Vulnerability Remediation & Patch Management
- Forensic

Soluzione CybersecurIT®
con SOC 24/7 integrato a MS365

Il prodotto **CybersecurIT®** è dotato di **SOC attivo 24/7**, offre un'**integrazione completa con Microsoft 365**, rappresentando un importante valore strategico per la piattaforma.
Questa integrazione estende la visibilità e il controllo ben oltre l'endpoint, abilitando una **protezione EDR** (Extended Detection and Response) realmente efficace, in grado di individuare compromissioni trasversali che coinvolgono email, identità e dispositivi.

Grazie a questa architettura, la soluzione si configura come ideale per aziende che utilizzano **Microsoft 365**, ma non dispongono di un SOC interno o di un'infrastruttura SIEM avanzata.

Protezione Modulare (3 componenti principali)

Managed EDR

Managed Identity

Managed SIEM

Managed EDR

Protezione avanzata degli endpoint, con monitoraggio continuo e intervento diretto del SOC (attualmente in lingua inglese).

Managed Identity (opzione consigliata)

Sicurezza degli account cloud e gestione delle identità in ambiente Microsoft 365.
Protegge gli account cloud, con particolare attenzione a Microsoft 365. Rileva e blocca attività anomale relative agli accessi e alla gestione identità, difendendo da:

- Accessi da località/orari/dispositivi inconsueti
- Escalation non autorizzate di privilegi
- App OAuth potenzialmente dannose
- Creazione o modifica di regole email sospette
- Attività automatizzate che indicano compromissione

Il modulo si integra via API con Microsoft 365 e viene supervisionato dal SOC attivo 24/7, che arricchisce gli alert e supporta con azioni dirette (disattivazione, reset credenziali, investigazione).

Ideale per aziende prive di un SOC interno o SIEM, offre sorveglianza continua sulle identità cloud senza configurazioni complesse e con tempi di reazione rapidi.

Managed SIEM (opzione consigliata)

Una soluzione SIEM **completamente gestita**, che unisce raccolta intelligente dei log e intervento SOC per rilevamento, risposta e conformità. Le funzionalità principali sono:

- **Smart Filtering dei log:** Raccolta mirata da endpoint, firewall, VPN, AD, password manager, ecc. Riduce falsi positivi e costi di storage.
- **SOC 24/7:** Monitoraggio continuo, threat hunting e remediation dettagliata.
- **Visibilità estesa:** Integrazione log da firewall (Fortinet, Palo Alto) e servizi PAM (Duo, 1Password, Keeper).
- **Retention fino a 7 anni:** Conforme a normative come PCI-DSS, CMMC. Archiviazione cifrata e sicura.
- **Integrazione flessibile :** Supporto per agent già in uso (EDR/SIEM) o collector Syslog.

Vuoi scoprire come CybersecurIT® può proteggere la tua azienda? Contattaci!