1. **SIEM e Ingestion dei Log:** *All'interno di un'architettura SIEM, come affronterebbe il problema del bilanciamento tra la necessità di raccogliere log in modo capillare (es. log di endpoint, firewall, application server) e i limiti di banda o di licenza (EPS/GB al giorno)? Quali log considererebbe "indispensabili"?*

2. **Gestione dello Shadow IT:** *Nel mondo della ricerca è frequente l'uso di software open-source non validati o di servizi cloud di terze parti scelti autonomamente dai singoli team scientifici (Shadow IT). Quali azioni organizzative, policy e strumenti di governance implementerebbe per censire e normare questo fenomeno?*

3. **Prioritizzazione del budget di sicurezza:** *Se si trovasse a gestire un budget limitato e dovesse scegliere tra investire nel potenziamento del SOC/SIEM (rilevamento) o nel rinnovo/potenziamento dell'infrastruttura di backup immutabile (resilienza/ripristino), quali criteri di business e di rischio utilizzerebbe per guidare la scelta della Direzione?*

4. **Incident Response e Digital Forensics:** *Durante la fase di contenimento di un potenziale attacco ransomware su un server critico, quali manufatti o evidenze forensi andrebbero preservati e analizzati prioritariamente prima di procedere al ripristino o all'isolamento?*

5. **Gestione del rischio e framework nazionali:** *Come imposterebbe il processo di analisi del rischio cyber nell'Ente utilizzando framework di riferimento? Come documenterebbe il legame tra i rischi individuati e le misure di mitigazione approvate dalla Direzione?*

Fabiana Brancolini
06.07.2026 13:29:12
GMT+02:00