Sistema di difesa di Cyber Security avente le seguenti caratteristiche:

1. Sistema che utilizza Deep Machine Learning e Intelligenza Artificiale per auto apprendere il comportamento naturale dei device e degli utenti della intera infrastruttura di rete (Lan e Internet) per poi evidenziarne lo scostamento
2. Deve essere in grado di individuare anomalie comportamentali in tempo reale
3. Non deve essere basato su regole e signature
4. Deve rilevare attacchi sia dall'interno (insider threat) che dall'esterno della rete LAN
5. Deve segnalare anomalie tramite interfaccia web, email, alert con un'APP su smartphone o tramite servizio di segnalazione telefonica.
6. Deve consentire effettuazione di analisi di tipo forensico (log non modificabili).
7. Deve mostrare la provenienza geografica delle eventuali minacce
8. Deve essere integrabile con Active Directory
9. Deve effettuare analisi in modalità passiva senza creare rallentamenti di rete
10. Deve essere scalabile.
11. Deve rendere possibile l'interazione con gli analisti tramite l'interfaccia utente
12. Deve consentire la creazione di modelli matematici specifici per la propria rete
13. Deve identificare il traffico di tutto ciò che ha un indirizzo IP o un account utente (inclusi stampanti, telecamere, sistemi VOIP)
14. Deve essere un sistema totalmente agentless
15. Deve essere in grado di analizzare tutti gli ambienti IT: fisici, cloud, virtuali etc
16. Deve essere nativamente integrabile con SIEM e Firewall
17. Deve essere nativamente integrabile con servizi IASS e SAAS in particolar modo con i servizi di Microsoft Office 365 e DROPBOX
18. Deve essere utilizzabile anche come tool di asset discovery
19. Deve consentire la produzione automatica di reportistiche dettagliate o di alto livello delle minacce / anomalie riscontrate
20. Deve consentire di assegnare privilegi diversi agli utenti, in modo granulare, permettendo anche di mascherare le informazioni.
21. Opzionalmente il sistema deve avere un sistema di protezione che reagisca attivamente alle minacce riscontrate.
22. Il produttore deve essere certificato ISO 27001:2013