Nanitor
Global CTEM leader

ARGO
make IT work

Nanitor Whitepaper: Migliorare la Cybersecurity attraverso CTEM

Potenziare le organizzazioni tramite una gestione delle vulnerabilità real-time e la mitigazione completa delle minacce attraverso la piattaforma CTEM di Nanitor

Introduzione

Nell'odierno panorama digitale in rapida evoluzione, le organizzazioni si trovano ad affrontare un'ondata senza precedenti di minacce alla sicurezza informatica. Queste minacce non solo aumentano in frequenza, ma anche in complessità, ponendo rischi significativi per le aziende di ogni dimensione.

Dalle vulnerabilità negli ambienti cloud alle errate configurazioni di sistema e alla debolezza nella sicurezza delle identità, le aziende moderne devono affrontare un panorama di minacce complesso e in continua evoluzione. Non affrontare queste sfide può portare a gravi conseguenze, tra cui violazioni dei dati, perdite finanziarie e danni alla reputazione aziendale.

Per contrastare queste minacce crescenti, Nanitor ha sviluppato una piattaforma innovativa di Gestione Continua dell'Esposizione alle Minacce (CTEM). Questa soluzione rivoluzionaria consente alle organizzazioni di anticipare i potenziali rischi informatici, fornendo rilevamento in tempo reale dei problemi di sicurezza su tutte le risorse.
Oltre all'identificazione, la piattaforma CTEM di Nanitor offre la possibilità di dare priorità a ogni vulnerabilità nota con precisione, accompagnata da indicazioni chiare e concrete per la risoluzione. Grazie ad un approccio unificato su gestione delle vulnerabilità, monitoraggio di configurazioni, sicurezza di identità, applicazione di patch e gestione della superficie di attacco, Nanitor rende la protezione della tua organizzazione più semplice, intelligente ed efficace.

Cosa rende CTEM di Nanitor unica?

La piattaforma CTEM di Nanitor (Continuous Threat Exposure Management) offre un approccio senza precedenti alla moderna sicurezza informatica, garantendo la raccolta automatizzata e in tempo reale dei dati su tutte le risorse all'interno della rete di un'organizzazione.

Il motore di rilevamento della piattaforma analizza e filtra continuamente questi dati attraverso le policy e framework di conformità di un'organizzazione, fornendo informazioni dettagliate sulle vulnerabilità di sicurezza. Il punto di forza di Nanitor è nella combinazione di potenti funzionalità che semplificano e migliorano la gestione delle minacce.

Funzionalità chiave di Nanitor:

Nanitor Diamond™ per gestione delle priorità: Nanitor Diamond™ organizza visivamente i problemi di sicurezza in base al loro potenziale impatto, consentendo di concentrarsi prima sulle vulnerabilità più critiche.

Scansione in tempo reale: la scansione continua ed in tempo reale basata su agenti garantisce il rilevamento rapido di vulnerabilità e problemi relativi alle risorse, consentendo di intervenire in modo proattivo.

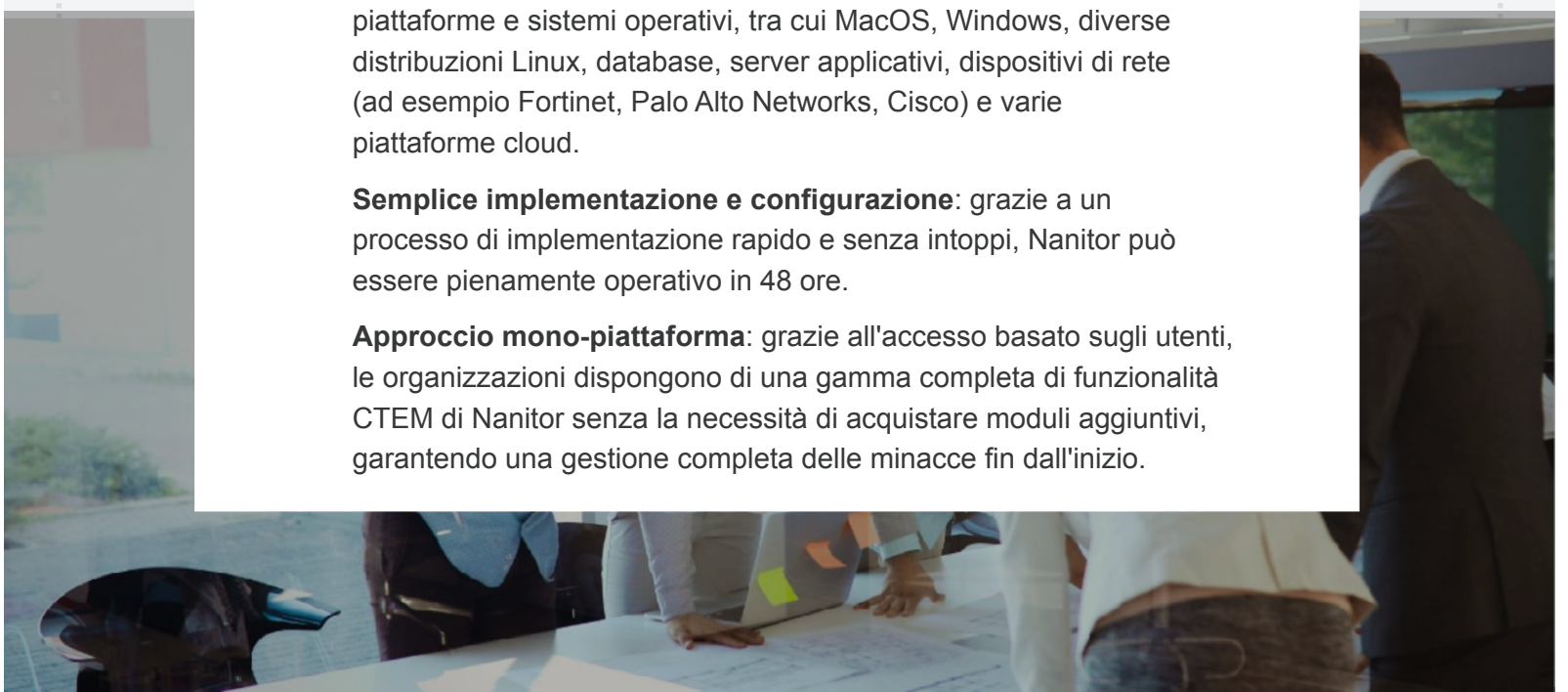
Basato su asset: Nanitor assegna priorità ai problemi di sicurezza in base alla criticità degli asset interessati, garantendo che i sistemi e i repository di dati essenziali ricevano attenzione prima delle problematiche a priorità inferiore.

Framework di conformità: Nanitor si integra perfettamente con i framework di conformità (ISO27001, PCI, NIST, NIS2, DORA, ecc.), consentendo alle organizzazioni di mantenere la conformità normativa insieme a una maggiore sicurezza.

Supporto multi-piattaforma: Nanitor supporta un'ampia gamma di piattaforme e sistemi operativi, tra cui MacOS, Windows, diverse distribuzioni Linux, database, server applicativi, dispositivi di rete (ad esempio Fortinet, Palo Alto Networks, Cisco) e varie piattaforme cloud.

Semplice implementazione e configurazione: grazie a un processo di implementazione rapido e senza intoppi, Nanitor può essere pienamente operativo in 48 ore.

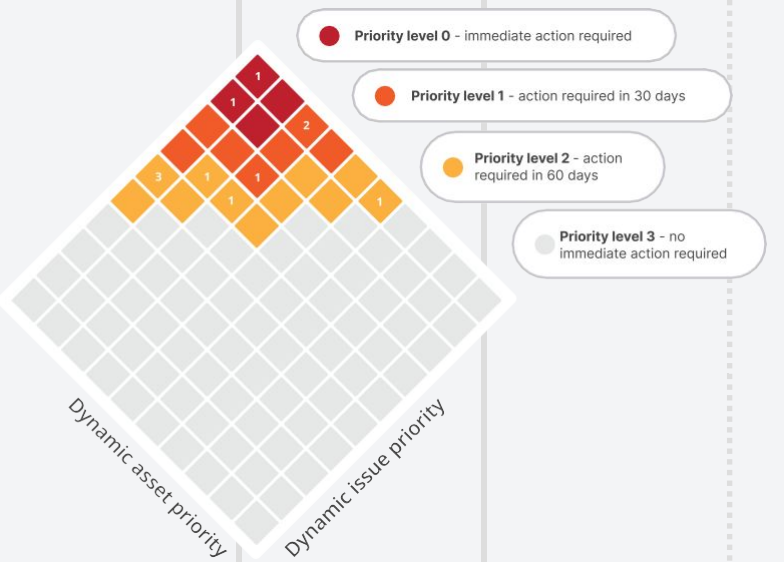
Approccio mono-piattaforma: grazie all'accesso basato sugli utenti, le organizzazioni dispongono di una gamma completa di funzionalità CTEM di Nanitor senza la necessità di acquistare moduli aggiuntivi, garantendo una gestione completa delle minacce fin dall'inizio.



Prioritizzazione

Nanitor Diamond™ fornisce una prioritizzazione visiva in tempo reale delle vulnerabilità di sicurezza, categorizzate in base alla criticità del problema e all'importanza delle risorse. Questo permette di identificare e affrontare rapidamente i rischi più critici per i sistemi vitali. Il punteggio di prioritizzazione (NPS) di Nanitor classifica le vulnerabilità in base al loro potenziale impatto, semplificando le risposte e garantendo che i problemi ad alto rischio vengano gestiti per primi.

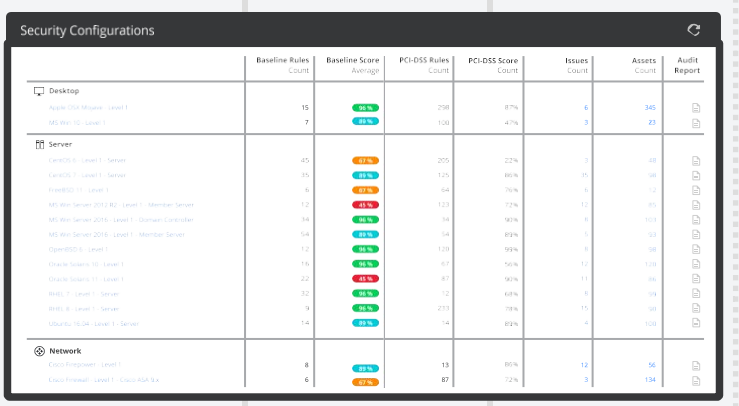
Grazie alla priorità dinamica dei problemi (DIP) e alla priorità dinamica delle risorse (DAP), Nanitor regola continuamente le classifiche in tempo reale, adattandosi alle minacce emergenti e consentendo agli utenti di concentrare gli sforzi sulle problematiche P0, considerate le minacce più critiche fin dall'inizio. L'etichettatura personalizzabile e le valutazioni di impatto RISC migliorano ulteriormente la definizione delle priorità.

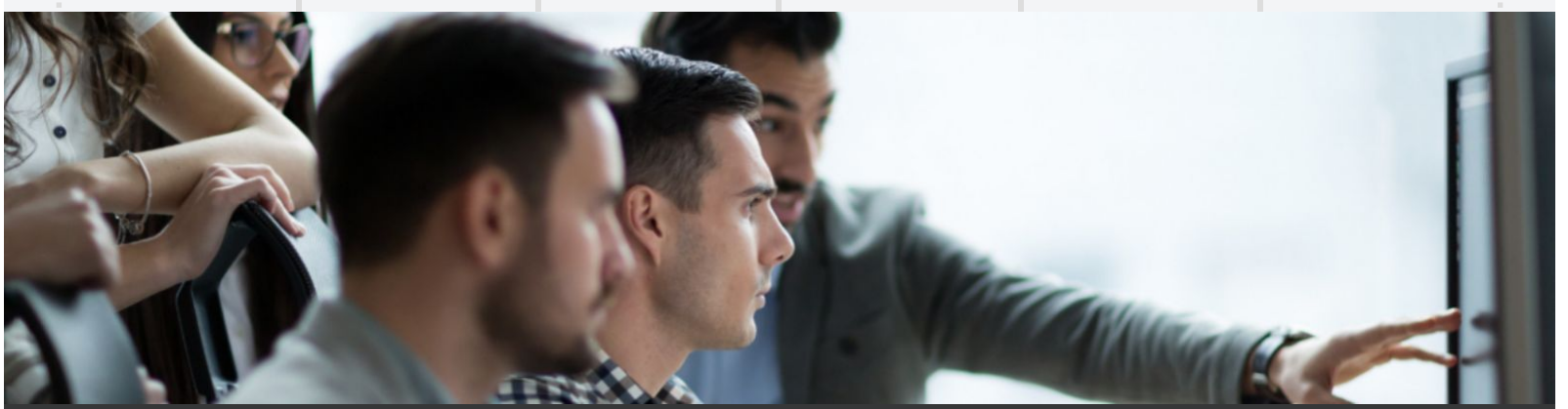


Gestione delle configurazioni

Sfruttando i benchmark CIS, Nanitor identifica e assegna priorità alle configurazioni errate in base sia alla gravità del problema che alla criticità della risorsa interessata. Ciò consente di concentrarsi sulla risoluzione dei problemi di sicurezza più critici, mantenendo un elevato livello di sicurezza in tutta l'organizzazione.

L'ampia portata di Nanitor copre piattaforme come MacOS, Windows, Linux, ambienti cloud, e dispositivi come Fortinet, Palo Alto Networks e Cisco.





Patching

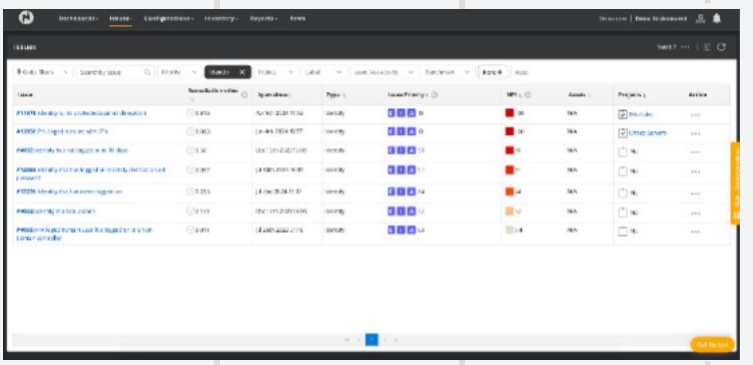
Nanitor offre visibilità in tempo reale su tutte le patch mancanti nella tua infrastruttura, consentendoti di stabilire le priorità in base alla gravità di ciascun problema e alla criticità della risorsa interessata. Grazie a Nanitor Diamond™, gli utenti possono identificare rapidamente i sistemi che necessitano di un aggiornamento immediato, garantendo che le patch più critiche vengano applicate per prime.

Nanitor offre anche report dinamici, fornendo una panoramica completa dello stato delle patch, incluse quelle in sospeso, scadute e risolte. Semplificando l'identificazione e la definizione di priorità delle patch, Nanitor garantisce vista mirata sulle vulnerabilità più critiche.

Identity Security

Analizzando e monitorando continuamente le impostazioni di identità sia negli ambienti on-premise che in quelli cloud, la piattaforma rileva e segnala automaticamente le configurazioni che potrebbero esporre percorsi di attacco, consentendo di intervenire rapidamente sulle configurazioni di sicurezza dell'identità deboli.

Grazie alla visibilità e alla prioritizzazione in tempo reale, Nanitor contribuisce a garantire che la sicurezza delle identità rimanga solida, riducendo il rischio di escalation dei privilegi e di movimenti laterali da parte degli aggressori. Questo approccio proattivo assicura che le vulnerabilità delle identità vengano affrontate prima che possano essere sfruttate.



Cloud Security

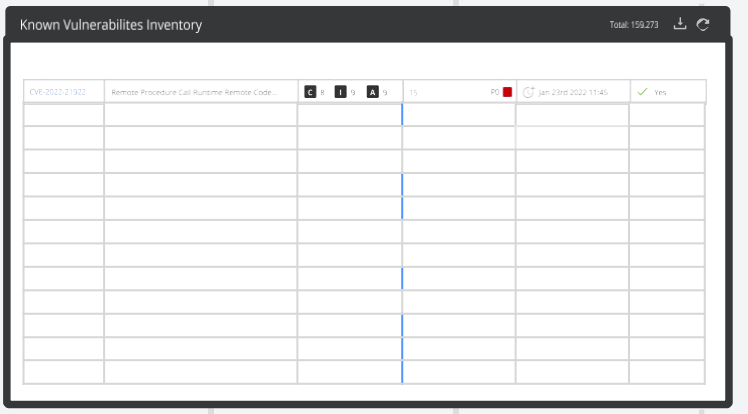
Nanitor offre monitoraggio e valutazione continui dei tuoi ambienti cloud, inclusi AWS, Azure e GCP. Sfruttando le raccomandazioni di sicurezza standard del settore, Nanitor garantisce che la tua infrastruttura cloud soddisfi rigorosi standard di sicurezza. Quando vengono identificate vulnerabilità o configurazioni errate, Nanitor fornisce un elenco prioritario di problemi, consentendo di affrontare prima i rischi più critici.

Questo approccio garantisce che i tuoi ambienti cloud siano costantemente protetti, riducendo l'esposizione a potenziali minacce. Nanitor contribuisce a salvaguardare la tua superficie di attacco in continua espansione, intervenendo sulle vulnerabilità prima che gli aggressori possano sfruttarle, mantenendo la sicurezza del tuo cloud robusta e aggiornata.

Vulnerability Management

Nanitor semplifica la gestione delle vulnerabilità identificando e assegnando continuamente priorità ai problemi di sicurezza nell'intera infrastruttura, incluse reti cloud, server, database e apparecchiature di rete. Utilizzando diversi metodi di punteggio come CVSS ed EPSS, Nanitor garantisce che le vulnerabilità più critiche e le risorse interessate vengano affrontate per prime.

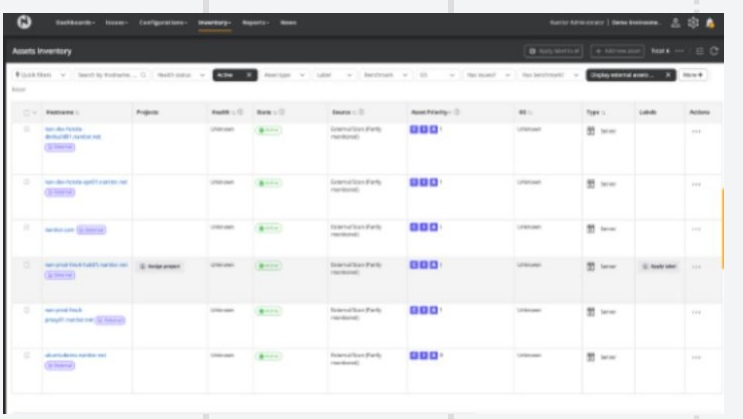
Grazie agli aggiornamenti in tempo reale provenienti da fonti come NIST NVD e altri feed di vulnerabilità autorevoli, Nanitor mantiene aggiornato il database delle vulnerabilità, individuando e segnalando automaticamente le vulnerabilità non appena emergono. La visione prioritaria dei problemi semplifica la gestione delle vulnerabilità.

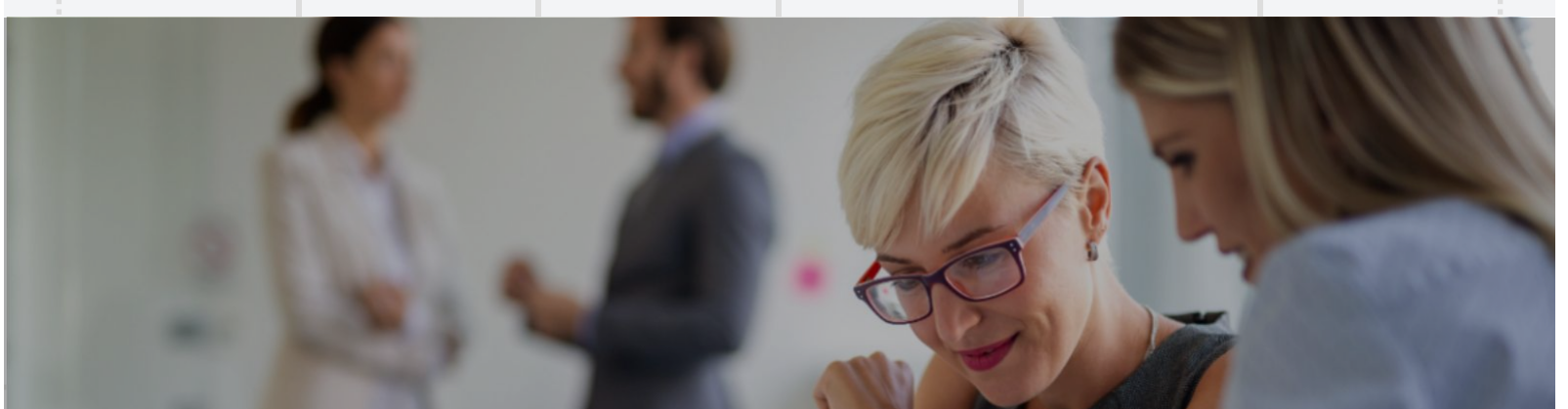


Gestione delle superfici di attacco

La gestione della superficie di attacco esterna (EASM) è essenziale per comprendere e mitigare i rischi associati alle risorse esposte pubblicamente. Nanitor raccoglie e analizza continuamente informazioni sulle tue risorse esterne, inclusi domini e indirizzi IP, per identificare potenziali vulnerabilità. Sfruttando database come Shodan, Nanitor fornisce una visione completa dei servizi esposti a Internet.

Nanitor non solo identifica queste vulnerabilità, ma le classifica anche in base alla gravità, garantendo che le esposizioni più critiche vengano gestite per prime. Questo approccio proattivo all'EASM aiuta le organizzazioni a minimizzare il rischio di attacchi esterni concentrandosi sulle minacce prioritarie prima che possano essere sfruttate.





- Leggero
- Non-Intrusivo
- Self-regulating
- Updates in 5 minuti
- Utilizzato su più di 50.000 asset critici in tutto il mondo

Core technology: Nanitor Discovery Engine™

Il Nanitor Discovery Engine™ raccoglie dati in tempo reale su informazioni di sistema, account utente, configurazioni, stato delle patch, vulnerabilità e software installato su tutte le risorse. Questi dati vengono archiviati sul server Nanitor della tua azienda, dove è possibile visualizzarli, cercarli e assegnare priorità ai problemi. L'istanza Nanitor della tua azienda è sicura e tutti i dati rimangono interni.

La funzione di Network Discovery aiuta a rilevare dispositivi non monitorati o non autorizzati all'accesso in rete, garantendo una copertura totale.

Copertura multi-piattaforma

Il Discovery Engine di Nanitor raccoglie dati da un'ampia gamma di piattaforme, tra cui desktop, server, dispositivi di rete, applicazioni e database. Questa ampia copertura consente di identificare continuamente le vulnerabilità prima che vengano sfruttate.

Grazie alla raccolta dati in tempo reale, Nanitor protegge l'intera superficie di attacco, garantendo una protezione cloud completa tramite il suo Agente o Collettore.