

Individua le lacune che possono fermare l'azienda.

Una revisione di sicurezza mirata per leader che hanno bisogno di risposte chiare su interruzioni, ripristino, esposizione degli accessi e resilienza operativa prima che un incidente imponga la discussione.

Autovalutazione gratuita in cinque minuti

audit.nulvex.com

AVVIA L'AUTOVALUTAZIONE GRATUITA

Gli incidenti sono tecnici. L'impatto è business.

Nulvex Baseline trasforma l'incertezza di sicurezza in chiarezza per la direzione. Aiuta a capire cosa fallirebbe per primo, cosa verrebbe ripristinato per primo e cosa richiede attenzione prima di una vera interruzione.

01

Priorità di interruzione

Identifica quali sistemi tengono in piedi l'azienda e chi decide l'ordine di ripristino.

02

Fiducia nel ripristino

Distingui l'esistenza dei backup da ripristini realmente testati, misurati e documentati.

03

Esposizione degli accessi

Capisci se un account compromesso potrebbe raggiungere troppo dell'azienda.

04

Visibilità operativa

Verifica se il team se ne accorgerebbe presto o solo dopo l'impatto sui clienti.

Una prima revisione pratica per operatori seri.

Nulvex Baseline è il punto di partenza prima di hardening, monitoraggio o risposta. Mappa i punti deboli che creano esposizione business e offre alla direzione una vista chiara e prioritaria dei prossimi passi.

Sintesi del rischio business

01

Una lettura chiara di ciò che potrebbe interrompere operazioni, ricavi o fiducia dei clienti.

Domande basate su evidenze

02

Controlli concreti che il team IT o il provider deve poter dimostrare.

Direzione del passo successivo

CLARITY · PRIORITY · A PRACTICAL NEXT STEP

Rispondi alle domande che il business non può permettersi di indovinare.

Questo controllo non è un penetration test e non sostituisce Nulvex Baseline. Fornisce un segnale immediato: chiaro, incerto o esposto.

01

Se i sistemi principali si fermassero domani, l'ordine di ripristino è già concordato?

Sì, documentato e assegnato · In parte, ma non testato di recente · Nessuna risposta chiara

02

Lo stesso incidente potrebbe danneggiare produzione e backup?

Backup isolati e ripristino testato · I backup esistono, ma l'isolamento non è chiaro · Non ne siamo sicuri

03

Un account compromesso esporrebbe troppo l'azienda?

Accesso limitato, revisionato e registrato · Alcuni controlli esistono, ma la copertura varia · Probabilmente, o non lo sappiamo

04

Sapresti di un problema serio prima dei clienti?

Sì, alert attivi e revisionati · Alcuni alert esistono, ma la risposta è informale · Solo dopo la segnalazione degli utenti

05

La direzione conosce il costo di un giorno offline?

Sì, con impatto operativo e clienti · A grandi linee, ma non formalizzato · Nessuna stima affidabile

Un provider serio dovrebbe accogliere domande chiare.

Se il provider IT o security attuale risponde alle domande Baseline con evidenze, è un buon segnale. Se le risposte sono vaghe, Nulvex Baseline offre un metodo strutturato per chiudere le lacune.

01

Chiedi prove

Test di ripristino, revisioni degli accessi, ownership degli alert, contatti incident e ipotesi di impatto business.

02

Dai priorità a ciò che conta

Parti da sistemi, account e percorsi di ripristino che proteggono ricavi e fiducia dei clienti.

03

Passa dalla revisione all'azione

Usa Baseline per decidere se servono Nulvex Core, Watch, Response o remediation mirata.

Inizia dalle lacune che possono fermare l'azienda.

Porta il PDF in una riunione di direzione, invialo al provider o chiedi a Nulvex di eseguire Baseline con te.

L'autovalutazione gratuita e il documento pubblico non includono scansioni, accesso ai sistemi o un parere formale di audit. La revisione a pagamento inizia solo dopo la definizione scritta dell'ambito e dell'autorizzazione. · audit.nulvex.com · contact@nulvex.com