Secure Online Desktop

Let's Secure, be safe! Cloud Computing Solutions

Vulnerability Assessment Continuativo

Testiamo le Vulnerabilità dei tuoi asset informatici in modo continuativo e ricorrente

Offriamo una protezione proattiva, identificando e priorizzando vulnerabilità per garantire la sicurezza e la conformità del tuo ambiente IT in modo tempestivo ed efficiente.

https://www.secure-od.com/

Vediamo nelle slide successive la differenza tra il Vulnerability assessment CLASSICO e CONTINUATIVO.

Vulnerability Assessment Classico

Il vulnerability assessment **è un processo attraverso il quale le vulnerabilità nei sistemi IT vengono identificate, quantificate e priorizzate.**
Questo processo consente alle organizzazioni di prendere decisioni informate sulla gestione dei rischi e sull'allocazione delle risorse per la mitigazione delle vulnerabilità.
Ogni assessment è una singola istanza, e non essendoci un monitoraggio costante tra una scansione e l'altra non può individuare le nuove vulnerabilità in tempo reale rendendo quindi il sistema, appunto, più vulnerabile.

Le fasi del processo di Vulnerability Assessment Classico

TEST

Tramite strumenti automatizzati si testa l'integrità della sicurezza dell'asset informatico per redigere l'elenco delle vulnerabilità.

ANALISI

L'obiettivo di questo passaggio è quello di identificare l'origine e la causa delle vulnerabilità identificate in precedenza.

ASSESSMENT

Definisce, classifica e assegna priorità alle diverse vulnerabilità, attribuendo un punteggio di gravità.

REMEDETION

L'obiettivo è quello di colmare le lacune di sicurezza, determinando il percorso più efficace per la mitigazione.

Vulnerability Assessment Continuativo

Si riferisce al processo regolare e ripetuto di identificazione, valutazione e priorità delle vulnerabilità nei sistemi informatici, al fine di garantire che le minacce emergenti siano affrontate tempestivamente e che le risorse di difesa siano allocate in modo efficiente.

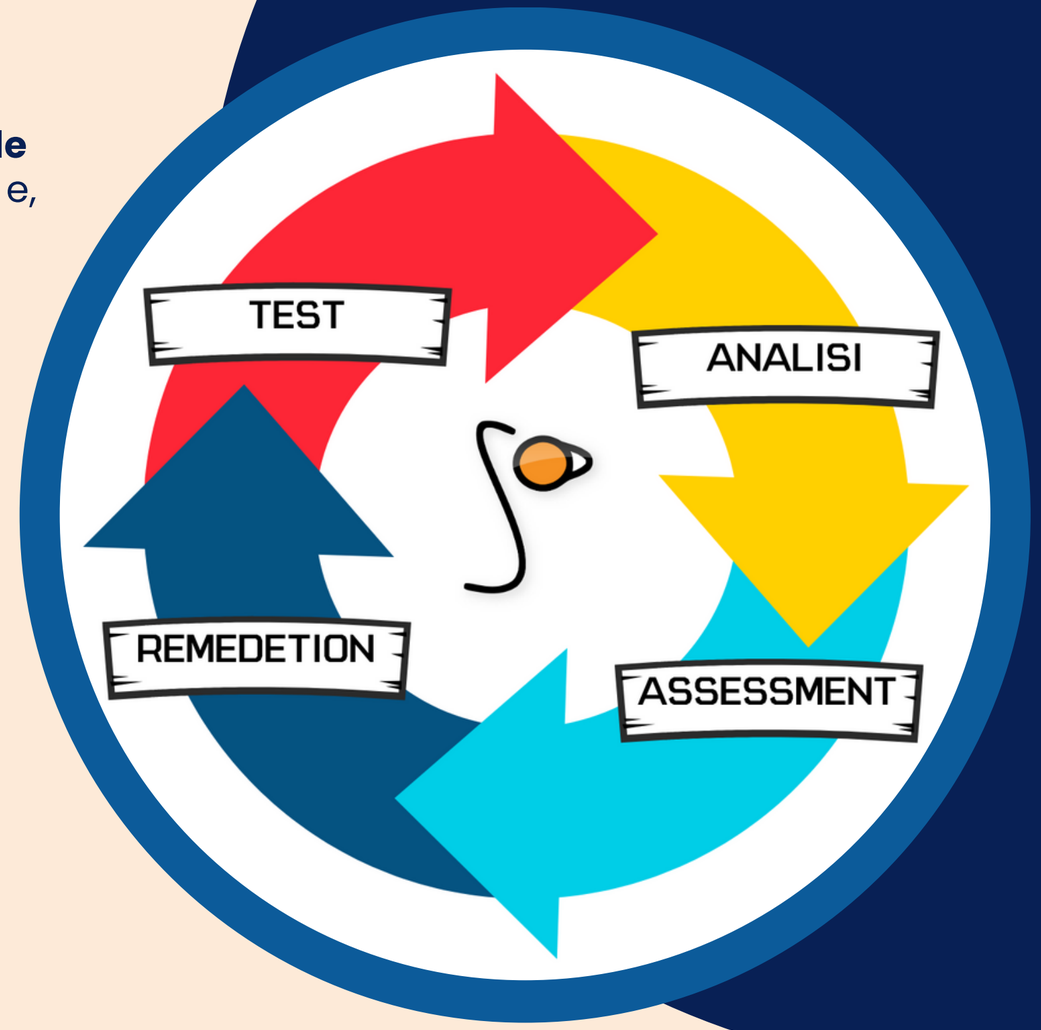
L'importanza di un assessment continuativo risiede nella natura mutevole delle minacce informatiche. Nuove vulnerabilità sono scoperte ogni giorno e, in un ambiente IT dinamico, nuovi sistemi e applicazioni vengono regolarmente aggiunti alla rete, o i sistemi esistenti vengono aggiornati, il che può introdurre nuove falle.

Continuità e Dinamicità

La scansione viene eseguita regolarmente o in tempo reale per garantire che le nuove vulnerabilità vengano identificate appena emergono.

Fornisce una visione aggiornata e in tempo reale della postura di sicurezza, permettendo all'organizzazione di reagire rapidamente alle nuove minacce.

Le fasi



Perchè dovrei scegliere il servizio di Vulnerabilty Assessment Continuativo?

Controllo continuo

Scansioni periodiche dei sistemi e delle applicazioni per identificare nuove vulnerabilità. Queste scansioni possono essere giornaliere, settimanali, mensili, o a qualsiasi altro intervallo appropriato in base alle necessità dell'organizzazione.

Valutazione e Prioritizzazione

Una volta identificate le vulnerabilità, vengono valutate in base alla loro gravità, all'esposizione del sistema e alla criticità del sistema o dell'applicazione per l'organizzazione.

Rimedio

Le vulnerabilità identificate, devono essere mitigate o corrette nel più breve tempo possibile.

Perchè è importante affidarsi ad un Provider?

Costi

Eliminazione di costi legati all'acquisto, manutenzione e aggiornamento del software, nonché dalla necessità di formare o assumere personale specializzato.

Falsi positivi/negativi

Profonda conoscenza e competenza, strumenti tecnologici avanzati e metodi di analisi personalizzati, garantiscono una maggiore accuratezza nella rilevazione delle vulnerabilità e una significativa riduzione dei falsi positivi e negativi.

Gerarchia delle priorità

Un provider specializzato facilita la gestione delle priorità identificando e classificando le vulnerabilità in base al rischio, offrendo raccomandazioni specifiche e integrandosi con i tuoi sistemi, permettendoti di affrontare le minacce più gravi con tempestività.

Aggiornamento

Aggiornamento continuo sulle nuove vulnerabilità e sulle tecniche di attacco.

Assistenza

Team di esperti a disposizione per fornire assistenza e supporto 24 ore su 24, 7 giorni su 7.

Strumenti e tecnologie all'avanguardia

Accesso a strumenti e tecnologie più avanzati di quelli disponibili commercialmente per l'uso interno, offrendo una valutazione più accurata e completa.

Esperienza

Esperienza decennale nell'ambito della Cybersecurity, Secure Online Desktop è un Managed Security Service Provider (MSSP) specializzato nella fornitura di soluzioni di sicurezza complete per aziende di tutte le dimensioni.

Dispongo già di altri sistemi di sicurezza, perché dovrei attivare la VA continuativo?

L’attivazione del servizio come complemento ai sistemi di difesa ed attacco esistenti contribuisce a rendere la sicurezza dell’azienda più completa e resiliente.
Si affianca perfettamente alle soluzioni già in essere per aumentare la sicurezza complessiva del sistema prevenendo il problema alla base.

Panoramica Servizi Cyber

Secure Online Desktop

Let's Secure, be safe! Cloud Computing Solutions

Da oltre 10 anni leader nel settore Cybersecurity e Sicurezza

Secure Online Desktop è un Managed Security Service Provider (MSSP) specializzato nella fornitura di soluzioni di sicurezza complete per aziende di tutte le dimensioni. In qualità di partner di fiducia, offriamo un'ampia gamma di servizi di sicurezza progettati per proteggere la tua organizzazione da minacce informatiche, violazioni dei dati e altri rischi per la sicurezza.

Visita il sito web

Contatti

+39 0522 1685330

www.secure-od.com

info@secure-od.com

Via Statuto 3, 42123 - Reggio nell'Emilia (RE)

Information Security Management System
ISO 27001
Certified