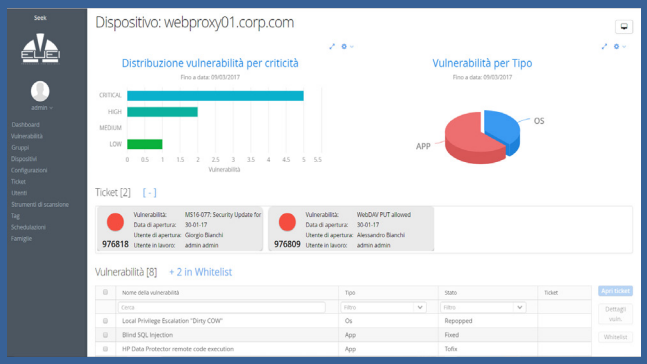
Seek è il servizio Euei di Vulnerability Management che ricerca le criticità software all'interno dei sistemi e degli apparati collegati in rete.

"Ci sono pericoli in ogni cosa che si fa, ma ci sono pericoli ancora più grandi nel non fare nulla." (Shirley Williams)

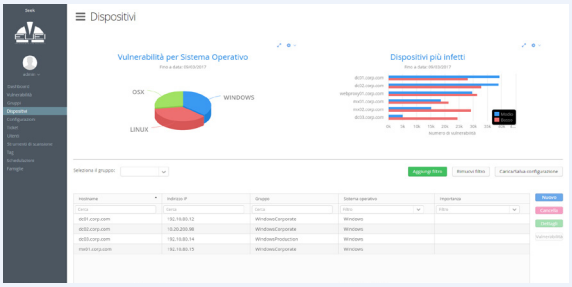
Le violazioni alla sicurezza dei sistemi aziendali sono all'ordine del giorno, non solo su realtà importanti per dimensioni e popolarità, ma anche alle infrastrutture di aziende di medie dimensioni. Strumenti tradizionali come anti virus, firewall e altri tool anti intrusione vengono utilizzati per combattere le conseguenze di una vulnerabilità, ma è necessario agire alla radice del problema andando a identificare i punti deboli.



Seek ricerca in modo automatico le vulnerabilità dei sistemi attraverso l'integrazione di strumenti esterni, aggregando i dati e presentandoli sotto forma di report.

Viene mantenuto uno storico delle falle identificate e di eventuali operazioni di risoluzione delle stesse, così come i KPI relativi alla sicurezza delle aree scansionate. L'ampio catalogo di strumenti esterni consente di effettuare analisi verticali su più protocolli e servizi, aumentando la precisione delle scansioni effettuate con gli strumenti leader di mercato.

Il servizio effettua una scansione completa e strutturata della rete, integrando i principali strumenti atti alla ricerca di vulnerabilità. I dettagli relativi alle falle rilevate vengono raccolti e catalogati, dando modo a chi opera nell'ambito dell'Information Security di richiedere la risoluzione delle problematiche identificate tramite un'applicazione di ticketing interna a Seek. La gestione a ticket permette di seguire il ciclo di vita delle falle rilevate, evidenziandone l'eventuale ricomparsa, fino alla loro risoluzione.

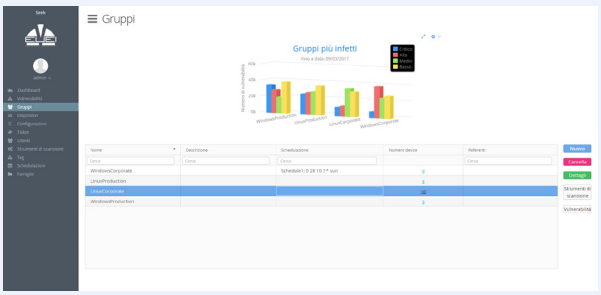


Anagrafica Macchine

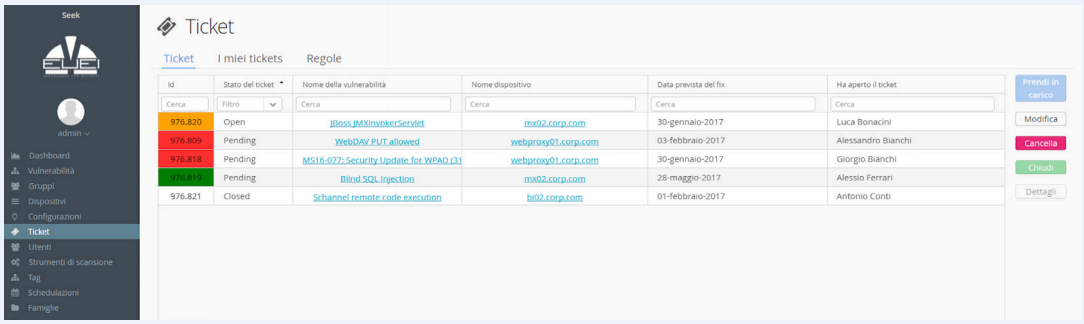
È il censimento delle macchine interessate dalle scansioni. La vista presenta gli estremi relativi ai dispositivi.
La compilazione può avvenire automaticamente, integrandosi a repository esterni, oppure manualmente.

Anagrafica Vulnerabilità

Seek segue il ciclo di vita delle vulnerabilità presenti sui sistemi, mostrando i dettagli utili a identificarne l'impatto e le risorse affette.



Le caratteristiche di Seek



Ticketing questa funzionalità consente di richiedere un intervento risolutivo alla vulnerabilità rilevata, mettendola in stato "To Fix". Il cambio di stato genera una email di notifica al referente della macchina.

L'avviso contiene, oltre ai dettagli tecnici, anche il link alle risorse utili. Il sistema prevede inoltre la possibilità di riaprire il ticket relativo a vulnerabilità precedentemente chiuse. Il cambio di stato può avvenire manualmente o automaticamente, nel caso Seek rilevi la stessa vulnerabilità in scansioni successive.

Accesso secondo ruoli Seek prevede diversi livelli di accesso secondo i ruoli e le policy aziendali, con viste differenti in base al profilo. Il sistema può essere integrato con strumenti di autenticazione centralizzata.

Anagrafica Strumenti di Scansione supporta la gran parte dei tool di scansione, configurabili dagli amministratori che potranno visualizzare l'elenco delle policy impostate sul tool esterno per associarle ai gruppi di macchine (gruppo definiti mediante TAG).

In questo modo Seek potrà creare le scansioni sugli strumenti esterni e lanciarle senza doversi occupare di creare policy.

Integrazione con Nexpose e Nessus Seek si integra con i tool di Rapid7 e Tenable, gli standard de facto per il Vulnerability Assessment.

Gli strumenti, costantemente aggiornati sulle nuove falle, forniscono risultati che vengono raccolti e elaborati da Seek per ottenere un'analisi il più precisa possibile dello stato di sicurezza della rete.

Dashboard Vulnerabilità la vista fornisce report relativi alle vulnerabilità presenti, mantenendo uno storico temporale utile per verificare i trend.

La dashboard principale mostra le informazioni di alto livello, tra cui le criticità della rete divise per gruppi.

Sono inoltre presenti dashboard tecniche con dati aggregati, per gruppo o device: i dettagli delle falle rilevate, l'ambito nel quale queste insistono, la loro criticità e le informazioni sulla loro risoluzione.

Reportistica i report forniti da Seek consentono la verifica e il monitoraggio continuo delle vulnerabilità. Questa funzionalità permette inoltre il controllo puntuale e continuo dei KPI (Key Performance Indicator) sulla base dei parametri fissati in fase di analisi. La reportistica può quindi essere profilata in base all'utente, permettendo di vedere solo i dati a cui si ha diritto ad accedere nella forma grafica più utile. Il tutto può essere inviato via email nei formati: PDF, CSV, XLSx, DOCx.

Audit Trail permette di mantenere i log di audit per tracciare le operazioni di modifica delle configurazioni effettuate dai diversi operatori e utenti sul sistema. Vengono mantenuti i dettagli delle azioni svolte sugli utenti e sulle configurazioni.

Backup e Restore sono previste le funzionalità di backup e restore delle configurazioni e dei dati che possono essere effettuate separatamente, manualmente o schedulate.

Notifiche il servizio prevede la comunicazione delle azioni compiute dagli utenti, dal sistema o al verificarsi di condizioni predefinite, quali ad esempio il cambio di stato di richieste via ticket. Le notifiche sono visualizzate in base agli accessi e ai diritti definiti, e quindi alle mansioni affidate agli operatori.

Le segnalazioni sono raggruppate e categorizzate anche per ogni utente, in questo modo è possibile individuare quali sono state lette e capire su quali si è già intervenuto.

Pubblicazione API Seek permette a sistemi di raccolta dati di leggere le informazioni relative alle scansioni effettuate mediante chiamate REST standard.

Euei
via Natalia Ginzburg, 40
41123 Modena (MO)

Tel: 059 7470498
euei.it - info@euei.it