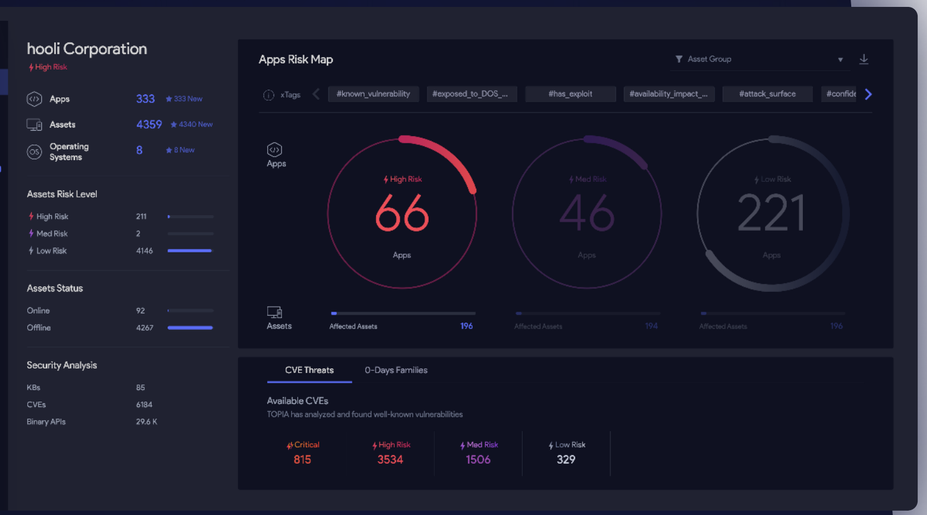
vicarius

# Le 5 domande e risposte principali dei clienti di TOPIA




## “Vogliamo consolidare gli strumenti?”

È comune trovare da tre a cinque strumenti in un programma di gestione delle vulnerabilità, a seconda delle dimensioni di un’organizzazione. Ciò crea complessità per ciò che riguarda integrità dei dati, efficienza dei processi e utilizzazione delle risorse. Vicarius prende la parte principale dei programmi di gestione delle vulnerabilità e li integra bene fra loro. Inventario degli asset, analisi, assegnazione delle priorità, risoluzione dei problemi e reportistica sono combinati assieme per limitare la quantità di strumenti necessari per arrivare a una riduzione del rischio.

## “Come risolviamo i casi d’uso del lavoro da casa, che potrebbero avere ripercussioni sulla gestione del rischio?”

Poiché sempre più persone lavorano da casa e l’infrastruttura diventa decentralizzata, la gestione delle vulnerabilità richiede una maggiore flessibilità. Vicarius ha creato Cloud First e la piattaforma Cloud Ready, che possono offrire la flessibilità per i requisiti in sede, oltre che per i lavoratori da remoto e gli asset su cloud. La soluzione è 100% SaaS, con funzioni in sede per aumentare i casi d’uso, come la distribuzione delle patch.

## “In che modo possiamo rendere il CVSS più preciso, per dare la priorità alla risoluzione dei problemi?”

Molte organizzazioni stanno usando, come punteggi principali, dei punteggi di rischio aziendale soggettivi. Il CVSS è un sistema sia tecnico che ambientale per misurare il rischio. La sfida meno apprezzata per ciò che riguarda i calcoli del CVSS è rappresentata dagli attributi temporali e ambientali che devono essere modificati per ottenere un punteggio accurato. Il punteggio “grezzo” non è personalizzato nell’ambiente client. I dati generati della macchina possono completare il punteggio del rischio CVSS, per rendere l’intero programma più preciso per le vulnerabilità di rischio più elevate. Vicarius automatizza questo processo per modificare il rischio aziendale, secondo una misura considerata opportuna dal cliente.

## “In che modo possiamo meglio assegnare le priorità?”

La quantità di vulnerabilità scoperte sta costantemente superando la quantità di risorse disponibili per porvi rimedio rapidamente. La correlazione fra i dati generati dalla macchina può portare ad avere dei processi decisionali migliori, che si incentrano sulle vulnerabilità di rischio più elevate nell’ambiente. Il punteggio di rischio aziendale, da solo, non prende in considerazione il modo in cui gli hacker vedono il movimento in entrata e laterale durante un attacco. I dati generati dalla macchina, correlati con le informazioni sulla vulnerabilità, possono allineare le risorse per meglio fronteggiare i rischi più elevati. Tali dati devono provenire dagli endpoint. Vicarius automatizza questo intero processo, dalla raccolta dei dati alla loro correlazione e alle opportunità di risoluzione automatica dei problemi.

## “Vogliamo automatizzare le attività di risoluzione dei problemi?”

Tradizionalmente, la presenza di più strumenti rende impossibile l’attuazione di un’automazione tramite middleware, poiché vi sono varie fonti di verità, il contesto è molto ridotto e i processi sono, per lo più, soggettivi. Vicarius rimuove il rischio soggettivo e automatizza la raccolta dei dati generati dalla macchina e la loro correlazione, assegnando le priorità in maniera più precisa. Tutto ciò permette a Vicarius di offrire un motore di automazione per risolvere i problemi di vulnerabilità.

vicarius.io info@vicarius.io