DATASHEET

WATCHGUARD ADVANCED REPORTING TOOL

Informazioni su IT e security intelligence

RAFFORZA LE TUE MISURE DI SICUREZZA IN MODO PROATTIVO

L'aumento significativo dei dati di sicurezza gestiti dalle aziende impedisce al personale IT di concentrarsi adeguatamente sui dettagli importanti. Queste informazioni possono essere usate per rilevare le violazioni e i rischi per la sicurezza, causati sia da fattori esterni sia dai dipendenti stessi.

I professionisti della sicurezza sono sommersi da una quantità enorme di dati. A causa dei grandi volumi di informazioni gestiti e della comparsa di malware di nuova generazione, molti dettagli vengono trascurati o semplicemente non registrati: ciò compromette la sicurezza dell'intero sistema.

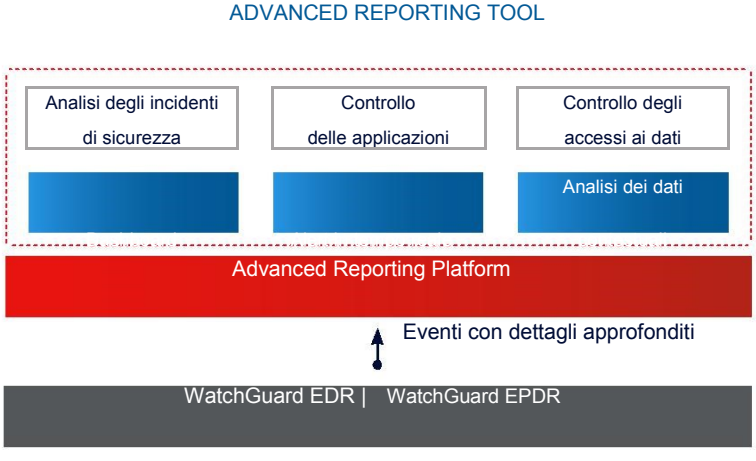
WATCHGUARD ADVANCED REPORTING TOOL

La piattaforma Advanced Reporting Tool (ART) automatizza l'archiviazione e la correlazione delle informazioni generate dall'esecuzione dei processi e dai relativi contesti ed estratte dagli endpoint tramite WatchGuard EPDR e WatchGuard EDR. Tutto ciò senza richiedere investimenti in infrastrutture, dispositivi di vario tipo né manutenzione.

Queste informazioni consentono a **WatchGuard Advanced Reporting Tool** di generare automaticamente una security intelligence e di fornire tutti gli strumenti che servono alle aziende per identificare attacchi e comportamenti insoliti, a prescindere dalla loro origine. Inoltre, permette di rilevare l'utilizzo interno inappropriato dei sistemi e della rete aziendale.

L'**Advanced Reporting Tool** fornisce alle aziende la capacità di ricercare, esplorare e analizzare i dati, offrendo informazioni preziose su IT e sicurezza per:

- Stabilire l'origine degli incidenti di sicurezza e implementare le misure opportune per prevenire gli attacchi futuri.
- Implementare policy più restrittive per accedere alle informazioni business critical.
- Monitorare e controllare l'utilizzo inappropriato delle risorse aziendali che potrebbe influenzare le prestazioni dei dipendenti e dell'azienda.
- Correggere il comportamento dei dipendenti che non è in linea con le policy di utilizzo dell'azienda.



VANTAGGI CHIAVE

Accesso alle informazioni critiche

- Massimizza la visibilità su tutti gli eventi che si verificano sui dispositivi e incrementa l'efficienza e la produttività del reparto IT.
- Accedi ai dati cronologici per analizzare gli indicatori di utilizzo e di sicurezza delle risorse aziendali.
- Ottieni informazioni dettagliate per isolare i rischi per la sicurezza e l'uso inappropriato dell'infrastruttura IT da parte dei dipendenti interni.

Individuazione dei problemi di rete

- Estrai schemi ricorrenti sul comportamento degli utenti e sull'uso delle risorse. Usa queste informazioni per formare gli utenti e implementare policy per ridurre i costi.
- Ottieni visibilità su computer e applicazioni in esecuzione sulla rete per migliorare la sicurezza e il controllo delle risorse aziendali.

Alert bidirezionali

- Trasforma il rilevamento di anomalie in report e alert in tempo reale.
- Consolida la fiducia aziendale segnalando in real time le anomalie di sicurezza e l'utilizzo improprio delle risorse IT da parte dei dipendenti.

Non farti cogliere impreparato in caso di incidenti di sicurezza

- Genera report configurabili per eseguire analisi metodiche della protezione aziendale e rilevare l'uso inappropriato delle risorse e le anomalie di comportamento.
- Mostra lo stato dei principali indicatori di sicurezza e monitorane l'evoluzione rispetto alle azioni correttive adottate.

ANALISI FLESSIBILI ADATTE A OGNI ESIGENZA

L'**Advanced Reporting Tool** integra dashboard con indicatori chiave, opzioni di ricerca e alert predefiniti per tre aree specifiche:

- Incidenti di sicurezza
- Accesso alle informazioni critiche
- Utilizzo delle applicazioni e delle risorse di rete
- Adatta alle tue esigenze aziendali gli alert relativi a ricerche e informazioni chiave.

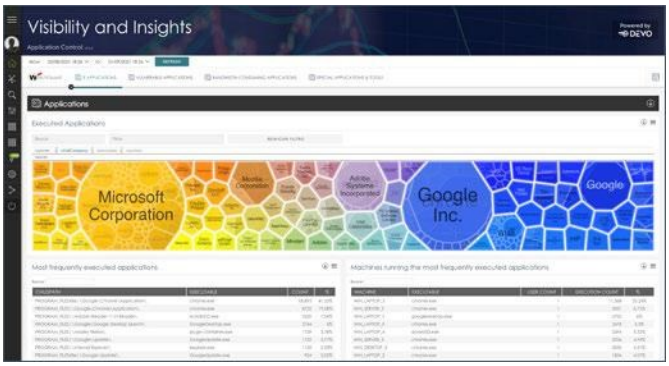
INFORMAZIONI SUGLI INCIDENTI DI SICUREZZA

Genera security intelligence elaborando e trovando le correlazioni negli eventi registrati durante i tentativi di attacco:

- Grafici suddivisi per data che indicano il malware, i PUP e gli exploit rilevati nel corso dell'ultimo anno.
- Computer con il maggior numero di tentativi di infezione e tipi di malware rilevati.
- Computer con applicazioni vulnerabili.
- Stato di esecuzione di malware, PUP ed exploit.

INDIVIDUAZIONE DI SHADOW IT

- Applicazioni con livelli massimi e minimi di esecuzioni.
- Applicazioni di scripting eseguite (PowerShell, shell di Linux, prompt dei comandi di Windows, ecc.).
- Applicazioni per l'accesso da remoto eseguite (TeamViewer, VNC, ecc.).
- Applicazioni freeware indesiderate eseguite (Emule, torrent, ecc.).



SCHEMI RICORRENTI SULL'USO DELLE RISORSE DI RETE

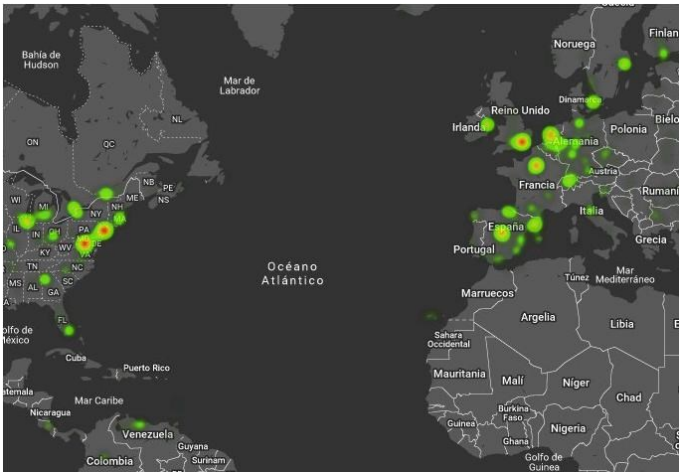
Rileva gli schemi ricorrenti sull'uso delle risorse IT per definire e applicare le policy di sicurezza:

- Applicazioni aziendali e non in esecuzione sulla tua rete.
- Applicazioni vulnerabili in esecuzione o installate sulla rete che potrebbero causare violazioni o influenzare le prestazioni aziendali.
- Controllo delle licenze di MS Office utilizzate rispetto a quelle acquistate.
- Applicazioni con i più alti livelli di consumo della larghezza di banda.

CONTROLLO DEGLI ACCESSI AI DATI AZIENDALI

Mostra l'accesso ai file con dati riservati all'interno della rete:

- File con il maggior numero di accessi ed esecuzioni da parte degli utenti della rete.
- Grafici e mappe suddivisi per data in cui si mostrano i dati inviati nel corso dell'ultimo anno.
- Utenti che hanno eseguito l'accesso a computer specifici sulla rete.
- Paesi che ricevono il maggior numero di connessioni dalla rete.



ALERT IN TEMPO REALE

Configura gli alert in base agli eventi che possono rivelare una violazione della sicurezza o di una policy aziendale per la gestione dei dati:

- Alert predefiniti che indicano situazioni di rischio.
- Alert personalizzati in base alle query create dagli utenti.
- Sette modalità di notifica (sullo schermo e tramite e-mail, JSON, Service Desk, Jira, Pushovery e PagerDuty).

Piattaforme supportate e requisiti di sistema di WatchGuard Advanced Reporting Tool

Compatibile con le seguenti soluzioni:
WatchGuard EPDR e WatchGuard EDR

Elenco dei browser compatibili:
Google Chrome e Mozilla Firefox (possibile compatibilità con altri browser).

Per informazioni contatta SOPHIANET SRL – commerciale@sophianet.it