TECH BRIEF

Managed detection and response

La soluzione ideale per garantire la protezione dei sistemi

aruba.it ENTERPRISE

MDR: cos'è

Il servizio ha come scopo quello di identificare e rispondere a minacce dirette alle risorse e alle informazioni del cliente, ospitate sui server amministrati da Aruba.

Offre una soluzione anti malware di ultima generazione, grazie alla professionalità di un team di esperti, con una significativa esperienza nella gestione e ottimizzazione di soluzioni di protezione e sicurezza.

Il servizio è prerequisito necessario dei servizi "Managed Linux Server" o "Managed Windows Server" e comprende le seguenti attività: monitoraggio, classificazione e analisi delle minacce rilevate, produzione e condivisione della reportistica di servizio.

MDR: le caratteristiche

Prodotti leader di mercato
Si appoggia a soluzioni versatili, compatibili con la maggior parte dei sistemi operativi e personalizzabili sulla base delle specifiche esigenze del cliente.

Rilevamento avanzato
Protezione anti-ransomware e malware in modalità “signature-based” e “AI-based” (anche file-less) per la detection di malware noti o ancora sconosciuti

Estrema compatibilità
Integrazione nativa con Threat Intelligence di terze parti (es. Virus Total) e inserimento di Indicatori di Compromissione (IoC)

Analisi avanzata
Colleziona e correla informazioni di telemetria dei server per la detection di pattern malevoli

Risposta proattiva
Abilita la risposta a minacce avanzate e attiva la quarantena automatica del file malevolo

aruba.it ENTERPRISE

MDR: come funziona

Monitoraggio 24/7
Il monitoraggio della soluzione e delle relative segnalazioni viene assicurato dal SOC (Security Operations Center) in modalità 24/7; le segnalazioni vengono investigate e riportate periodicamente al cliente nell'ambito dei service meeting.

Interoperabilità perfetta
La soluzione è corredata da documentazione relativa alla compatibilità con le principali versioni dei sistemi operativi Windows e Linux.

Intervento immediato
Nel caso di segnalazioni con rischio di compromissione del sistema e dei dati, la soluzione esegue azioni di mitigazione immediate, con rapida procedura di escalation (anche senza avvertire il cliente).

Attività di risposta
In caso di incidente la soluzione isola la macchina coinvolta e consente agli operatori di Security l'accesso da remoto per analisi e raccolta evidenze.

Supporto e SLA
Aruba mette a disposizione dei clienti dei Managed Services un servizio di assistenza dedicato con specifici canali e modalità di ingaggio, orari di erogazione del servizio e SLA.

aruba.it ENTERPRISE

MDR: processi gestiti

Processi	Attività
Gestione operativa	- Monitoraggio servizi, risorse e indicatori di performance. - Tuning dei sensori. - Analisi delle minacce rilevate. - Esecuzione di remediation, con eventuale coinvolgimento del cliente. - Reportistica sullo stato del servizio.
Service request (SR)	Massimo di 12 Service Request all'anno. SR incluse: -Richiesta di esclusione di specifici file o cartelle. -Comunicazione di modifiche alla configurazione servizi del cliente.
Change request (CR)	-Innesca un processo appositamente disegnato per il raggiungimento dello scopo. -È comunicata tramite l'apposita piattaforma di ticketing. -È registrata in log ed eseguita solo dopo l'approvazione dei nostri esperti, che ne analizzano rischi e impatto. -CR incluse: modifiche delle policy predefinite. Possono essere massimo tre all'anno

aruba.it ENTERPRISE

MDR: modello di governance

Responsabilità Aruba Enterprise

- Monitoraggio dei servizi, delle risorse e dei principali indicatori di performance.
- Tuning dei sensori.
- Analisi delle minacce rilevate.
- Esecuzione di azioni di remediation, con eventuale coinvolgimento del cliente se necessario.
- Reportistica sullo stato del servizio.
- Comunicazione di modifiche alla configurazione del servizio MDR

Responsabilità cliente

- Richiesta di esclusione di specifici file o cartelle.
- Comunicazione di modifiche ad applicazioni e servizi

MDR: vantaggi

Sicurezza totale
Gestione end to end: dagli aspetti fisici in Data Center Aruba agli aspetti di carattere applicativo

Gestione della complessità
Affidarsi ad un partner di fiducia che impiega esperti cybersecurity significa delegare la complessità

Elevata expertise
Esperienza pluriennale nella gestione della security per servizi cloud & Data Center di Aruba

Separazione dei ruoli
SOC basato su tecnici specialisti certificati per assicurare terziarietà rispetto ai team di gestione del cliente

Focus sul core
Delegare ad esperti esterni vuol dire investire maggiori risorse nel core business aziendale

Previsione certa dei costi
Una buona previsione aiuta a ridurre i costi operativi e gli sprechi dovuti alle spese improvvise

aruba.it ENTERPRISE

MDR: casi d'uso

Supporto reparto IT
Ideale per reparti IT di piccole dimensioni e poco strutturati che difficilmente riescono a garantire un monitoring H24 degli aspetti di sicurezza.

Assenza di competenze di Cyber Security
Un partner di fiducia può implementare una soluzione anti malware di ultima generazione facendo evitare i costi di acquisizione e il continuous improvement delle competenze.

Carico IT elevato
Per organizzazioni non in grado di intervenire tempestivamente in caso di incident o di adottare un approccio proattivo eseguendo tutti quei task volti a prevenire il verificarsi di attacchi malware.

Garantire la sicurezza del dato GDPR compliant
Un partner con esperienza offre strumenti di amministrazione che rispettano le tematiche di compliance, supportano gli audit periodici per la certificazione e governano la sicurezza.

Necessità di attivare un approccio Zero Day
Solo affidandosi ad un servizio di MDR si possono avere strumenti di analisi predittiva, basati su Machine Learning e AI, per rilevamento e protezione anche da malware ancora sconosciuti.

aruba.it ENTERPRISE

Vorresti una soluzione dedicata alla tua impresa? Costruiscila insieme a noi.

Il nostro team di solution architect lavora al fianco delle imprese nella progettazione di soluzioni complete, flessibili e personalizzate, per soddisfare le esigenze aziendali più complesse.

Contattaci

https://enterprise.aruba.it/richiedi-contatto.aspx

aruba.it
ENTERPRISE