GenData

CUSTODIAMO LA VOSTRA CONOSCENZA

Il nostro core business è la protezione del dato, la sua salvaguardia e per farlo costruiamo su misura un percorso ad hoc sempre diverso a seconda dell'esigenza del cliente.

SECURITY CHECK

CUSTODIAMO LA VOSTRA CONOSCENZA

Chi siamo

/ Chi siamo /
L'evoluzione tecnologica della nostra società corre ad un ritmo frenetico ed è fondamentale
coglierne tutte le opportunità.

Chi si affida a noi sa che può contare su un partner affidabile che lo accompagnerà in un percorso di miglioramento della qualità del lavoro grazie all'ottimizzazione dei tempi e delle modalità lavorative delle persone, consapevoli che la tecnologia sia oggi lo strumento centrale per combinare flessibilità e collaborazione. Noi di Gendata mettiamo al centro l'uomo, il rapporto umano e l'ascolto.

Il nostro obiettivo è migliorare la vita dei nostri partner cucendo su misura la soluzione migliore per risolvere concretamente ogni loro problematica in ambito informatico.

In pratica ciò si traduce nel fare del nostro meglio per disegnare un mondo di soluzioni atte a migliorare e a semplificare la "vita digitale" di ogni impresa che si affiderà a noi. Siamo consapevoli che si tratta di un impegno continuo e costante che trasformiamo ogni giorno in una sfida per migliorarci.

Gendata nel mese di luglio 2021 ha ottenuto la certificazione UNI EN ISO 9001:2015 "Progettazione ed erogazione di servizi di formazione relativi alla cybersecurity e alla digitalizzazione dei processi aziendali ".

Caratteristiche e obiettivi

È noto che molti attacchi informatici siano frutto di compromissioni che possono essere avvenute anche mesi prima del momento in cui ne siano visibili gli effetti.

Durante il periodo di tempo che intercorre tra la prima compromissione e l'attacco effettivo, l'attaccante studia in modo silente la rete del soggetto compromesso, con l'obiettivo di migliorarne la conoscenza e poter quindi mettere a segno un attacco che sia il più impattante possibile.

Il servizio denominato GD-Security ha l'obiettivo di determinare se la rete informatica oggetto delle attività sia stata compromessa, ovvero se siano presenti artefatti riconducibili ad agenti malevoli che indichino che una compromissione sia già avvenuta.

CUSTODIAMO LA VOSTRA CONOSCENZA

/ GD-SECURITY /
/ GD-SEC-EPP /
L'attività viene eseguita utilizzando una tecnologia EDR di ultima generazione che, per mezzo di un agente distribuito su tutti gli endpoint (server e client Linux, Windows e Mac OSX) presenti in rete, permette di analizzare il comportamento di utenti, file e processi alla ricerca di indicatori di compromissione (IoC) sintomatici della presenza di malware avanzati non rilevabili dagli antivirus standard.

/ GD-SEC-NET /
A seconda dell'estensione della rete da analizzare e della tipologia di dispositivi ad essa connessi, potrebbe essere necessario introdurre anche un secondo livello di analisi per mezzo di una tecnologia in grado di effettuare Anomaly Detection e Behavioral Analytics a livello network. Questo ulteriore strumento grazie all'utilizzo di algoritmi avanzati di Artificial Intelligence e mediante un'analisi passiva di tutto il traffico generato dalla rete in oggetto, permette di evidenziare eventuali anomalie che deviano da una baseline comportamentale standard dell'infrastruttura in esame.

/ GD-SEC-BCK /
Controllo delle procedure di backup e configurazione per ridurre al minimo le possibilità di compromissione del server backup e repository.

In ragione della dimensione e tipologia del perimetro, le attività di Security Sanity Check possono durare da un minimo di 1 settimana ad un massimo di 4 settimane. Al termine delle attività verrà prodotto un report riassuntivo delle evidenze trovate, con una eventuale indicazione delle azioni consigliate.

L'analisi, una volta effettuata l'attività di installazione e configurazione delle tecnologie introdotte, viene svolta con campionamenti giornalieri da parte dello specialista volti a verificare la presenza di minacce latenti all'interno dell'infrastruttura del Cliente. Non è, tuttavia, previsto un monitoraggio H24, né un intervento puntuale di verifica e sanificazione di qualsiasi minaccia rilevata.

Le soluzioni utilizzate sono configurate per generare allarmi nel caso in cui vengano rilevate minacce particolarmente critiche, e, in questo specifico caso, il Cliente viene tempestivamente informato al fine di concordare un'eventuale azione risolutiva senza attendere il termine dell'attività di Security Sanity Check.

Tali attività, se approvate dal Cliente, verranno svolte nell'ambito di un servizio di Incident Response dedicato, che esula lo scopo del presente servizio e verrà pertanto gestito in forma separata.

Svolgimento e durata del servizio

/ GD - Security Operation Center /
Dal momento dell'installazione, viene attivato, in collaborazione con i vendor, il servizio della squadra di sicurezza attivo 24/7.

Gendata arricchisce la sua tecnologia di protezione dalle minacce automatizzata con i servizi di sicurezza integrati, senza costi aggiuntivi.
Il gruppo operativo di analisti delle minacce e ricercatori di sicurezza, si avvale delle proprie competenze e dei feed di threat intelligence sulle minacce rilevate.
Viene inoltre fornita una gamma di servizi personalizzati in base alle specifiche esigenze e preferenze di sicurezza di ciascun cliente.

Risultati

L'attività descritta in precedenza permette agli specialisti Gendata di produrre un documento completamente customizzato che fornisce una visione chiara e puntuale degli esiti del GD-Security.

Il report è suddiviso in una parte destinata al Management (Report Executive + Executive Summary) dove sono riportate ad alto livello le problematiche riscontrate e in cui sono forniti svariati indicatori riassuntivi, ed una parte destinata al personale tecnico/operativo (Report tecnico + Conclusioni) dove le eventuali anomalie individuate vengono descritte nel dettaglio e ne viene formulata un'ipotetica causa.

Requisiti per l'attività

/ GD-SEC-EPP /
La tecnologia EDR utilizzata per l'esecuzione del GD-Security è compatibile con i seguenti sistemi operativi:

Microsoft 32\64 Bit	*Linux 32\64 Bit*	*Mac 64 Bit*
Windows XP SP2	Red Hat 6.4 +	MacOS Mavericks
Windows Vista	Fedora 21+	MacOS Yosemite
Windows 7	Ubuntu 14+	MacOS El Capitan
Windows 8/8.1	CentOS 6.7+	MacOS Sierra
Windows 10	SUSE 12+	MacOS High Sierra
Windows Server 2003 SP2	Debian 6+	MacOS Mojave
Windows Server 2008/R2		
Windows Server 2012/R2		
Windows Server 2016		
Windows Server 2019		

Nel caso di presenza di sistemi operativi non supportati, le attività di GD-Security saranno effettuate con modalità alternative preventivamente concordate con il cliente.

/ Postazioni (Desktop/Portatili) e Server /

Da	1	a	50
Da	51	a	100
Da	101	a	200
>	201		

/ GD-SEC-Net /
Network Anomaly Detection
Nel caso si renda necessario il deploy della tecnologia di Network Anomaly Detection, sarà richiesto di predisporre lo switch Core per inoltrare tutto il traffico mirrorato verso tale appliance.
A tal fine è pertanto necessario verificare la possibilità di attivare una o più porte di suddetto switch in modalità SPAN o Port mirroring.

Attivazione attivabile solo in abbinamento al GD-SEC-EPP

/ GD- SEC-BCK /
Disposizione delle credenziali per il/i server di backup e dei repository per eseguire un controllo approfondito delle configurazioni e dei permessi assegnati. Visione dell'eventuale manuale operativo per il ripristino dei dati e/o Disaster recovery.

Analisi da parte di un tecnico specializzato Gendata sulla sicurezza dei server dei backup, dei repository e delle policy di backup.

GenData
CUSTODIAMO LA VOSTRA CONOSCENZA

CUSTODIAMO LA VOSTRA CONOSCENZA

Perché scegliere Gendata

Il team Gendata vi aiuterà a eliminare i rischi per la vostra azienda e a raggiungere una posizione di sicurezza più forte, costruendo un programma di salvaguardia della vostra attività, solido e duraturo.

Il nostro compito è trasformare i problemi in soluzioni e le aspirazioni in realtà, attraverso servizi di consulenza studiati sulle vostre reali necessità, consigliandovi le migliori risorse presenti sul mercato.

FORLÌ | Via G. Spadolini, 31 | 47122
BOLOGNA | Via E. Mattei, 102 | 40138

+39 0543 752374
+ 39 051 19936408

info@gendata.it | gendata@pec.it
P.I. 04083330409 | REA FO – 328974