## Guida alle best practice per Advanced Malware Protection (AMP) su Cisco Email Security

## Sommario

Introduzione Verifica chiavi funzionalità Abilita Advanced Malware Protection Personalizza impostazioni globali di Advanced Malware Protection Impostazione soglia analisi file Integrazione di ESA con AMP for Endpoints Console Abilita correzione automatica cassetta postale (MAR) Configura Advanced Malware Protection (AMP) nei criteri di posta Integrazione di SMA con Cisco Threat Response (CTR) Conclusioni

## Introduzione

Advanced Malware Protection (AMP) è una soluzione completa che consente il rilevamento e il blocco di malware, l'analisi continua e la segnalazione retrospettiva. L'utilizzo di AMP con Cisco Email Security consente una protezione superiore attraverso il continuum degli attacchi, prima, durante e dopo un attacco, con l'approccio più conveniente e facile da implementare alla difesa avanzata dal malware.

Questo documento sulle best practice tratterà le funzionalità principali di AMP su Cisco Email Security Appliance (ESA), come indicato di seguito:

- Reputazione dei file: rileva un'impronta digitale di ciascun file mentre attraversa l'ESA e lo invia alla rete di intelligence basata su cloud di AMP per un verdetto di reputazione. Dati questi risultati, è possibile bloccare automaticamente i file dannosi e applicare i criteri definiti dall'amministratore.
- Analisi dei file: consente di analizzare i file sconosciuti che attraversano l'ESA. Un ambiente sandbox altamente sicuro consente ad AMP di ottenere dettagli precisi sul comportamento del file e di combinare tali dati con un'analisi dettagliata di persone e macchine per determinare il livello di rischio del file. Questa disposizione viene quindi inserita nella rete di intelligence basata su cloud AMP e utilizzata per aggiornare ed espandere dinamicamente il set di dati cloud AMP per una protezione avanzata.
- Monitoraggio e aggiornamento automatici delle caselle di posta (MAR): per Microsoft Office 365 ed Exchange 2013/2016 automatizza la rimozione dei messaggi di posta elettronica contenenti file che diventano dannosi dopo il punto di ispezione iniziale. Ciò consente agli amministratori di risparmiare ore di lavoro e di contenere l'impatto di una minaccia.
- Cisco AMP Unity: funzionalità che consente a un'organizzazione di registrare il proprio dispositivo abilitato per AMP, inclusa l'abbonamento ESA con AMP, nella console AMP for Endpoints. Con questa integrazione, Cisco Email Security può essere visto e interrogato per osservazioni di esempio allo stesso modo in cui la console AMP for Endpoints offre già per gli

endpoint e consente di correlare i dati di propagazione dei file tra tutti i vettori di minaccia in una singola interfaccia utente.

• Cisco Threat Response: è una piattaforma di orchestrazione che riunisce le informazioni sulla sicurezza provenienti da Cisco e da fonti di terze parti in un'unica console di indagine e risposta intuitiva. Lo fa attraverso un design modulare che funge da struttura di integrazione per i log degli eventi e le informazioni sulle minacce. I moduli consentono una rapida correlazione dei dati creando grafici delle relazioni che, a loro volta, consentono ai team di sicurezza di ottenere una visione chiara dell'attacco e di intraprendere rapidamente azioni di risposta efficaci.

## Verifica chiavi funzionalità

- Sull'ESA, selezionare System Administration> Feature Keys (Amministrazione sistema)
- Cercate le chiavi della feature Reputazione file (File Reputation) e Analisi file (File Analysis) e assicuratevi che gli stati siano **Attivo (Active)**

## **Abilita Advanced Malware Protection**

- Sull'ESA, selezionare Security Services >Advanced Malware Protection File Reputation and Analysis
- Fare clic sul pulsante **Enable** (Abilita) in **Advanced Malware Protection** Global Settings (Impostazioni globali di protezione da malware avanzato):

Advanced Helware Protection			
	File Reputation:	Enabled	
	File Analysis:	Enabled	
		Edit Global Settings	

• Eseguire il commit delle modifiche.

#### Personalizza impostazioni globali di Advanced Malware Protection

- AMP è ora abilitato. Fare clic su Modifica impostazioni globali per personalizzare le impostazioni globali.
- L'elenco delle estensioni di file verrà aggiornato automaticamente di tanto in tanto, quindi visitare sempre questa impostazione e assicurarsi che tutte le estensioni di file siano selezionate:



- Espandi impostazioni avanzate per reputazione file
- La selezione predefinita per File Reputation Server è AMERICA (cloud-sa.amp.cisco.com)
- Fare clic sul menu a discesa e scegliere i File Reputation Server più vicini (in particolare per i

clienti APJC ed EUR	OPE):		
T Advanced Settings for File Reputation	File Reputation Server	V ANCHIGAS (cloud-secure) class core	
	ANP for Endpoints Canada Integration/ $\Xi$	AMERICAGE Ageogr (Cristel - sa anguistation of the control of the	areac @ deregister
	551; Communication for file Reputation:	ommunication for Rie Reputation APIC (cloud-exac)(campulate cont) Printer reputation divid Tament Press (California)	
		Server:	he:
	Heartbeat Interval	23 minutes	
	Query Timesut:	D Horse D	
	Processing Timesus:	UI work	
	File Reputation Clark 20:	be79abd0-4462-4653-868a-72a342a0434	
	File Retraspective:	Suppress the worket update alorts (8)	

- Espandi impostazioni avanzate per analisi file
- La selezione predefinita per l'URL di File Analysis Server è AMERICAS (https://panacea.threatgrid.com)
- Fare clic sul menu a discesa e scegliere i File Reputation Server più vicini (in particolare per i clienti EUROPA):

* Advanced Settings for His Analysis	File Analysis Server URL	<ul> <li>Alef BCAS Interclasteria Provigid coni EURIPE (Interclasteria Envelopid e.d.)</li> </ul>	0
	File Analysis Chart XD: Private analysis stoud		F-Ad177168/BJC_CLORK_000080
Eache Settings	Advanced settings for Cache		

#### Impostazione soglia analisi file

(Facoltativo) È possibile impostare il limite superiore per il punteggio accettabile dell'analisi del file. I file bloccati in base alle impostazioni di soglia vengono visualizzati come Soglia personalizzata nella sezione File delle minacce di malware in ingresso del report Protezione avanzata da malware.

- Nella pagina delle impostazioni globali dell'AMP, espandere Impostazioni soglia.
- Il valore predefinito del servizio cloud è 95.
- Scegliere il pulsante di opzione **Immettere valore personalizzato** e modificare il valore (ad esempio 70):

* Thrashaki Settinga	File Analysis Threshold Score:	<ul> <li>Bee take from Clead Service (M)</li> </ul>
		Driver Ouebern Welse: 10

• Fare clic su Sottometti e su Conferma modifiche

#### Integrazione di ESA con AMP for Endpoints Console

(Solo per i clienti di AMP for Endpoints) Tramite la console di AMP for Endpoints è possibile creare un elenco di blocco dei file personalizzato unificato (o un elenco dei file consentiti) che può essere distribuito senza problemi in tutta l'architettura di sicurezza, compresa l'ESA.

- Nella pagina delle impostazioni globali di AMP espandere **Impostazioni avanzate per la reputazione dei file**
- Fare clic sul pulsante Registra accessorio con AMP for Endpoints:
- Fare clic su **OK** per reindirizzare al sito della console AMP for Endpoints per completare la registrazione.
- Accedere alla console AMP for Endpoints con le credenziali utente
- Fare clic su Allow authoring the ESA registration (Consenti autorizzazione alla registrazione

LON).			
The VINESABODIE1_564D58189564A76C416D-6F8AA6579D18 (ESA endpoint) is requesting the following authorizations:	Applications external to AMP for Endpoints, such as Osco's Enepower Management Center, can be authorized to access your business' data.		
Device Registration	Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.		
	Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.		
	Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.		
Deny Allow	1		

La console AMP for Endpoints esegue automaticamente il pivot della pagina verso ESA.
Verificare che lo stato della registrazione sia SUCCESS:

```
JHP for Endpoints Console Integration () VLNESA000181_S64D58189594A76C416D-4F8AA6579018 () December VSUCCESS
```

• Fare clic su Invia e su Conferma modifiche

ECV).

## Abilita correzione automatica cassetta postale (MAR)

Se si dispone di cassette postali O365 o di Microsoft Exchange 2013/2016, la funzione di risoluzione automatica delle cassette postali (MAR) consente di eseguire l'azione quando il verdetto della reputazione del file passa da Pulito/Sconosciuto a Dannoso.

- Passare a Amministrazione sistema > Impostazioni account
- In **Profilo account**, fare clic su **Crea profilo account** per creare un profilo di connessione API con Office 365 e/o le cassette postali di Microsoft Exchange:

Account Profiles 🖸					
Create Account Profile					
Account Profile Name	Profile Type	Description	Delete		
exchange	Exchange On Premise		8		

- Fare clic su Invia e su Conferma modifiche
- (Facoltativo) Profilo concatenato è un insieme di profili. È possibile configurare il profilo concatenato solo quando gli account a cui accedere risiedono in tenant diversi di tipi diversi di distribuzioni.
- Fare clic sul pulsante **Crea mapping di dominio** per mappare il profilo dell'account con il dominio del destinatario. Le impostazioni consigliate sono le seguenti:

Domain Mapping D			
Domain Mapping configuration is not available since all profiles are already mapped			
Maibox Profile/Chained Profile	Recipient Domain(s)	Delete	
eschenge	domein.com		

• Fare clic su Invia e su Conferma modifiche

# Configura Advanced Malware Protection (AMP) nei criteri di posta

Dopo aver configurato AMP e MAR a livello globale, è possibile abilitare i servizi per le policy di posta.

- Selezionare Mail Policies > Incoming Mail Policies (Policy di posta > Criteri posta in arrivo)
- Personalizzare le impostazioni di Advanced Malware Protection per un criterio Posta in arrivo facendo clic sul collegamento blu in Advanced Malware Protection per il criterio che si desidera personalizzare.
- Ai fini di questo documento, fare clic sul pulsante di opzione accanto a Abilita reputazione file e selezionare Abilita analisi file:



- Si consiglia di includere un'intestazione X con il risultato AMP in un messaggio.
- Le tre sezioni seguenti consentono di selezionare l'azione che l'ESA deve eseguire se un allegato viene considerato non scansionabile a causa di errori nei messaggi, limiti di velocità o se il servizio AMP non è disponibile. L'azione consigliata è Consegna così com'è con testo di avviso anteposto all'oggetto del messaggio:

Unscannable Actions on Message Errors		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No • Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
	1050	Host:
Unscannable Actions on Rate Limit		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No Ves
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination Host:	No Yes
		Host:
Unscannable Actions on AMP Service Not Av	ailable	
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No • Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	💌 No 💮 Yes
		Address:
	Send Message to Alternate Destination Host:	No Yes
		Host:

• La sezione successiva configura l'ESA in modo che elimini il messaggio se un allegato è considerato dannoso:

Messages with Halware Attachments:	
Action Applied to Message:	Drop Hessage •
Archive Original Message:	© No  ₩ Yes
Drop Malware Attachments:	If No. U Yes
Hodily Hessage Subject:	No. * Prepend Append
	WARNING: MALWARE DETECTED)
> Advanced	Optional sattings.

• L'azione consigliata è quella di mettere in quarantena il messaggio se l'allegato viene inviato per l'analisi dei file:

Hessages with File Analysis Pending:		
Action Applied to Message:	Quarantine *	
Archive Original Message:	© No . # Yes	
Modify Nessage Subject:	© No * Prepard © Appand	
	[WARNING: ATTACHMENT(S) HAY CONTAIN	
F Advanced	Optional settings.	

 (Solo per i criteri della posta in arrivo) Configurare le azioni correttive da eseguire sul messaggio recapitato agli utenti finali quando il verdetto della minaccia diventa dannoso. Le impostazioni consigliate sono le seguenti:

Enable Mailbox Auto Remediation (MAR)			
Mailton Auto Remediation Actions apply only if Account Settings are configured. See System Administration > Account Settings .			
Action to be taken on message(s) in user's mailbox:	Forward to:     Forward to:     and Delete		

• Fare clic su Invia e su Conferma modifiche

## Integrazione di SMA con Cisco Threat Response (CTR)

L'integrazione di un modulo di posta elettronica SMA richiede l'utilizzo di SSE (Security Services Exchange) tramite CTR. SSE consente a uno SMA di effettuare la registrazione con Exchange e consente esplicitamente a Cisco Threat Response di accedere ai dispositivi registrati. Il processo prevede il collegamento dell'SMA all'SSE tramite un token generato quando si è pronti per il collegamento.

- Sul portale CTR (<u>https://visibility.amp.cisco.com</u>), eseguire l'accesso con le credenziali utente.
- CTR utilizza un modulo per l'integrazione con altri prodotti di sicurezza Cisco, tra cui ESA. Fare clic sulla scheda **Moduli**.

<ul> <li>Scegliere Dispositivi e fare clic su Gestisci dispositivi:</li> </ul>							
alialia	Threat Response	Investigate	Snapshots	Incidents Beta	Intelligence	Modules	

cisco mieat Response	intelligence incluence intelligence intelligence
Settings > Devices	
Settings	Devices
Your Account	
Devices	Manage Devices Reload Devices
API Clients	Reload Devices

- CTR eseguirà il pivot della pagina su SSE.
- Fare clic sull'icona + per generare un nuovo token e fare clic su Continua.
- Copiare il nuovo token prima di chiudere la casella:

Add Devices and Generate Tokens 💿					
The following tokens have been generated and will be valid for	1 hour(s):				
Tokens					
0ac7c30df02c0abfbe4869b8085445c8					
Close Copy to Clipboard	Save To File				

- Nella scheda SMA, selezionare Management Appliance > Rete > Impostazioni servizio cloud
- Fare clic su Modifica impostazione e verificare che l'opzione Risposta alla minaccia sia Abilita.
- La selezione predefinita per l'URL del server di risposta alle minacce è AMERICAS (apisse.cisco.com). Per i clienti EUROPA, fare clic sul menu a discesa e scegliere EUROPA (api.eu.sse.itd.cisco.com):

Cloud Service Settings						
Edit Cloud Services						
Threat Response:	i Enable					
Threat Response Server:	AMERICAS (aprilate disco.com)					
Cancel	EUROPE (api.eu.sse.bd.cisco.com) Submit					

- Fare clic su Invia e su Conferma modifiche
- Incollare la chiave del token (generata dal portale CTR) nell'impostazione dei servizi cloud e fare clic su **Registra**:

Cloud Services Settings					
Registration Token: 🖲	Dec7c30df02c0a1/be405910005445c5	Register			

- Il completamento del processo di registrazione richiederà alcuni minuti. Tornare a questa pagina dopo alcuni minuti per verificare di nuovo lo stato.
- Tornare a CTR > Moduli > Dispositivo e fare clic sul pulsante Ricarica dispositivo per verificare che lo SMA sia visualizzato nell'elenco:

cisco Threat	t Response	vestigate Snapshots	Incidents Beta Intelligence	Modules			?		
Settings > Device	ces								
Settings		Devices							
Your Account									
Devices		Managa Devices							
API Clients		Manage Devices Reload Devices							
> Modules		Name	Туре	Version	Description	ID	IP Address		
Users		sma1	SMA	13.0.0-187	SMA	1	127.0.0.1		

## Conclusioni

Questo documento ha lo scopo di descrivere le configurazioni predefinite o le best practice per Cisco Advanced Malware Protection (AMP) in Email Security Appliance. La maggior parte di queste impostazioni è disponibile nei criteri per la posta elettronica in entrata e in uscita e la configurazione e il filtro sono consigliati in entrambe le direzioni.