# Cisco Email Security의 AMP(Advanced Malware Protection)를 위한 모범 사례 가이드

# 목차

소개 기능 키 확인 AMP(Advanced Malware Protection) 활성화 AMP(Advanced Malware Protection) 전역 설정 사용자 지정 파일 분석 임계값 설정 ESA와 AMP for Endpoints 콘솔 통합 사서함 자동 교정 사용(MAR) 메일 정책에서 AMP(Advanced Malware Protection) 구성 SMA와 Cisco CTR(Threat Response) 통합 결론

## 소개

AMP(Advanced Malware Protection)는 악성코드 탐지 및 차단, 지속적인 분석, 회귀적 알림 기능을 제공하는 포괄적인 솔루션입니다.AMP with Cisco Email Security를 활용하면 공격 전, 중, 후 전 단 계에 걸쳐 지능형 악성코드 방어에 가장 경제적이고 쉽게 구축할 수 있는 접근 방식을 통해 공격의 전 범위에서 탁월한 보호 기능을 제공합니다.

이 모범 사례 문서에서는 아래 나열된 Cisco ESA(Email Security Appliance)에서 AMP의 주요 기능을 다룹니다.

- **파일 평판** ESA를 통과하는 각 파일의 핑거프린트를 캡처하여 평판 판정을 위해 AMP의 클라 우드 기반 인텔리전스 네트워크에 전송합니다.이러한 결과를 통해 악성 파일을 자동으로 차단 하고 관리자가 정의한 정책을 적용할 수 있습니다.
- **파일 분석** ESA를 통과하는 알 수 없는 파일을 분석하는 기능을 제공합니다.매우 안전한 샌드 박스 환경을 통해 AMP는 파일의 동작에 대한 정확한 세부 정보를 수집하고 해당 데이터를 세 부적인 인적 및 머신 분석과 결합하여 파일의 위협 수준을 확인할 수 있습니다.그런 다음 이러 한 성향은 AMP 클라우드 기반 인텔리전스 네트워크에 전달되며 AMP 클라우드 데이터 세트를 동적으로 업데이트 및 확장하는 데 사용되어 보호를 강화합니다.
- MAR(Mailbox Auto Remediation) Microsoft Office 365 및 Exchange 2013/2016의 경우, 초기 검사 시점 이후에 악성으로 변한 파일이 포함된 이메일의 제거를 자동화합니다.따라서 관리자 의 업무 시간이 절약되고 위협의 영향을 억제하는 데 도움이 됩니다.
- Cisco AMP Unity 조직이 AMP for Endpoints Console에서 AMP 서브스크립션으로 ESA를 비 롯한 AMP 지원 디바이스를 등록할 수 있는 기능입니다.이러한 통합을 통해 Cisco Email Security는 AMP for Endpoints 콘솔이 이미 엔드포인트에 대해 제공하는 것과 동일한 방식으로 샘플 관찰을 확인하고 쿼리할 수 있으며, 단일 사용자 인터페이스의 모든 위협 벡터에서 파일 전파 데이터를 상호 연결할 수 있습니다.
- Cisco Threat Response Cisco 및 서드파티 소스의 보안 관련 정보를 직관적인 단일 조사 및 응답 콘솔로 통합하는 오케스트레이션 플랫폼입니다.이는 이벤트 로그 및 위협 인텔리전스를 위한 통합 프레임워크 역할을 하는 모듈형 설계를 통해 이루어집니다.모듈을 사용하면 관계 그

래프를 구축하여 데이터를 신속하게 상관관계를 분석할 수 있으며, 이를 통해 보안 팀은 공격에 대한 명확한 관점을 확보하고 효과적인 대응 조치를 신속하게 취할 수 있습니다.

## 기능 키 확인

- ESA에서 System Administration(시스템 관리)> Feature Keys(기능 키)로 이동합니다.
- 파일 평판 및 파일 분석 기능 키를 찾고 상태가 활성 상태인지 확인합니다.

## AMP(Advanced Malware Protection) 활성화

- ESA에서 Security Services(보안 서비스) >Advanced Malware Protection File Reputation and Analysis(Advanced Malware Protection 파일 평판 및 분석)로 이동합니다.
- Advanced Malware **Protection** Global Settings(**Advanced Malware Protection 전역 설정**)에서 Enable(활성화) 버튼을 클릭합니다.

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

• 변경 사항을 커밋합니다.

#### AMP(Advanced Malware Protection) 전역 설정 사용자 지정

- 이제 AMP가 활성화되어 있습니다. Edit Global Settings(전역 설정 수정)를 클릭하여 전역 설정 을 사용자 지정합니다.
- 파일 확장명 목록은 때때로 자동으로 업데이트되므로 항상 이 설정을 방문하여 모든 파일 확장 명이 선택되었는지 확인하십시오.



- 파일 평판 고급 설정 확장
- File Reputation Server의 기본 선택 사항은 AMERICA(cloud-sa.amp.cisco.com)입니다.
- 드롭다운 메뉴를 클릭하고 가장 가까운 파일 평판 서버(특히 APJC 및 유럽 고객의 경우)를 선 택합니다.

" Advented Settings for Pile Regulation	File Reputation Server	AMERICAS (cloud-ox and cloce core)	
	AMP for Endpoints Console Integration/3	AMERICALLAGED) (class-salarsp.sauxofin.com) EUROPE (closed-salarsp.class.com)	Mat () Dempirer
	554 Communication for File Reputation:	AFUC (cloud-secular sequences provide secular sequences provide secular secula	he _
	Pearlbeat Interval	23 rinte	
	Query Timesut:	D seconds	
	Processing Timeout:	UT work	
	File Reputation-Claim 30:	be79abd0-4463-4453-668a-73a342a0404	
	File Retraspective:	Suppress the vertilet update alorts (2)	

#### • 파일 분석에 대한 고급 설정 확장

- File Analysis Server URL의 기본 선택 사항은 AMERICAS(<u>https://panacea.threatgrid.com</u>)입니 다.
- 드롭다운 메뉴를 클릭하고 가장 가까운 파일 평판 서버(특히 유럽 고객의 경우)를 선택합니다.



#### 파일 분석 임계값 설정

(선택 사항) 허용되는 파일 분석 점수에 대한 상한 임계값을 설정할 수 있습니다.임계값 설정에 따라 차단된 파일은 Advanced Malware Protection 보고서의 Incoming Malware Threat Files 섹션에 Custom Threshold로 표시됩니다.

- AMP 전역 설정 페이지에서 Threshold Settings를 확장합니다.
- 클라우드 서비스의 기본값은 95입니다.
- Enter Custom Value(사용자 정의 값 입력) 라디오 버튼을 선택하고 값을 변경합니다(예: 70).

Driver Quetern Value: 50

• Submit and Commit 변경 사항을 클릭합니다.

#### ESA와 AMP for Endpoints 콘솔 통합

(AMP for Endpoints 고객만 해당) AMP for Endpoints 콘솔을 통해 통합 맞춤형 파일 차단 목록(또는 파일 허용 목록)을 생성할 수 있으며, ESA를 비롯한 보안 아키텍처 전반에 제약 전략을 원활하게 배 포할 수 있습니다.

- AMP 전역 설정 페이지에서 Advanced settings for **File Reputation(파일 평판 고급 설정)을 확장** 합니다.
- 버튼 클릭 AMP for Endpoints에 어플라이언스 등록:

- OK(**확인)**를 클릭하여 AMP for Endpoints 콘솔 사이트로 리디렉션하여 등록을 완료합니다.
- 사용자 자격 증명을 사용하여 AMP for Endpoints 콘솔에 로그인합니다.

ANY for Endpoints Canada 3 Telepican (8) Japanes Applanes with Anti-

• Allow authorization the ESA registration(ESA 등록 권한 부여 허용)을 클릭합니다.

The VINEIA000181_564D581855BA7ECE16D-eFBAA6579D18 (ESA endpoint) is requesting the following authorizations: • Device Registration	Applications external to AMP for Endpoints, such as Osco's Firepower Management Center, can be authorized to access your business' data. 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.
Deny Altow	Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.

- AMP for Endpoints 콘솔은 자동으로 페이지를 다시 ESA로 피벗합니다.
- 등록 상태가 SUCCESS로 표시되는지 확인합니다.

AMP for Endpoints Console Entegration 🛞 VLNESA000181\_564D58189584A76C436D-4F8AA6579018 🛞 Deregister 🗸 SUCCESS

• Submit and **Commit**을 클릭합니다.

# 사서함 자동 교정 사용(MAR)

O365 사서함 또는 Microsoft Exchange 2013/2016이 있는 경우 MAR(Mailbox Auto Remediation) 기능을 사용하면 파일 평판 판정이 Clean/Unknown에서 Malicious로 변경될 때 작업을 수행할 수 있 습니다.

- System Administration(시스템 관리) > Account Settings(계정 설정)로 이동합니다.
- 계정 프로필에서 계정 프로필 만들기를 클릭하여 Office 365 및/또는 Microsoft Exchange 사서
- 함으로 API 연결 프로필을 만듭니다.

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

- Submit and **Commit**을 클릭합니다.
- (선택 사항) Chained Profile(체인으로 연결된 프로파일)은 여러 구축 유형의 여러 테넌트에 액 세스할 어카운트가 있을 때만 체인으로 연결된 프로파일을 구성합니다.
- Create **Domain Mapping(도메인 매핑 생성**) 버튼을 클릭하여 계정 프로필을 수신자 도메인과 매핑합니다.권장되는 설정은 다음과 같습니다.

Domain Happing 🖸		
Domain Mapping configuration is not available since all profiles are already mapped		
Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
exchange	domain.com	

• Submit and **Commit**을 클릭합니다.

# 메일 정책에서 AMP(Advanced Malware Protection) 구성

AMP와 MAR이 전역으로 구성되면 이제 서비스를 통해 메일 정책을 활성화할 수 있습니다.

- Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)로 이동합니다.
- 맞춤화하려는 정책에 대해 Advanced Malware Protection 아래의 파란색 링크를 클릭하여 수신 메일 정책에 대한 Advanced Malware Protection 설정을 사용자 지정합니다.
- 이 모범 사례 문서의 목적을 위해 Enable File Reputation(파일 평판 활성화) 옆의 라디오 버튼 을 클릭하고 Enable File Analysis(**파일 분석 활성화)를** 선택합니다.

Advanced Malware Protection Settings		
Policy:	DEFAULT	
Enable Advanced Malware Protection for This Policy:	Enable File Reputation Enable File Analysis No	

- AMP 결과에 X 헤더를 포함하는 것이 좋습니다.
- 다음 3개 섹션에서는 메시지 오류, 속도 제한 또는 AMP 서비스를 사용할 수 없는 경우 ESA에 서 수행할 작업을 선택할 수 있습니다.권장 작업은 메시지 제목에 경고 텍스트가 추가되어 있는 그대로 전달을 수행하는 것입니다.

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
	Host:	Host:
Unscannable Actions on Rate Limit		
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 AMP Service Not Av	ailable	
Action Applied to Message:	Deliver As Is 🔻	
✓ Advanced	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
	Host:	Host:

### • 다음 섹션에서는 첨부 파일이 악성으로 간주될 경우 메시지를 삭제하도록 ESA를 구성합니다.

nessages with nativate attactments:		
Action Applied to Message:	Drop Hessage *	
Archive Original Message:	O No # Yes	
Drop Malware Attachments:	18 No 0 Yes	
Hodify Hessage Subject:	No  Prepend Append	
	WARNING: MALWARE DETECTED)	
> Advanced	Optional settings.	

#### • 파일 분석을 위해 첨부 파일이 전송된 경우 메시지를 격리하는 것이 좋습니다.

Hessages with File Analysis Pending:	
Action Applied to Message:	Quarantine *
Archive Original Message:	O No 🕷 Yes
Modify Nessage Subject:	© No ® Prepend © Append
	WARNING: ATTACHMENT(S) HAY CONTAIN
> Advanced	Optional settings.

• (수신 메일 정책에만 해당) 위협 판정이 악성으로 변경될 때 최종 사용자에게 전달된 메시지에 대해 수행할 교정 작업을 구성합니다.권장되는 설정은 다음과 같습니다.

Enable Matthex Auto Remediation (MAR)		
Haitbox 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:	
	* Oeiete	
	Forward to: and Delete	

• Submit and **Commit**을 클릭합니다.

## SMA와 Cisco CTR(Threat Response) 통합

SMA 이메일 모듈을 통합하려면 CTR을 통한 SSE(Security Services Exchange)를 사용해야 합니다 .SSE를 사용하면 SMA가 Exchange에 등록되고 Cisco Threat Response가 등록된 디바이스에 액세 스할 수 있는 명시적 권한을 제공할 수 있습니다.이 프로세스에는 SMA를 연결할 준비가 되었을 때 생성되는 토큰을 통해 SSE에 연결하는 작업이 포함됩니다.

- CTR 포털(<u>https://visibility.amp.cisco.com</u>)에서 사용자 자격 증명으로 로그인합니다.
- CTR은 모듈을 사용하여 ESA를 비롯한 다른 Cisco 보안 제품과 통합합니다. **모듈** 탭을 클릭합 니다.
- Devices(디바이스)를 선택하고 Manage Devices(디바이스 관리)를 클릭합니다.

cisco Threat Response	Investigate Snapshots Incidents Beta Intelligence Modules
Settings > Devices	
Settings	Devices
Your Account	
Devices	Manage Devices Reload Devices
API Clients	Reload Devices

- CTR은 페이지를 SSE로 피벗합니다.
- 새 토큰을 생성하려면 + 아이콘을 클릭하고 Continue를 클릭합니다.
- 상자를 닫기 전에 새 토큰을 복사합니다.

Add Devices and Generate Tokens (2)	×
The following tokens have been generated and will be valid for 1 ho	ur(s):
Tokens	
0ac7c30df02c0abfbe4869b8085445c8	
Close Copy to Clipboard Sa	ve To File

- SMA에서 Management Appliances 탭 > Network > Cloud Service Settings로 이동합니다.
- Edit Setting(설정 편집)을 클릭하고 Threat Response(위협 응답) 옵션이 Enable(활성화)인지 확인합니다.
- Threat Response Server URL의 기본 선택 항목은 AMERICAS(api-sse.cisco.com)입니다. 유럽 고객의 경우 드롭다운 메뉴를 클릭하고 유럽(api.eu.sse.itd.cisco.com)을 선택합니다.

Cloud Service Settings		
Edit Cloud Services		
Threat Response:	i € Enable	
Threat Response Server:	AMERICAS (api-ssa.cisco.com)	
Canod	EUROPE (spi.eu.sse.bd.cisco.com)	Submit

- Submit and **Commit**을 클릭합니다.
- Cloud Services Setting(클라우드 서비스 설정)에 CTR 포털에서 생성한 토큰 키를 붙여넣고 Register(**등록)**:

Registration Token: ③ pactu30/distribui400930005445c5 Register

- 등록 프로세스를 완료하는 데 다소 시간이 걸립니다. 잠시 후에 이 페이지로 이동하여 상태를 다시 확인하십시오.
- CTR > Modules > Device로 돌아가 Reload Device(디바이스 다시 로드) 버튼을 클릭하여 SMA가 목록에 나타나는지 확인합니다.

threat Response	Investigate Snapshots Incidents	Beta Intelligence	Modules			? 🔅		
Settings > Devices								
Settings	Devices							
Your Account								
Devices	Managa Devices Polos							
API Clients	Manage Devices							
> Modules	Name	Туре	Version	Description	ID	IP Address		
Users	sma1	SMA	13.0.0-187	SMA	I	127.0.0.1		

# 결론

이 문서에서는 Email Security Appliance의 Cisco AMP(Advanced Malware Protection)에 대한 기본 또는 모범 사례 컨피그레이션에 대해 설명합니다.이러한 설정 중 대부분은 인바운드 및 아웃바운드 이메일 정책 모두에서 사용할 수 있으며, 구성 및 필터링은 양방향으로 권장됩니다.