AMP Threat Grid Appliance

FAQ(자주 묻는 질문)

최종 업데이트: 2017년 1월 19일

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 여기에 언급된 서드파티 상표는 해당 소유자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다.

목차

Threat Grid Appliance FAQ(자주 묻는 질문)

이 문서에서 해당하는 내용을 찾을 수 없는 질문이 있는 경우 support@threatgrid.com으로 문의하십시오. 감사합니다!

Threat Grid Appliance란?

Threat Grid Appliance는 AMP Threat Grid의 위협 인텔리전스의 모든 기능의 지원을 받는 로컬 악성코드 분석에 사용되는 전용 UCS 서버(UCS C220-M3 또는 UCS C220-M4)입니다. 이 서버는 데이터 프라이버시에 대한 요구사항이 더 강력한 조직을 위한 것입니다. 예를 들어, AMP Threat Grid 클라우드 기반 솔루션의 사용을 방지하는 엄격한 프라이버시 정책 및 기타 규정 준수 지침에 따라 민감한 데이터를 다루는 공공 조직이나 기관이 있습니다.

이러한 조직들은 Cisco AMP Threat Grid Appliance(구축형)를 유지 보수함으로써 고유한 네트워크의 보안 및 프라이버시의 허가 없이 분석을 위해 잠재적으로 해로운 문서 및 파일을 전송할 수 있습니다.

Threat Grid Appliance의 릴리스 노트 위치는?

OpAdmin Portal(OpAdmin 포털) > Operations menu(작업 메뉴) > Update Appliance (어플라이언스 업데이트)

온라인에서 사용 가능한 형식화된 PDF 버전: Cisco 웹 사이트의 Threat Grid Appliance 설치 및 업그레이드 가이드 페이지

Threat Grid Appliance의 사용자 가이드 위치는?

Threat Grid Appliance 사용자 설명서는 Cisco 웹 사이트의 Threat Grid Appliance 설치 및 업그레이드 가이드 페이지에서 확인할 수 있습니다.

Threat Grid 포털이란?

Threat Grid에 대한 웹 기반 인터페이스입니다.

Threat Grid Portal 릴리스 노트 및 온라인 도움말 위치는?

네비게이션 바의 도움말 메뉴 아래에 있습니다.

API 설명서 위치는?

API 설명서는 Threat Grid 포털의 주요 도움말 페이지에서 확인할 수 있습니다.

Threat Grid Appliance를 인터넷에 연결해야 하나요? 아니면 Air-Gap이 가능한가요?

기술적으로는, 인터넷 액세스 없이 Threat Grid Appliance를 실행하는 것이 가능하지만 악성코드 분석을 효과적으로 수행하기 위해서는 인터넷 액세스가 필요합니다. 일부 악성코드의 경우 C2 서버, SMTP 서버 등에 연결해야 하기 때문에 인터넷 액세스를 사용하지 않을 경우 분석 결과의 유효성이 매우 줄어듭니다.

Threat Grid Appliance가 피드를 포함하나요?

아니요. Threat Grid Appliance는 AMP Threat Grid Curated 피드를 포함하지 않습니다.

하루에 몇 개의 샘플을 제출할 수 있나요?

하루에 분석되는 파일의 최대 수는 AMP Threat Grid Appliance 라이선스를 기준으로 하며 다음과 같습니다.

- Cisco AMP Threat Grid 5000 및 5004: 1,500개의 샘플
- Cisco AMP Threat Grid 5500 및 5504: 5,000개의 샘플

세 가지 인터페이스 속도 설정이란?

Clean/Dirty 인터페이스의 경우 최대 1Gb이며 관리자는 연결되는 방식과 연결되는 대상에 따라 최대 10Gb까지 속도를 높일 수 있습니다.

Threat Grid Appliance의 스토리지 용량을 어디에서 확인할 수 있나요?

OpAdmin > Configuration(컨피그레이션) > Storage(스토리지)

Threat Grid가 OpenDNS와의 통합을 지원하나요?

OpenDNS 지원에 대해 논의 중이지만 아직 로드맵이 결정되지 않았습니다. Threat Grid Cloud는 첫 번째로 통합되는 지점이 될 수 있습니다.

Threat Grid Appliance 업그레이드

빌드 번호/릴리스 버전 조회 표

빌드 번호	릴리스 버전	릴리스 날짜	참고
2016.05.20170105200233.32f70432.rel	2.1.6	2017-01-07	OpAdmin/tgsh-dialog를 위한 LDAP 인증 지원
2016.05.20161121134140.489f130d.rel	2.1.5	2016-11-21	ElasticSearch5, CSA 성능 수정
2016.05.20160905202824.f7792890.rel	2.1.4	2016-09-05	제조업 관련 주요 사항
2016.05.20160811044721.6af0fa61.rel	2.1.3	2016-08-11	오프라인 업데이트 지원 키, M4 초기화 지원
2016.05.20160715165510.baed88a3.rel	2.1.2	2016-07-15	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	2016-07-06	
2016.05.20160621044600.092b23fc	2.1	2016-06-21	
2015.08.20160501161850.56631ccd	2.0.4	2016-05-01	2.1 업데이트를 위한 시작점. 2.1로 업데이트하기 전에 2.0.4가 있어야 합니다.
2015.08.20160315165529.599f2056	2.0.3	2016-03-15	AMP 통합, CA mgmt. 및 스플릿 DNS 도입
2015.08.20160217173404.ec264f73	2.0.2	2016-02-18	
2015.08.20160211192648.7e3d2e3a	2.0.1	2016-02-12	
2015.08.20160131061029.8b6bc1d6	v2.0	2016-02-11	이 버전에서 2.0.1로 강제 업데이트
2014.10.20160115122111.1f09cb5f	v1.4.6	2016-01-27	2.0.4 업데이트를 위한 시작점
2014.10.20151123133427.898f70c2	v1.4.5	2015-11-25	
2014.10.20151116154826.9af96403	v1.4.4		

빌드 번호	릴리스 버전	릴리스 날짜	참고
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		중요한 네트워킹 변경사항: v1.3 이전 버전에서는 모든 아웃바운드가 Dirty 인터페이스에 있습니다. v1.3은 Clean 인터페이스에서 이메일 지원을 도입합니다. 이전에 해결책을 통합한 경우 v1.3과 계속해서 호환되는지 여부를 확인하십시오.
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix1		1.1에서 강제 업데이트 참고: 인터넷을 통해 업데이트를 다운로드할 경우에만 필요합니다. Air-Gap(미디어) 업데이트는 이 요건을 공유하지 않습니다.
2014.10.20150203155142.b06f7b4f	v1.1		

빌드 번호	릴리스 버전	릴리스 날짜	참고
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0+hotfix2		1.0에서 강제 업데이트 **참고:** 1.0+hotfix2는 대용량 파일을 중단 없이 처리할 수 있도록 업데이트 시스템 자체를 수정하는 **필수 업데이트**입니다. 인터넷을 통해 업데이트를 다운로드할 경우에만 필요합니다. Air-Gap(미디어) 업데이트는 이 요건을 공유하지 않습니다.
2014.10.20141125162159+hotfix1.8afc5e2f	v1.0+hotfix1		
2014.10.20141125162158.8afc5e2f	v1.0		

업데이트 설치

새 버전의 Threat Grid Appliance를 업데이트하기 전에, AMP Threat Grid Appliance 설정 및 컨피그레이션 가이드의 설명대로 초기 설정 및 컨피그레이션 단계를 완료해야 합니다. 이 내용은 AMP Threat Grid Appliance 제품 설명서 페이지에서 확인할 수 있습니다.

새 어플라이언스: 이전 버전과 함께 제공된 새로운 어플라이언스가 있고 업데이트를 설치하려는 경우, 초기 컨피그레이션을 먼저 완료해야 합니다. 모든 어플라이언스 컨피그레이션을 완료할 때까지 업데이트를 적용하지 마십시오.

어플라이언스 업데이트는 라이선스가 설치되어야만 다운로드할 수 있으며 데이터베이스를 포함하여 어플라이언스가 완전히 구성되지 않은 경우에는 올바르게 적용되지 않습니다.

Threat Grid Appliance 업데이트는 OpAdmin 포털을 통해 적용됩니다.

업데이트는 한 방향으로 이루어지므로 더 최신 버전으로 업그레이드한 후에는 이전 버전으로 되돌릴 수 없습니다.

업데이트는 자동입니다. 그러나 경우에 따라 약간의 지연이 있을 수 있으므로 가장 최신 버전인지 확인하려면 최신 업데이트가 완료되자마자 새로운 업데이트를 수동으로 즉시 재확인할 것을 권장합니다.

업데이트를 테스트하려면 분석을 위해 샘플을 제출합니다.

기존 Threat Grid Appliance의 업그레이드 경로는?

기존 어플라이언스의 업그레이드 경로는 1.0 -> 1.0+hotfix2 -> 1.4.6 -> 2.0.4 -> 2.1 -> 2.1.3입니다.

2.1 업그레이드

버전 2.1로 업그레이드하려면 버전 2.0.4를 사용 중이어야 합니다.

2.0.4 업그레이드

2.0.4 업데이트를 완료하려면 1.4.6 이상 버전을 사용 중이어야 합니다.

2.0 업그레이드

먼저, 2.0 업그레이드 이전의 중간 단계인 1.4.6 업그레이드를 완료합니다.

1.4.6 업그레이드를 완료하고 2.0 업그레이드로 계속 진행하기 전에 다음 오류가 발생했는지 여부를 확인하려면 Threat Grid 포털에서 알림을 확인합니다.

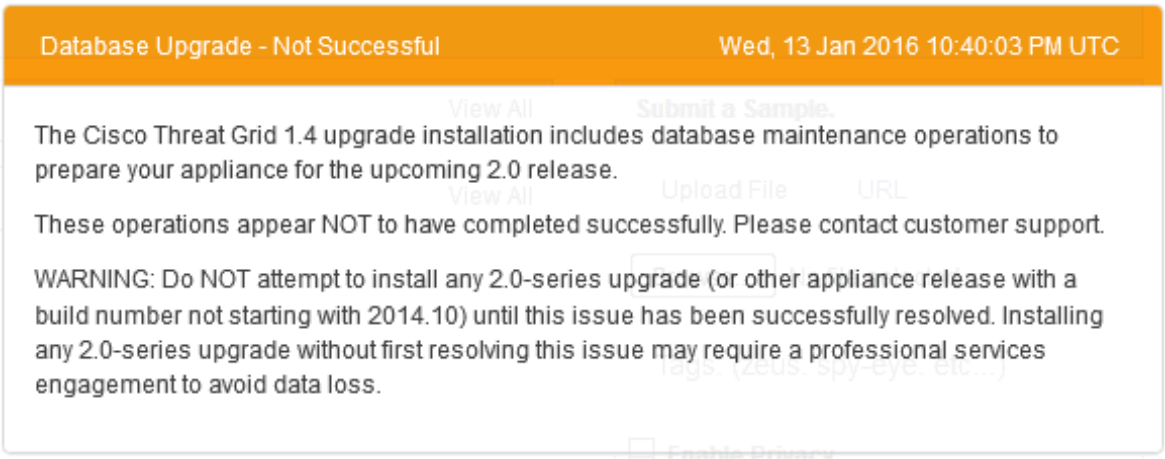

그림 1 데이터베이스 업그레이드 실패 알림

"데이터베이스 업그레이드 - 실패" 메시지는 새로운 어플라이언스가 예상한 버전보다 이전 버전의 PostgreSQL을 실행 중이며 자동 데이터베이스 마이그레이션 프로세스가 실패했음을 의미합니다.

오류 알림이 표시되지 않은 경우 2.0 업그레이드를 진행할 수 있습니다.

2.0 업그레이드에 필요한 시간

2.0 업그레이드는 대규모 ElasticSearch 데이터베이스를 사용할 경우 최대 몇 시간 정도의 시간이 걸릴 수 있다는 점에 유의하십시오.

업그레이드가 완료되기 전에 업그레이드를 중단하지 마십시오. 중단할 경우 지원 조치가 필요할 수 있습니다. 진행 중인 업그레이드의 상태를 확인하기 위해 가장 좋은 방법은 콘솔 액세스를 통해 확인하는 것입니다.

1.4 이전 릴리스에서 업그레이드

1.4 이전 릴리스에서 업그레이드하는 경우, 릴리스 노트의 섹션을 꼭 읽어 보십시오.

1.0+hotfix2 업데이트 필수

1.0+hotfix2는 대용량 파일을 중단 없이 처리할 수 있도록 업데이트 시스템 자체를 수정하는 필수 업데이트입니다.

참고: 이 업데이트는 인터넷을 통해 업데이트를 다운로드할 경우에만 필요합니다. Air-Gap(미디어) 업데이트는 이 요건을 공유하지 않습니다.

지원되는 파일 유형은?

다음 파일 유형을 분석을 위해 Threat Grid에 제출할 수 있습니다.

- PE32 파일(자세한 정적 포렌식):
  - 실행 파일(.EXE)
  - 라이브러리(.DLL)
- PE32+ 파일 -- win7-x64 VM에서만 사용 가능:
  - 실행 파일(.EXE)
  - 라이브러리(.DLL)
- Java 아카이브(.JAR)

참고: JAR은 매우 부정확한 파일 유형입니다. 원래 Threat Grid 파일 수락 시스템은 JAR 파일의 기본 요건에 부합하는 모든 파일을 사용하지만 [3.4.34 release](/doc/main/release_notes.html#3-.- 4-.-34)에서 도입된 Cisco의 새로운 시스템인 PREP2는 그렇지 않습니다. 대신, 새로운 준비 프로세스는 항목이 실제로 JAR(예: Android APK 파일)의 하위 형식 요건을 충족하는지 여부를 확인하기 위해 추가로 검사를 합니다. 이때 파일은 JAR 파일이지만 Threat Grid 환경에서 실행되지 않습니다. 안타깝게도, 이것은 JAR 파일처럼 보이지만 Windows용이 아니라 실제로 사용자의 전화기용입니다.

따라서, 더 이상 APK 파일을 수락하지 않습니다. 이 파일은 JAR 파일처럼 보일 수 있지만 Threat Grid에서 실행되지 않습니다.

- JavaScript (.JS) -- 파일이 .js 확장명을 지녀야 합니다.
- PDF(Portable Document Format)(자세한 정적 포렌식, JavaScript 리소스 포함) -- 3.4.34 포털 릴리스 노트에서 PDF 처리 변경사항을 참조하십시오.
- Office 문서(.DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX)(제한된 정적 포렌식)
- XML 기반 Office 문서 유형(.DOCX, .XLSX, .PPTX)
- XML - Extensible Markup Language(.XML)
  - Office의 XML은 해당하는 프로그램(Office 2K3)에서 열립니다.
  - 기타 모든 XML이 IE에서 열립니다.

- 아카이브 및 격리 형식:
  - 컨테이너 형식의 ZIP(.ZIP), 아카이브의 중첩 없음, 비밀번호 없음 또는 '감염됨' Cisco는 알려진 압축 해제 공격(AV 서비스에 대해 잘 알려진 공격인 42.zip을 포함하는 zip bombs 및 quine 등) 때문에 중첩된 ZIP 아카이브를 지원하지 않습니다.
  - ZIP 아카이브는 최대 100 개의 파일을 포함할 수 있습니다. 100개 이상의 파일을 지닌 아카이브는 분석을 반환하지 않으며 너무 많은 파일을 찾았음을 알리는 오류를 표시합니다. ZIP 아카이브 내에 있는 각 파일의 최대 파일 크기는 25MB입니다.
  - 격리(.VBN, .SEP)
  - xz(.xz), gzip(.gz), bzip2(.bz2), tar(.tar) -- 파일이 적절한 확장명을 지녀야 합니다.
- MIME HTML 파일(.MHTML)
- 플래시 파일(.SWF)
- URL(인터넷 바로가기 파일 또는 URL을 직접 제출합니다. 자세한 정적 포렌식 또는 JavaScript 리소스)
- MSI - Microsoft 설치 프로그램 파일(.MSI)
- LNK - Windows 바로가기 파일(.LNK)
- win7-x64-jp VM에서만 사용 가능(Ichitaro에 따라 다름) 중요 참고사항 – Threat Grid Appliance에서 사용할 수 없음:
  - .JTD, .JTT, .JTDC, .JTTC
- win7-x64-kr VM에서만 사용 가능(Hancom Office에 따라 다름). 중요 참고사항 –Threat Grid Appliance에서 사용할 수 없음:
  - .HWP, .HWT, .HWPX
- 배치(.BAT) -- 파일이 .bat 확장명을 지녀야 합니다.
- HTML 애플리케이션(.HTA) -- 파일이 .hta 확장명을 지녀야 합니다.
- Powershell(.PS1) --파일이 .ps1 확장명을 지녀야 합니다.
- Visual Basic 스크립트(.VBS) -- 파일이 .vbs 확장명을 지녀야 합니다.
- Windows 스크립트 파일(.WSF) -- 파일이 .wsf 확장명을 지녀야 합니다.
- 인코딩된 JavaScript(.JSE) -- 파일이 .jse 확장명을 지녀야 합니다.
- 인코딩된 Visual Basic(.VBE) -- 파일이 .vbe 확장명을 지녀야 합니다.
- 컴파일된 HTML 도움말(.CHM) -- Microsoft 컴파일 HTML 도움말입니다.

지원되지 않는 파일 유형은?

기타 파일 유형은 제출 시 악성코드 샌드박스에서 거부되며 Threat Grid 포털 인터페이스 및 API에서 "지원되지 않는 파일 유형"으로 플래그가 지정됩니다.

참고: .TXT는 지원되지 않습니다.

또한 Threat Grid는 이메일 헤더를 분석하지 않습니다. 본문을 살펴보고 기본적으로 네트워크 아티팩트로 처리하므로 몇 가지 검사가 여기에서 실행됩니다. 예를 들어 파일이 이메일로 전송되는 경우가 해당됩니다.

기타 파일 유형 제한이 있나요?

예:

- 샘플 파일 이름은 길이가 유니코드 59자 이하여야 합니다.
- 파일 크기는 0 바이트(즉, 비어 있음)는 가능하며 크기가 100MB보다 클 수 없습니다.

Threat Grid 지원에 문의하는 방법은?

도움이 필요한 경우, 다음과 같이 여러 가지 방법으로 Threat Grid Appliance 엔지니어의 지원을 요청할 수 있습니다.

이메일: support@threatgrid.com

지원 사례 열기 - 지원 사례를 열려면 Cisco.com ID가 있어야 합니다(없을 경우 생성). 또한 주문 송장에 포함된 서비스 계약 번호가 있어야 합니다.

통화 - http://www.cisco.com/c/en/us/support/index.html 참조

M3와 M4 서버의 주요 차이점은?

C220-M4 업그레이드(2016년 11월)는 기본적으로 하드웨어 새로 고침 및 추가 보안 부팅으로 구성됩니다. Threat Grid는 계약된 수명 주기가 만료될 때까지 M3를 계속해서 지원할 예정입니다. M4의 동일한 기능도 기존 M3의 유선을 통한 업데이트로 사용할 수 있습니다.

M3에서 M4 서버로의 마이그레이션 정보를 어디에서 확인할 수 있나요?

Cisco는 기존의 M3 및 M4 고객이 고객의 요구사항에 가장 적합한 서버 업그레이드와 데이터 마이그레이션, 백업, 출시 전략 등에 대한 질문을 논의하려는 경우 support@threatgrid.com에 직접 문의할 것을 강력하게 권장합니다.