Cisco AMP Threat Grid
프라이버시 및 샘플 가시성

최종 업데이트: 2016년 8월 10일

Cisco Systems, Inc. www.cisco.com

Cisco는 전 세계 200개가 넘는 지사를 운영하고 있습니다. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에 나와 있습니다.

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley (UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급자는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여
(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

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.

표지 사진: 아치스 국립공원 안내소 위의 높은 산등성이에 피어 있는 구화 선인장입니다. 이 선인장은 거칠고 척박한 환경에서도 위험을 효과적으로 방어하고 자원을 최대한 활용하며 잘 자랍니다. Copyright © 2015 Mary C. Ecsedy. All rights reserved. 사전 허락 없이 사용할 수 없습니다.

프라이버시 및 샘플 가시성

분석을 위해 Threat Grid에 샘플을 제출할 때 중요한 고려 사항은 콘텐츠의 프라이버시입니다. 프라이버시는 Threat Grid 액세스 특히 검색 API를 사용하는 사용자가 민감한 자료를 찾는 일이 비교적 쉽기 때문에 분석을 위해 민감한 문서 또는 아카이브 유형을 제출한 경우 특히 중요한 고려 사항입니다.

프라이버시는 온프레미스 Threat Grid Appliance로 샘플을 제출할 때는 Threat Grid Cloud로 제출할 때보다 상대적으로 문제가 심각하지 않지만, TGA 관리자라면 반드시 프라이버시 및 샘플 가시성의 기본사항을 이해하고 있어야 합니다.

Threat Grid로 샘플을 제출하기 위한 프라이버시 및 샘플 가시성 모델은 비교적 간단합니다. 샘플이 프라이빗으로 지정되어 있지 않은 한, 제출자의 조직 외부에 있는 사용자가 볼 수 있습니다. 일반적으로 *프라이빗*으로 지정된 샘플은 샘플을 제출한 사용자와 같은 조직에 있는 Threat Grid 사용자만 볼 수 있습니다.

Threat Grid Appliance의 프라이버시 및 가시성

프라이버시 및 샘플 가시성 모델은 "CSA Integrations"에서 제출되는 샘플에 맞게 Threat Grid Appliance에서 수정됩니다. CSA Integrations는 CSA API를 통해 Threat Grid Appliance와 통합(등록)된 ESA/WSA 어플라이언스 및 기타 디바이스 또는 서비스와 같은 Cisco 제품입니다.

Threat Grid Appliance에서 수행되는 모든 샘플 제출의 기본값은 퍼블릭이며, 소속 조직과 관계없이 CSA Integrations를 비롯한 다른 모든 어플라이언스 사용자가 볼 수 있습니다.

모든 어플라이언스 사용자는 다른 모든 사용자가 제출한 샘플의 세부사항을 볼 수 있습니다.

비CSA Threat Grid 사용자는 Threat Grid Appliance로 프라이빗 샘플을 제출할 수 있으며, 이 경우 해당 샘플은 CSA Integrations를 비롯하여 제출자의 조직에 속한 다른 Threat Grid Appliance 사용자에게만 보입니다.

프라이버시 및 샘플 가시성 모델은 다음과 같은 용어를 사용하며 아래 표에 설명되어 있습니다.

CSA Integrations	CSA Integrations는 CSA API를 통해 Threat Grid Appliance에 등록된 ESA/WSA 어플라이언스 및 기타 Cisco 디바이스 또는 서비스입니다. CSA Integrations에 의해 Threat Grid Appliance로 제출된 샘플의 기본값은 퍼블릭입니다.
기타 통합	동일한 기본 프라이버시 규칙이 FireAMP Private Cloud와 같은 기타 통합에 적용됩니다.
Threat Grid 사용자 - 퍼블릭	정상적인 Threat Grid 사용자(즉, 비CSA Integrations)에 의해 Threat Grid Appliance로 제출되는 퍼블릭 샘플입니다. 예를 들어, Threat Grid Portal UI를 통해 또는 Threat Grid 네이티브 API를 사용하여 샘플을 제출하는 어플라이언스 관리자 또는 악성코드 분석가가 여기에 해당합니다.

Threat Grid 사용자 - 프라이빗 정상적인 Threat Grid 사용자가 Threat Grid Appliance에 제출하는 프라이빗 샘플입니다.

이 경우 프라이빗 샘플은 제출자의 조직 외부에 있는 다른 모든 어플라이언스 사용자에게는 보이지 않습니다. 샘플은 제출자와 같은 조직에 속한 CSA Integrations에만 보입니다.

그림 1 - Threat Grid Appliance의 프라이버시 및 가시성

	다음에서 액세스할 경우의 샘플 가시성:			
샘플 전송자:	같은 조직의 Threat Grid 사용자	다른 조직의 Threat Grid 사용자	같은 조직의 CSA Integration	다른 조직의 CSA Integration
Threat Grid 사용자 - 퍼블릭	풀패키지 구매	풀패키지 구매	풀패키지 구매	풀패키지 구매
Threat Grid 사용자 - 프라이빗	풀패키지 구매	없음	풀패키지 구매	없음
CSA Integrations(ESA/WSA 어플라이언스 등) Threat Grid Appliance에 제출되는 모든 CSA 기본값은 퍼블릭임	풀패키지 구매	풀패키지 구매	풀패키지 구매	풀패키지 구매

FireAMP Private Cloud와 Threat Grid Appliance 통합에도 동일한 기본 프라이버시 규칙이 적용됩니다.

Threat Grid Cloud의 프라이버시 및 가시성

프라이빗 샘플이 CSA API(Cisco Sandbox API)를 통해 Threat Grid Cloud에 제출된 경우, "삭제한" 버전을 기타 CSA Integrations와 공유할 수 있습니다.

다음 표는 Threat Grid Cloud의 샘플 프라이버시 및 가시성을 설명합니다.

* **참고:** 삭제한 보고서에서 샘플에 대한 모든 잠재적으로 민감한 정보가 제거됩니다. 파일 이름, 프로세스 이름 등이 없습니다. 샘플이 다운로드되지 않을 수 있습니다.

그림 2 - Threat Grid Cloud Portal의 프라이버시 및 가시성

	다음에서 액세스할 경우의 샘플 가시성:			
샘플 전송자:	같은 조직의 Threat Grid 사용자	다른 조직의 Threat Grid 사용자	같은 조직의 CSA Integration	다른 조직의 CSA Integration
Threat Grid 사용자 - 퍼블릭	풀패키지 구매	풀패키지 구매	풀패키지 구매	삭제됨*
Threat Grid 사용자 - 프라이빗	풀패키지 구매	없음	풀패키지 구매	없음
CSA Integrations(ESA/WSA 어플라이언스 등) Threat Grid Appliance에 제출되는 모든 CSA 기본값은 프라이빗임	풀패키지 구매	없음	풀패키지 구매	삭제됨*

자세한 내용은 cisco.com의 **Threat Grid Install and Upgrades(Threat Grid 설치 및 업그레이드)** 페이지에 있는 설명서를 참조하십시오.