



2022년 4월

2022년 4월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

- [MITRE ATT&CK®와의 정렬, 1 페이지](#)

MITRE ATT&CK®와의 정렬

전역 위협 알림의 위협 정보 레코드가 MITRE ATT&CK® 프레임워크에 맞게 조정되었습니다.

- 해당하는 경우 ATT&CK 프레임워크에서 제공하는 명명 규칙을 바로 사용합니다.
- 전역 위협 알림 위협 정보는 관련 ATT&CK Tactics(전술), Techniques(기술) 및 Software(소프트웨어) 항목에 대한 참조를 제공합니다.

그림 1:

Critical Risk	
When:	February 5th - May 3rd
Modified:	yesterday
Threats:	WannaCry (S0366), Emotet (S0367), SMB service discovery (T1018)
Asset Groups:	Catch All
Affected Assets:	2 assets
Username:	demo_keturah.gaunt, dusti.hilton
IP Addresses:	10.102.77.196 <input type="checkbox"/> , 10.201.3.51 <input type="checkbox"/>

그림 2:

SMB service discovery

Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE v

High Severity 1,000+ affected assets in 100+ companies

Device is performing a scan of SMB services on TCP port 445 (SMB) (T1018), potentially typical for variants of WannaCry (S0366) or WCry ransomware and unlikely to be intended behavior of the device.

Category: Attack Pattern - scanning

이러한 개선 사항 덕분에 인시던트 대응을 위한 기존 표준 운영 절차와의 프로세스 통합이 더 쉬워지고 새로운 분석가의 학습 곡선이 단축됩니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.