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:*

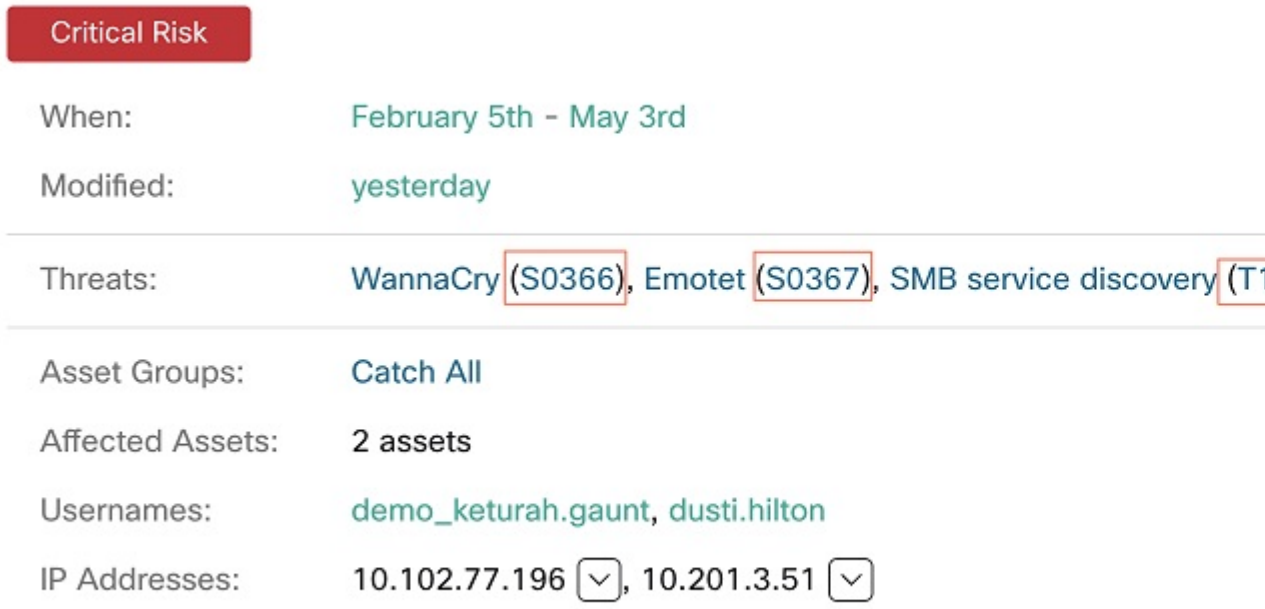
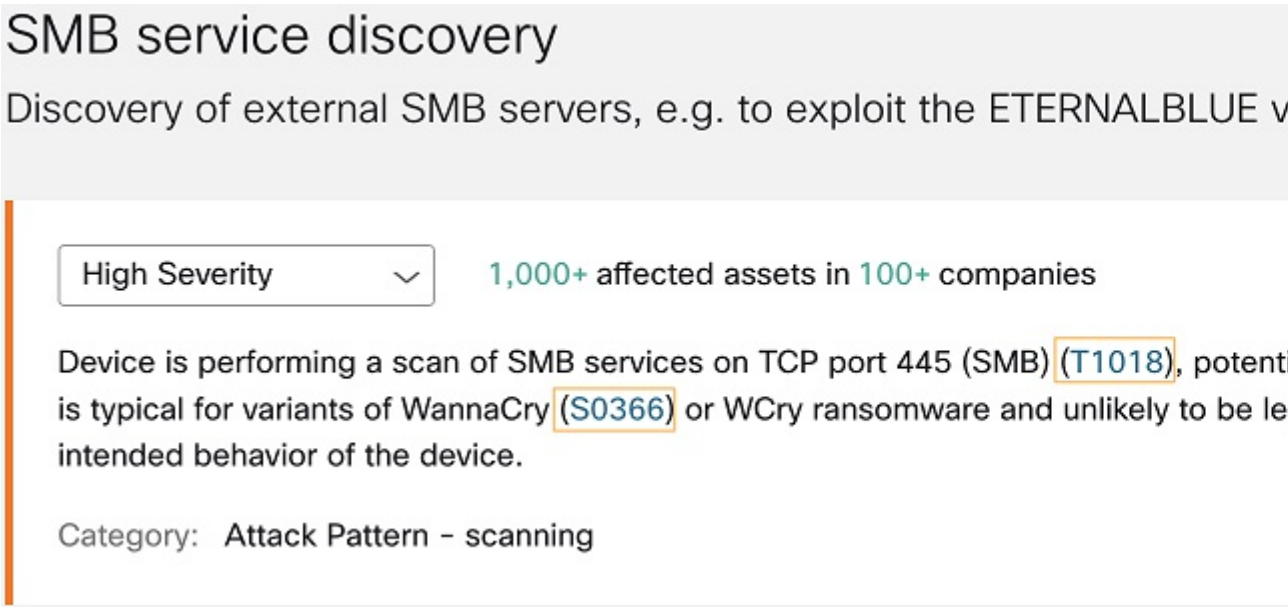


그림 *2:*



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