제목	DDos 장비 위협 IP 차단결과 보고		
등록자	박종순	**요청일**	2018-03-22 09:20
변경등급	EM	**변경근거**	보안
변경구분	기타		
자산변경유무	자산변경 없음	**서비스중단유무**	서비스중단 없음
작업 계획 시간	2018-03-21 13:00 ~ 2018-03-21 13:30 30분		

장비

대상장비	부품구분	제조사	부품변경	모델	수량
SCC-F-SE-0005-0000 프론트 오피스 디도스방지시스템#1					
SCC-F-SE-0006-0000 프론트 오피스 디도스방지시스템#2					

작업자	안우석	**알람 해제 여부**	알람해제 없음

변경내용

-개요 : 1, 2월 DDos 장비 차단 1순위 패턴에 대한 조치사항으로 위협IP를 블랙리스트에 등록하여 차단하기 위함
- 변경내용 : source ip 차단설정 등록
. R-project 사이트(137.208.57.37)에서 빅데이터캠퍼스방화벽(175.193.200.26)으로 tcp ack flooding 공격
. KT사용 ip(14.63.224.210)에서 175.193.202.43 등 다수의 상수도 서비스로 slow read defense 공격

변경절차

1. 해당 접근 목적지인 프론트망 프로토콜 취약점 방어 내용 확인
2. 사용자 정의 차단 설정에서 source_IP 블랙리스트 등록
3. 차단 설정 및 공격 로그 확인 등 모니터링
* 작업결과 상세내용은 붙임 참고

복구대책

차단 설정 해제