일일 보안관제 보고서

2025년 5월 29일(목)

결재	기안	1차검토	2차검토	결재

1. 시스템 운영

업무 내용

1. 시스템 장애 : 특이사항 없음.
2. 작업 : 특이사항 없음.
3. 정보시스템 장비 Splunk 연동 현황

(단위 : 개)

일자	구분	계	정상	단절	로그 미수집	Standby 장비
5. 29(목)	보안장비	3	3	0	0	0
	서버	2	2	0	0	0
	웹서버	1	1	0	0	0
	총계	6	6	0	0	0

※ Splunk 로그 수집 연동 이상 없음.

2. 보안관제 업무

사이버위협 탐지 및 대응 현황

구분	계		웹해킹		비인가접근		악성코드		서비스거부		스캐닝		기타	
	탐지	대응	탐지	대응	탐지	대응	탐지	대응	탐지	대응	탐지	대응	탐지	대응
현황	46,774	3	46,639	3	135	0	0	0	0	0	0	0	0	0

업무 내용	건수	내 역
보안이벤트 탐지	3	[웹해킹] SQL Injection UNION SELECT 공격 탐지 1건 [웹해킹] SQL Injection SQLMap 공격 탐지 1건 [비인가접근] Brute-Force 공격 탐지 1건

1. [IPS/웹해킹] SQL Injection UNION SELECT 공격_250529_01
 - 이벤트 : SQL Injection Attempt - UNION SELECT
 - 트래픽 : 192.168.0.41(대한민국) → 192.168.0.39(뭉치시스템)
 - 내 용 : 웹 서버에 존재하는 SQL Injection 취약점에 UNION SELECT 구문을 활용한 접근이 탐지됨. 공격이 성공하여 고객의 아이디, 메일 주소 및 비밀번호 데이터베이스가 유출되었을 가능성 존재함.

* RawData
: GET /rest/products/search?q=|%27))%20union%20select%20id,email,password,4,5,6,7,8,9%20from%20users-- HTTP/1.1
Host: 192.168.0.39:3000
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: language=en; PHPSESSID=fa17404001c2b0abc7830218466d6396
If-None-Match: W/"1219-rO7d1Av5Kp/7uXwmF+3QGsWOOQU"

2. [IPS/웹해킹] SQL Injection 공격 탐지_250529_02
- 이벤트 : SQL Injection - sqlmap User-Agent Detected
- 트래픽 : 192.168.0.133(대한민국) → 192.168.0.39(뭉치시스템)
- 내 용 : 웹 서버에서 공격 자동화 도구인 SQLMap 접근을 탐지하였고 전체 서버 내 광범위한 데이터베이스가 유출되었을 가능성이 존재함.

* RawData
: GET /rest/products/search?q=test%25%27%20AND%20SUBSTR%28%28SELECT%20COALESCE%28createdAt%2CCHAR%2832%29%29%20FROM%20Wallets%20LIMIT%200%2C1%29%2C27%2C1%29%3ECHAR%2867%29%20AND%20%27TWtw%25%27%3D%27TWtw HTTP/1.1
Cache-Control: no-cache
User-Agent: sqlmap/1.9.2#stable (https://sqlmap.org)
Referer: http://192.168.0.39:3000/rest/products/search
Host: 192.168.0.39:3000
Accept: */*
Accept-Encoding: gzip,deflate
Connection: close

3. [IPS/비인가접근] Brute-Force 공격 탐지_250529_03
- 이벤트 : Brute Force - Login Attempt
- 트래픽 : 192.168.0.133(대한민국) → 192.168.0.39(뭉치시스템)
- 내 용 : 로그인 페이지를 대상으로 다중 계정 및 비밀번호 조합의 Brute-Force 공격이 탐지됨. 고객의 메일 주소와 비밀번호가 암호화되지 않은 상태로 유출되었을 가능성

있음. 공격자 IP를 차단하고 pfSense상의 Brute-Force 탐지 정책을 조정함.

* RawData
: POST /attack/rest/user/login HTTP/1.1
Host: 192.168.0.39
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate, br, zstd
Accept: */*
Connection: keep-alive
Content-Type: application/json
Content-Length: 54

{"email": "kisia@juice-sh.op", "password": "qwer1234"}

□ 유해 IP 차단

순번	트래픽	공격 유형
1	192.168.0.41(대한민국) → 192.168.0.39(뭉치시스템)	SQL Injection
2	192.168.0.133(대한민국) → 192.168.0.39(뭉치시스템)	SQL Injection
3		Brute-Force

※ 탐지된 공격 IP는 평판 조회 결과 유해 IP로 확인되어 방화벽 차단 적용

업무 내용	건수	내 역
침해사고 예방	2	보안뉴스 1건, 보안권고문 1건

1. 보안뉴스
1) 시카고대병원, 환자 • 직원 정보 무더기 유출 (출처 : 중앙일보)
- URL : https://www.koreadaily.com/article/20250528122331327
2. 보안권고문
1) Broadcom 제품 보안 업데이트 권고 (출처 : KISA 보안공지)
- URL : https://knvd.krcert.or.kr/detailSecNo.do?IDX=6488
※ 첨부파일 참조

업무 내용	건수	내 역
정책 및 탐지 Rule 적용	2	IPS 정책 작성 2건

1. [pfSense] 유해 IP 차단 정책 (2건)
1) IP 주소 : 192.168.0.133 / 192.168.0.41

2. [pfSense] Brute-Force 공격 탐지 룰 조정 (1건)

1) Snort rule : alert tcp any any -> any any (msg:"Brute Force - Login Attempt"; content:"/rest/user/login"; http_uri; nocase; threshold:type threshold, track by_src, count 10, seconds 10; sid:3000003; rev:1;)

3. 기타

구 분	내 역
기타 특이사항	특이사항 없음.