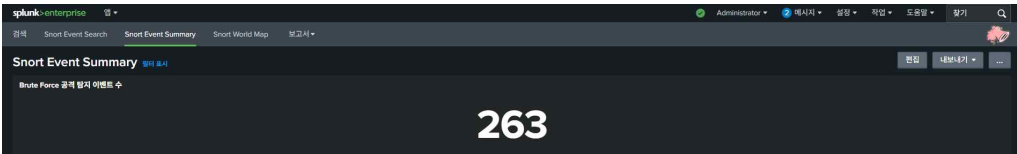
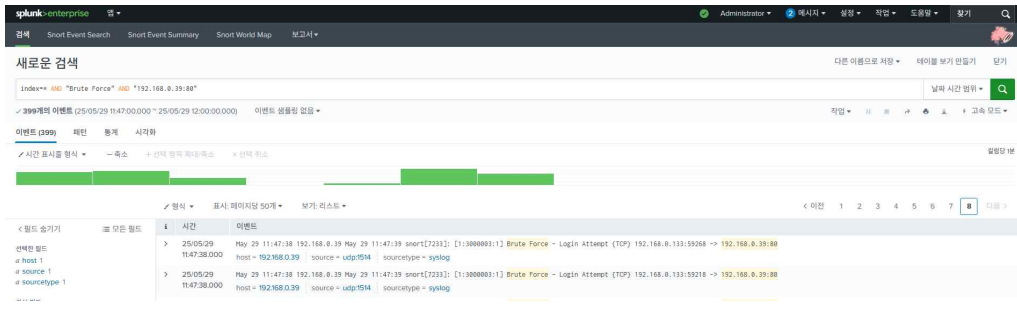


Brute-Force 침해사고 대응보고서

탐지 일시	2025. 05. 29. (목) 11:47											
공격 유형	Brute-Force											
탐지 장비	pfSense(IPS), Splunk <div></div>											
근무자 / 연락처	소속: 보안관제팀 / 직급: 선임 / 이름 : 김지선 / 연락처 : 010-1234-9876											
공격자 정보	<table><tr><td>구분</td><td>IP</td><td>Port</td><td>국적</td></tr><tr><td>내용</td><td>192.168.0.133</td><td>80</td><td>대한민국</td></tr></table>				구분	IP	Port	국적	내용	192.168.0.133	80	대한민국
구분	IP	Port	국적									
내용	192.168.0.133	80	대한민국									
목적지 정보	192.168.0.39:3000(문치시스템) <div></div>											
RawData	<div>POST /attack/rest/user/login HTTP/1.1</div> <div>Host: 192.168.0.39</div> <div>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/120.0.0.0 Safari/537.36</div> <div>Accept-Encoding: gzip, deflate, br, zstd</div> <div>Accept: */*</div> <div>Connection: keep-alive</div> <div>Content-Type: application/json</div> <div>Content-Length: 54</div> <div><div>{"email": "kisia@juice-sh.op", "password": "qwer1234"}</div></div> <div>HTTP/1.1 200 OK</div> <div>Date: Thu, 29 May 2025 05:55:37 GMT</div> <div>Server: Apache/2.4.41 (Ubuntu)</div> <div>Access-Control-Allow-Origin: *</div>											

	X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 809 ETag: W/"329-7Va1/FtLh8qN2wnsxdDsJYE03FY" Vary: Accept-Encoding Keep-Alive: timeout=5, max=100 Connection: Keep-Alive
대응 방법	<ul style="list-style-type: none"> - 탐지된 공격자 IP 192.168.0.133(brute-force)를 pfSense 방화벽을 통해 차단 - Snort 룰을 확인하여 탐지 룰이 정상적으로 작동하는지 검토 - 모든 계정에 대해 9자리 이상의 복잡한 비밀번호 사용 및 2차 인증(MFA) 적용 - 계정 보호 강화를 위해 로그인 시도 횟수 제한 정책을 적용함 - 사건 내용을 내부 보안팀에 공유하고, 필요 시 CERT와 연계 대응을 검토함
확인 및 조치 사항	공격에 대한 로그인 시도 관련 보안 로그(예: 인증 서버, 방화벽, IDS 등) 확인 및 캡처 후, 보안관제센터에 회신(이메일) 공격 확인 후 침해사고로 판단 시 해당 시스템은 즉시 네트워크와 절체 및 침해분석 인력이 현장에 도착 시까지 타 인원 접근 금지 공격에 대한 문의사항은 보안관제센터 유선(02-0000-0000) 또는 이메일로 연락

시스템 관리자 조치 결과

- 공격자 IP 192.168.0.133에 대해 pfSense 방화벽에 차단 정책을 등록함
- Snort 탐지 로그(alert.log)를 통해 공격을 식별하고, 탐지를 위한 커스텀 룰을 적용함
- 공격 시점 로그 분석 결과, 차단 룰이 정상적으로 작동하여 로그인 인증을 통과하지 못한 것으로 확인됨
- 아래는 pfSense 방화벽에서 차단 정책이 실제로 적용되고 기록된 로그




1. pfSense 방화벽 로그를 통해 **차단된 IP(192.168.0.133)**로부터 반복적인 접속 시도가 있었으며, 해당 트래픽이 정상적으로 차단되었음을 확인(Reject 적용)

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
 0/213 KiB	IPv4 TCP	192.168.0.133	*	192.168.10.100	*	*	none		Rejected IP manually	  

2. 차단 룰이 실효성 있게 작동함을 로그로 입증할 수 있었음(Reject 방식)

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
	Jun 2 11:23:45	WAN	 Rejected IP manually (1748829297)	 192.168.0.133:47650	 192.168.10.100:80	TCP:S