

ES for an Internet Service Provider:

How Splunk ES changed the way we
work and changed the organization

Kyoung Geun Lee | SK Broadband

Daesoo Choi | Splunk

Oct 2019 | Version 2



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

.conf19

splunk>



Kyoung Geun Lee

SOC Senior Manager | SK Broadband
Security Tech Team, SOC Operation



Daesoo Choi

Sr Sales Engineer | Splunk

Agenda

1. Who is SK Broadband? What SK Broadband Network Security Center do?
2. Use Case in ISP Security: DNS Hijacking
3. Customizing Enterprise Security for SOC Operation
4. Summary

1

Introducing SK Broadband Network Security Center

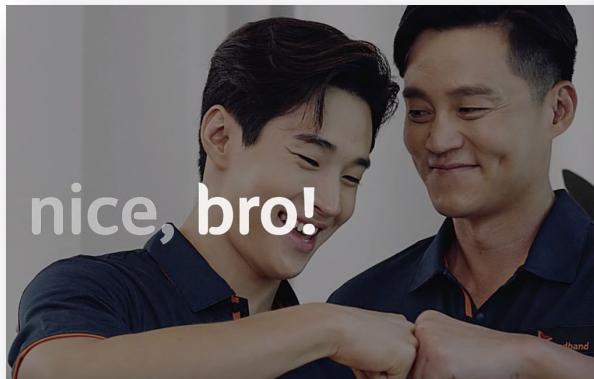
.conf19
splunk>



SK Broadband

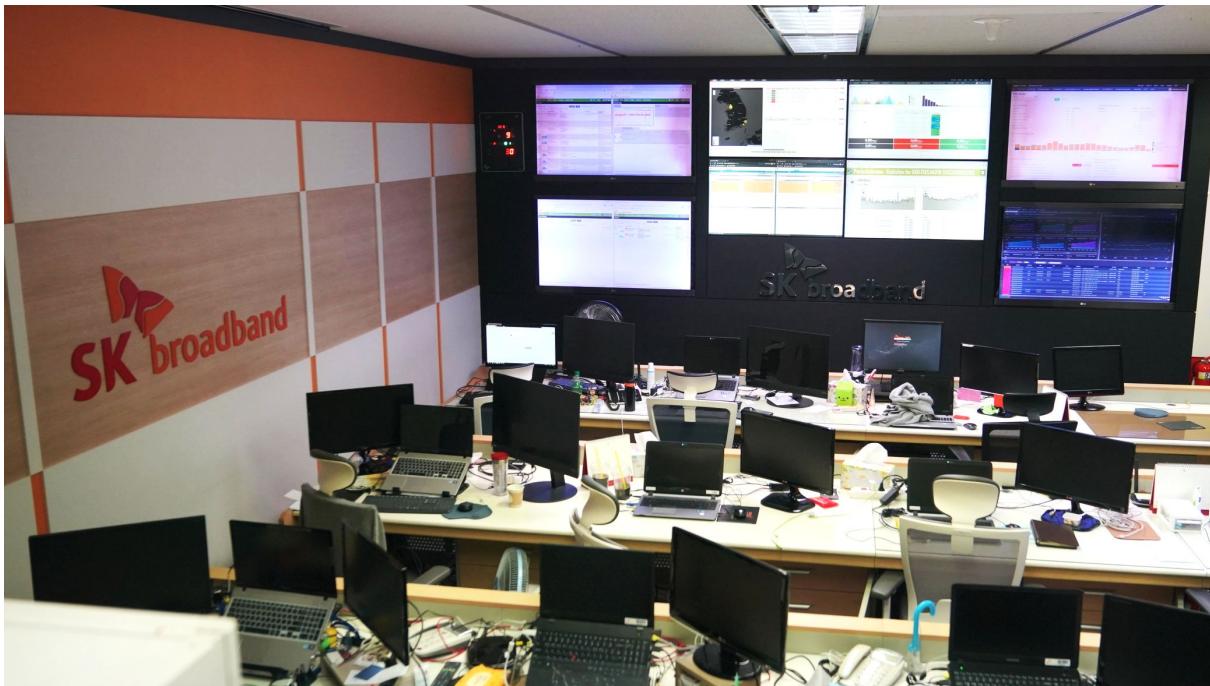
South Korean based Tier 1 ISP, Media Platform(IPTV) Service Provider

- ▶ Founded 1997, 2000+ Employees
- ▶ World First commercialized ADSL service
- ▶ ISP, IPTV : total **24M+** subscribers
- ▶ B tv : **5M+** subscribers
- ▶ Mobile IPTV (Oksusu) : **10M+** subscribers



SK Broadband Network Security Center

- ▶ N/W Security, Service Infra Security, B2B security(DDoS clean zone)



B2B Service Security Operation Center



Network Security Operation Center

Service Infra Security

Clean Network Pipe

SK Broadband Network Security Platform

Splunk Enterprise + Enterprise Security + SKB N/W Security Framework



Scalable DataStore



Monitoring



Search & Analyze



Alert



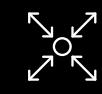
Dashboards



Machine learning



Notable Events



Adaptive Response

Risk Scoring Framework

Event Correlation Analytics

Security Intelligence Map

Open Security Platform

splunk®



Splunk Enterprise
Security™

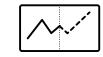
SK Broadband Network Security Framework



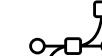
Intrusion
Detection&
Prevention



Malware
Detection Sys.



N/W Traffic
Anomaly
Detection



Flow/DNS
traffic



Threat
Intelligence



Vulnerability
Scans

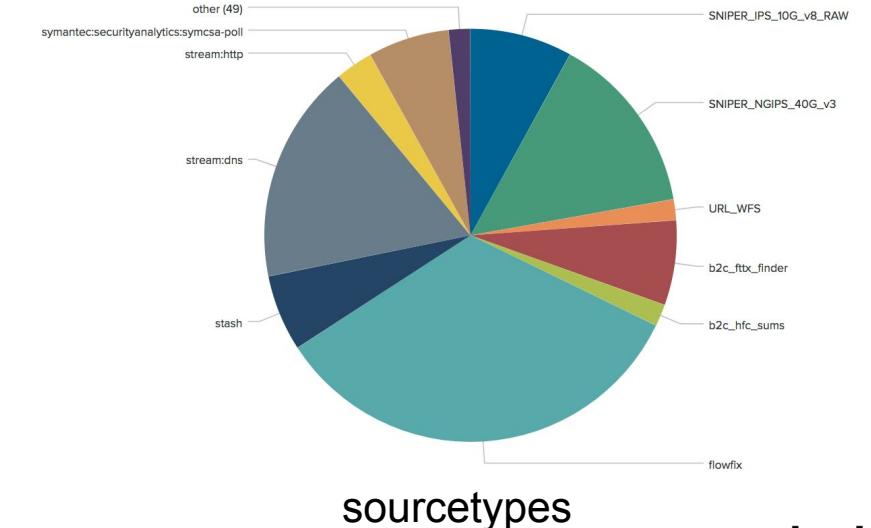
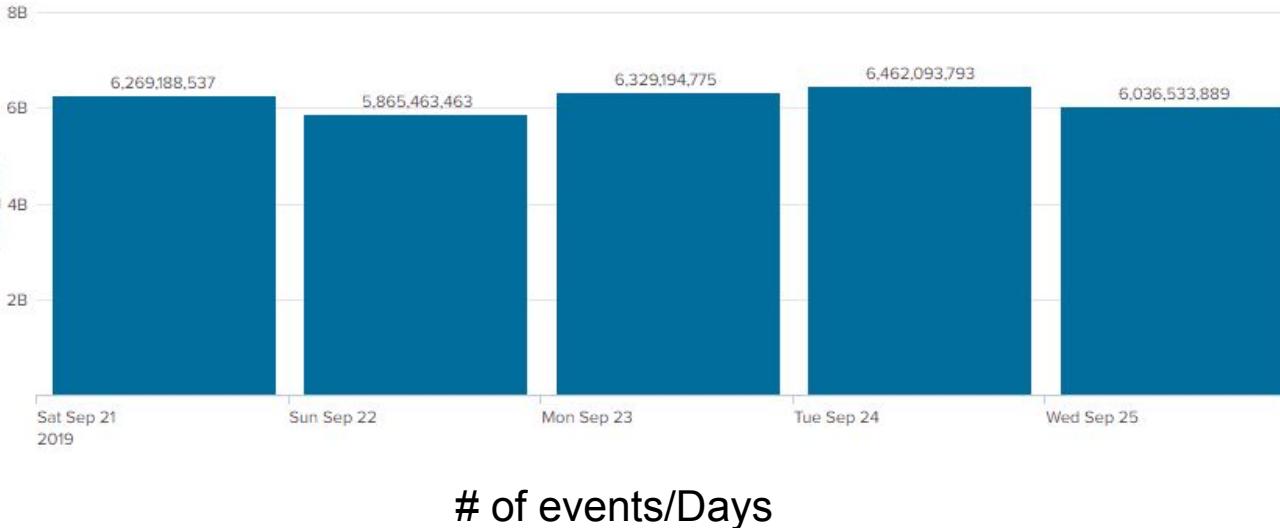


N/W
Protection

Data Sources

6B+ Events Per Day

- ▶ IDS / NG-IPS / IPS, Malware, Ransomware
- ▶ DNS Query, VoIP, HTTP, NetFlow, DHCP, Traffic Metadata
- ▶ SKB Threat Intelligence, OSINT, Private Intelligence
- ▶ B2C, B2B Customer Information
- ▶ Service Infra Asset Information, Other System Logs



Daily Event & Action Statistics

6B+ Events Per Day

4~4.
5B

2~3K

1~1.
5K

185~
200M

Raw Data
(Stream, Logs
NetFlow,
System logs etc)

Security
Sensor Logs
(IDS/IPS/DDoS
Malware etc)

Notable
events

Adaptive
Response
Actions

Security
Defense
Actions
(Block Attack
Count)

Security Posture

Home Security Posture Incident Review Security Investigator SoC Workflow Security Feedback Center Security Analytics Domain Security Intelligence Security AI Center_Beta Audit Search Configure Enterprise Security

Security Posture

Edit **Export** **...**

보안이벤트 현황 Intrusion Total Count **1.1b** **+25.3m**

EXCESS NOTABLE EVENTS Total Count **1.5k** **+93**

BTV 이벤트 현황 BTV Count **1m** **-142.8k**

VOIP 이벤트 현황 VoIP Count **4.1m** **-2.1m**

전진배치 IPS 이벤트 현황 FS_DDX Count **3.7m** **-2.3m**

PBR IPS 차단 현황 PBR Defense Count(Active) **185.9m** **+11.4m**

CNC 차단 현황 Block Count **325** **-13**

Notable Event Map(Last24H) A map of South Korea with regions colored according to event counts. A legend on the right shows values from 1 to 5.

Notable Events By Urgency A horizontal bar chart showing the count of notable events categorized by urgency: high (blue), informational (green), and low (yellow).

Risk Score by Time A line chart showing the risk score over time, with a secondary y-axis for the count of events.

Notable Events Over Time A line chart showing the count of notable events over time, with specific event types labeled: malware_analysis, network_anomaly, security_analysis, security_scanning, threat.

Top Notable Events A pie chart showing the distribution of top notable events, with labels for SKB_MA, SKB_SA, and SKB_ESS detection rules.

주요 악성코드 - Word Cloud A word cloud visualization of various malicious codes, with the most prominent being "Trojan.HOPLOADER".

주요 보안 이벤트 - Word Cloud A word cloud visualization of various security events, with the most prominent being "suspicious_detect_1".

2

Use Case : DNS Hijacking Defense

.conf19
splunk>

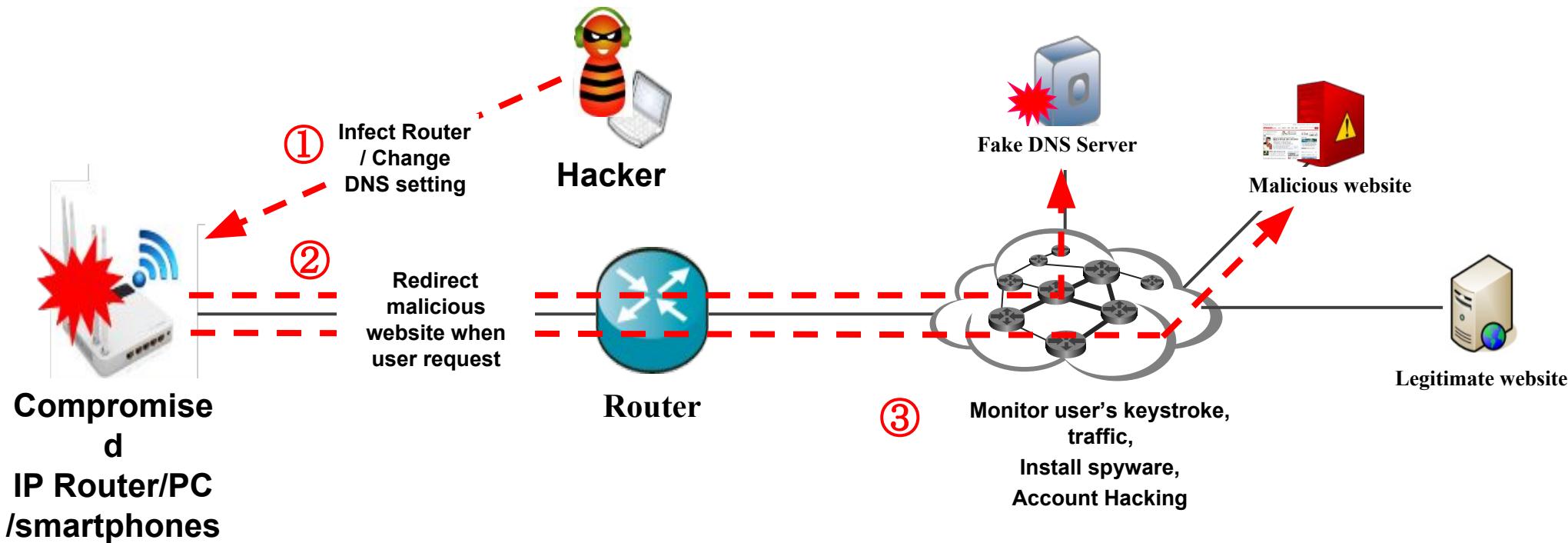


Detecting Home Router DNS hijacking attack

Use case of ISP security analysis and response

► Home router DNS Hijacking attack ?

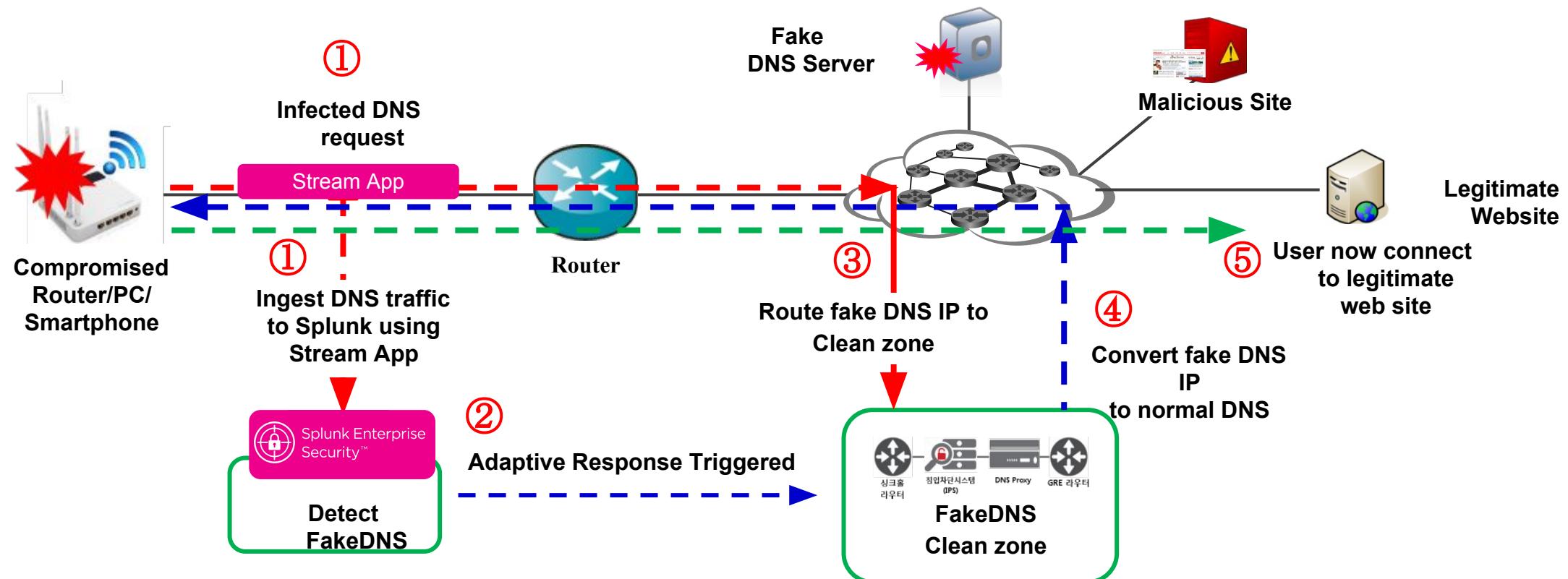
- Attackers install Trojan malware into Home Routers and change local **DNS** settings to redirect your traffic to malicious websites.



SK Broadband provides the secure protection for this attack as a part of free-of-charge service

Detecting Home Router DNS hijacking

Detecting fake DNS and response in ISP



Ingesting DNS data using Stream App

Analyzing and Detecting fake DNS with ES Correlation

Executing defense action with ES Adaptive Response

Sustaining clean internet service

Detecting Home Router DNS hijacking

▶ Correlation Search

```
1 | tstats `summariesonly` values(DNS.answer) as answer count from datamodel=Network_Resolution.DNS WHERE sourcetype=stream:dns  
    index=gi_dns DNS.message_type=RESPONSE DNS.reply_code_id=0 `removequery` `removequery_fakedns` DNS.record_type="A"  
2 | inputlookup fakedns_detect_domain.csv  
3 | rename domain as DNS.query  
4 | table DNS.query]  
  
13 | where match(query,"^(?!-)(?:[a-zA-Z\d\-\-]{0,62}[a-zA-Z\d]\.){1,126}(?!d+)[a-zA-Z\d]{1,63}$")  
14 | rename answer as request_answer  
15 | mvexpand request_answer  
16 | where match(request_answer,"\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}")  
17 | `skb_iplocation(request_answer, request_answer)`  
18 | `skb_lookup(dest,dest)`  
19 | where isnull(dest_domain)  
  
24 | lookup dns_whitelist dns_ip as request_answer OUTPUT dns_ip ASN as request_answer_dns_ip ASN  
25 | where isnull(request_answer_dns_ip ASN)  
26 | `sinkhole_check(dest)`  
27 | `fakedns_lookup(query,request_answer)`  
28 | `threatintel_multilookup(dest)`  
29 | `threatintel_multilookup(request_answer)`  
30 | rename query as check_domain
```

Home Router DNS hijacking Defense

Adaptive Response

i	Time	Security Domain	Src	Dest	CnC	Title	Urgency	Status	Owner	Actions																																																			
▼	8/31/19 11:27:01.000 PM	Security_analysis		82.163.142.3	SKB_SA - International	FakeDNS Affected IP Detect (By GI_DNS Query)	! Medium	New	SPC_SA	▼																																																			
<p>Description: FakeDNS 로 의심되는 해외 IP가 탐지되었습니다. 분석 후 대응해주시기 바랍니다. (탐지 Source : 국제 DNS 캐리 DATA)</p> <table border="1"> <thead> <tr> <th>Additional Fields</th> <th>Value</th> <th>Action</th> </tr> </thead> <tbody> <tr><td>FakeDNS Check Query</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Result (Cloudflare)</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Server (Cloudflare)</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Destination</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Destination ASN</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Destination Country</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Destination ISP</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Result (Google)</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Server (Google)</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>FakeDNS Query 응답값</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>FakeDNS Answer ASN</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>FakeDNS Answer Country</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>FakeDNS Answer ISP</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>싱크홀 우회 여부</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Result (SKB BNS1)</td><td>[REDACTED]</td><td>▼</td></tr> <tr><td>Check DNS Server (SKB BNS1)</td><td>[REDACTED]</td><td>▼</td></tr> </tbody> </table> <p>Related Investigations: Currently not investigated.</p> <p>Correlation Search: Security_analysis - SKB_SA - International FakeDNS Affected IP Detect (By GI_DNS Query) - Rule</p> <p>History: View all review activity for this Notable Event</p> <p>Adaptive Responses: ○ Loading...</p> <p>Next Steps:</p> <ul style="list-style-type: none"> ● 싱크홀 : Send to sinkhole ● SMS 발송 : Send SMS ● URL차단 : Send to 국내 URL 차단 											Additional Fields	Value	Action	FakeDNS Check Query	[REDACTED]	▼	Check DNS Result (Cloudflare)	[REDACTED]	▼	Check DNS Server (Cloudflare)	[REDACTED]	▼	Destination	[REDACTED]	▼	Destination ASN	[REDACTED]	▼	Destination Country	[REDACTED]	▼	Destination ISP	[REDACTED]	▼	Check DNS Result (Google)	[REDACTED]	▼	Check DNS Server (Google)	[REDACTED]	▼	FakeDNS Query 응답값	[REDACTED]	▼	FakeDNS Answer ASN	[REDACTED]	▼	FakeDNS Answer Country	[REDACTED]	▼	FakeDNS Answer ISP	[REDACTED]	▼	싱크홀 우회 여부	[REDACTED]	▼	Check DNS Result (SKB BNS1)	[REDACTED]	▼	Check DNS Server (SKB BNS1)	[REDACTED]	▼
Additional Fields	Value	Action																																																											
FakeDNS Check Query	[REDACTED]	▼																																																											
Check DNS Result (Cloudflare)	[REDACTED]	▼																																																											
Check DNS Server (Cloudflare)	[REDACTED]	▼																																																											
Destination	[REDACTED]	▼																																																											
Destination ASN	[REDACTED]	▼																																																											
Destination Country	[REDACTED]	▼																																																											
Destination ISP	[REDACTED]	▼																																																											
Check DNS Result (Google)	[REDACTED]	▼																																																											
Check DNS Server (Google)	[REDACTED]	▼																																																											
FakeDNS Query 응답값	[REDACTED]	▼																																																											
FakeDNS Answer ASN	[REDACTED]	▼																																																											
FakeDNS Answer Country	[REDACTED]	▼																																																											
FakeDNS Answer ISP	[REDACTED]	▼																																																											
싱크홀 우회 여부	[REDACTED]	▼																																																											
Check DNS Result (SKB BNS1)	[REDACTED]	▼																																																											
Check DNS Server (SKB BNS1)	[REDACTED]	▼																																																											

Detecting suspicious fake DNS

- ✓ Check DNS query
- ✓ Compare DNS reply with multiple Clean DNS query results (using SKB DNS, Cloudflare, Google, etc)
- ✓ Check Threat Intelligence

After reviewing information, conducting response actions

- ✓ Send IP to Change BGP Routing(FakeDNS CleanZone)
- ✓ Send SMS message to Network Security Team
- ✓ Customer POP-Notification

Home Router DNS hijacking Defense

Response Home Router DNS hijacking

▶ Adaptive Response

Adaptive Response Actions

Select actions to run.

+ Add New Response Action ▾

Send to sinkhole

Security Policy Name: 정책명 FakeDNS_SH

IP Field: dest

Router Desc: 라우터 Desc FakeDNS

Router Desc Description: 입력한 내용이 [SPC_입력한내용_날짜] 형식으로 라우터 description에 들어갑니다.

Detect Group: FakeDNS_IP

Detect Desc: FakeDNS

Detect Desc Description: (optional) DAPS에 표기되는 항목입니다. 이벤트의 필드명을 "필드명" 형식으로 입력 후 문구 추가 가능합니다.

- ▶ Pop-up on customer computer to warn and update router setting



Custom ES correlation searches

250+ Correlation Searches to defense latest ISP Security Threats

i	Name	Name	Name
>	SKB_SA_CNC_TR-069 SOAP RCE NewNTPServer exploit (KR)	SKB_SA_C2_Scanning IP Detect - Exist Src_Reserve_Domain	SKB_MA_CNC_Ransomware Cryptowall Download
>	SKB_SA_CNC_TUTOS 1.3 Remote Command Execution	SKB_SA_C2_Win Trojan Adylkuzz	SKB_MA_CNC_Ransomware Cryptowall Download (KR)
>	SKB_SA_CNC_TUTOS 1.3 Remote Command Execution (KR)	SKB_SA_C2_Win Trojan Adylkuzz (KR)	SKB_MA_CNC_Ransomware GandCrab Query URL Detect
>	SKB_SA_CNC_Vacron NVR Remote Command Execution	SKB_SA_C2_Win Trojan Jenxcus(H-Worm)	SKB_MA_CNC_Ransomware GandCrab Query URL Detect (KR)
>	SKB_SA_CNC_Vacron NVR Remote Command Execution (KR)	SKB_SA_C2_Win Trojan Jenxcus(H-Worm) (KR)	SKB_MA_CNC_ScamPage URL Detect
>	SKB_SA_CNC_Wireless IP Camera - Remote Command Execution	SKB_SA_C2_Win Trojan njRAT	SKB_MA_CNC_ScamPage URL Detect (KR)
>	SKB_SA_CNC_Wireless IP Camera - Remote Command Execution (KR)	SKB_SA_C2_Win Trojan njRAT (KR)	SKB_MA_CNC_Trojan Drunkbot Download
>	SKB_SA_CNC_WordPress DZS-VideoGallery - Command Injection	SKB_SA_C2_Win Trojan RevengeRAT	SKB_MA_CNC_Trojan Nemucod Download
>	SKB_SA_CNC_WordPress DZS-VideoGallery - Command Injection (KR)	SKB_SA_C2_Win Trojan RevengeRAT (KR)	SKB_MA_CNC_Trojan Nemucod Download (KR)
>	SKB_SA_CNC_ZTE router backdoor RCE	SKB_SA_CNC_ActiveMQ Web Shell Upload	SKB_MA_CNC_Trojan Nemucod Download MailList
>	SKB_SA_CNC_ZTE router backdoor RCE (KR)	SKB_SA_CNC_ActiveMQ Web Shell Upload (KR)	SKB_MA_CNC_Trojan Nemucod Download MailList (KR)
>	SKB_SA_CNC_Zyxel - OS Command Injection	SKB_SA_CNC_AirLink101 OS Command Injection	SKB_MA_CNC_Trojan.Ramnit URL Detect
>	SKB_SA_CNC_Zyxel - OS Command Injection (KR)	SKB_SA_CNC_AirLink101 OS Command Injection (KR)	SKB_MA_CNC_Trojan.Ramnit URL Detect (KR)
>	SKB_SM - BRAIN Correlation Rule Backup	SKB_SA_CNC_Android Debug Bridge - Remote Access	SKB_MA_CNC_WordPress SocialWarfare XSS
>	SKB_SM - BRAIN_internal splunkd log Monitoring	SKB_SA_CNC_Android Debug Bridge - Remote Access (KR)	SKB_MA_CNC_WordPress SocialWarfare XSS(KR)
>	SKB_SM - BRAIN_Physical Memory AND Disk Usage Monitoring	SKB_SA_CNC_Apache PHP cgi-bin Remote Code Execution	SKB_MA_CNC_Worm.Conficker URL Detect
>	SKB_SM - BRAIN_report_message_log failed	SKB_SA_CNC_Apache PHP cgi-bin Remote Code Execution (KR)	SKB_MA_CNC_Worm.Conficker URL Detect (KR)

3

Customizing Enterprise Security for SOC Operation



Splunk ES customizations

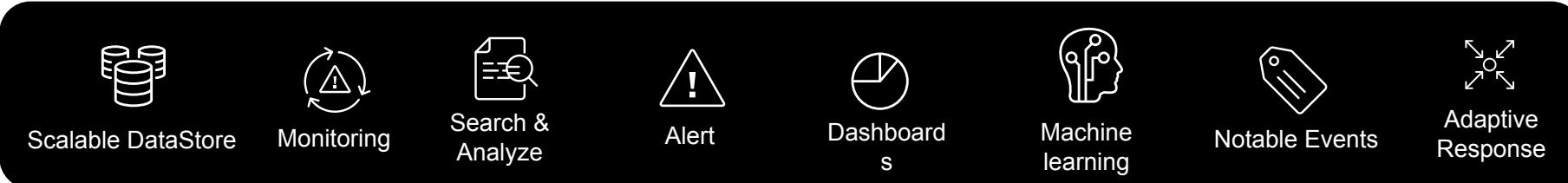
Integrating SOC workflow into Splunk ES

SOC Workflow
into Notable
Event Framework

Flexible
Bulletin Boards
for Everyone

SOC Report
Automation

Team
Transformation



SOC Workflow Into Notable Framework

Integrating daily SOC workflow into single Notable Event Framework

The screenshot shows a ticket creation form with the following fields:

- 접수구분:** 특이사항 (Selected)
- 상태구분:** Closed
- 접수시간:** 2019-09-09 22:13:00
- 접수번호:** 20190909-221302214
- 도메인:** Security_Mon
- 긴급도:** Informational
- 제목:** [Redacted]
- 내용:**
 - 시 간 : 00:00
 - 내 용 :
 - 대 응 :
 - 결 과 :
- 설명:** [Redacted]
- 작업자:** [Redacted]
- 정책구분:** 보안장비 정책관리 (Selected)
- 접수구분:** *보안장비 정책관리
- 접수시간:** 2019-09-09 22:13:02214
- 도메인:** 이경근/k3igun
- 긴급도:** 보안관제센터
- 제목:** [Redacted]
- 정책구분:** 보안장비 정책관리 (Selected)
- 접수구분:** 보안장비 정책관리 (1225) 인수인계 (758) ArborDDoS
- 접수번호:** 20190909-221302214
- 접수자:** 이경근/k3igun
- 소유자:** 보안관제센터
- 조회:** [Green button]

The screenshot shows a search results page with the following details:

- 검색 문자열:** [Redacted]
- 검색 기간:** 전체 기간
- 접수 구분:** 1, 2, 3 (Selected)
- 보안장비정책관리 (1225) 인수인계 (758) ArborDDoS**
- 인수인계:**
 - 접수 시작: 2019-09-09 18:33:47 [CERT4] [2019-09-09 아간 전달]
 - 접수 시작: 2019-09-09 10:02:02 [CERT4] [2019-09-09 주간 전달]
 - 접수 시작: 2019-09-08 22:05:31 [CERT4] [2019-09-08 아간 전달]
 - 접수 시작: 2019-09-08 09:38:03 [CERT4] [2019-09-08 주간 전달]
 - 접수 시작: 2019-09-07 18:58:21 [CERT4] [2019-09-07 아간 전달]
- 세부 내용:**
 - rule_description: 특정 웹사이트 접속 불가
 - 내용: 대상: https://pconestop.sk broadband.com/... 대상: 16.0.0.1 웹사이트 모니터링 중 connection
- 전체 검색:** IP, Domain, 제목, 내용
- 전체 검색:** 158 개별 검색
- 선택:**
 - 보안장비 정책관리
 - 인수인계
 - ArborDDoS
 - CleanZone
 - NW세이프존
 - Phishing
 - 서비스클리언트
 - 악성코드
 - 예방접수
 - 웹변조
 - 이벤트
 - 작업/문의/요청
 - 특이사항
 - 서비스클립온
- 페이지당 10개:** [Buttons: 이전, 다음, 초기화]

Integrating siloed SOC workflow systems into single framework □ Efficiency ↑

Customized ES Notable Event Creation

Customized ES Notable Event

- ▶ Splunk ES Notable Event Creation
- ▶ Customized “BrainNotable” Event Creation

New Notable Event

[Back to ES Configuration](#)

Title *	Type a title for the notable event.
Security Domain	Access ▾
Urgency	Informational ▾
Owner	unassigned ▾
Status	New ▾
Description *	Type a description for the notable event.



이벤트 접수 **Customized Category**

접수구분	예방접수	상태구분	Closed
접수시간	2018-11-14 13:53:49	접수번호	
도메인	Security_Monitoring	접수자	Administrator/admin
긴급도	Informational	소유자	보안관제센터
제목 *	<input type="text"/>		
요청자	<input type="text"/>		
차단IP	<input type="text"/>		
차단Domain	<input type="text"/>		
내용 *	<div style="border: 1px solid #ccc; padding: 5px;"> - 대 응 : - 내 용 : - 결 과 : </div>		
설명	<input type="text"/>		
<input type="button" value="File Attach"/>			
<input type="button" value="저장"/> <input type="button" value="취소"/>			

View ACL History

Brain Board (SOC Bulletin Board)

Increasing SOC efficiency with Information Sharing & Tracking

The screenshot displays the Brain Board application interface, which serves as a central hub for monitoring and managing security incidents and service status across various systems.

Top Navigation Bar:

- SMS ▾
- brainboard
- Brain Report ▾
- Brain Work ▾
- Brain Notable ▾
- 검색
- 데이터 집합
- 보고서
- 경고
- 대시보드
- App SA-brainplus

Left Panel: 장비이슈현황 (Equipment Issue Status)

This panel lists equipment issues with the following details:

No	제목	상태	장비분류	이슈일자	등록자	등록일	수정자
420	[DAPS] 차단불가IP 검색 기능 오류 현상 문의	완료	DAPS	2019.08.31		2019-08-31 23:57:26	이병권/skin049
419	[DOJ_FS1N_NGIPS1] lcm: Fail 로그 발생	진행중	NGIPS	2019.08.30		2019-08-30 22:15:32	최우준/skinj237
418	[POP_ICNAD_NGIDS_2] 특이로그 발생	진행중	NGIDS	2019.08.30		2019-08-30 21:40:41	최우준/skinj237
417	[SLSBK_GNS_C_VOIP_1,2] lcm: Warning 로그 발생	완료	IPS	2019.08.27			
416	[SPC v2.0] Slave3 특이로그 발생	진행중	SPC v2.0	2019.08.27			
415	[NGN-CZ-PI] Sample Packets 확인 불가 문의	완료	PeakFlow	2019.08.23			
414	[DAPS] 'HTTP Error 500: INTERNAL SERVER ERROR' 현상 문의	완료	DAPS	2019.08.22			
413	[IDC_MYIDC_IPS_1] 특이로그 및 데몬 다운 발생	완료	IPS	2019.08.22			
412	[POP-DJ-FireEye2] Splunk 이벤트 미수집 발생	완료	FireEye	2019.08.21			
411	[BRAIN ES3, ES4] BRAIN 캡틴 변경 문의	완료	Splunk	2019.08.21			

Right Panel: 서비스 클린존 (Service CleanZone)

This panel shows a service cleanup log entry for SKT's self-healing process:

제 목	등록자	등록일	수정자	수정일	상태
[SKT] 자동 우회 및 해제 - IP : 223.33.178.8	Administrator/admin	2018-09-06 17:51:51	Administrator/admin	2018-09-07 09:32:49	완료

Details of the service cleanup entry:

- 대상 : 223.33.178.8[SKT]
- 내용 : DDoS 공격 발생으로 인한 클린존 자동 우회
 - 서비스 클린존 SKT_Mitigation 자동 우회 확인
 - 00:26, DDoS클린존 우회 및 일임/차단 확인(전체: 최대 113.2 Mbps 입/차단량 30.4 Mbps)
 - 00:30, 공격 종료 및 차동 우회 해제
 4. DDoS공격 발생 정보 공유 및 매일 전달
- 결과 : NW보안팀 정준희M 보고 완료

Log entry timestamp: 2018-09-06 00:26:00

Completion timestamp: 2018-09-06 00:30:00

Attachment file: 0

Navigation links: 이전글 [SKT] 자동 우회 및 해제 - IP : 223.33.178.8 | 테스트 생선 | 다음글

Flexible Bulletin boards for Everyone – Work Efficiency + Sharing Culture

Brain Board (SOC Bulletin Board)

Everything is SPL based

- ▶ SPL based “Brainboard” , all data in KVstore
- ▶ Flexible Fields for each boards

작업/문의/요청

일반검색 SPL검색 ?

example) 제목=""*미수집*" AND (접수시간>="2018-06-15" AND 접수시간<="2018-07-31")

제목	상태	접수시간	완료시간	등록자	등록일
1 PBR IPS ACL 정책 추가	완료	2018-07-07 18:00:00	2018-07-07 18:02:00	2018-07-
2 PBR IPS ACL 정책 추가	완료	2018-07-07 18:50:37	2018-07-07 18:53:37	2018-07-
3 PBR IPS ACL 정책 추가	완료	2018-07-07 21:06:18	2018-07-07 21:08:18	2018-07-
4 PBR IPS ACL 정책 추가	완료	2018-07-08 01:40:00	2018-07-08 01:43:00	2018-07-
5 보안관제 침해 위협 차단 현황 작성	완료	2018-07-08 04:00:28	2018-07-08 04:02:28	2018-07-
6 PBR IPS ACL 정책 추가	완료	2018-07-08 05:41:23	2018-07-08 05:43:23	2018-07-
7 PBR IPS ACL 정책 추가	완료	2018-07-08 06:40:31	2018-07-08 06:43:31	2018-07-
8 [ES] 악성코드 C&C 서버 IP 차단 (2018.07.07)	완료	2018-07-08 09:30:02	2018-07-08 09:32:02	2018-07-
9 PBR IPS ACL 정책 추가	완료	2018-07-08 11:30:20	2018-07-08 11:33:20	2018-07-
10 PBR IPS ACL 정책 추가	완료	2018-07-08 11:40:46	2018-07-08 11:41:46	2018-07-

게시판 설정

게시판 명 * 작업/문의/요청

상태구분 값 접수,대응,완료

입력 템플릿

- 대 상 :
- 요청자 :
- 내 용 :
- 분 석 :

추가 필드 1 접수시간

추가 필드 2 완료시간

추가 필드 3

추가 필드 4

추가 필드 5

Notable Events View

Customized UI & SMS/Email Notification

- ▶ Customized “BrainNotable” Event List
- ▶ Bulletin Boards for daily workflow

↔ 반입/반출 이력

검색 기간: 2018-11-14 ~ 2018-11-14, 00:00:00 ~ 23:59:59

종류	반입	반출				
요청자	문서번호					
제목						
물품목록	품명	시리얼	규격	수량	위치	비고
	+ (New)					

문서번호: 0-20181114-131811
제목: 노후 장비 반출
보고서 등록
반출 확정
I-20181114-131706
서버 증설을 위한 하드웨어 반입 요청
반입 확정

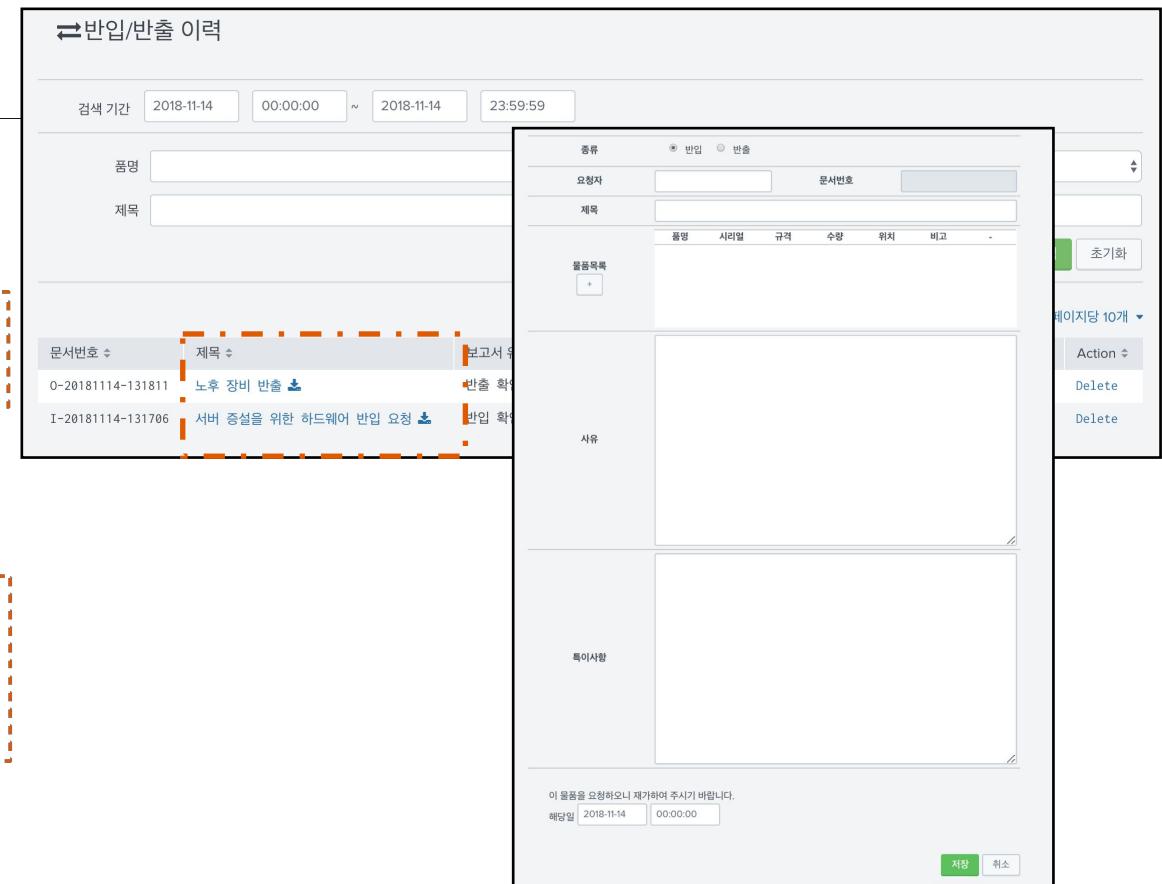
사유

특이사항

이 물품을 요청하오니 재가하여 주시기 바랍니다.
해당일: 2018-11-14 00:00:00

초기화
페이지당 10개
Action
Delete
Delete

저장 취소



SOC Report Automation

Significantly reduce time to create daily/weekly/monthly reports



Report Automation Management

No	보고서명	보고서 조회	생성자
18	일간_일일보고서	Link	[...]
17	ES_TMS SRC 수집	Link	[...]
16	주간_관제보고서_NMC 보고용_sk브로드밴드 일별 보안 지수	Link	[...]
15	(테스트)일간_일일보고서	Link	[...]
14	일별_인덱스 데이터 저장 기간	Link	[...]
13	일별_통계데이터_DDoS 이벤트	Link	[...]
12	월간_관제보고서_NMC 보고용_sk브로드밴드 일별 보안 지수	Link	[...]
11	일별_통계데이터_Cleanzone운영실적통계	Link	[...]
10	일별_통계데이터_SA_분석실적로그	Link	[...]
8	이번_통계데이터_M4_분석시작로그	Link	[...]

보고서 생성

보고서명*: Report Automation Test

실행주기: 한번 일간 주간 월간 분기

삽입문구: \$TEXT1\$ Text to Excel Index [+추가]

데이터를 데이터: \$DATA1\$ index=// Report SPL [+추가]

\$DATA2\$ index=// Report SPL [-삭제]

메일발송:

Saved Search returns SPL results □ Excel cells with macro

Saved Search returns
SPL results □ Excel cells with macro

2+ Hour / day □ 1 min

SOC Report Automation

Everything is SPL based

SPL results into Excel Template

보고서 생성

보고서 번호 20180629174853

보고서명* 일간_일일보고

실행주기 한번 일간 주간 월간 분기

삽입문구 SPL

\$TEXT1\$ [+추가]

테이블 데이터

- \$DATA1\$ | inputlookup brainboard | search board.
- \$DATA2\$ | rest /services/server/status/resource-use
- \$DATA3\$ | rest /services/server/status/partitions-sp
- \$DATA4\$ | inputlookup brainboard | search board.
- \$DATA5\$ | search earliest=-1d@d latest=@d index=_i

Template Upload

일간_일일보고.xlsx (26.3 KB)

메일발송

수신인*

제목*

내용*

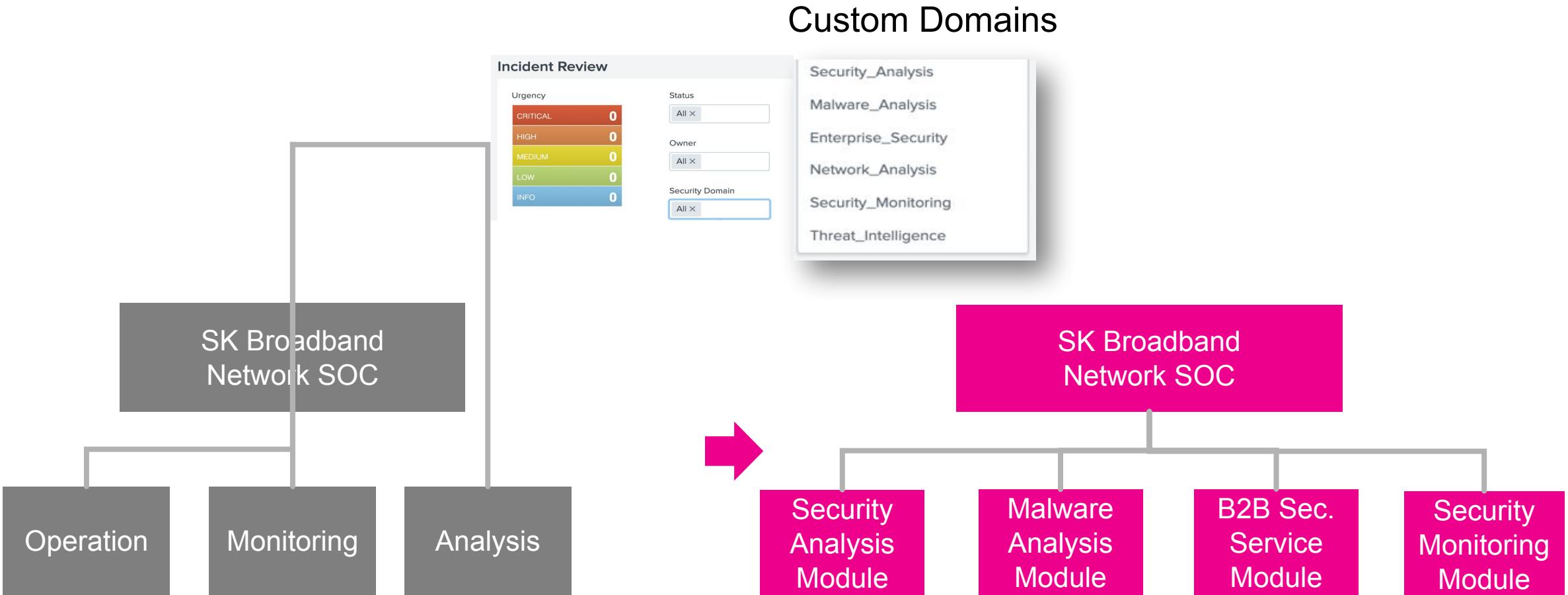
Excel Template

SPC 일일 근무 일지

근무시간				결재			조장	담당자	센터장
근무시간	\$TEXT1\$			근무자	주간	\$TEXT3\$			
보고일자	\$TEXT2\$			아간		\$TEXT4\$			
보안침해현황							100.00%		
사이버위기 경보 단계				정상			SKB 침해사고 경보 단계	CERT4	
자산 현황									
유형	IDS	IPS	NGIPS	기타	총 연동장비수	일반장애	서비스장애	총장애시간	
	10	104	9	47	170	0분	0분	0분	
수행 내 역 현황									
작업/문의/요청	Phishing			웹변조	이벤트	특이사항	악성코드		
CleanZone	ArborDDoS			서비스 블리즌	NW세이프존	예방접수			
수행 내 역									
구분	시작시간	종료시간	상세내역						
예방접수	4:50:00	5:03:00	상황전파문(제2018-0562호)						
			- 내용 : [Domain] bestsvil.club 외 3건, [IP] 114.43.96.237[TW]						
			- 악성앱 유포지, 악성앱 정보유출지						
	15:50:00	15:57:00	상황전파문(제2018-0563호)						
			- 내용 : [IP] 114.36.15.195[TW]						
			- 악성앱 유포지						
	4:00:00	4:10:00	대 우 도자 폐쇄화 기기터 정유(우선화)						
			... 보안관련 치해 위험 확인 완료						

Reorganize roles with customized domain

Team Transformation with Splunk ES



Transform team organization with Enterprise Security Domain base □ Increase Visibility/Performance

4

Summary

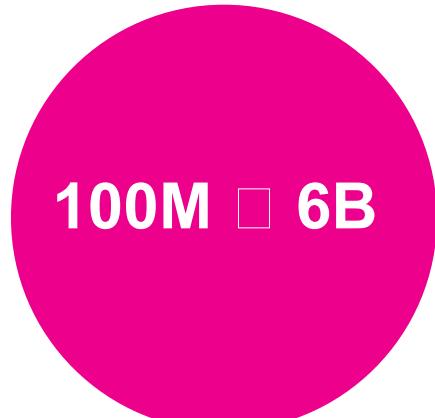
.conf19

splunk>



Splunk@SK Broadband Today

Before & After Splunk



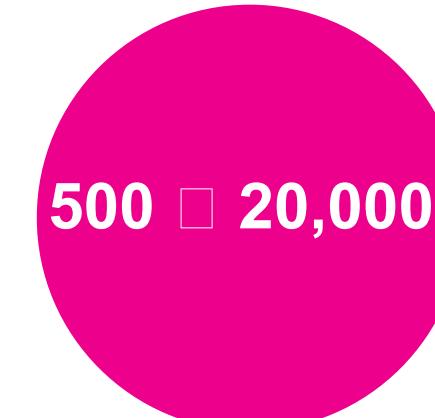
100M □ 6B

Daily Process
Security Events



3hrs □ 5 min

New Security Issues
Investigation/Response
Time



500 □ 20,000

Daily Process
Incidents



**2~3 Hrs
□ 1 min**

Daily Report
generation Time

Key Takeaways

1. Increased Work Efficiency and Visibility
@SK Broadband ISP SOC with Splunk Enterprise Security
2. Notable Event Framework is Fantastic, even Customization is easy
3. You can use ES to make your SOC perfect !

.conf19[®]

splunk[®]>

Thank
You!