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.

.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

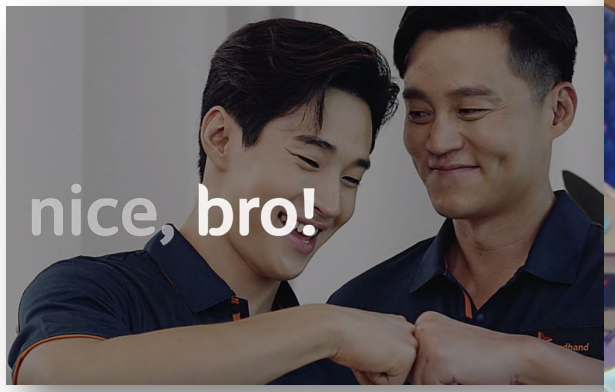
- Founded 1997, 2000+ Employees
- World First commercialized ADSL service
- ISP, IPTV : total **24M+** subscribers
- B tv : **5M+** subscribers
- Mobile IPTV (Oksusu) : **10M+** subscribers

SK broadband

B 전화 B 인터넷

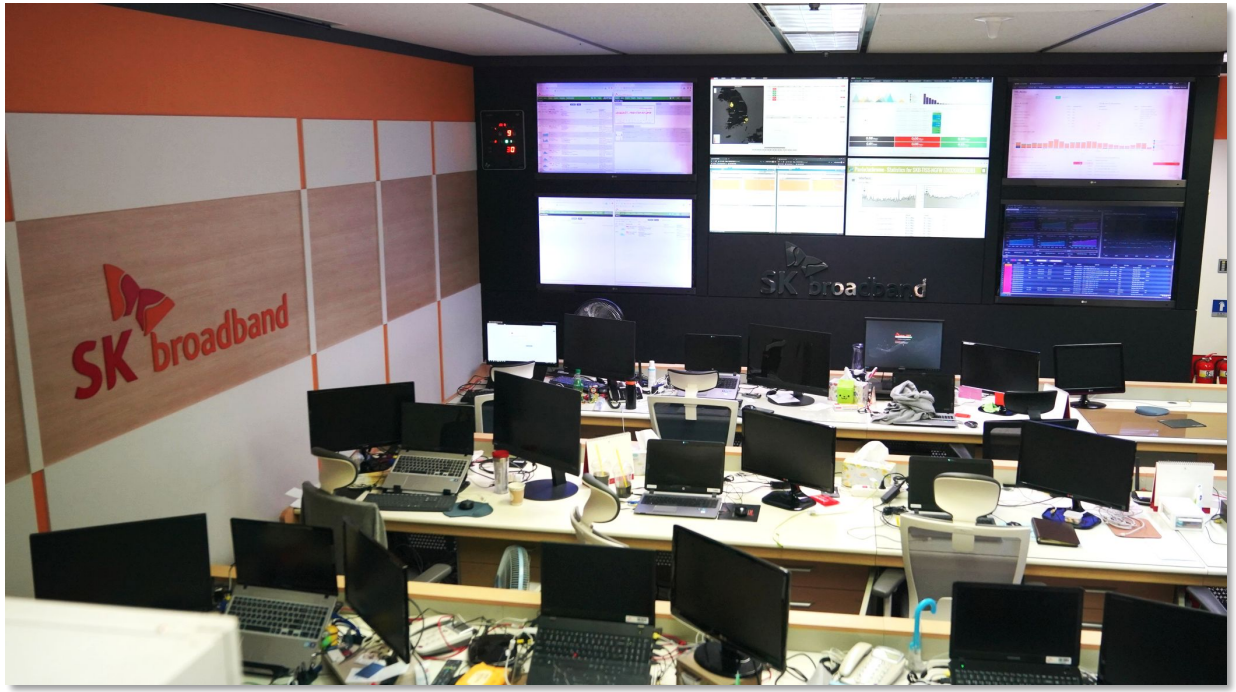
B 인터넷전화

B tv oksusu



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

SK broadband BRAIN Big-data Research Analysis In Network

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™

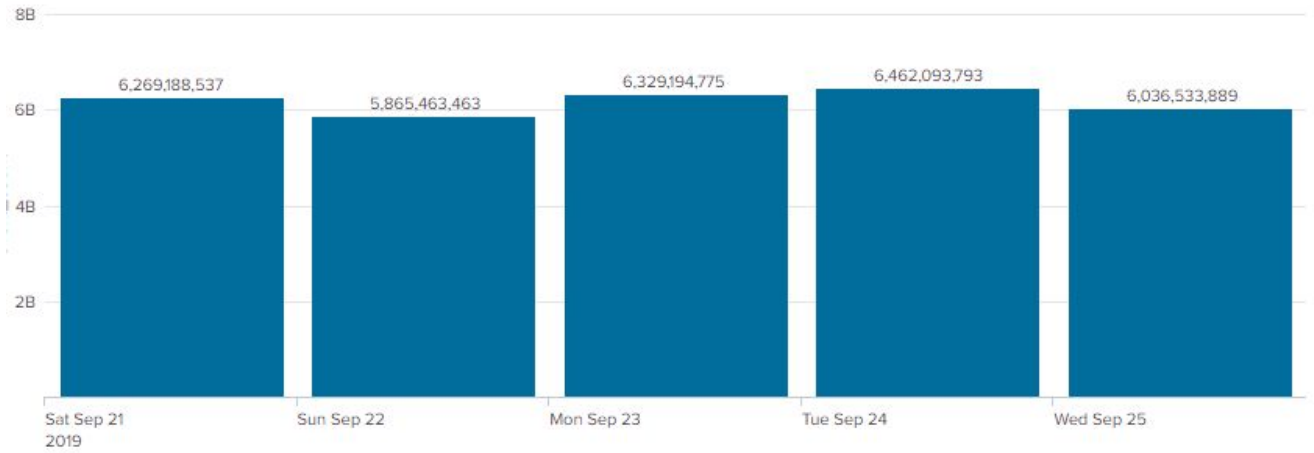
SK Broadband Network Security Framework

- Intrusion Detection& Prevention
- Malware Detection Sys.
- N/W Traffic Anomaly Detection
- Flow/DNS traffic
- Threat Intelligence
- Vulnerability Scans
- N/W Protection

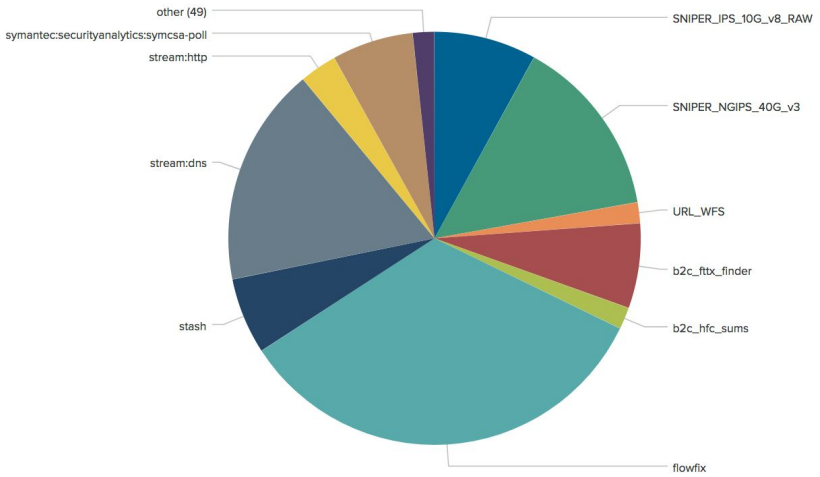
Data Sources

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



# of events/Days



sourcetypes

splunk> .conf19

Daily Event & Action Statistics

6B+ Events Per Day

Raw Data

(Stream, Logs NetFlow, System logs etc)

Security Sensor Logs

(IDS/IPS/DDoS Malware etc)

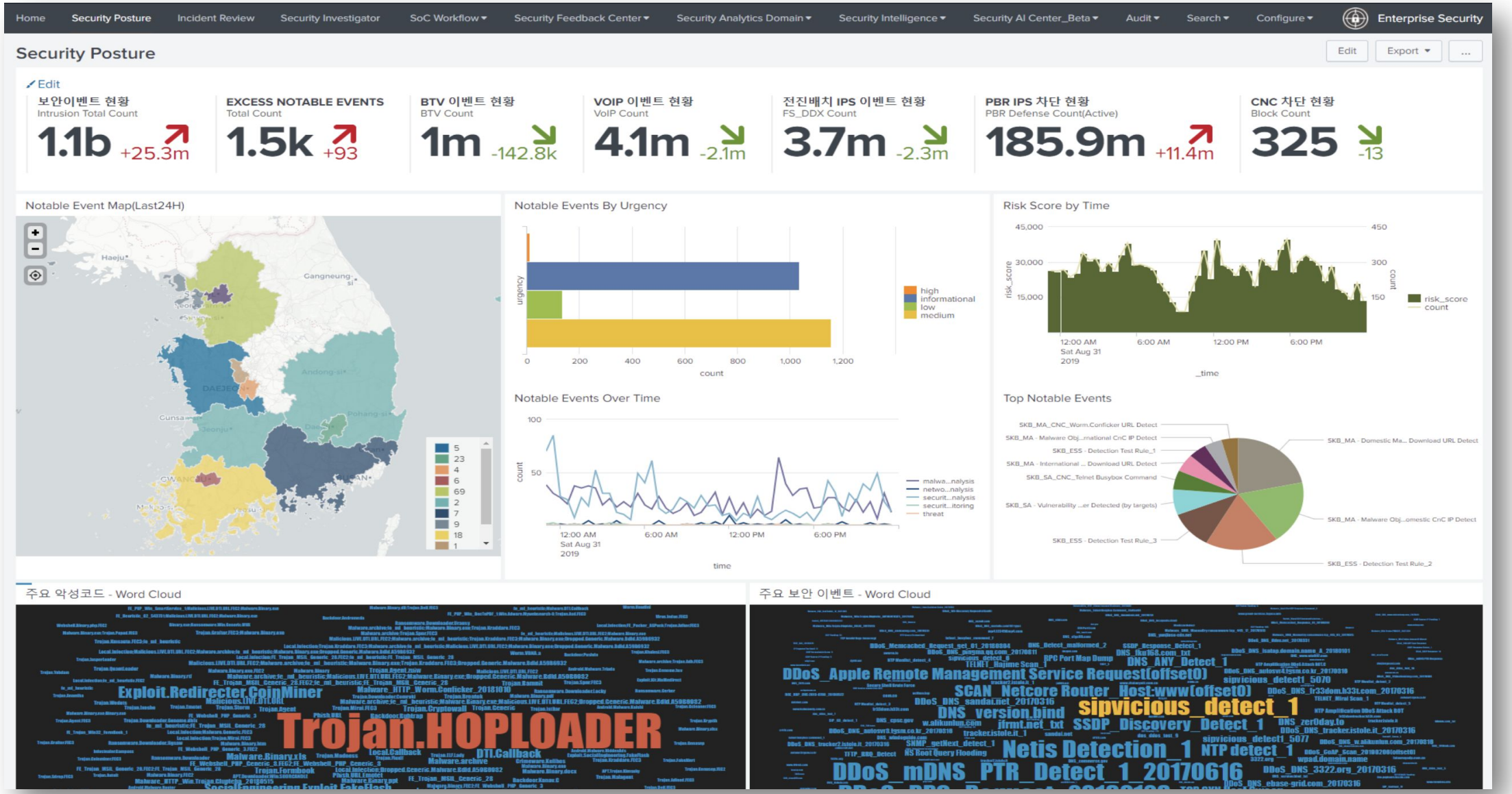
Notable events

Adaptive Response Actions

Security Defense Actions

(Block Attack Count)

Security Posture



splunk> .conf19

2

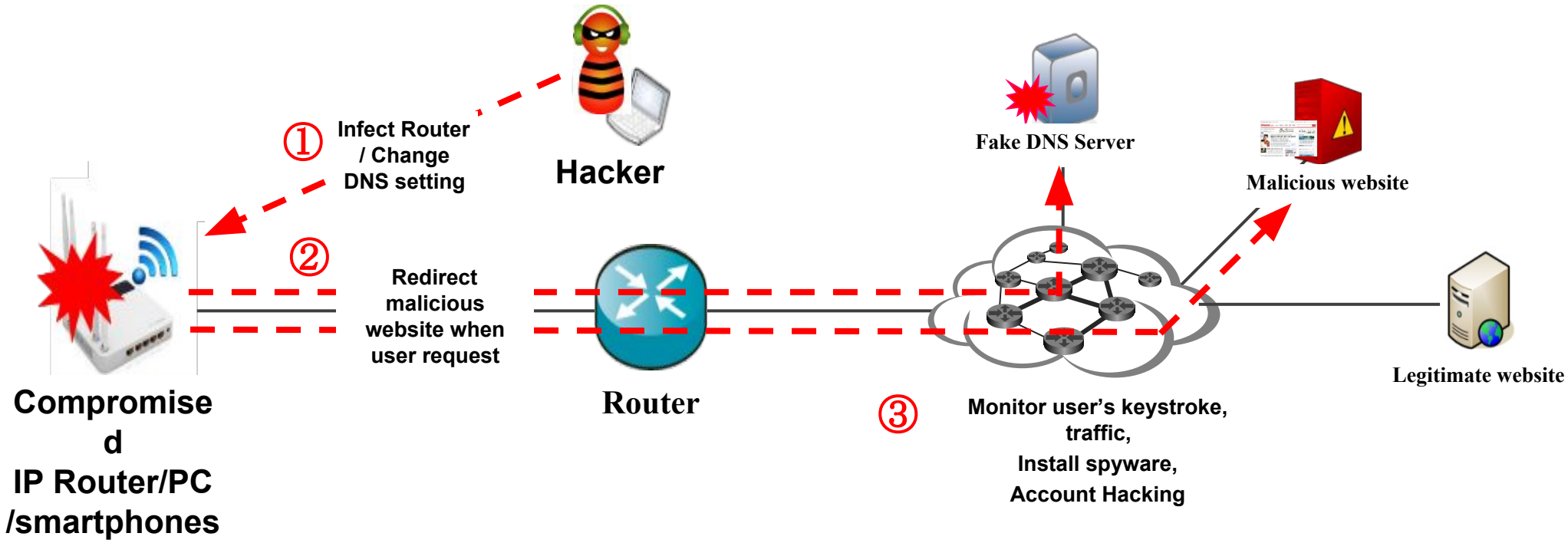
Use Case :
DNS Hijacking Defense

.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.

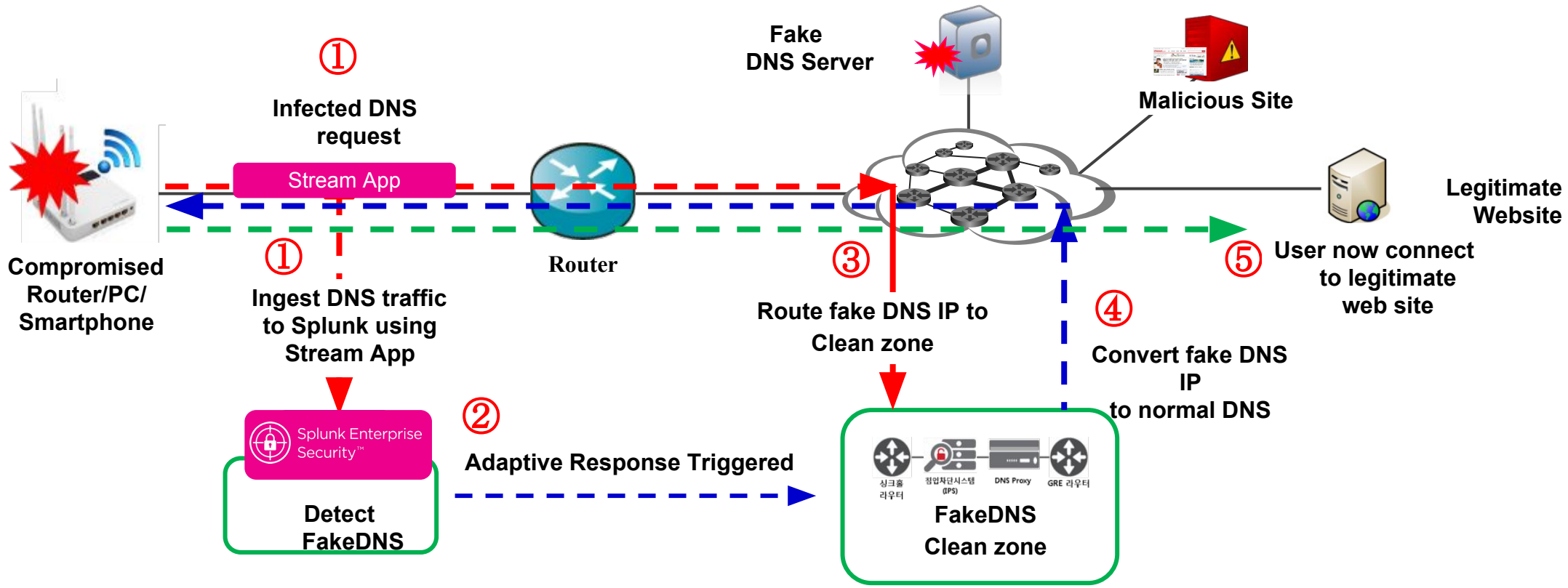


SK Broadband provides the secure protection for this attack as a part of free-of-charge service

Ref: https://www.cactusvpn.com/beginners-guide-online-security/dns-hijacking/

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

splunk> .conf19

Detecting Home Router DNS hijacking

- Correlation Search

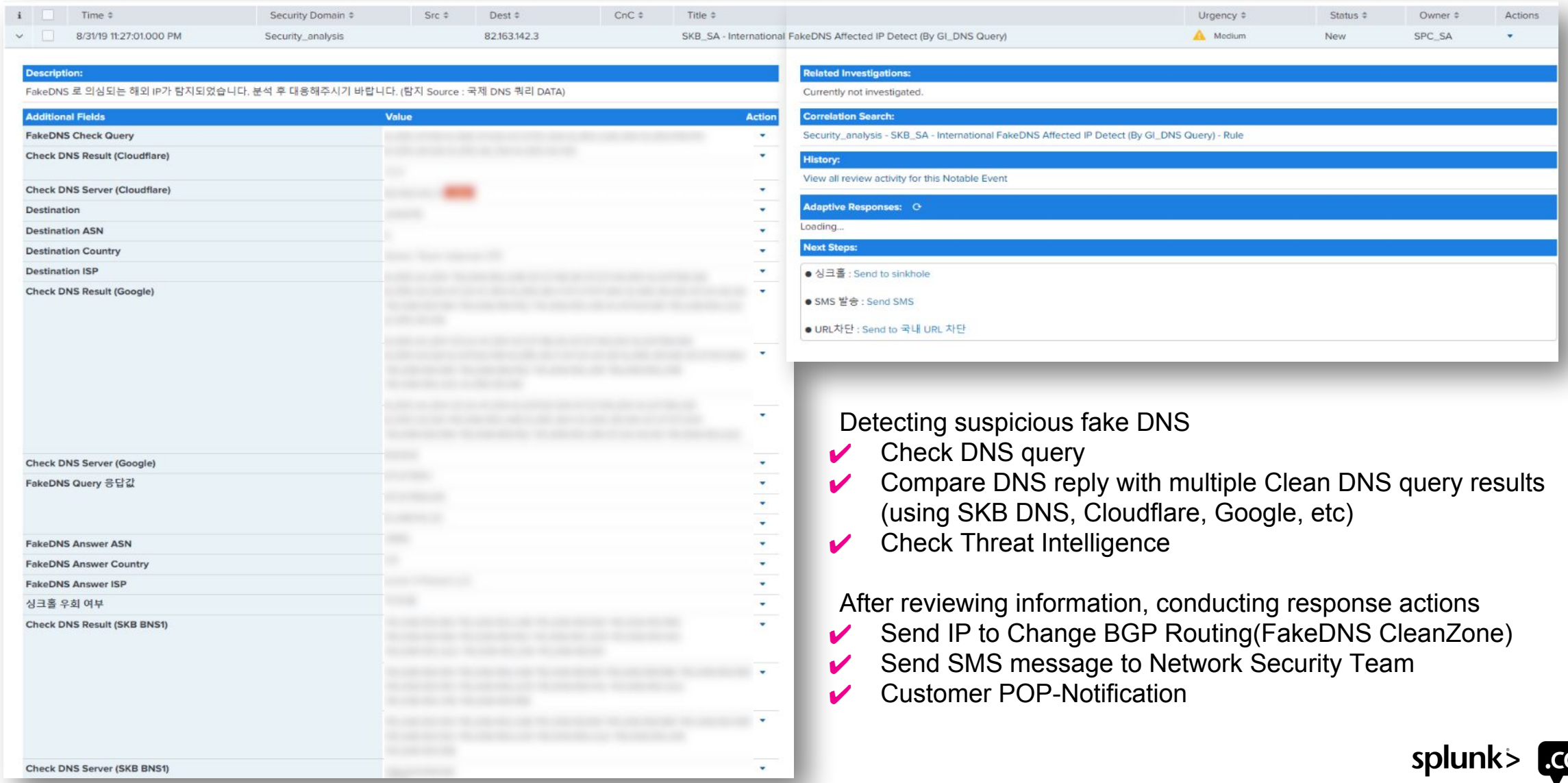
```
| tstats `summariesonly` values(DNS.answer) as answer count from datamodel=Network_Resolution.DNS WHERE sourcetype=stream:dns
  index=gi_dns DNS.message_type=RESPONSE DNS.reply_code_id=0 `removequery` `removequery_fakedns` DNS.record_type="A"
  [| inputlookup fakedns_detect_domain.csv
  | rename domain as DNS.query
  | table DNS.query]
```

```
| where match(query,"^(?!\-)(?:[a-zA-Z\d\-]{0,62}[a-zA-Z\d]\.){1,126}(?!\d+)[a-zA-Z\d]{1,63}$")
| rename answer as request_answer
| mvexpand request_answer
| where match(request_answer,"\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}")
| `skb_iplocation(request_answer, request_answer)`
| `skb_lookup(dest,dest)`
| where isnull(dest_domain)
```

```
| lookup dns_whitelist dns_ip as request_answer OUTPUT dns_ip_ASN as request_answer_dns_ip_ASN
| where isnull(request_answer_dns_ip_ASN)
| `sinkhole_check(dest)`
| `fakedns_lookup(query,request_answer)`
| `threatintel_multilookup(dest)`
| `threatintel_multilookup(request_answer)`
| rename query as check_domain
```

Home Router DNS hijacking Defense

Adaptive Response



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

splunk> .conf19

Home Router DNS hijacking Defense

Response Home Router DNS hijacking

- Adaptive Response

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

Custom ES correlation searches

250+ Correlation Searches to defense latest ISP Security Threats

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

.conf19

splunk>

Splunk ES customizations

Integrating SOC workflow into Splunk ES

SOC Workflow into Notable Event Framework

Flexible Bulletin Boards for Everyone

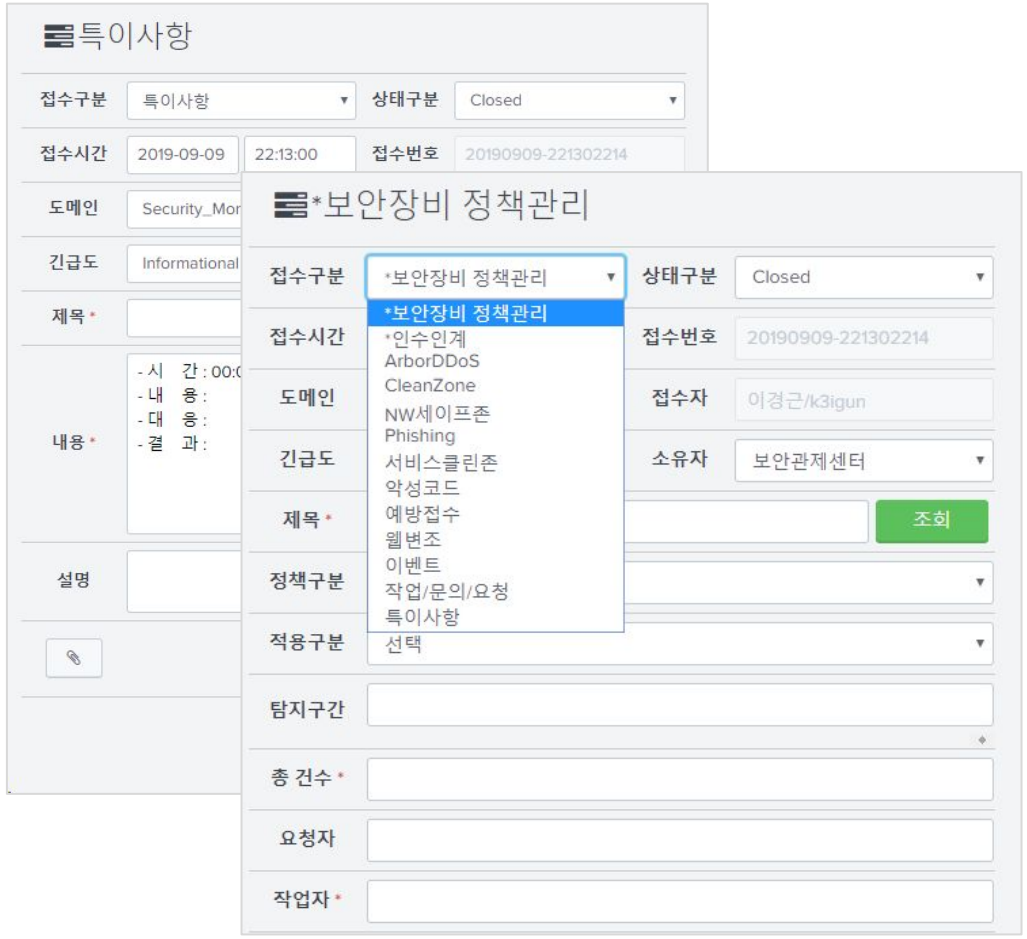
SOC Report Automation

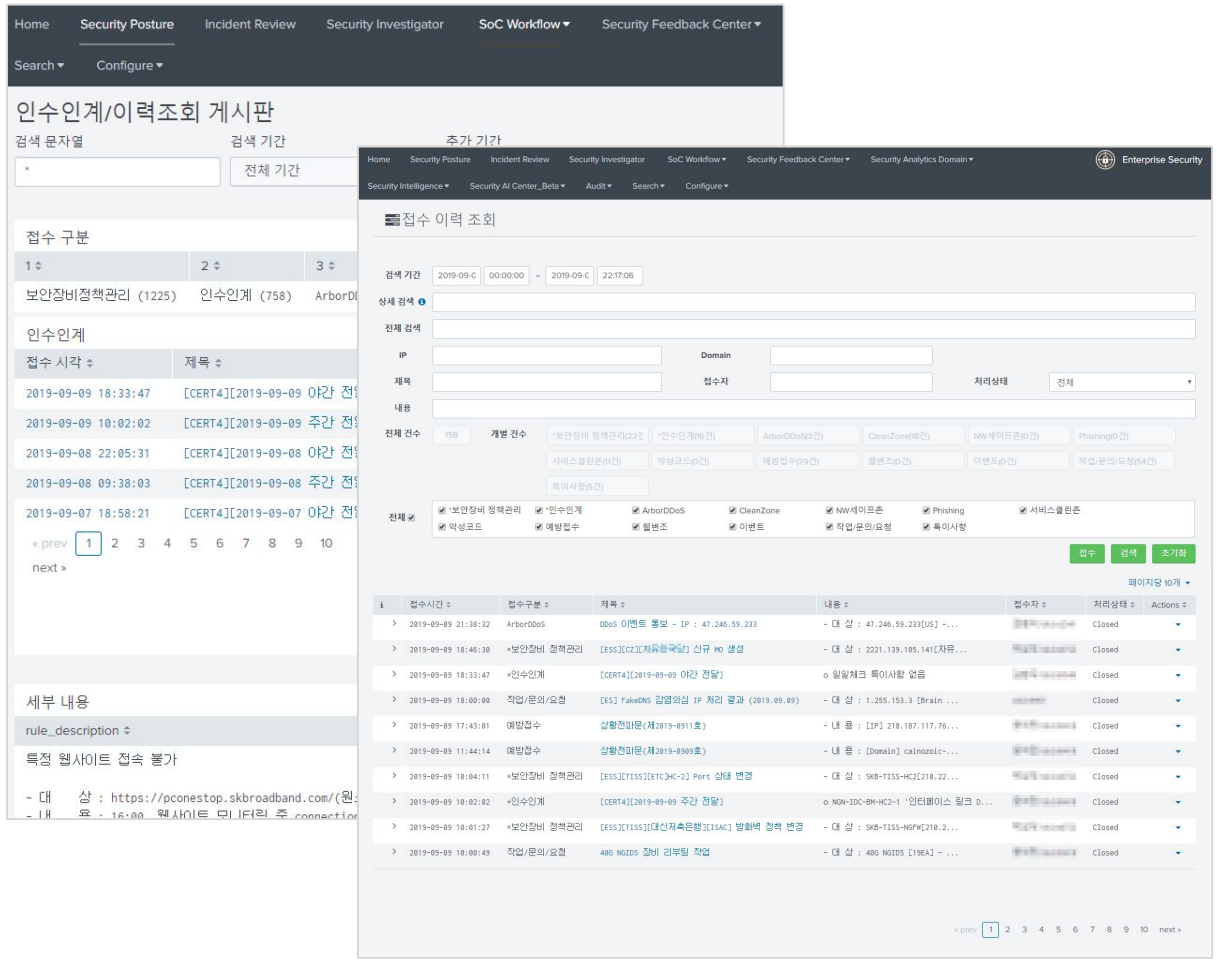
Team Transformation

SK broadband BRAIN Big-data Research Analysis In Network

SOC Workflow Into Notable Framework

Integrating daily SOC workflow into single Notable Event Framework





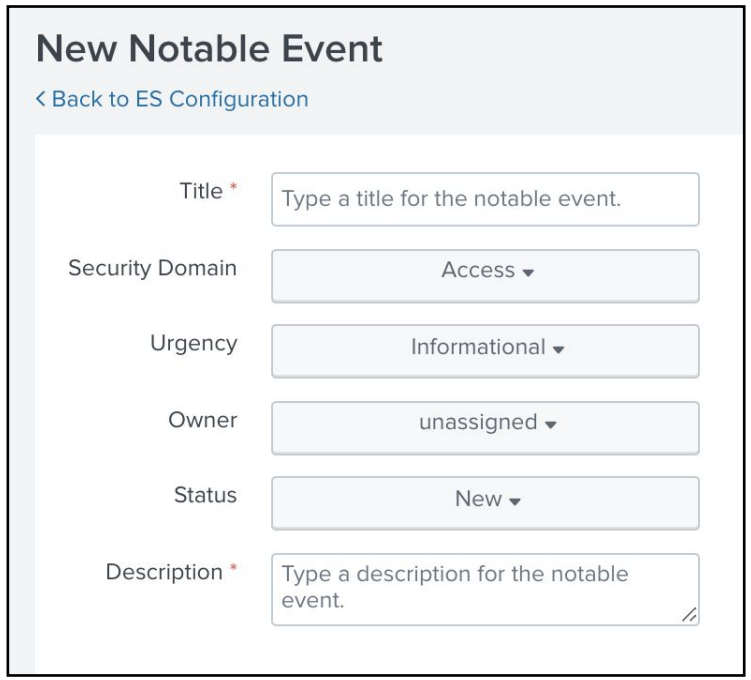
Integrating siloed SOC workflow systems into single framework □ Efficiency ↑

splunk> .conf19

Customized ES Notable Event Creation

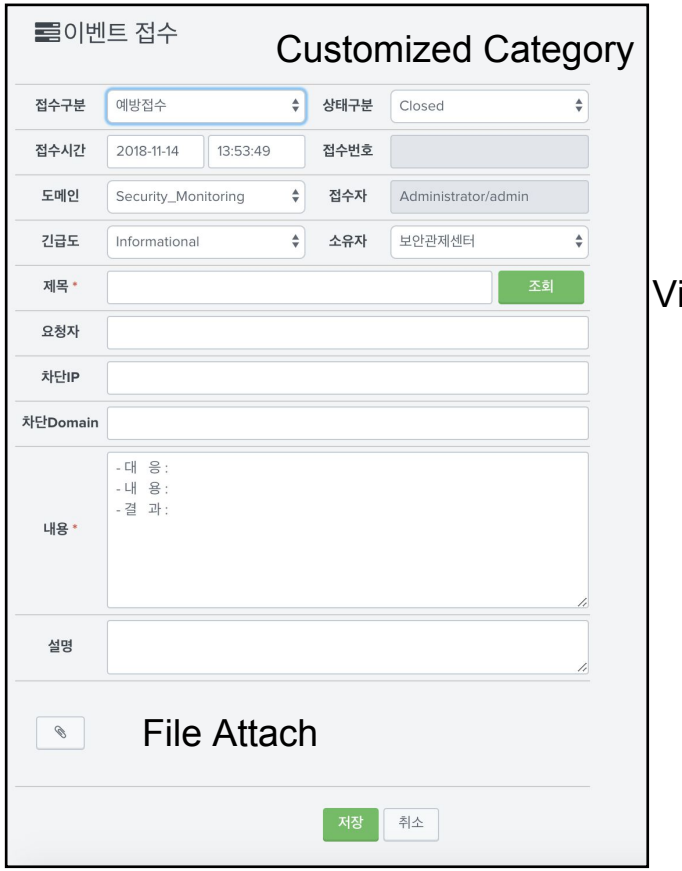
Customized ES Notable Event

- Splunk ES Notable Event Creation



customization

- Customized “BrainNotable” Event Creation

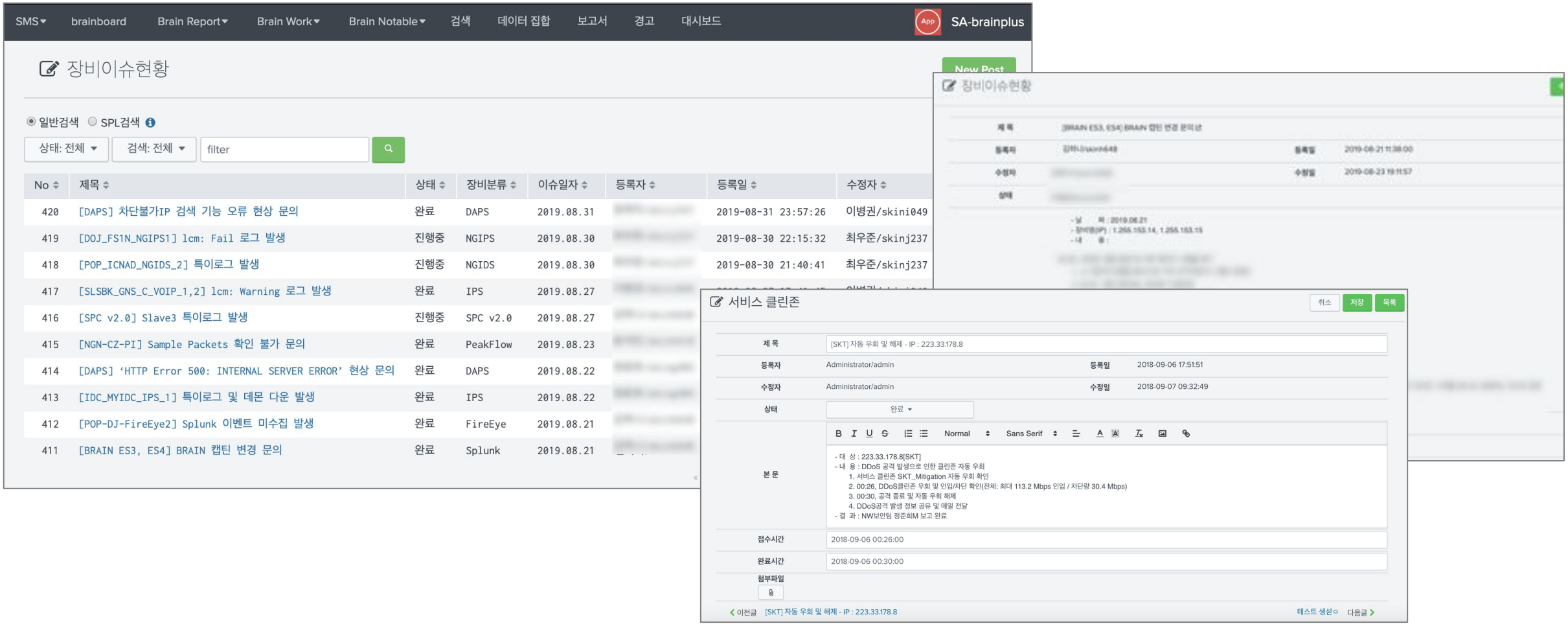


View ACL History

splunk> .conf19

Brain Board (SOC Bulletin Board)

Increasing SOC efficiency with Information Sharing & Tracking



Flexible Bulletin boards for Everyone – Work Efficiency + Sharing Culture

splunk> .conf19

Brain Board (SOC Bulletin Board)

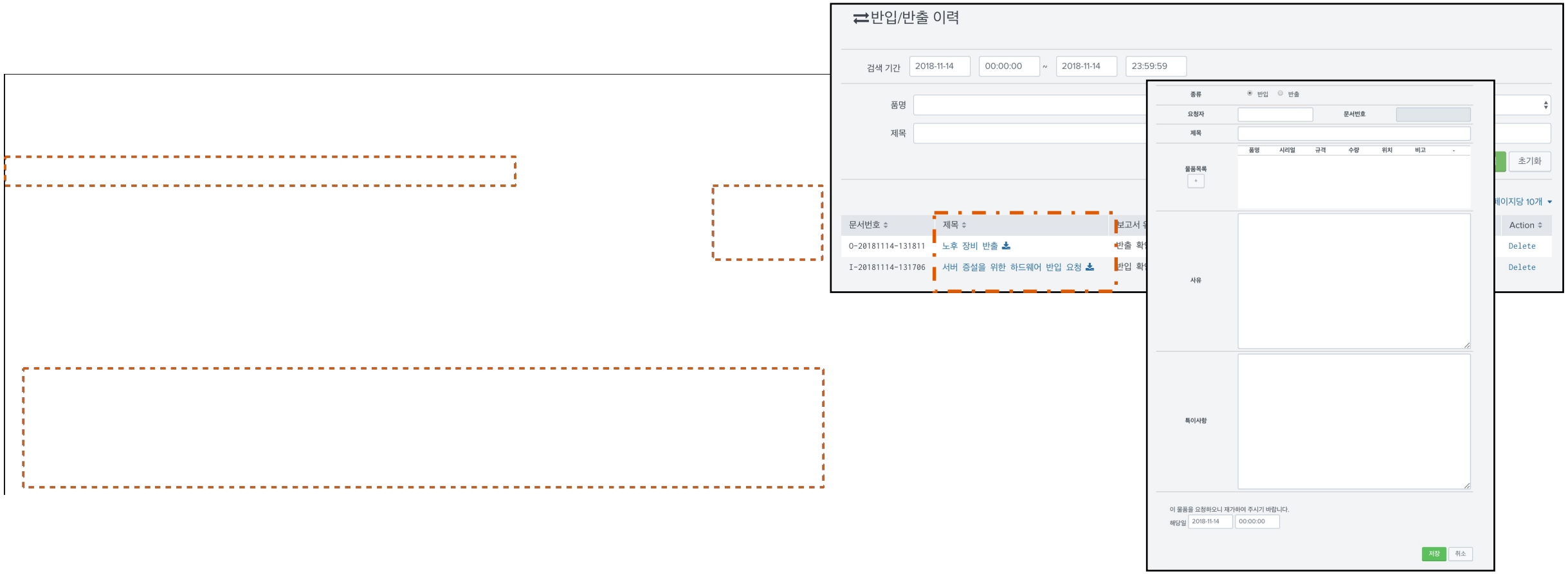
Everything is SPL based

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

Notable Events View

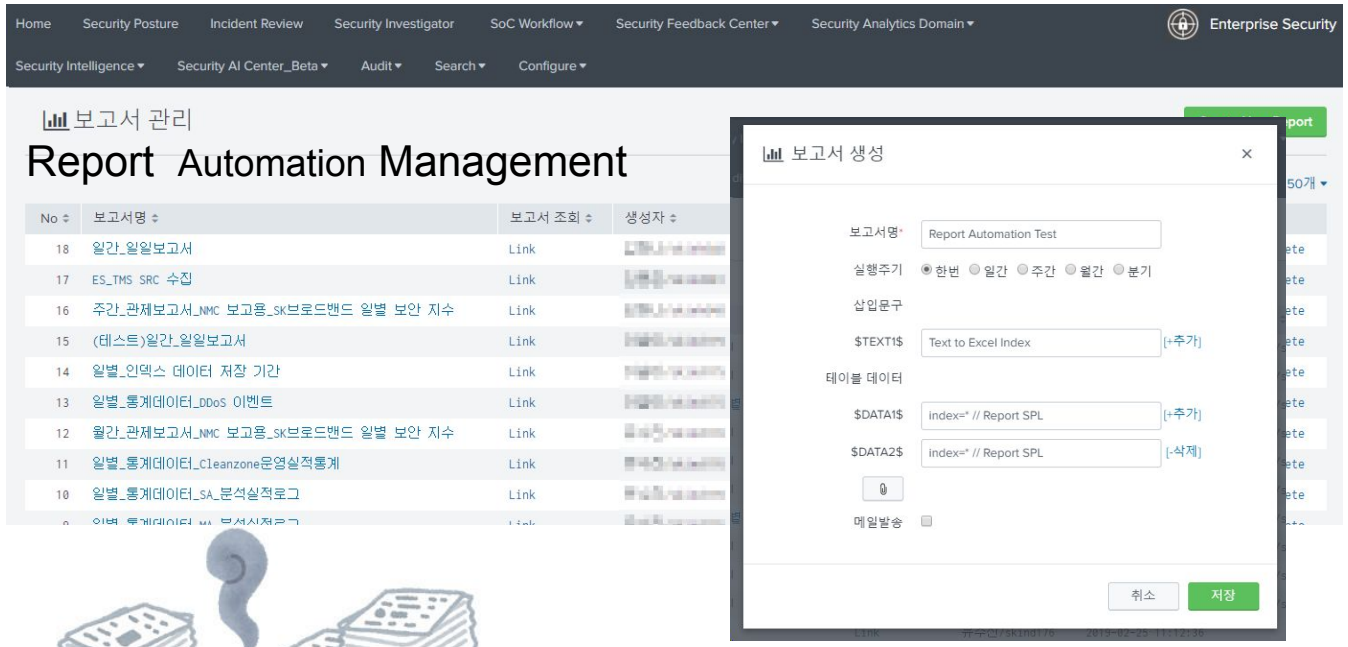
Customized UI & SMS/Email Notification

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

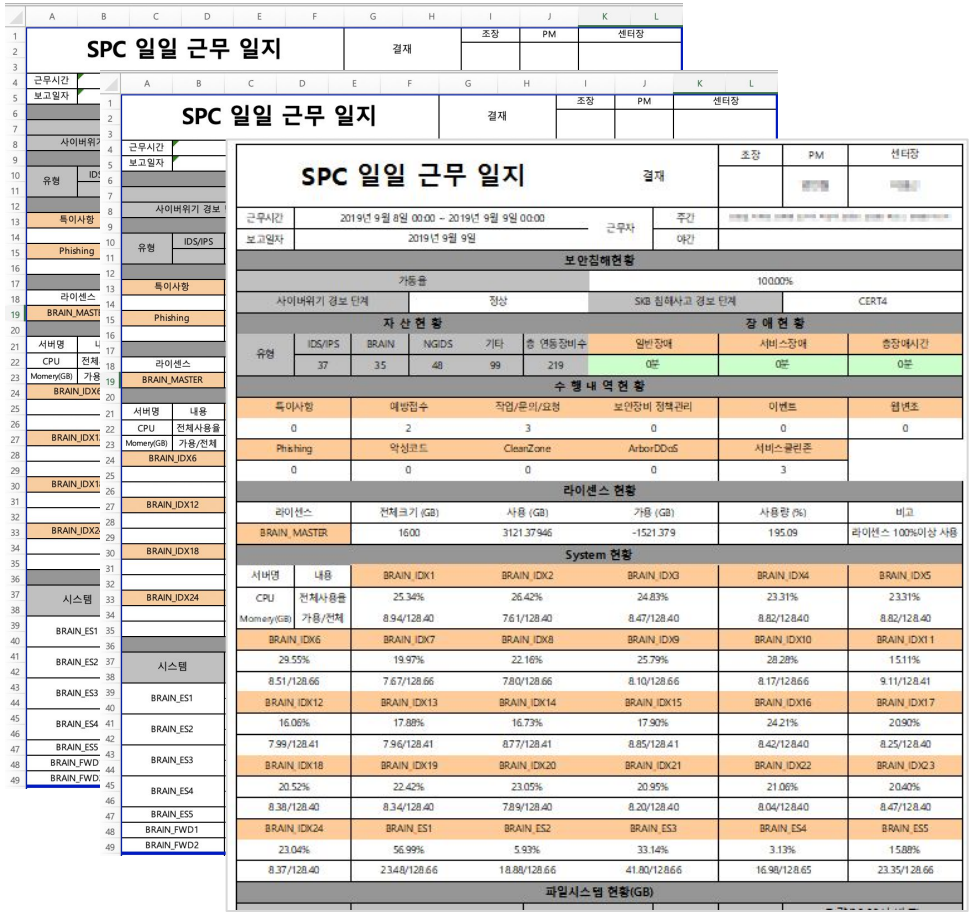


SOC Report Automation

Significantly reduce time to create daily/weekly/monthly reports



Saved Search returns
SPL results → Excel cells with macro



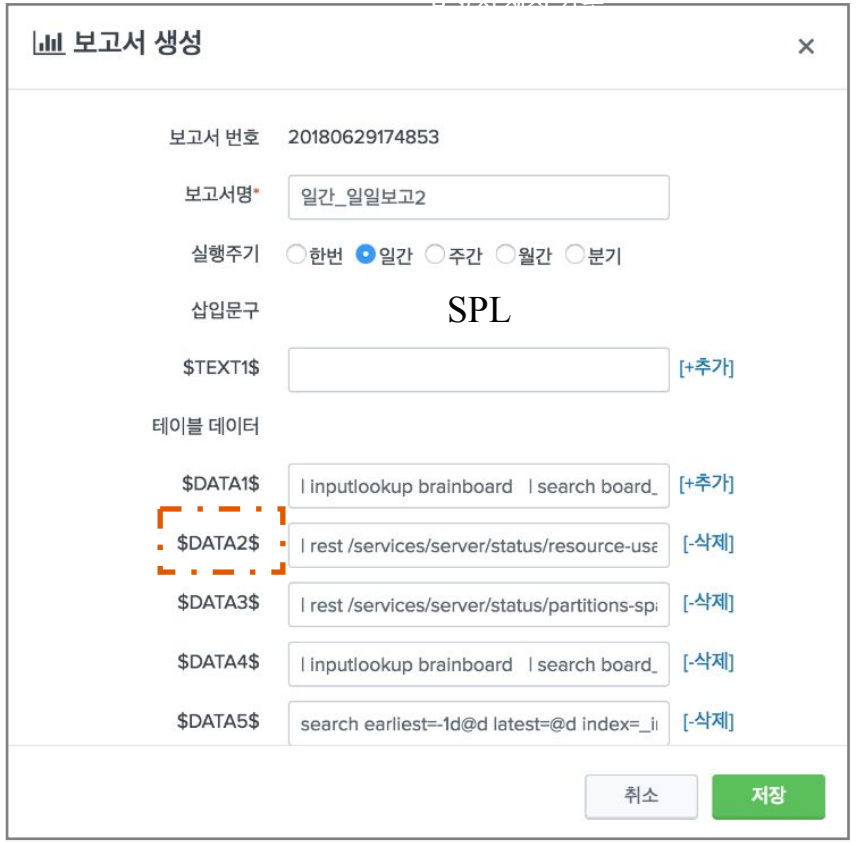
2+ Hour / day → 1 min

splunk> .conf19

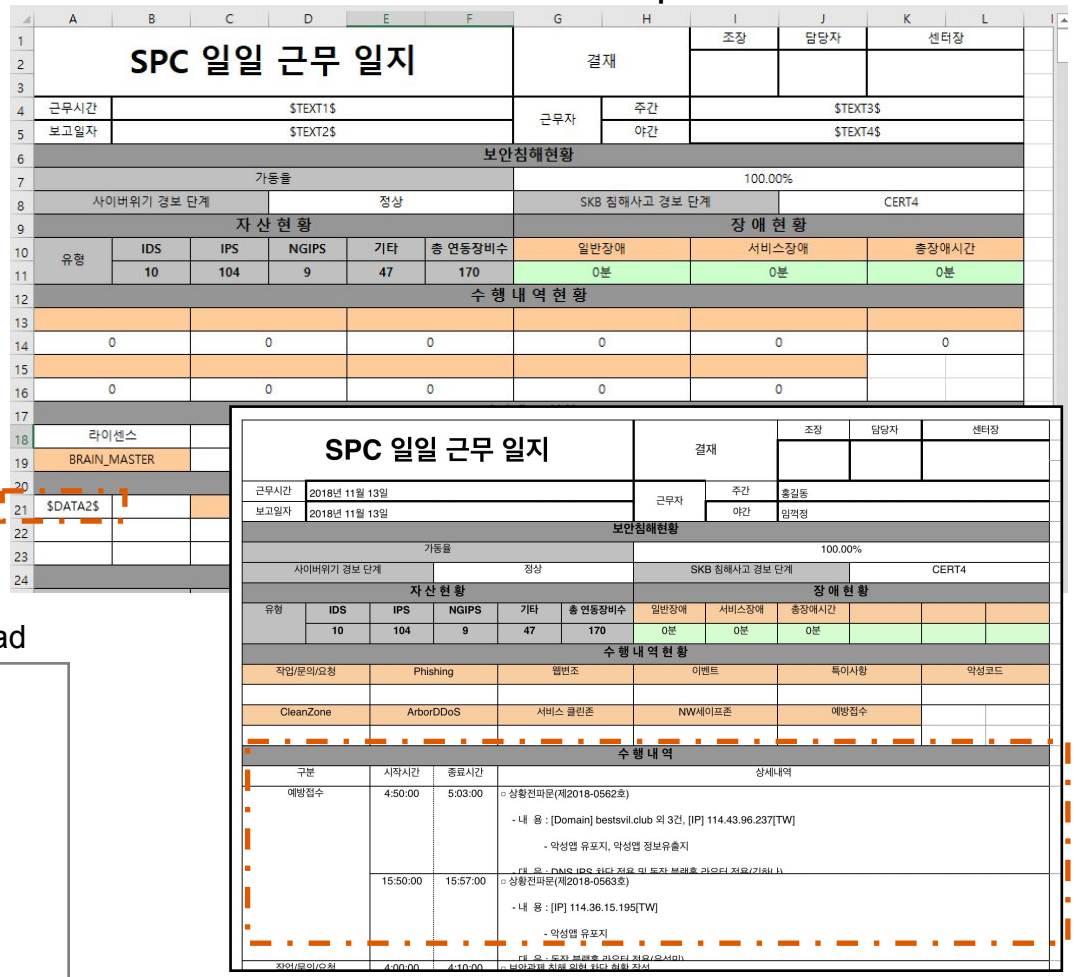
SOC Report Automation

Everything is SPL based

- SPL results into Excel Template



Excel Template

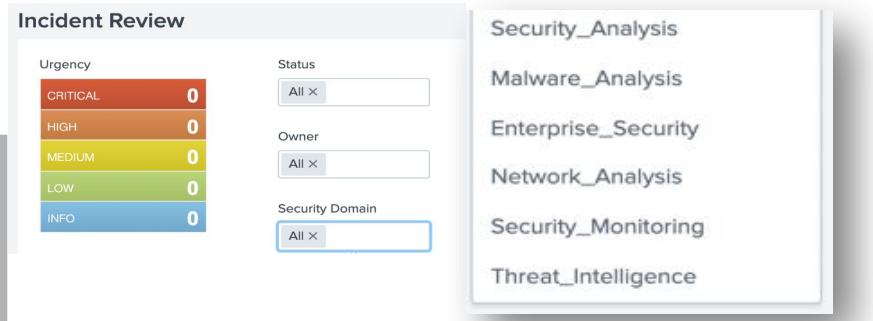


Template Upload

Reorganize roles with customized domain

Team Transformation with Splunk ES

Custom Domains



SK Broadband Network SOC

Operation | Monitoring | Analysis

SK Broadband Network SOC

Security Analysis Module | Malware Analysis Module | B2B Sec. Service Module | Security Monitoring Module

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

splunk> .conf19

4
Summary

.conf19
splunk>

Splunk@SK Broadband Today

Before & After Splunk

Daily Process Security Events

New Security Issues Investigation/Response Time

Daily Process Incidents

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 !

splunk>

Thank You!