How an ISP Uses Splunk Enterprise Security

To protect 24M subscribers from 100M attacks daily

Kyoung Geun Lee | SK Broadband

Seung Don Choi | Splunk

October 2018 | Version 1.0

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> .conf18

Our Speakers

KYOUNG GEUN LEE

SK Broadband
NW Security Team
Security Tech Engineering
& SOC Operation

SEUNG DON CHOI

Splunk
Senior Sales Engineer

Where's ~~North~~ South Korea?

https://www.youtube.com/watch?v=-ugJZhL-cbc

Did You Know…?

- South Korea has the fastest average internet connection, 4x world avg
- 1Gbit/s connection – 142x world avg, 79x US avg

Update: Top 10 Average Internet Speeds Comparison - Q1 2017

Country	Q1 2017 Avg. Mbps	YoY Change
Global Average	7.2	15%
South Korea	28.6	-1.7%
Norway	23.5	10%
Sweden	22.5	9.2%
Hong Kong	21.9	10%
Switzerland	21.7	16%
Finland	20.5	15%
Singapore	20.3	24%
Japan	20.2	11%
Denmark	20.1	17%
United States	18.7	22%

https://en.wikipedia.org/wiki/Internet_in_South_Korea
https://www.fastmetrics.com/internet-connection-speed-by-country.php#top-10-comparison-2017

- 10Gbps plan will be released in 2H 2018

Subscription Plan (max. throughput)	Smart (100M)	Giga Lite (500M)	Giga (1G)	Giga Premium (2.5G)
No Contract	33	45	50	55
3 yr Contract	20	30	35	40

※ Subscription price per month in USD

https://www.netmanias.com/en/?m=view&id=reports&no=13836

SK Broadband

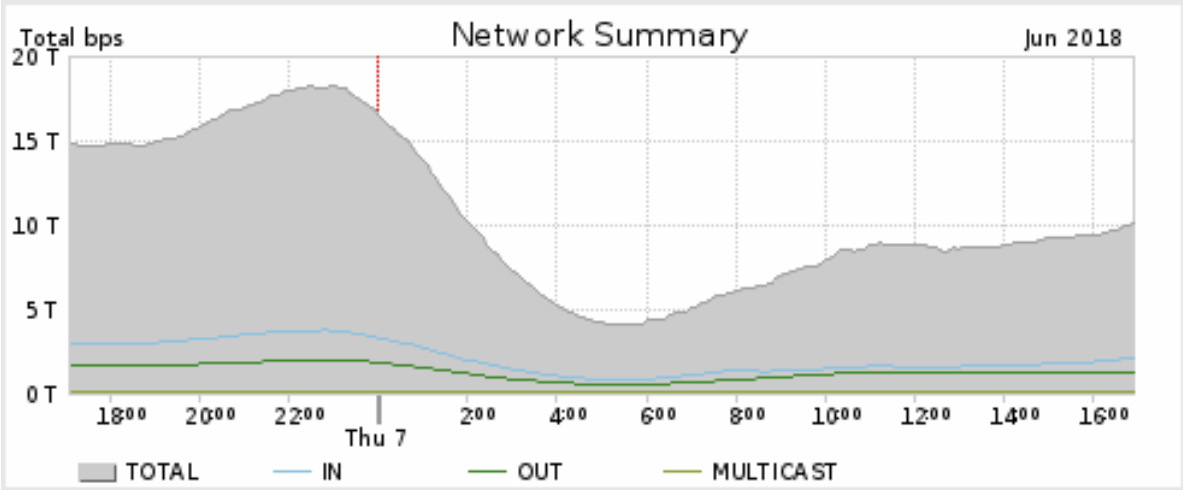
South Korean based Tier 1 ISP, Media Platform(IPTV) Service Provider

- Founded 1997, 2000 Employees
- World First commercialized ADSL service
- ISP, IPTV – total 14M subscribers
- Mobile IPTV (Oksusu) - 9M subscribers

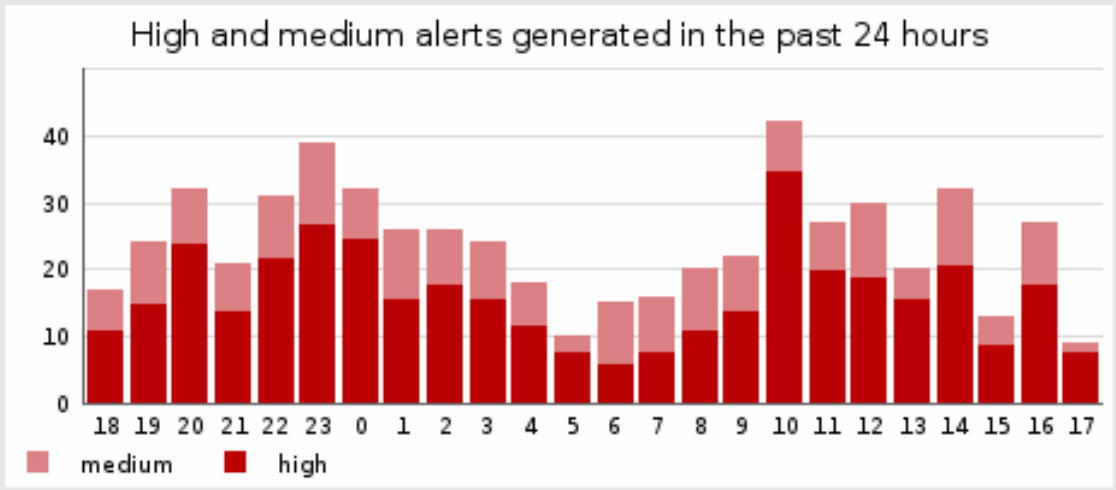
B tv B 전화 B 인터넷 B 인터넷전화 oksusu

Security Challenge on the ISP Network

More Traffic , More Threats



Current: **10.2 Tbps**
Max: **18.3 Tbps**
Average: **10.5 Tbps**
95th Percentile: **18.1 Tbps**



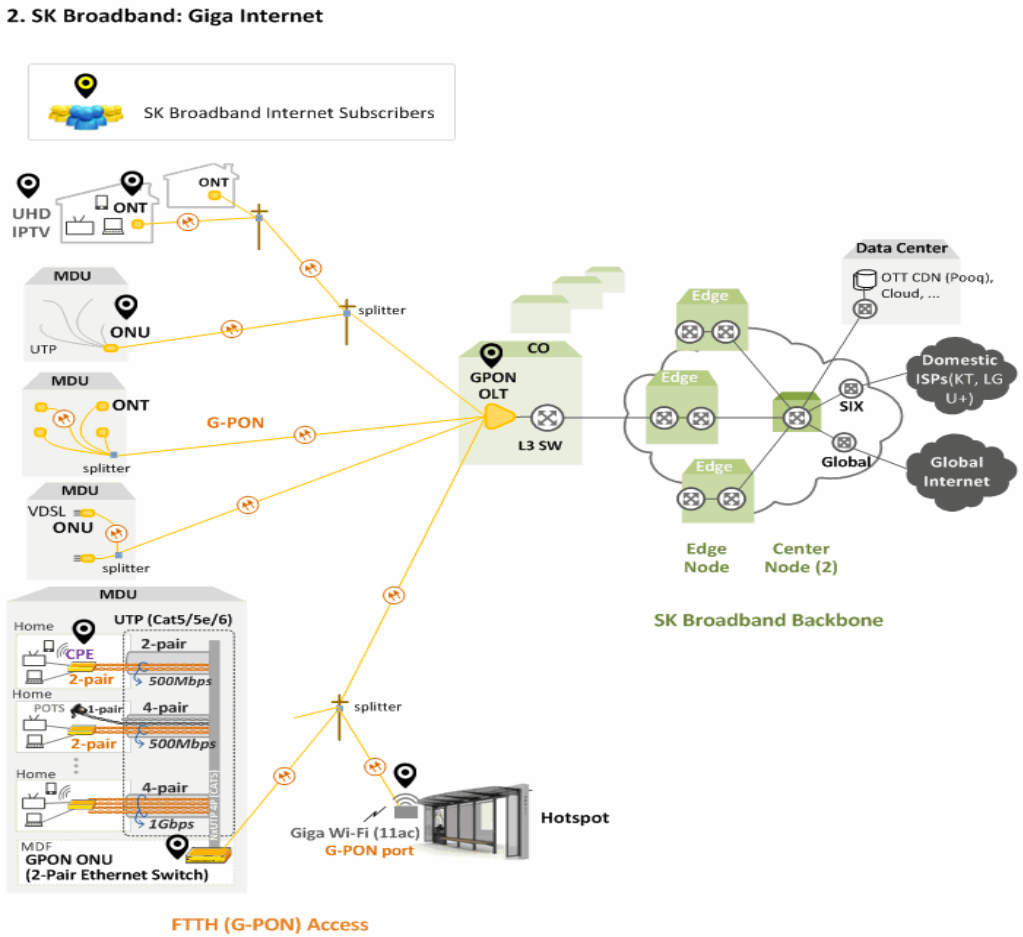
Number of all ongoing alerts: **11**
Current ongoing unclassified: **11**
100.0%
All Alerts created in past 24hrs: **573**
Change from previous 24hrs: **-7%**

- **220 PB** Daily , 18.3Tbps peak time
- More DDoS attack: 600~1,000 DDoS Attack Daily, **256Gbps** peak time this year
- DDoS, SCAN, Malware, Reflection Attack

splunk> .conf18

Security Challenge on the ISP Network

Vulnerability on your ICT devices



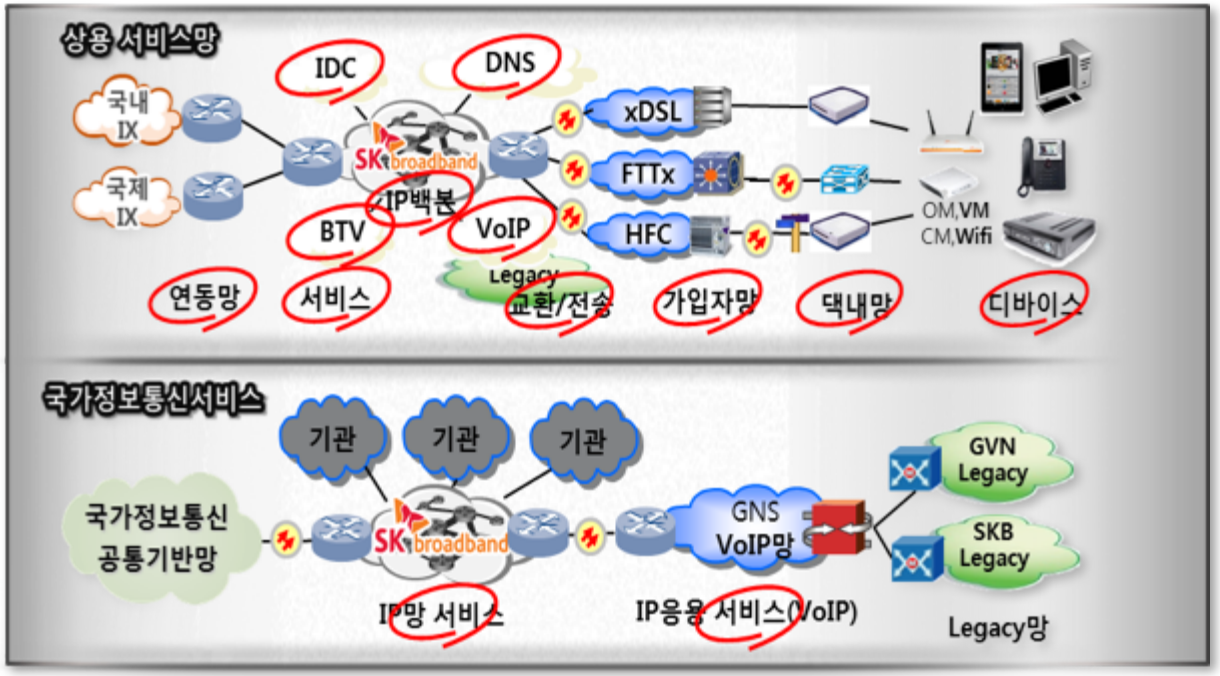
SK Broadband Network Topology

- Home router, ICT, IoT devices cause security leaks
- More advanced hacking technique
- New Type of Security Threat increased
  - Wannacry
  - Faked DNS
  - Busybox command injection(IoT)
  - Zeroday attacks
  - Advanced Malwares

…

Network Security Center

- N/W Security, Service Infra Security, B2B security(DDoS cleanzone)



Service Infra Security

Clean Network Pipe

splunk> .conf18


Complex Architecture
Massive Scale of Data Traffic
New Security Threats

SK Broadband Network Security Platform

Splunk Enterprise 7.1 + Enterprise Security 5.1 + SKB NW Security Framework

SK broadband BRAIN Big-data Research Analysis In Network

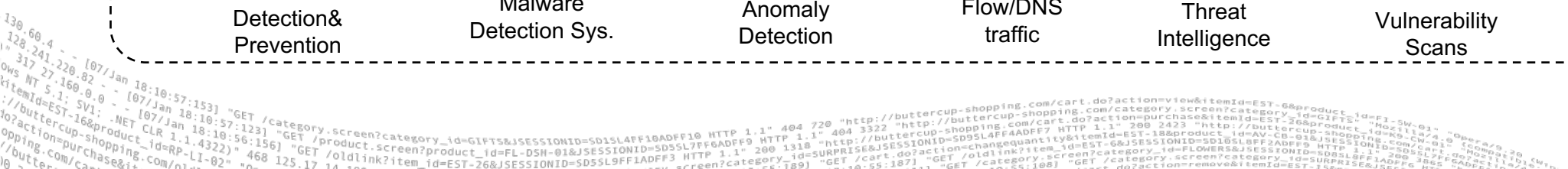
Scalable DataStore | Monitoring | Search & Analyze | Alert | Dashboards | Machine learning | Notable Events | Adaptive Response

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

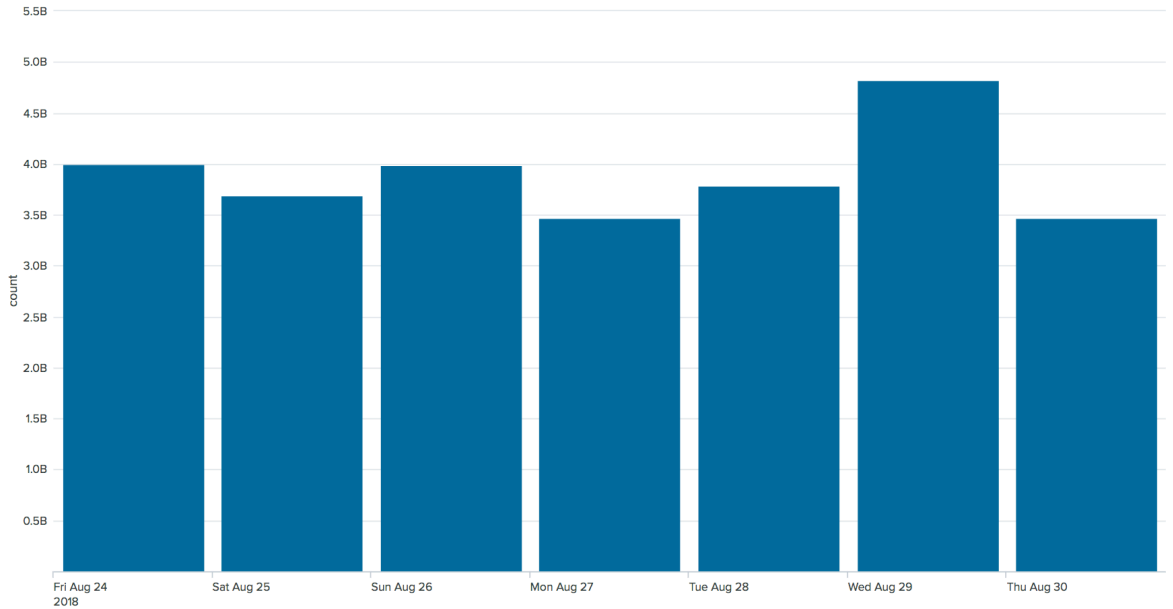


splunk> .conf18

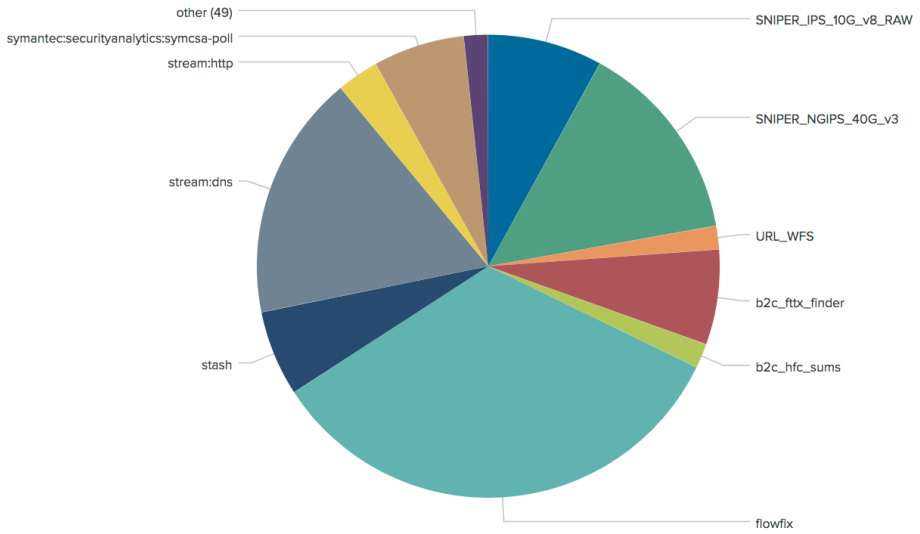
Data Sources

6B Events Per Day

- IDS / IPS, Malware
- DNS, Netflow, DHCP, stream
- Penetration test result/Vulnerability scan result
- SKBB Cyber Threat Intelligence
- Asset Information



# of events/Days

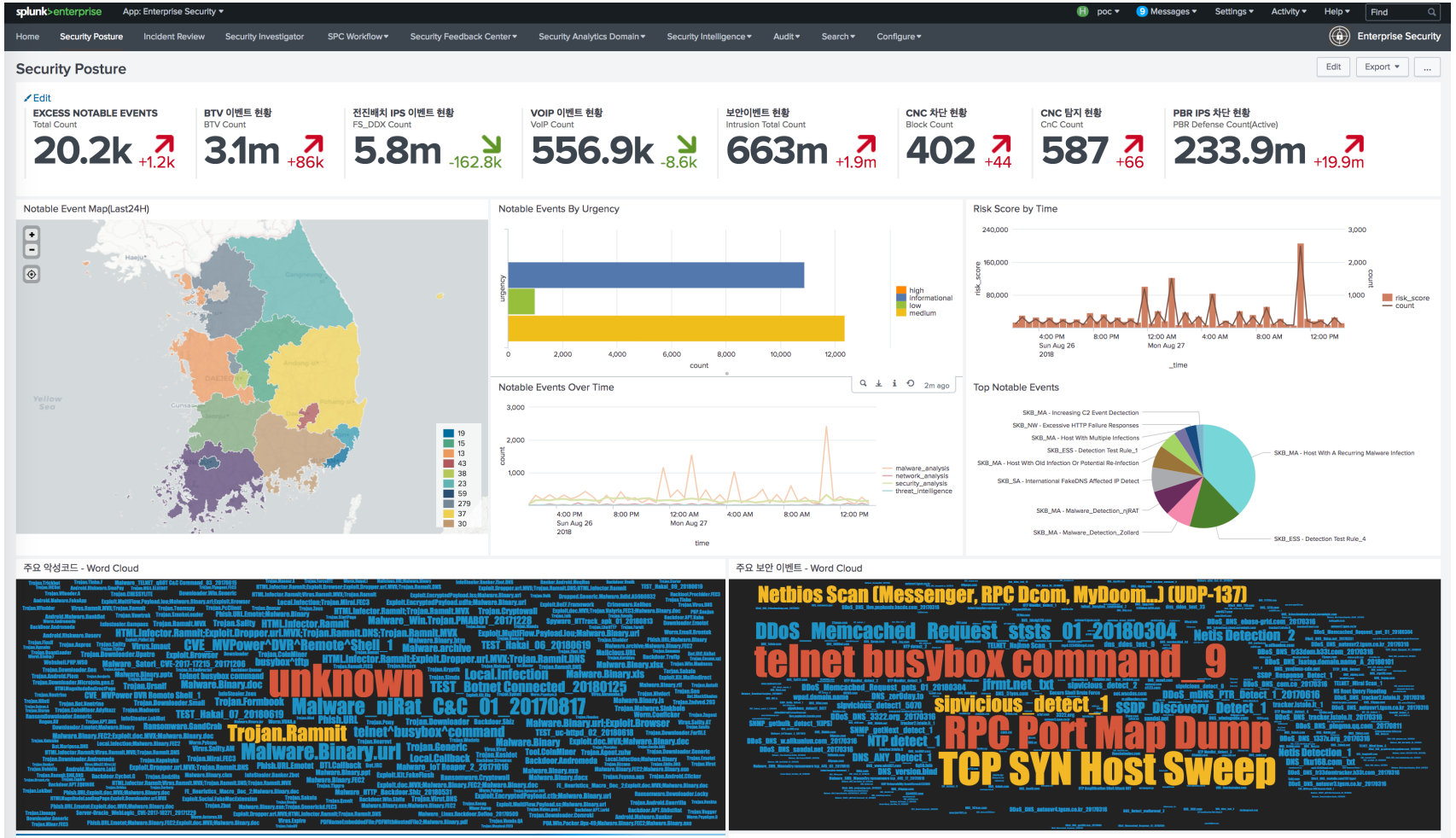


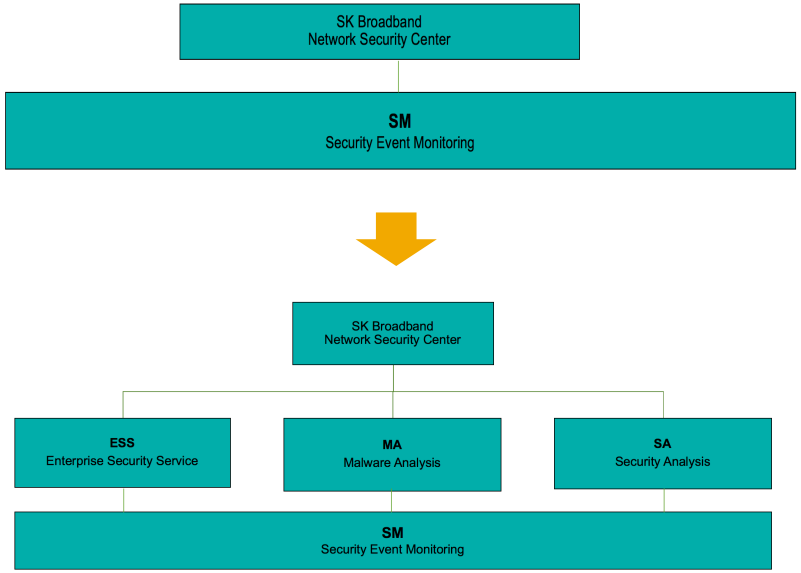
sourcetypes

splunk> .conf18

SKB Security Platform Security Posture

Team Transformation with Customized Domain



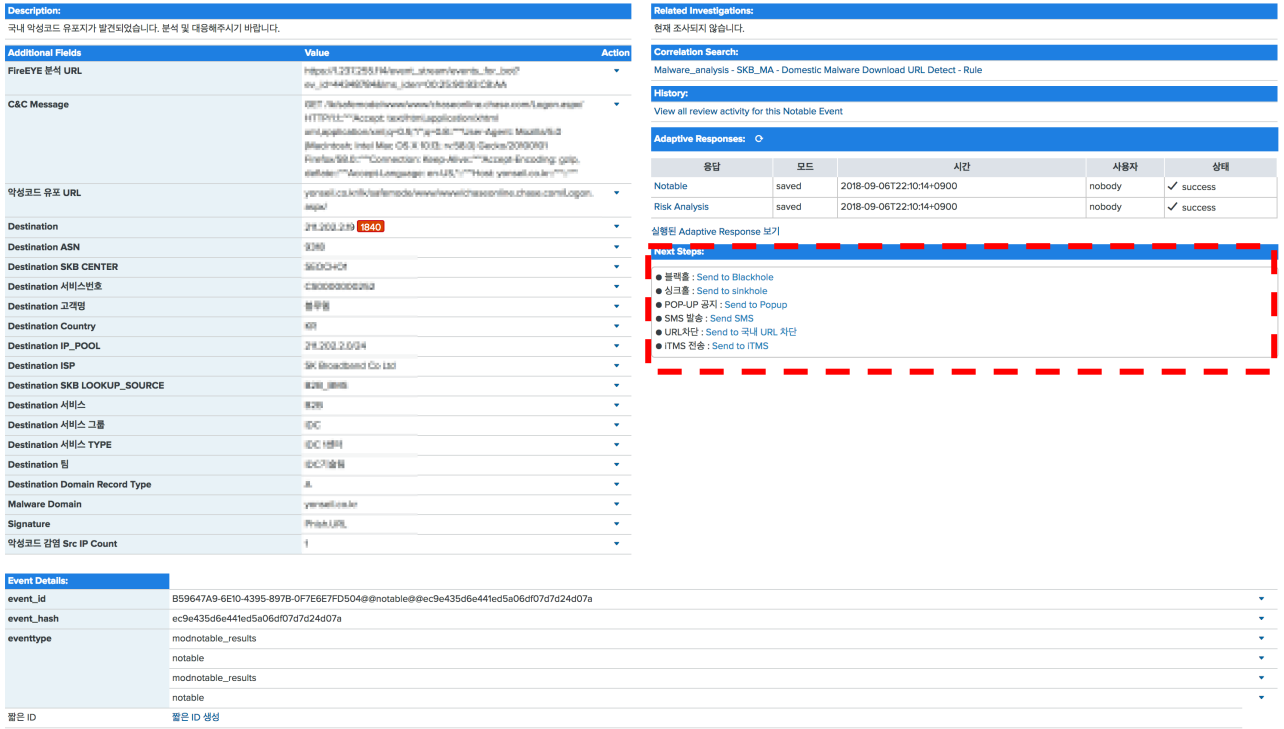


SoC Organization Structure

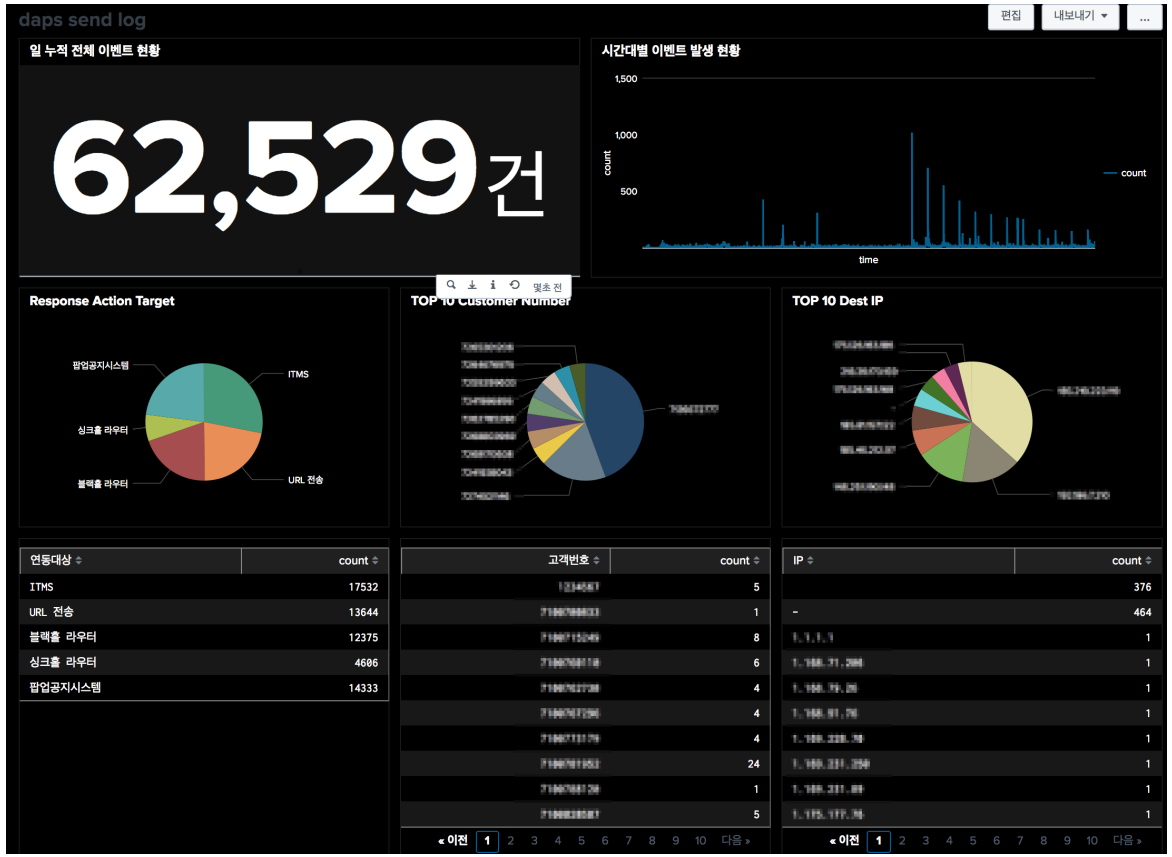
splunk> .conf18

Leverage Adaptive Response to Real Time Action

- Send suspicious IP to blackhole/ DNS sinkhole, URI block, send SMS, route message to call center/on-site engineers



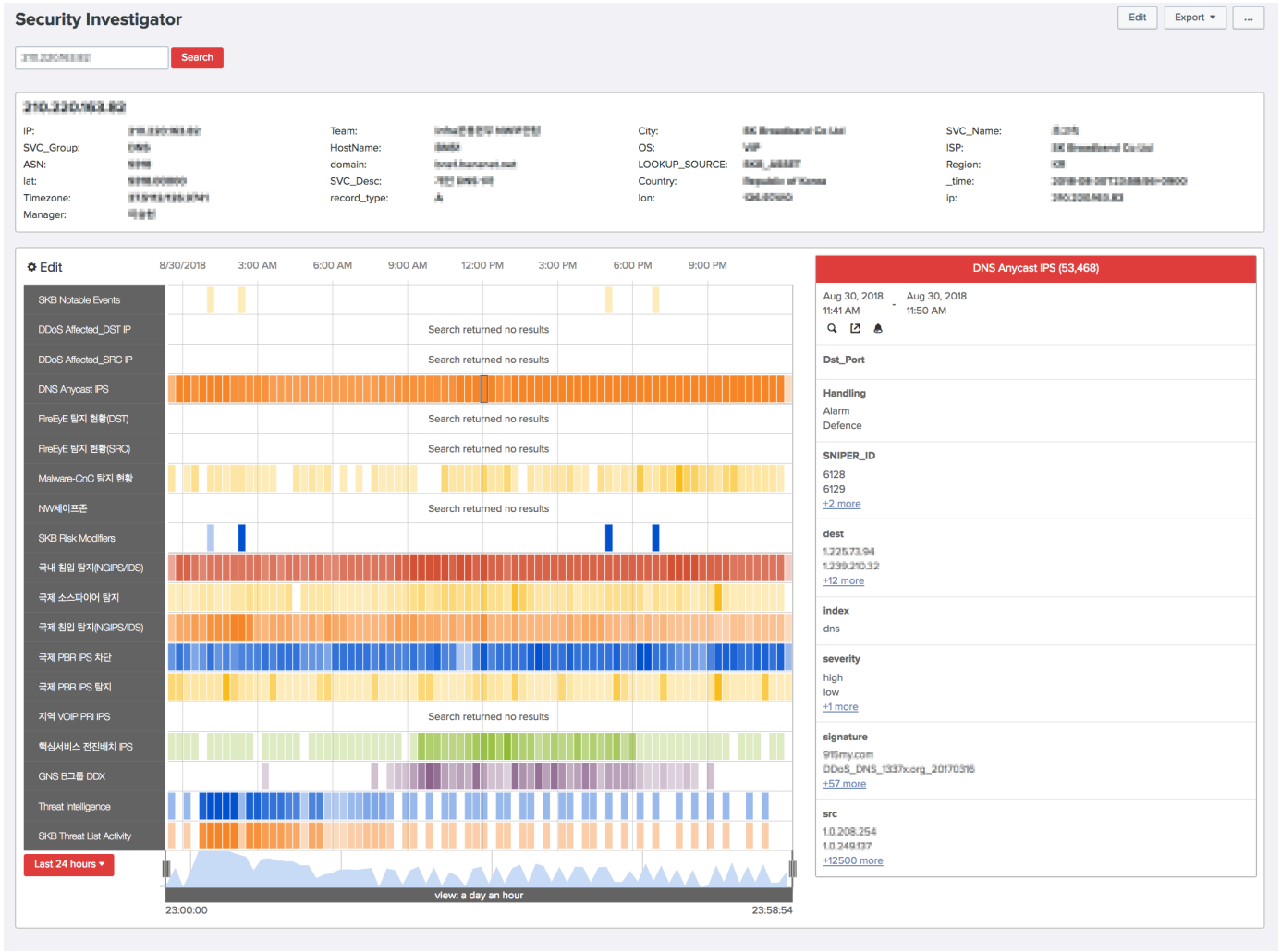
Notable Event

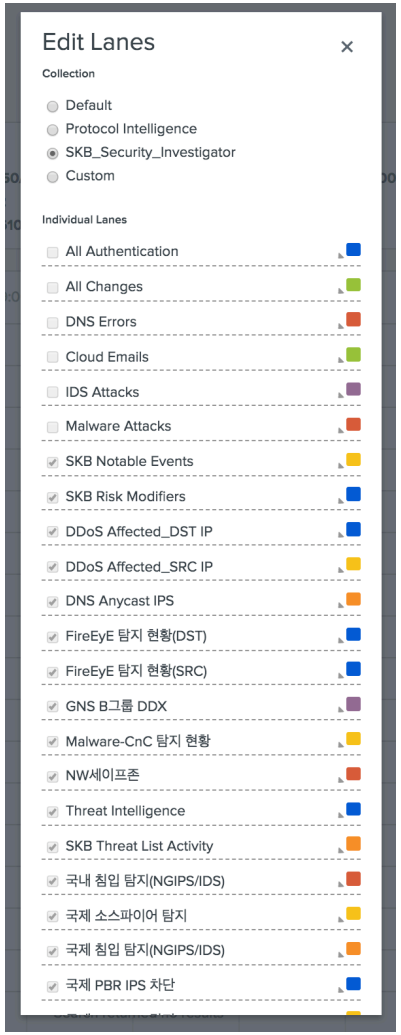


splunk> .conf18

Custom Swim Lane for Deeper Analysis

Increase End-to-End Visibility , Faster Resolution time





Threat Intelligence

SK Broadband SoC Workflow

SKBB SoC Analysts

Intrusion Detection& Prevention

Malware Detection Sys.

N/W Traffic Anomaly Detection

Flow/DNS traffic

Vulnerability Scans

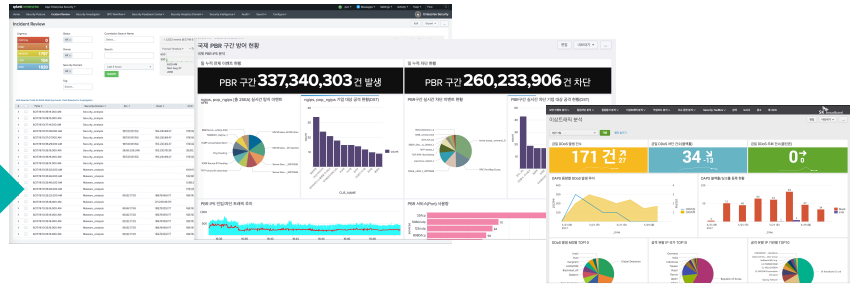
N/W Protection

Security Events

SK broadband Brain

Big-Data Reasearch Anaysis In Network

Notable Events



Security Analysis

\+

Cyber Threat Intelligence Service

1.8M

OF INDICATORS

Policy/Threat update

Threat Information update

splunk> .conf18

Bundle Size Matters

IPs in ISP are huge. So huge

- Large + High cardinality IP/DNS lookup can be problematic
- Search Head Cluster Issues
- Managing Bundle Size is important, pre-shipped threat/lookup gen searches can cause issues

Title: **Threat - Network Resolution Matches - Threat Gen**

Description: optional

Search:

```
1  | `tstats` values(sourcetype),values(DNS.src),values(DNS.dest) from datamodel
     =Network_Resolution.DNS by DNS.query,DNS.answer
2  | eval query='DNS.query'
3  | eval answer='DNS.answer'
4  | `tstats` append=true values(sourcetype) from datamodel=Domain_Analysis
     .All_Domains by All_Domains.domain,All_Domains.resolved_domain
5  | eval query=if(isnull(query),'All_Domains.domain',query)
6  | eval answer=if(isnull(answer),'All_Domains.resolved_domain',answer)
7  | stats values(sourcetype) as sourcetype,values(DNS.src) as src,values(DNS
     .dest) as dest by query,answer
8  | `threatintel_multilookup(query)`
9  | `threatintel_multilookup(answer)`
10 | search threat_collection_key=*
11 | `mvtruncate(src)`
12 | `mvtruncate(dest)`
13 | `zipexpand_threat_matches`
14 | table sourcetype,src,dest,query,answer,threat*,weight
```

Title: **SKB_Threat - Network Resolution Matches - Threat Gen**

Description: DNS Threat Gen

Search:

```
1  | `tstats` values(sourcetype),values(DNS.src),values(DNS.dest) from datamodel
     =Network_Resolution.DNS where sourcetype=stream:dns by DNS.query,DNS
     .answer
2  | eval query='DNS.query'
3  | eval answer='DNS.answer'
4  | `tstats` append=true values(sourcetype) from datamodel=Domain_Analysis
     .All_Domains by All_Domains.domain,All_Domains.resolved_domain
5  | eval query=if(isnull(query),'All_Domains.domain',query)
6  | eval answer=if(isnull(answer),'All_Domains.resolved_domain',answer)
7  | stats values(sourcetype) as sourcetype,values(DNS.src) as src,values(DNS
     .dest) as dest by query,answer
8  | `threatintel_multilookup(query)`
9  | `threatintel_multilookup(answer)`
10 | search threat_collection_key=*
11 | `zipexpand_threat_matches`
12 | mvexpand src
13 | mvexpand dest
14 | eval autofocus_id=if(isnull(autofocus_id),"autofocus_null",autofocus_id)
15 | eval new_threat_dns_key=md5(src."|".query."|".answer."|"
     .threat_collection_key."|".autofocus_id)
16 | lookup skb_threat_dns_key skb_threat_dns_key as new_threat_dns_key
     OUTPUTNEW white
17 | eval white= if(isnull(white),"0","1")
18 | search white!="1"
19 | table sourcetype,src,dest,query,answer,threat*,weight,new_threat_dns_key,
     autofocus_*, confidence, share_level, *_seen, type
20 | eval white="1"
21 | rename new_threat_dns_key as skb_threat_dns_key
22 | outputlookup append=t skb_threat_dns_key
```

Customize Your mmdb

- Rebuild MaxMind mmdb column to add more context for lookup/iplocation

```
1 index=netflow
2 | head 10
3 | `skb_iplocation(dest)`
4 | table ASN  Country City ISP Region lat lon Timezone
```

Last 24 hours

✓ 10 events (9/5/18 9:00:00.000 PM to 9/6/18 9:30:05.000 PM) No Event Sampling Job Fast Mode

Events Patterns Statistics (10) Visualization

100 Per Page Format Preview

ASN	Country	City	ISP	Region	lat	lon	Timezone
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	126.97830	37.5985/126.9783
10066	Republic of Korea	CJ Hello Co. Ltd.	CJ Hello Co. Ltd.	KR	10066.00000	126.97410	37.5112/126.9741
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	126.97410	37.5112/126.9741
45758	Thailand	Triple T Internet/Triple T Broadband	Triple T Internet/Triple T Broadband	TH	45758.00000	101.21470	14.2031/101.2147
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	126.97830	37.5985/126.9783
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	126.97410	37.5112/126.9741
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	127.25000	37.6000/127.2500
9318	Republic of Korea	SK Broadband Co Ltd	SK Broadband Co Ltd	KR	9318.00000	128.59110	35.8703/128.5911
38095	Republic of Korea	QRIXNETSDM-AS-	QRIXNETSDM-AS-	KR	38095.00000	126.97830	37.5985/126.9783
36351	United States	SoftLayer Technologies Inc.	SoftLayer Technologies Inc.	US	36351.00000	-97.82200	37.7510/-97.8220

Original Column	Modified Column	Example
City	ISP	SK Broadband co ltd
Country	Country	Republic of Korea
Region	Country Code	KR
Metrocode	ASN	9318
timezone	Lat/lon	37.5112/126.97410

skb_iplocation(1)	iplocation allfields=t ip | rename Continent as ISP MetroCode as ASN	ip
skb_iplocation(2)	iplocation allfields=t ip prefix=$source$_ | fields - $source$_Country $source$_City $source$_Timezone $source$_lat $source$_lonl rename $source$_Continent as $source$_ISP $source$_MetroCode as $source$_ASN $source$_Region as $source$_Country	ip,source

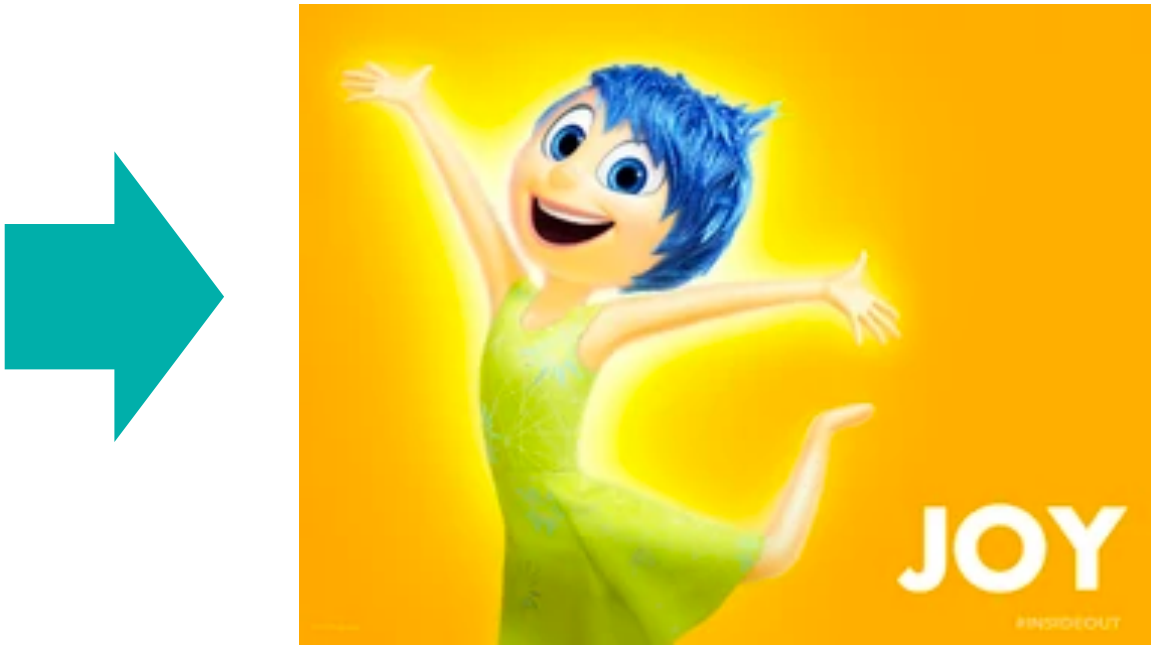
splunk> .conf18

Summary

Splunk@SK Broadband Today

Before & After Splunk

- Daily Process Security Event: **100M → 6B**
- New Security Issue Investigation/Response Time : **180 min → 5 min**
- Daily Process Incident : **500 → 15,000**
- Daily Defensed Attacks : **200M**



Splunk@SK Broadband Tomorrow

What's Next?

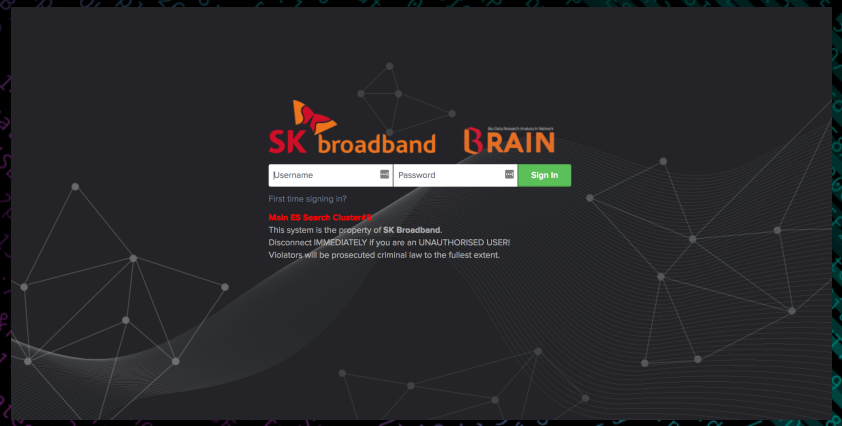
More Data!

Machine Learning!

Automation!

splunk> .conf18

Key Takeaways



1. Splunk Enterprise Security is very customizable and Extendable.
2. Leverage Adaptive Response, for real time action
3. You can use ES for ISP!

Thank You
감사합니다

Don't forget to rate this session in the .conf18 mobile app

splunk>