

# 디지털 네트워크 변화에 따른 보안 가시성 확보 전략

Jinhyun Lee (이진현)

Consulting Systems Engineer – Security APJC

Cisco Systems



# DIGITAL TRANSFORMATION

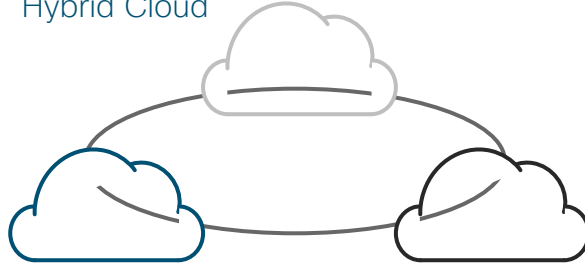
DEVICE  
IOT, BYOD, Mobility

Automation  
Software Defined

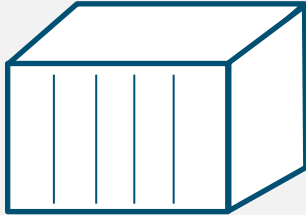
Intelligence  
Machine-Learning

# And.. Cloud!!

Hybrid Cloud



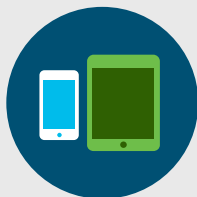
Container



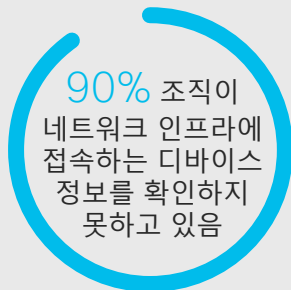
Micro Service



# 디지털 변화에 따른 보안 챌린지



Enterprise  
Mobility



Cloud

21B

2020년까지 증가할  
IOT 단말 수

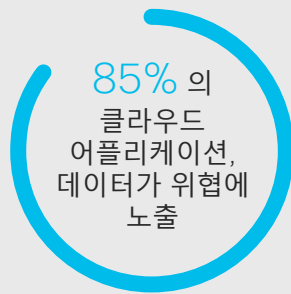


Encrypted  
Traffic

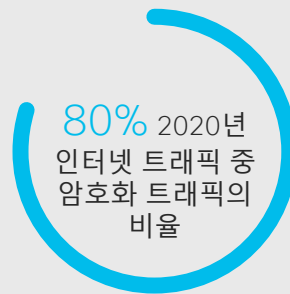
2/3

2020년 까지 총 IP  
트래픽에서 모바일 및  
무선 네트워크 단말이  
차지하는 비율

Acquisitions &  
Partnerships



Internet  
of Things



# 네트워크 보안 가시성의 요구



기존 보안 장비가 제공해 주지 못하는 전체적인 네트워크 통신 가시성이 필요합니다



멀웨어, 웜 발생 시 내부 전파 여부와 같은 영향도 확인과 검증이 어렵습니다



각각의 통신이 컴플라이언스를 준수하는 지에 대한 확인이 필요합니다



보안 이벤트 발생 시 인텔리전스를 활용한 조사 시간의 단축이 필요합니다



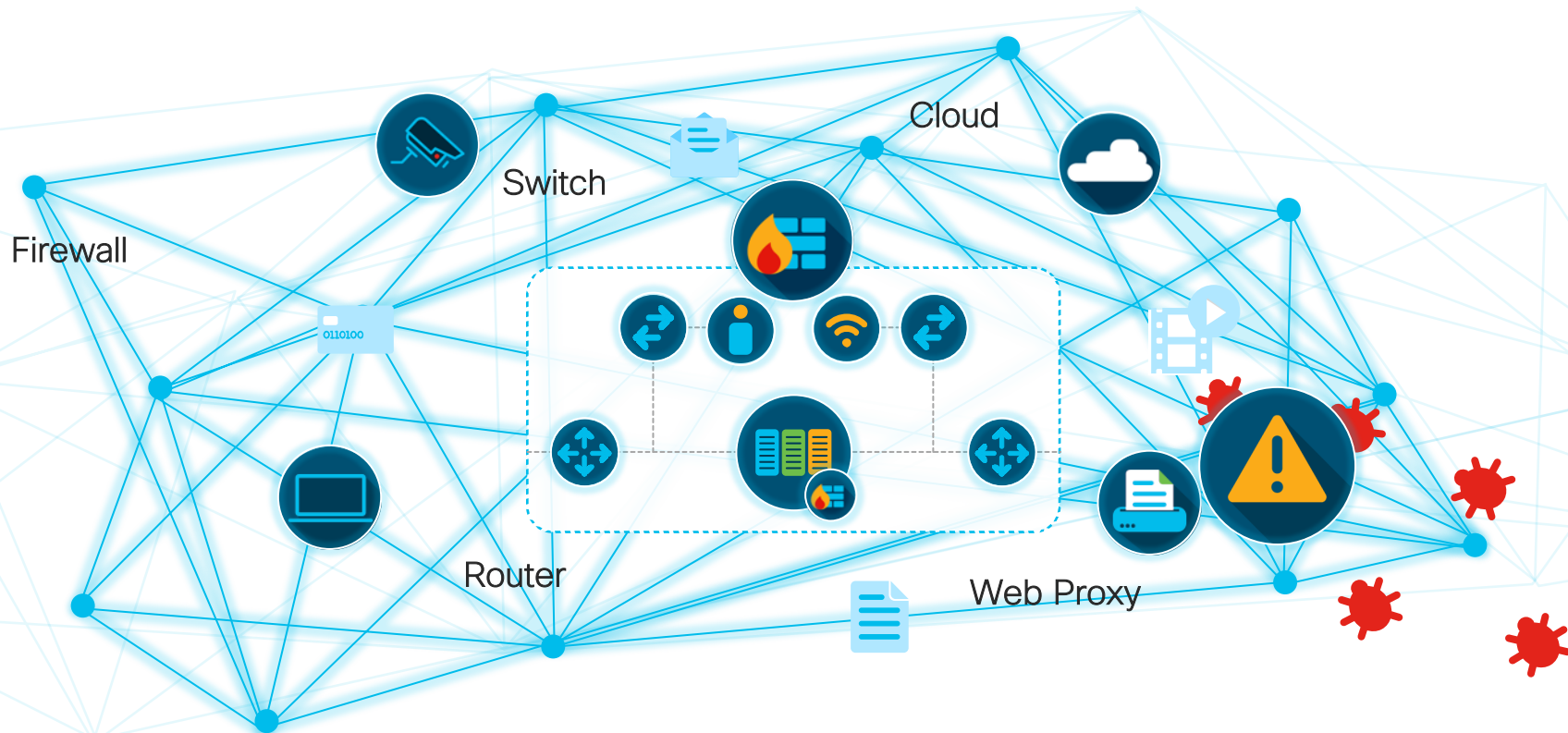
보안 이벤트 발생 시 개별 세션 단위의 히스토리 정보가 필요 합니다



멀티/하이브리드 클라우드와 컨테이너 환경에 대한 보안 가시성 확보를 대비해야 합니다

# 솔루션 : Network + Security

기존 인프라 장비들을 보안에 활용하다

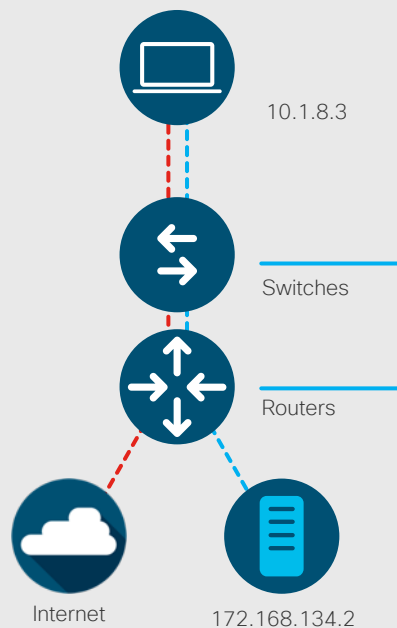


기존 인프라가 제공하는 기능을  
활용한 보안 가시성 확보

# 네트워크 장비를 센서로 - Netflow (라우터, 스위치, 방화벽)

## What it provides:

- 네트워크 상의 모든 통신 기록
- 네트워크 인프라 전체에 걸친 통신 레코드 정보 (Routers, Switches, Firewalls)
- 네트워크 통신 사용량 정보
- North-South 통신 뿐만 아니라 East-West 통신을 볼 수 있는 능력
- Switched Port Analyzer (SPAN) 데이터 대비 훨씬 가볍고 부하가 적으면서, 보다 폭넓은 전체 네트워크의 가시성 확보
- Indications of compromise (IOC)
- 보안 그룹 정보



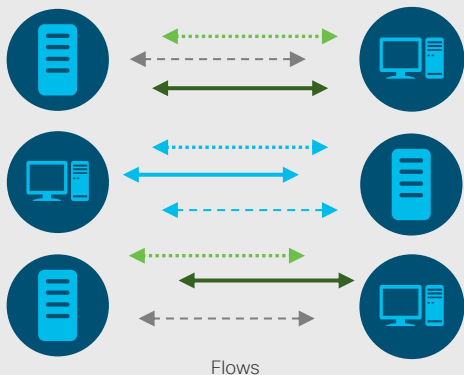
| Flow Information    | Packets          |
|---------------------|------------------|
| SOURCE ADDRESS      | 10.1.8.3         |
| DESTINATION ADDRESS | 172.168.134.2    |
| SOURCE PORT         | 47321            |
| DESTINATION PORT    | 443              |
| INTERFACE           | Gi0/0/0          |
| IP TOS              | 0x00             |
| IP PROTOCOL         | 6                |
| NEXT HOP            | 172.168.25.1     |
| TCP FLAGS           | 0x1A             |
| SOURCE SGT          | 100              |
| :                   | :                |
| APPLICATION NAME    | NBAR SECURE-HTTP |



# Netflow를 활용한 네트워크 행위 기반 분석 및 학습

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



Create a baseline of normal behavior

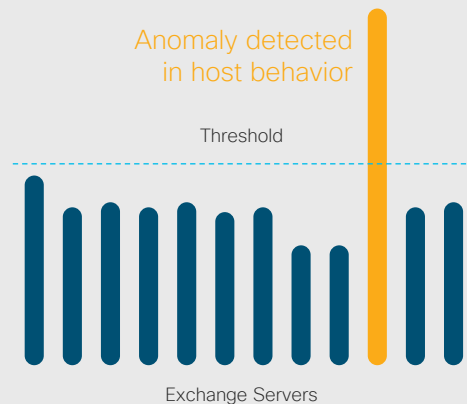
Security events to detect anomalies and known bad behavior

~ 100 Security Events

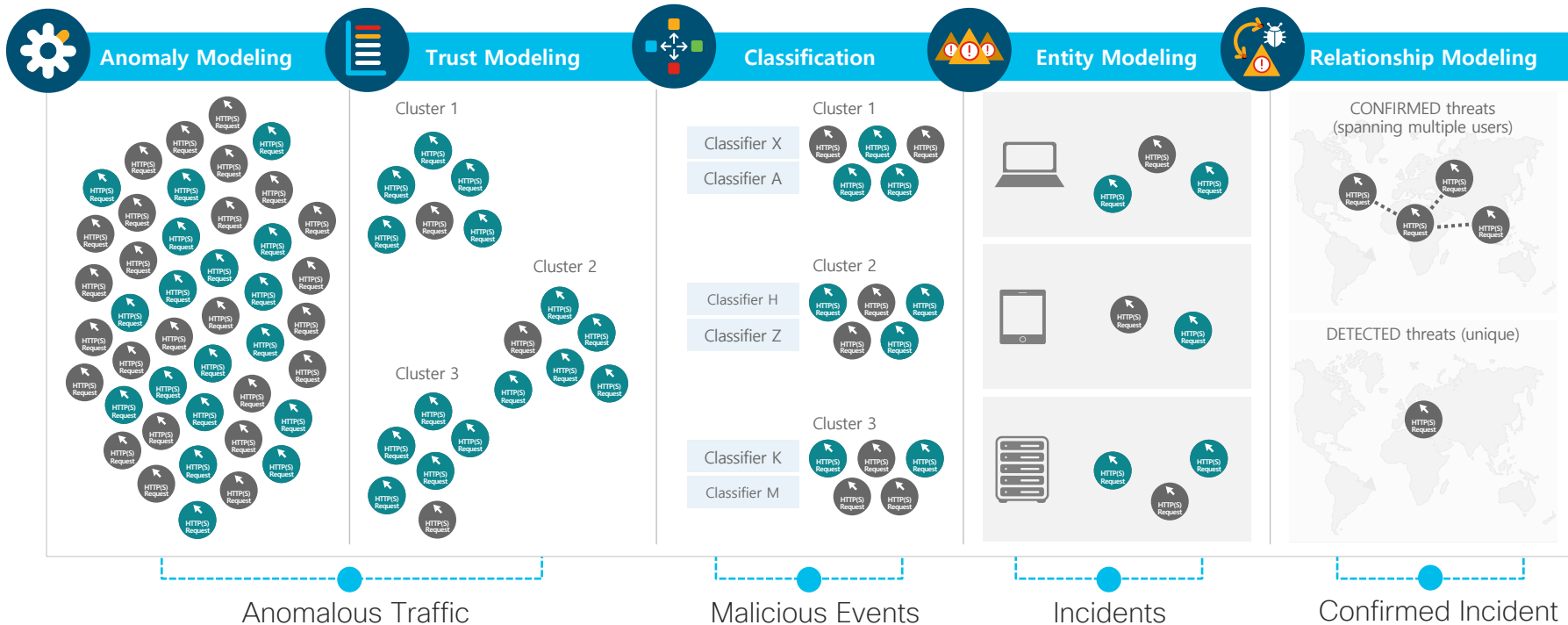
|                            |                     |                           |
|----------------------------|---------------------|---------------------------|
| Number of concurrent flows | New flows created   | Number of SYNs received   |
| Packet per second          | Number of SYNs sent | Rate of connection resets |
| Bits per second            | Time of day         | Duration of the flow      |

Alarm on anomalies and behavioral changes

Alarm categories for high-risk, low-noise alerts for faster response



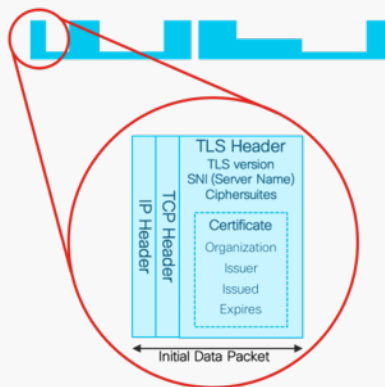
# Netflow 와 웹 프록시 로그 정보를 활용하다



# 암호화 트래픽 위협 분석 - TLS/SSL 정보를 활용

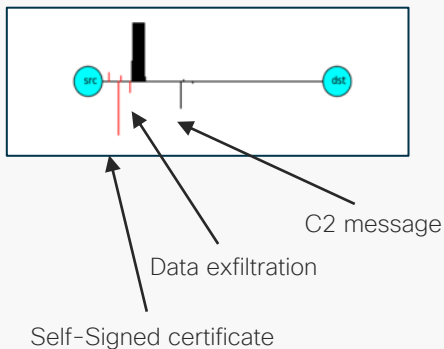
## Initial data packet

Make the most of the unencrypted fields



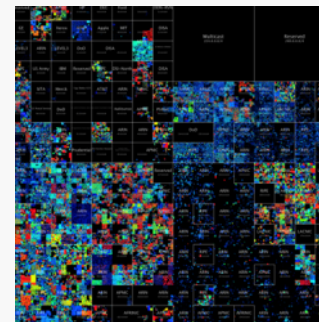
## Sequence of packet lengths and times

Identify the content type through the size and timing of packets



## Threat intelligence map

Who's who of the Internet's dark side



Broad behavioral information about the servers on the Internet.

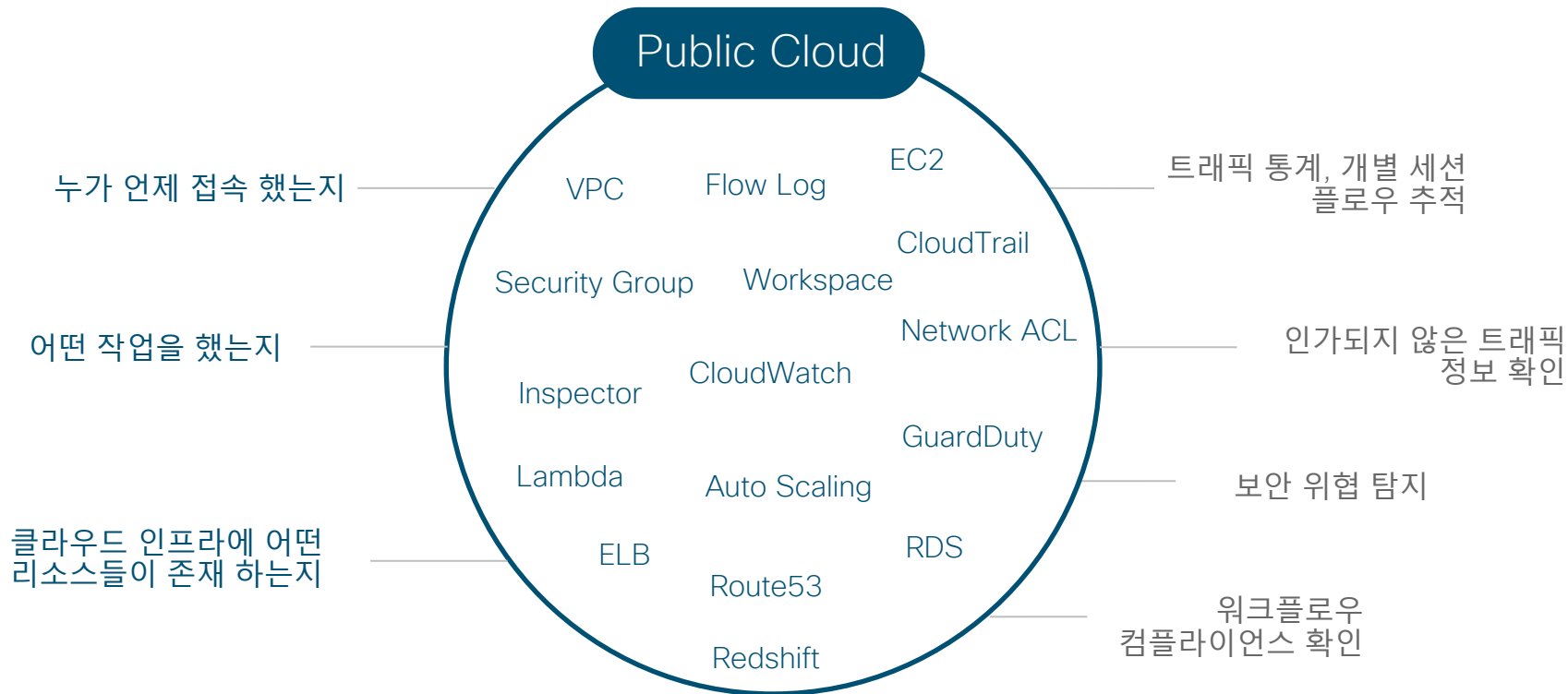


# 클라우드 트래픽 가시성 확보 - VPC Flow Log

|           | Flow Information | Traffic Information                          |
|-----------|------------------|----------------------------------------------|
| 트래픽<br>정보 | Account - ID     | 123456789010                                 |
|           | Interface - ID   | eni-abc123de                                 |
|           | Source IP        | 172.32.9.69                                  |
|           | Destination IP   | 172.32.9.12                                  |
|           | Source Port      | 4096                                         |
|           | Destination Port | 80                                           |
|           | Protocol         | 6                                            |
|           | Packets          | 20                                           |
|           | Bytes            | 4249                                         |
|           | Start / End Time | 12.34.10.10.01.01.18<br>45.54.10.10.01.01.18 |
| 보안<br>정보  | Action           | ACCEPT ,REJECT                               |
|           | Log-Status       | OK, NODATA, SKIPDATA                         |



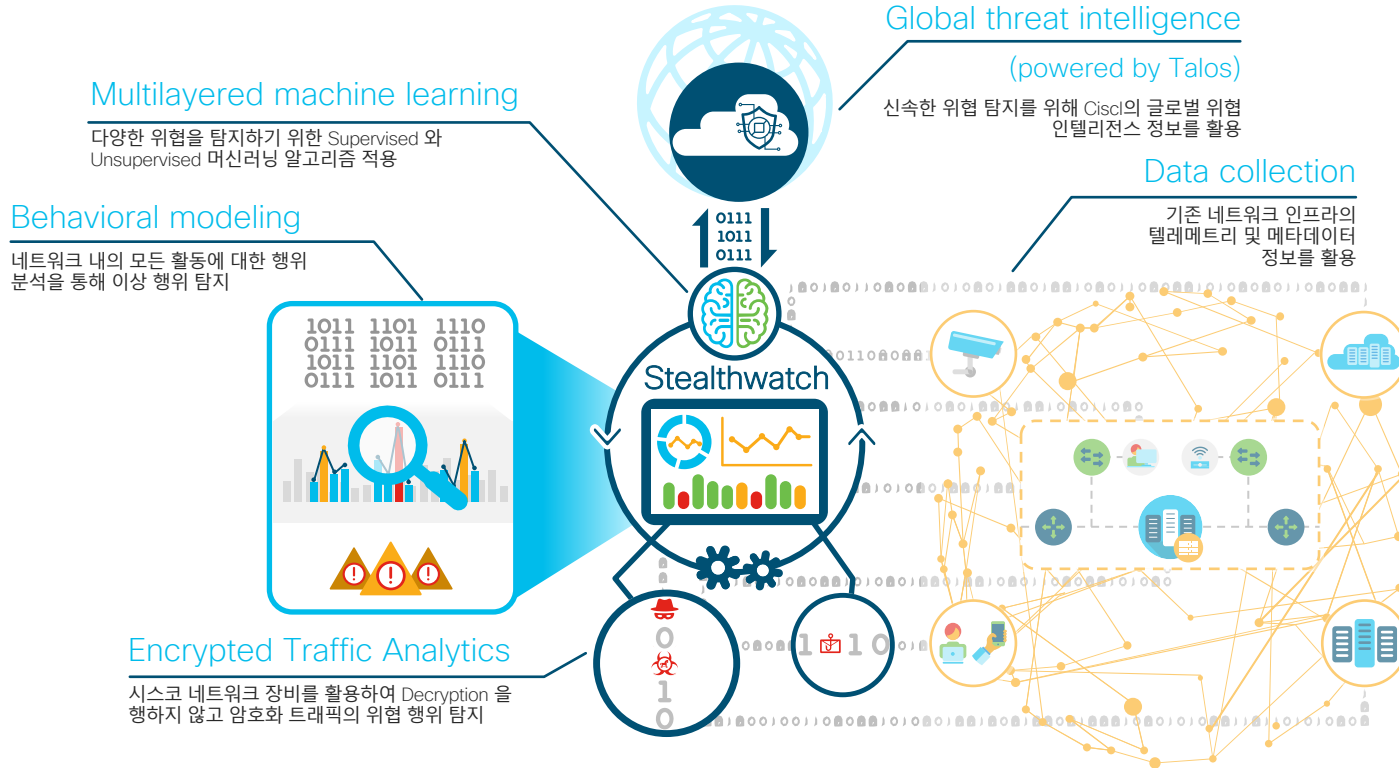
# 클라우드가 제공하는 정보를 최대한 활용



\*AWS 기능 기준

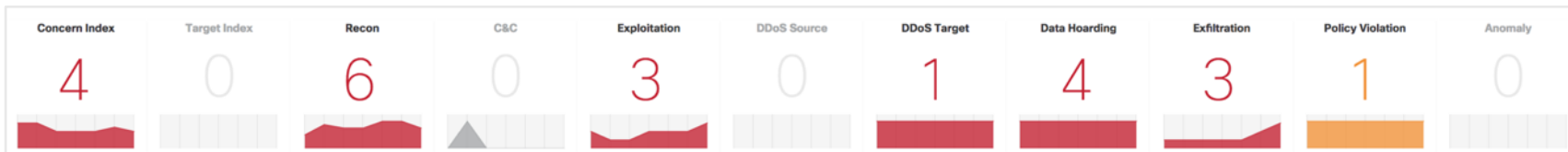
시스코  
보안 가시성과 인텔리전스 솔루션  
=> Stealthwatch

# Stealthwatch 보안 가시성 분석



# 운영자가 반드시 알아야 할 이벤트에 대한 정보 제공

| 악의적인 행위의 단말 또는 대상                      | 정찰 (Recon)                     | C&C                   | DDoS 공격                   | 내부자 위협             |
|----------------------------------------|--------------------------------|-----------------------|---------------------------|--------------------|
| 다양한 이벤트를 수집을 통해 관리 및 조치가 필요한 단말에 대한 정보 | 취약점 스캐닝, 사용중인 서비스 등에 대한 포트 스캐닝 | 멀웨어 감염등으로 인한 C&C서버 통신 | 다양한 유형의 트래픽 플러딩을 통한 자원 고갈 | 데이터 수집 및 데이터 유출 행위 |

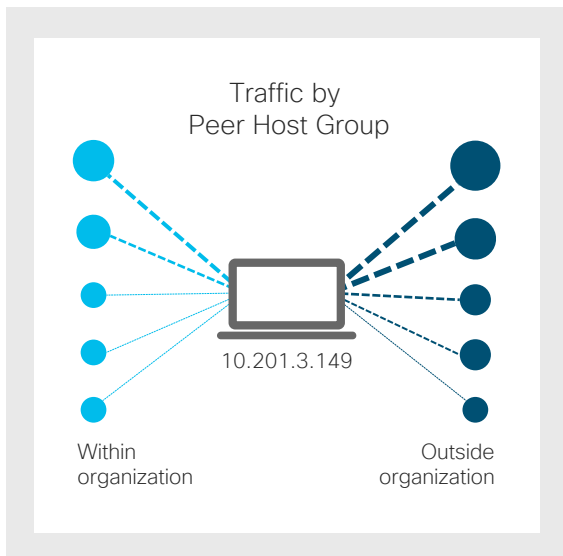




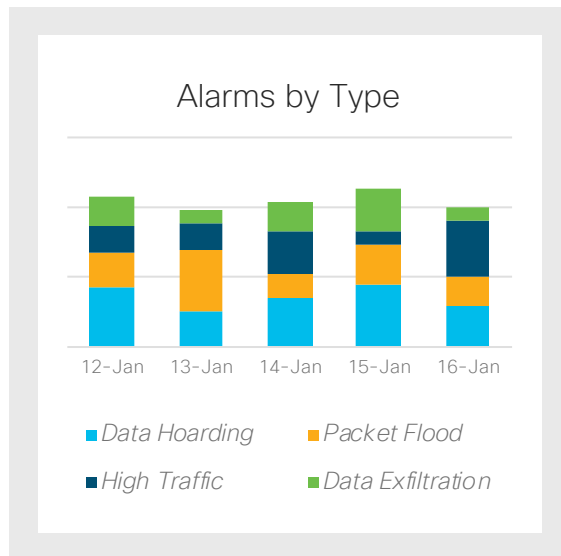
# 전체 / 그룹 / 호스트 단위의 분석과 통계 정보



Summary of aggregated host information



Observed communication patterns



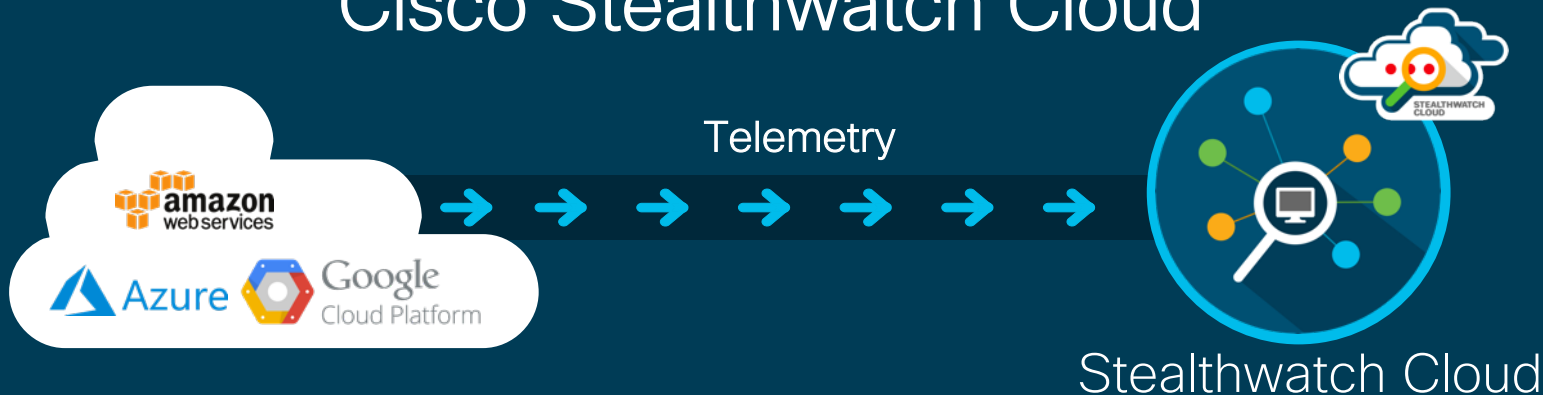
Historical alarming behavior

# Stealthwatch Use Case

네트워크 인프라의 전방위적인 가시성과 보안 인텔리전스 제공



# <쉽고, 빠른> 클라우드의 가시성 확보 Cisco Stealthwatch Cloud



빠르고 쉬운 연동  
단 5분만에 설정  
완료



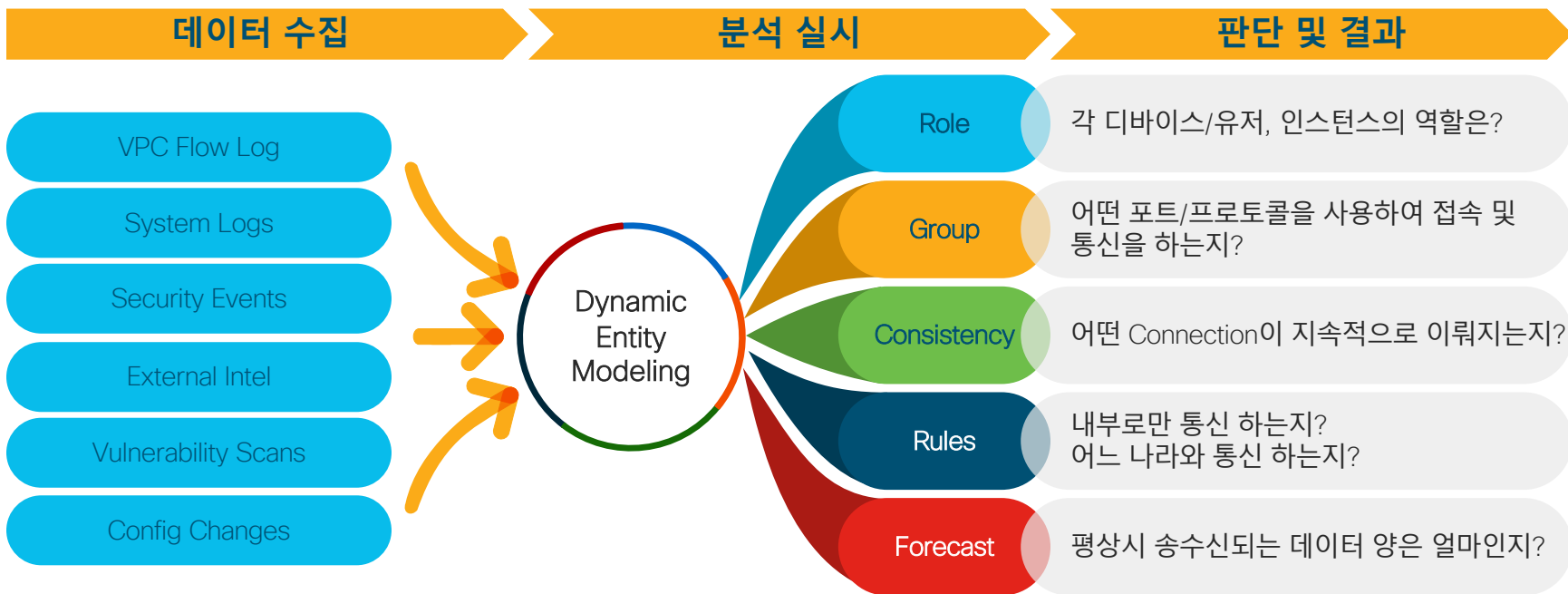
모든 행위 확인  
트래픽 및 리소스와  
컴플라이언스 확인



유용한 가시성 정보 제공  
비정상 행위와 보안 위협  
경보

# 어떻게 동작 하나요? - VPC Flow 로그와 리소스 분석의 학습

- Dynamic Entity Modeling



# 비정상 행위와 보안 위협 경고 Alert!!

- Automatic security event detection

**Potential Database Exfiltration** - postgres-db-01

Status: Open

ID: 598

Description: A statistically unusual amount of data was transferred from a database server to a client.

Updated: Nov 18, 2016 12:02:33 AM

Created: Nov 18, 2016 12:02:33 AM

IPs at the time of alert: 10.0.0.241

Hostname at the time of alert: postgres-db-01

Assignee: Nobody

Tags: Data exfiltration

[Close Alert](#)

**Supporting Observations**

New High Throughput Connection Observation

Device has exchanged a large amount of traffic with a new host.

20 records per page

| Time             | Source         | Connected IP | Local Connection | In            | Out            | Time Window |
|------------------|----------------|--------------|------------------|---------------|----------------|-------------|
| 11/17/16 2:13 PM | postgres-db-01 | 2.63.255.251 | no               | 1,989,892,515 | 17,967,298,803 | 9h 48m 51s  |

[CSV](#) Showing 1 of 1

**Watchlist Interaction Observation**

Device communicated with an IP address that is on a watchlist (either explicitly or implicitly via a domain name).

| Time             | Source | Watchlists      | External IP  | Domain | In  | Out   | Bytes |
|------------------|--------|-----------------|--------------|--------|-----|-------|-------|
| 4/17/18 11:06 AM |        | Ransomware - IP | 78.47.159.97 |        |     |       |       |
| 3/20/18 11:15 AM |        | Bitnodes        |              |        | 240 | 1,136 |       |
| 3/29/18 5:31 PM  |        | Bitnodes        |              |        | 120 | 568   |       |
| 3/29/18 5:31 PM  |        | Bitnodes        |              |        | 160 | 608   |       |
| 3/29/18 5:30 PM  |        | Bitnodes        |              |        | 160 | 608   |       |

# 상세 트래픽 정보 및 SG 정보 제공

## 개별 세션 로그

## SG 트래픽 통계

### Session Traffic

Q active filters

Filter by a list of IPs or CIDR ranges. Use "-" to exclude an IP (e.g. "10.0.0.1, 10.0.10.0/24, -10.0.1.7").

IP

Connected IP

Filter by a list of ports or port ranges. Use "-" to exclude a port. (e.g. "22-25, 80, -443").

Port

Connected Port

Filter by low-level protocol.

Protocol

Filter by bytes or packets.

Bytes to

Packets to

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date

### Traffic

Bytes transferred via security group routes over the selected time range.

**Note:** Traffic and connection data depend on this service being configured to collect data relevant to each security group. Zeroes in either column may not reflect the true usage of the security group if the traffic associated with it is not monitored.

Q filters from 2019-02-13 15:34 to 2019-02-13 21:34

10 records per page

| Account      | Name                  | Identifier           | CIDR      | Ports   | Connections | Traffic |
|--------------|-----------------------|----------------------|-----------|---------|-------------|---------|
| 299015533822 | GSSO VPC - Any to Any | sg-33791b43          | 0.0.0.0/0 | 0-65535 | 1503        | 93 MB   |
| 845574328132 | launch-wizard-2       | sg-2b51f85e          | 0.0.0.0/0 | 0-65535 | 619         | 36 kB   |
| 299015533822 | launch-wizard-5       | sg-03b5cbb520f9bd256 | 0.0.0.0/0 | 22      | 257         | 372 kB  |
|              |                       | i27a4                | 0.0.0.0/0 | 0-65535 | 122         | 158 MB  |
|              |                       | i228b97af2f1b0       | 0.0.0.0/0 | 22      | 0           | 0 B     |
|              |                       | i79531023ac2b4       | 0.0.0.0/0 | 0-65535 | 0           | 0 B     |

Enter a start date/time and end date/time for the search. Longer time ranges will take longer to load.

Start Date  Start Time

End Date  End Time

Traffic Traffic Chart **Rejects** Connections Graph

Table of matching rejects.

20 records per page

| Time            | IP            | Connected IP    | Port               | Connected Port | Protocol | Bytes | Packets |
|-----------------|---------------|-----------------|--------------------|----------------|----------|-------|---------|
| 2/13/19 9:19 PM | 10.10.2.31    | 104.131.145.139 | 139 (netbios-ssn)  | 34414          | TCP      | 40    |         |
| 2/13/19 9:19 PM | 10.10.2.31    | 185.95.228.106  | 445 (microsoft-ds) | 50746          | TCP      | 40    |         |
| 2/13/19 9:19 PM | 10.10.2.31    | 71.6.232.5      | 25 (smtp)          | 33428          | TCP      | 40    |         |
| 2/13/19 9:18 PM | 192.168.73.77 | 123.126.108.150 | 1433 (ms-sql-s)    | 54270          | TCP      | 40    |         |
| 2/13/19 9:18 PM | 192.168.73.77 | 23.94.66.186    | 445 (microsoft-ds) | 52915          | TCP      | 40    |         |
| 2/13/19 9:18 PM | 10.10.2.31    | 222.43.4.43     | 23 (telnet)        | 15054          | TCP      | 40    |         |
| 2/13/19 9:18 PM | 10.10.2.31    | 187.198.35.2    | 2323               | 64874          | TCP      | 44    | 1       |
| 2/13/19 9:18 PM | 10.10.2.31    | 185.95.228.106  | 139 (netbios-ssn)  | 50746          | TCP      | 40    | 1       |

SG/ACL을 통한 차단  
트래픽 상세 확인

# 사용자 컴플라이언스 정보 및 관리

The screenshot displays the Cisco Stealthwatch Cloud interface. At the top, there's a navigation bar with 'Stealthwatch Cloud', 'Dashboard', 'Alerts', 'Observations', and 'Models'. Below this, the 'AWS Visualizations' section is active, with sub-tabs for 'CloudTrail', 'Network Graph', 'Security Groups', 'IAM', and 'Inspector'. The main area shows a table of AWS CloudTrail logs with columns for Time, Username, Source IP, Event, Request, and Response. The table contains several entries for 'root' users performing 'AuthorizeSecurityGroupIngress' and 'AddUserToGroup' actions. To the right, there are two callout boxes: a green one for 'Console, CLI, API 사용 정보' and an orange one for 'Watchlist 를 통한 컴플라이언스 관리'. Below the orange box, the 'AWS CloudTrail Alert Watchlist' section is visible, showing a table with 'Account ID' and 'Event' columns, and a form to 'Add AWS CloudTrail Watch' with fields for 'Account ID' and 'Event'.

Console, CLI, API 사용 정보

Watchlist 를 통한 컴플라이언스 관리

**AWS CloudTrail Alert Watchlist**

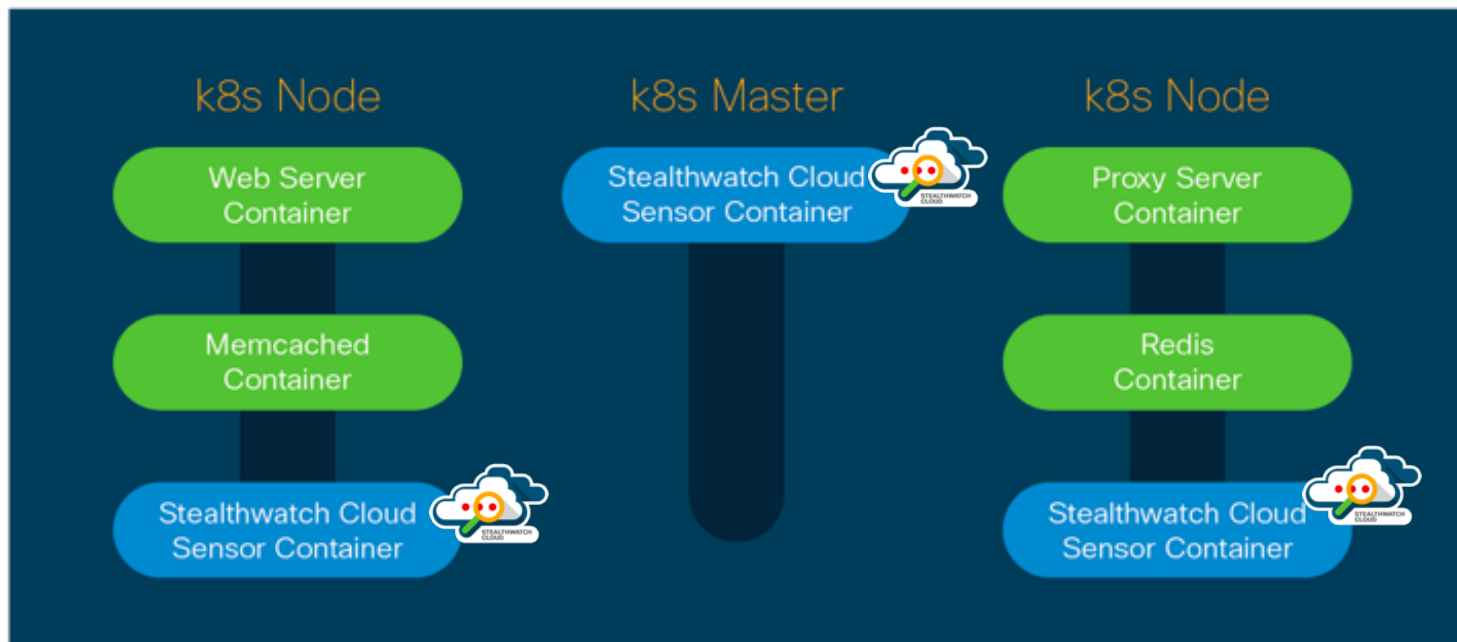
| Account ID   | Event          |
|--------------|----------------|
| 069624403551 | AddUserToGroup |

**Add AWS CloudTrail Watch**

Account ID:

Event:

# Stealthwatch Cloud for Kubernetes



Daemonset 실행 한번으로 K8S Cluster의 모든 트래픽 가시성 확보!!



# Cisco 데모 부스에 방문하셔서 확인하세요!





Go From Breached To Blocked

Cisco.  
Security above everything.

### Cisco Stealthwatch Enterprise

비즈니스 전반의 네트워크 가시성 및 보안 분석

Cisco Stealthwatch는 지능형 위험 방지, 실행 조치 및 인스펙션 보드와 1세 커넥션실용우려 7종, 네트워크 인프라의 복잡성을 사용한다. 인기 인증된 머신러닝 및 행동 모델링을 통해 사할 비정상적 서 시공은 위협에 비대 대응할 수 있습니다.

- 이벤트 가시성
- 시각화 및 분석
- 네트워크 보드
- 가시성
- 사할 비정상적 서공
- 이벤트 분석
- 신호

---

### Cisco Firepower Next-Generation Firewall

Cisco NGFW는 보안 정책을 시공으로 방지 하는 동시에 네트워크 침투 수, 보드 공격 방어 시공된 위험도 확으로 방지하고 차단할 수 있습니다.

최신 위협지능수를 적용하여 네트워크 및 보안 직업을 자동화하여 시간을 절약할 수 있습니다.

- 위협 지능
- 1대1
- 위협 지능
- 신호
- 위협 지능
- 신호
- 위협 지능
- 신호

