디지털 네트워크 변화에 따른 보안 가시성 확보 전략

Jinhyun Lee (**이 진 현**)

Consulting Systems Engineer – Security APJC

Cisco Systems

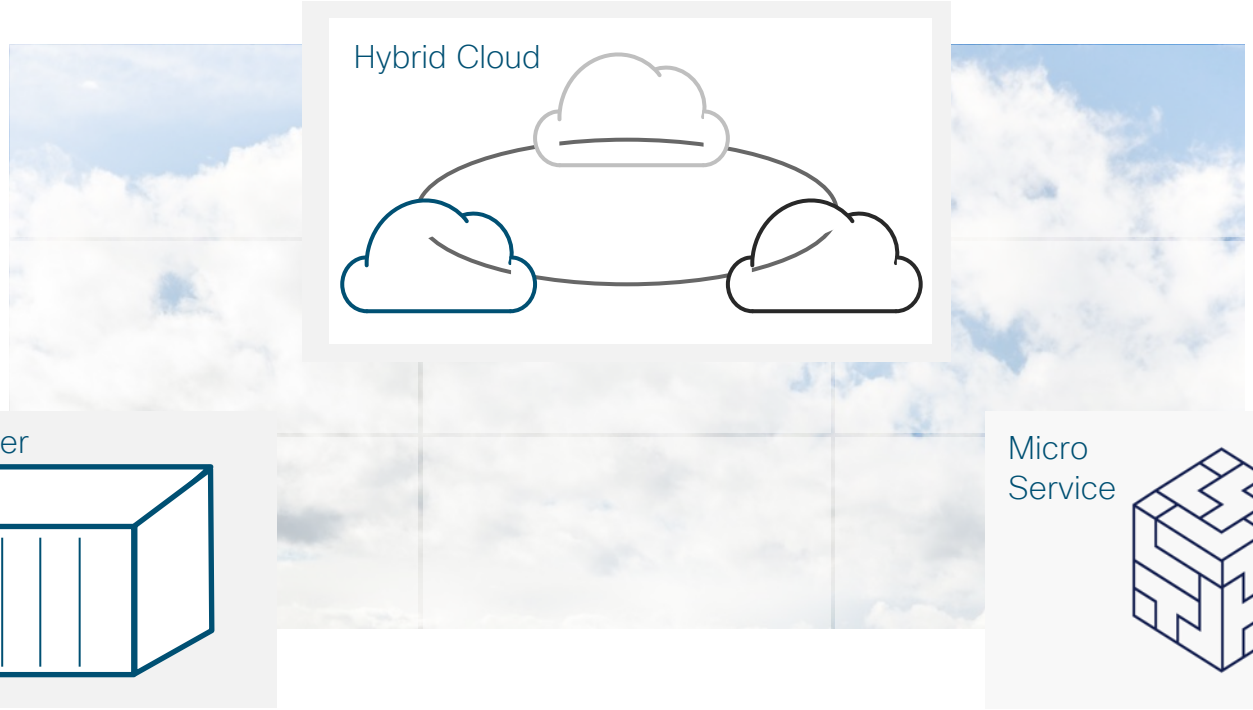
DIGITAL TRANSFORMATION

DEVICE
IOT, BYOD, Mobility

Automation
Software Defined

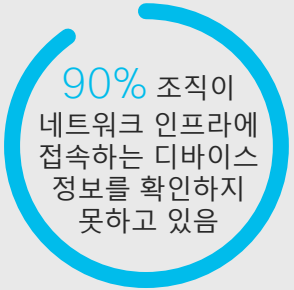
Intelligence
Machine-Learning

And.. Cloud!!



디지털 변화에 따른 보안 챌린지

Enterprise Mobility



90% 조직이 네트워크 인프라에 접속하는 디바이스 정보를 확인하지 못하고 있음

Cloud

21B

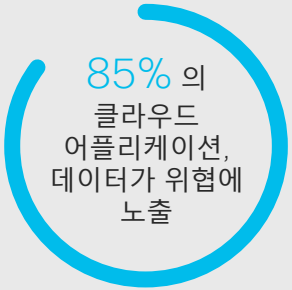
2020년까지 증가할 IOT 단말 수

Encrypted Traffic

2/3

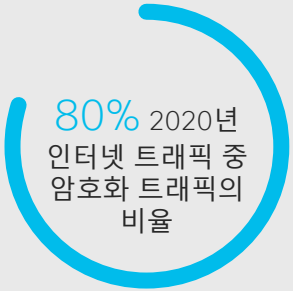
2020년 까지 총 IP 트래픽에서 모바일 및 무선 네트워크 단발이 차지하는 비율

Acquisitions & Partnerships



85% 의 클라우드 어플리케이션, 데이터가 위협에 노출

Internet of Things



80% 2020년 인터넷 트래픽 중 암호화 트래픽의 비율

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 필요 합니다

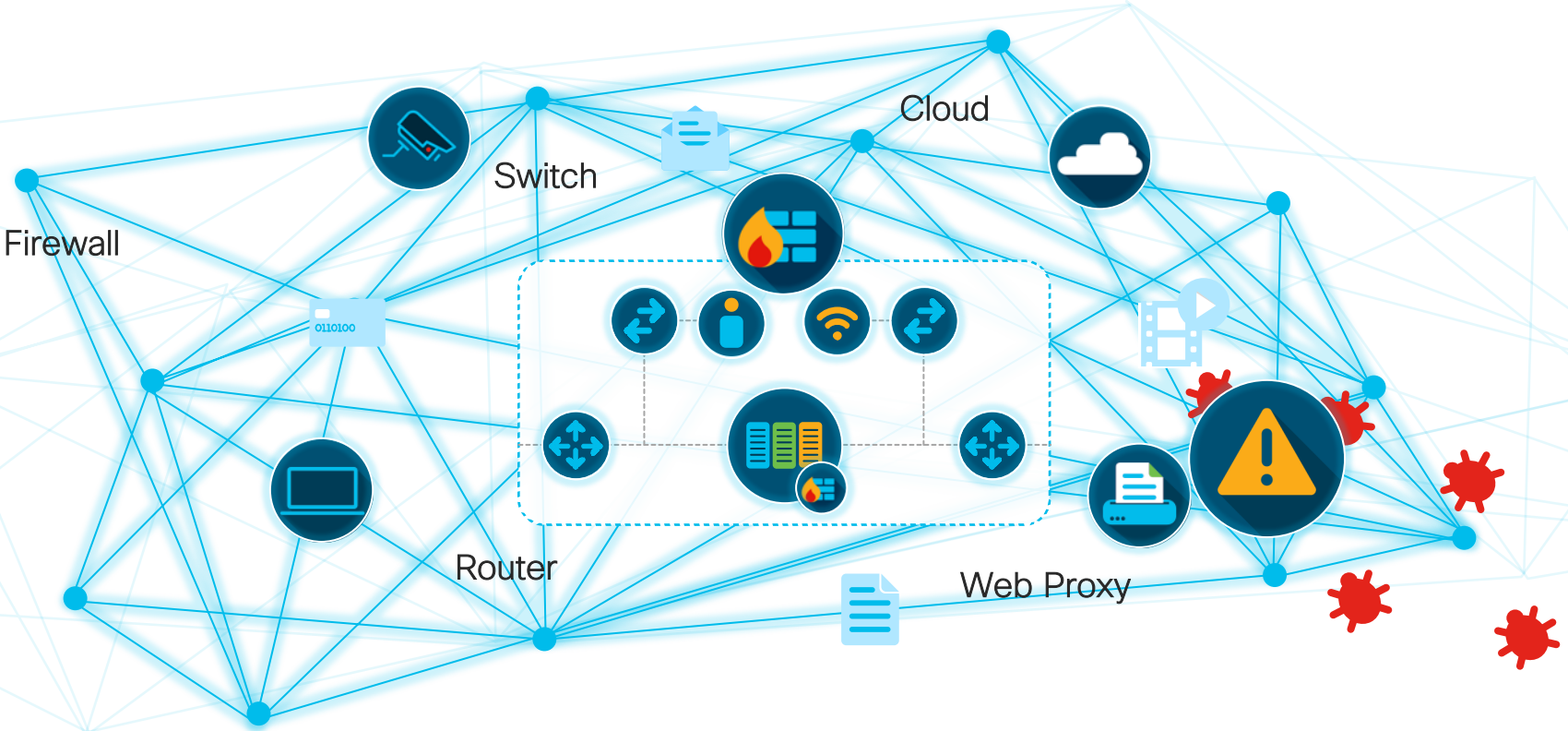
보안 이벤트 발생 시 인텔리전스를 활용 한 조사 시간의 단축이 필요 합니다

보안 이벤트 발생 시 개별 세션 단위의 히스토리 정보가 필요 합니다

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

솔루션 : Network + Security

기존 인프라 장비들을 보안에 활용하다

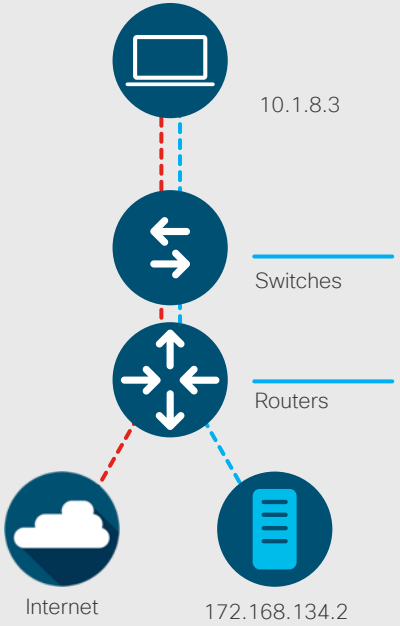


기존 인프라가 제공하는 기능을 활용한 보안 가시성 확보

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

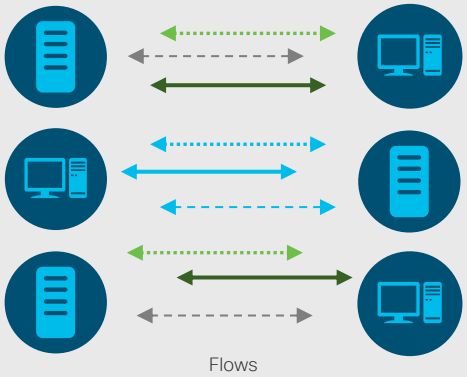


Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP

Netflow를 활용한 네트워크 행위 기반 분석 및 학습

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



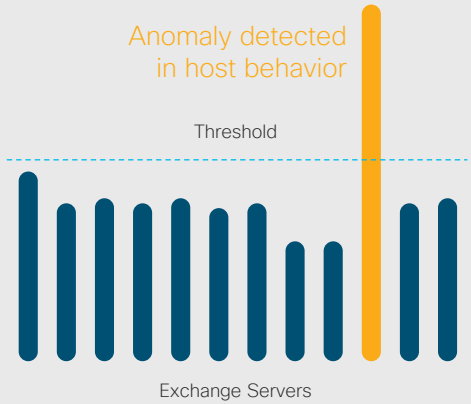
Create a baseline of normal behavior

Security events to detect anomalies and known bad behavior

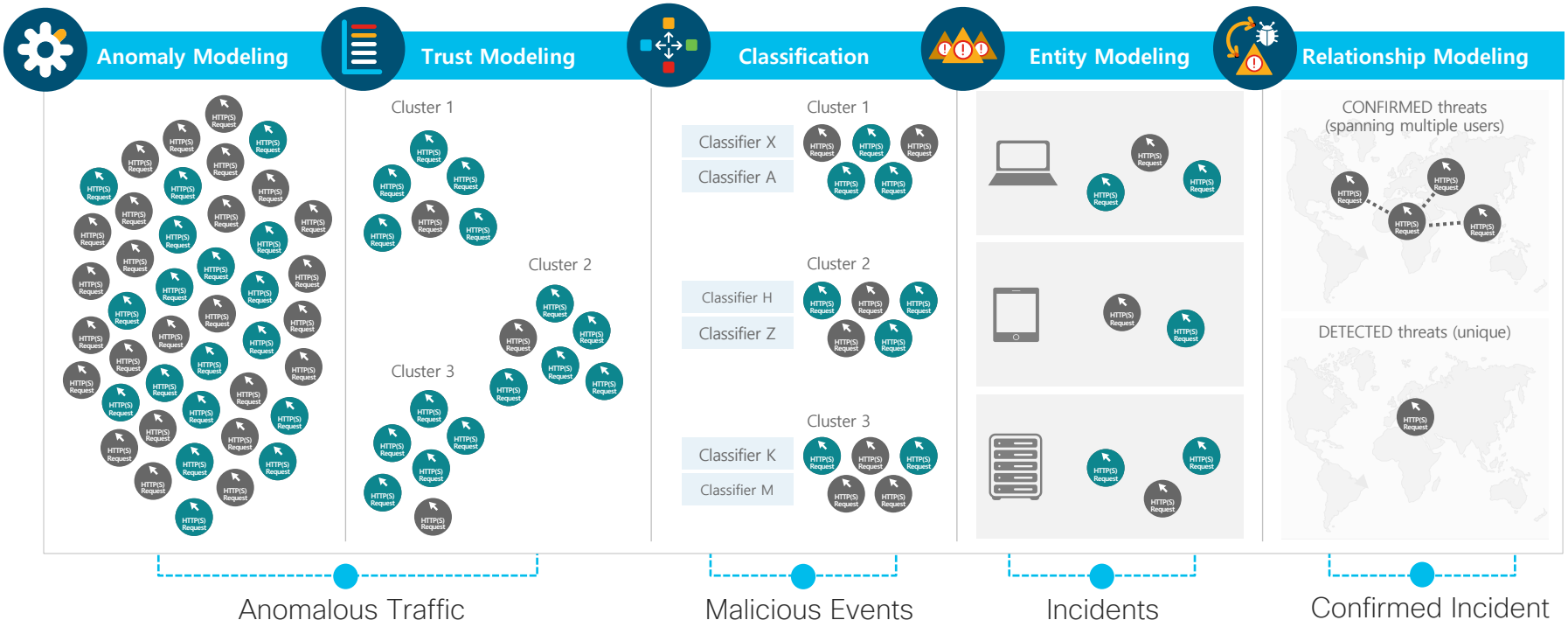
~100 Security Events		
Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Alarm on anomalies and behavioral changes

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



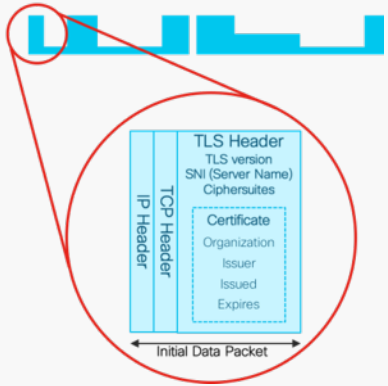
Netflow 와 웹 프록시 로그 정보를 활용하다



암호화 트래픽 위협 분석 – TLS/SSL 정보를 활용

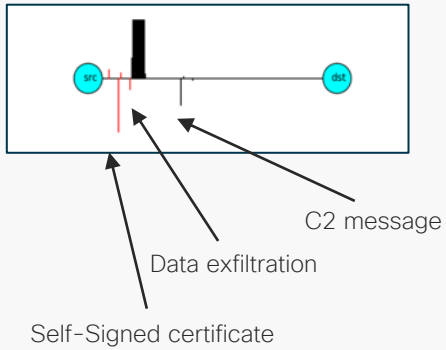
Initial data packet

Make the most of the unencrypted fields



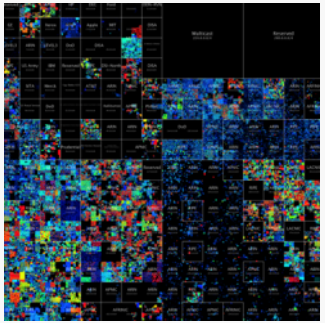
Sequence of packet lengths and times

Identify the content type through the size and timing of packets



Threat intelligence map

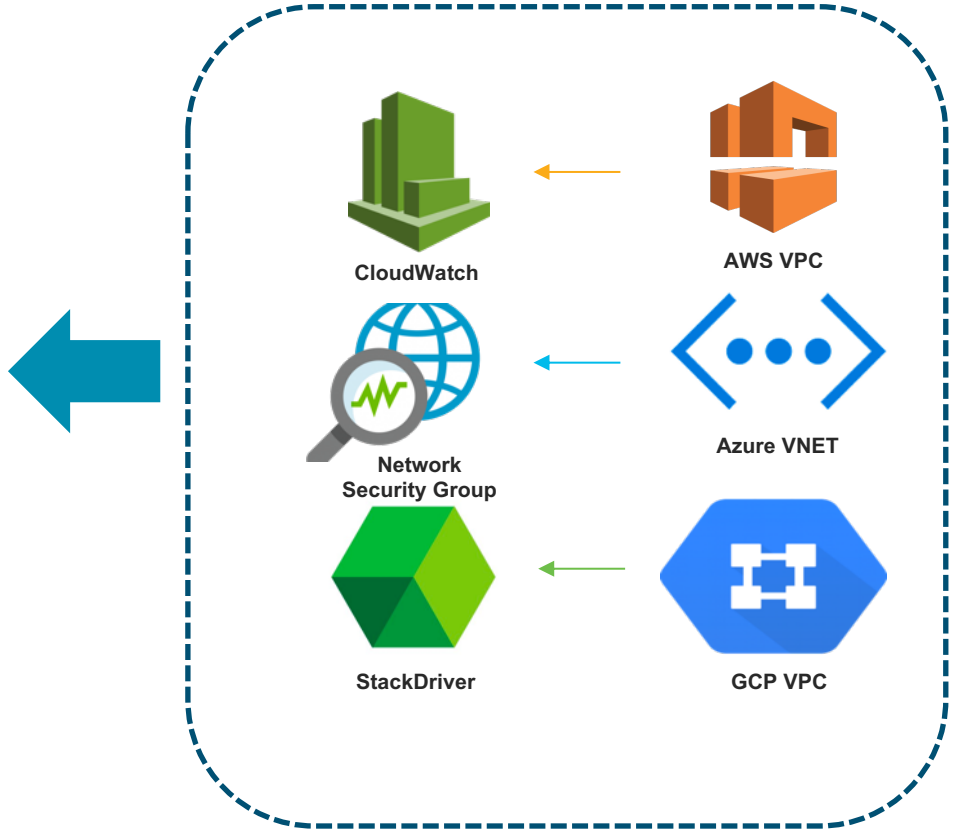
Who's who of the Internet's dark side



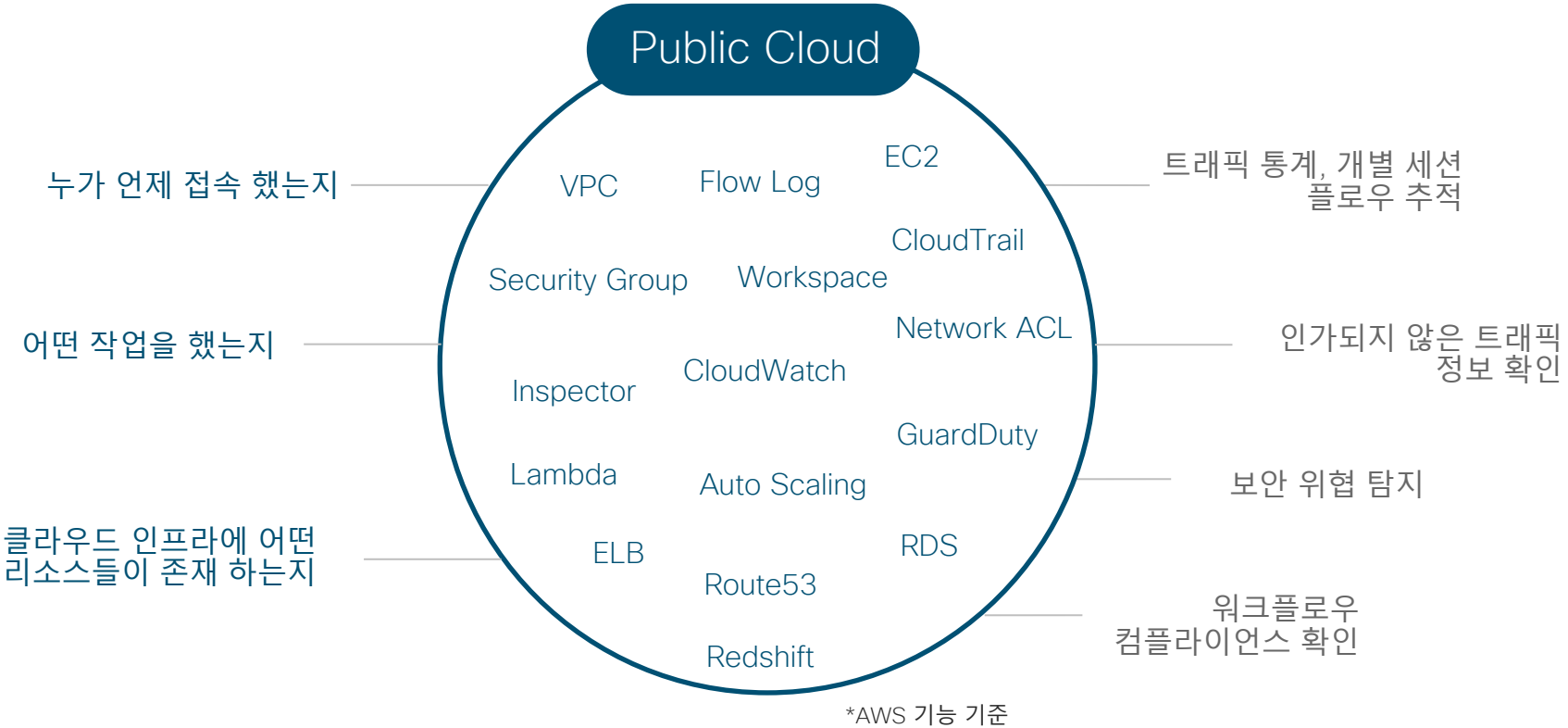
Broad behavioral information about the servers on the Internet.

클라우드 트래픽 가시성 확보 – VPC Flow Log

	Flow Information	Traffic Information
트래픽 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 45.54.10.10.01.01.18
보안 정보	Action	ACCEPT ,REJECT
	Log-Status	OK, NODATA, SKIPDATA



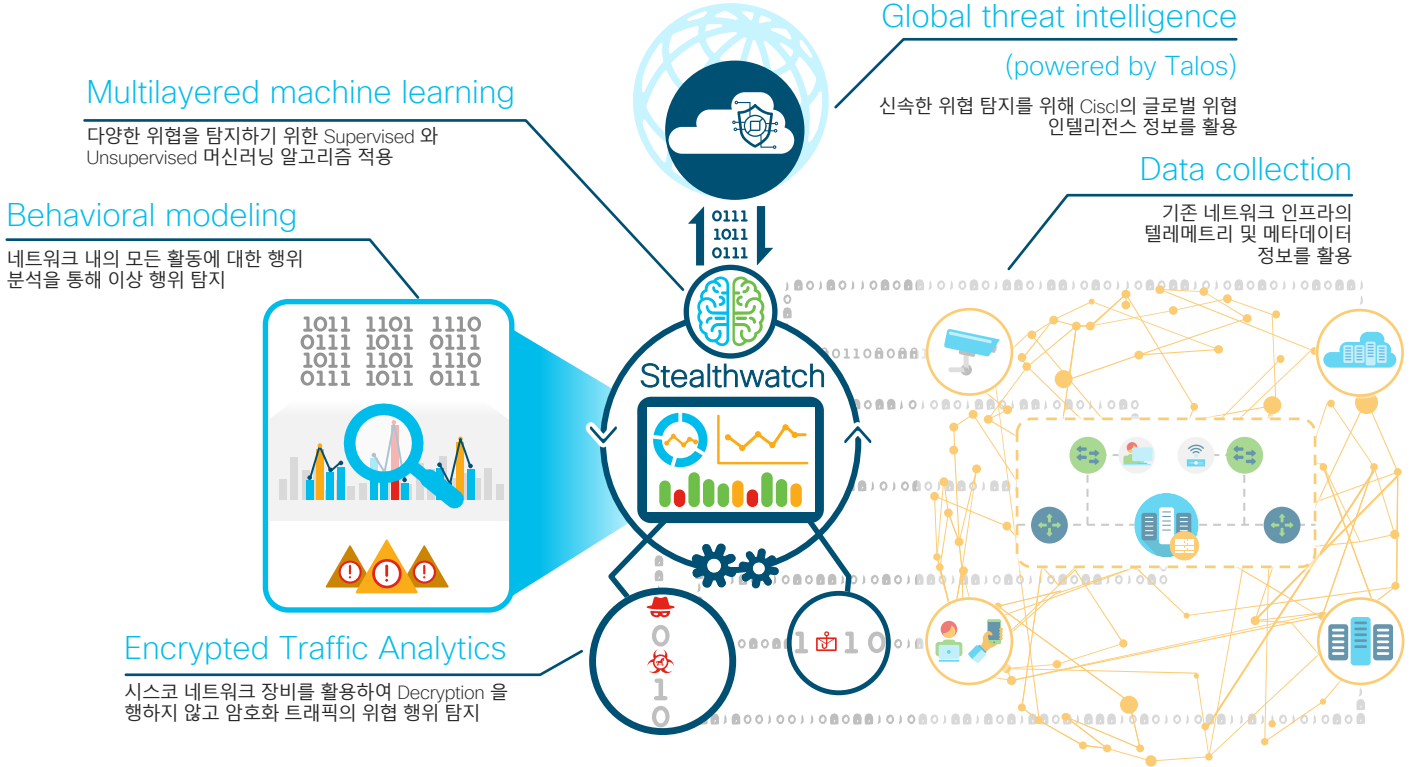
클라우드가 제공하는 정보를 최대한 활용



*AWS 기능 기준

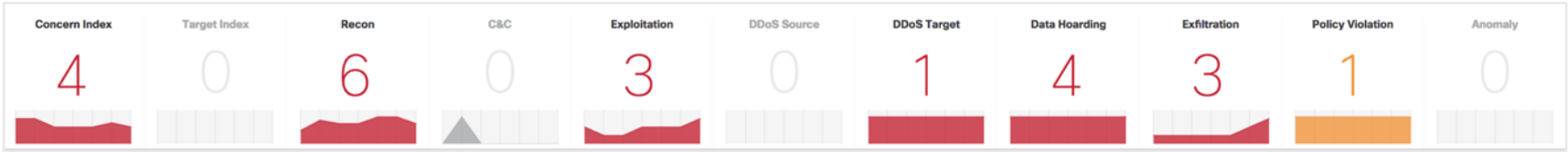
시스코
보안 가시성과 인텔리전스 솔루션
=> Stealthwatch

Stealthwatch 보안 가시성 분석

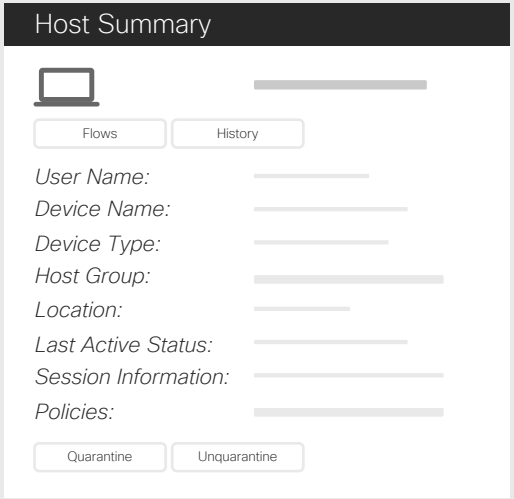


운영자가 반드시 알아야 할 이벤트에 대한 정보 제공

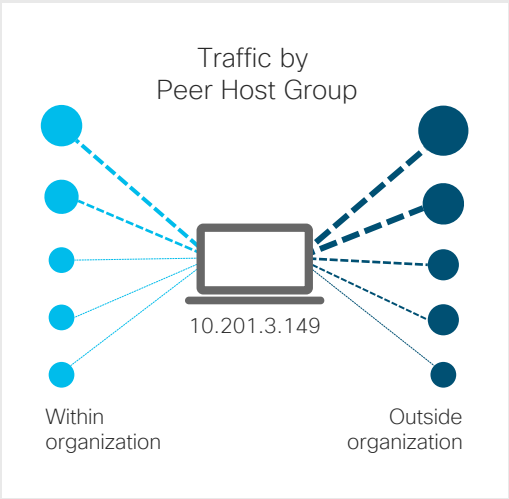
악의적인 행위의 단말 또는 대상	정찰 (Recon)	C&C	DDoS 공격	내부자 위협
다양한 이벤트 수집을 통해 관리 및 조치가 필요한 단말에 대한 정보	취약점 스캐닝, 사용중인 서비스 등에 대한 포트 스캐닝	멀웨어 감염등으로 인한 C&C서버 통신	다양한 유형의 트래픽 플러딩을 통한 자원 고갈	데이터 수집 및 데이터 유출 행위



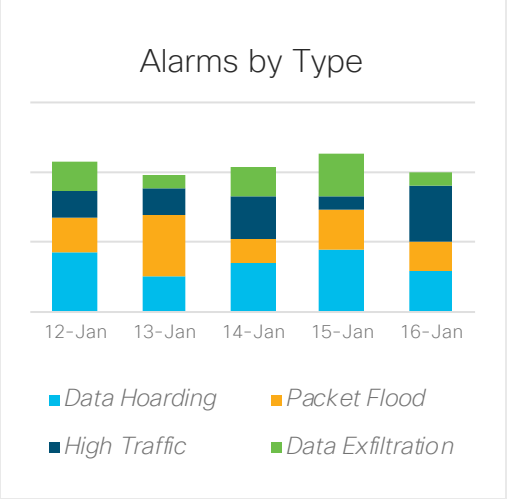
전체 / 그룹 / 호스트 단위의 분석과 통계 정보



Summary of aggregated host information



Observed communication patterns



Historical alarming behavior

Stealthwatch Use Case

네트워크 인프라의 전방위적인 가시성과 보안 인텔리전스 제공

트래픽 리포팅

위협 트래픽 및 호스트 탐지

통신 규정 / 세그멘테이션 정보

데이터 수집 및 유출 행위 탐지

어플리케이션 사용 정보

멀웨어, 애드웨어, 크립토 마이닝, DNS 위협 탐지

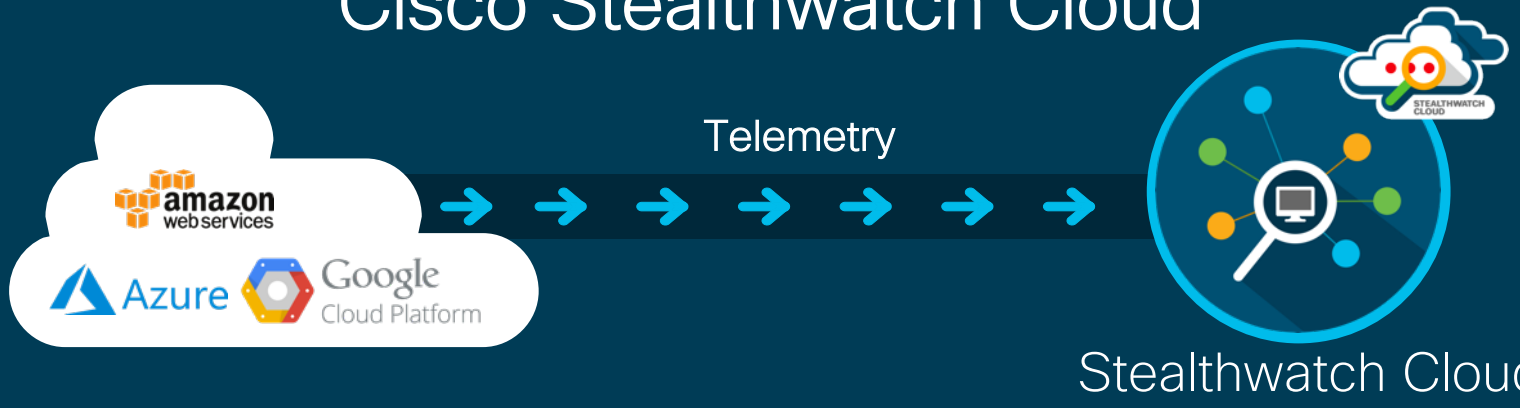
통신 지연 정보

사용자 이벤트 제공

시스코 TALOS 인텔리전스 제공

암호화 통신의 위협 탐지

<쉽고, 빠른> 클라우드의 가시성 확보
Cisco Stealthwatch Cloud



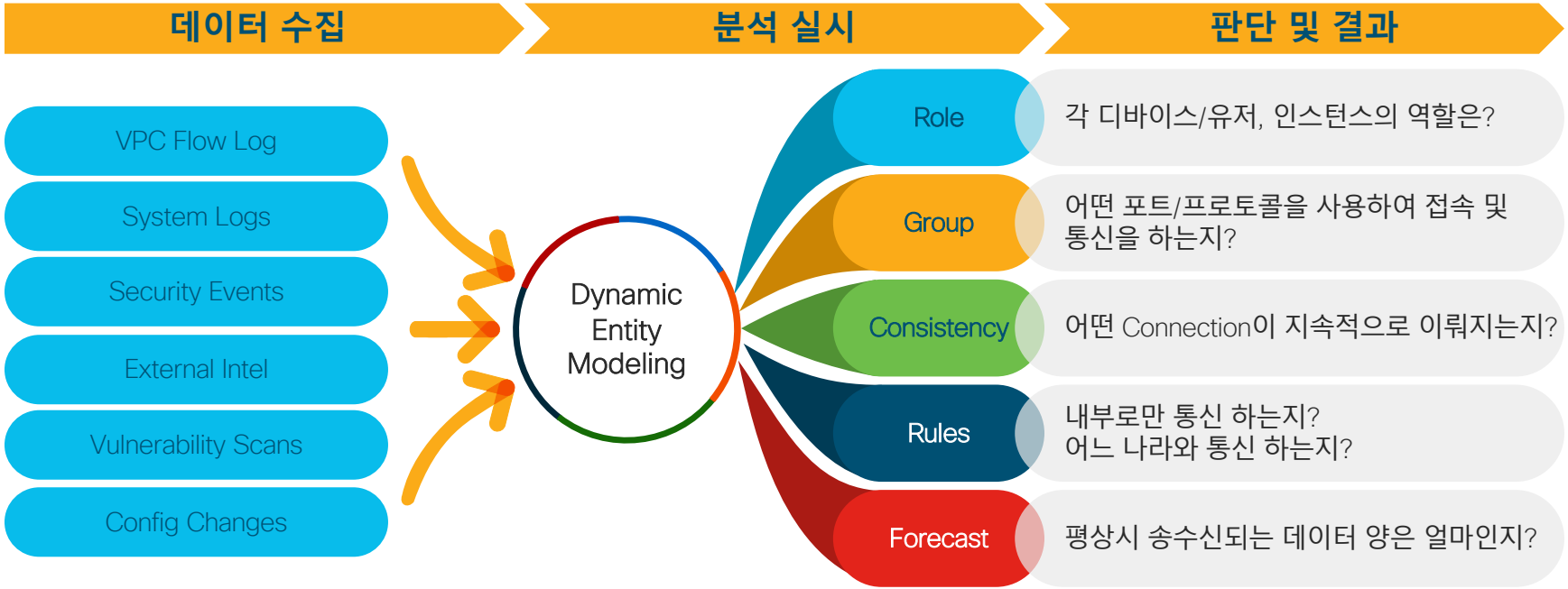
빠르고 쉬운 연동
단 5분만에 설정 완료

모든 행위 확인
트래픽 및 리소스와 컴플라이언스 확인

유용한 가시성 정보 제공
비정상 행위와 보안 위협 경보

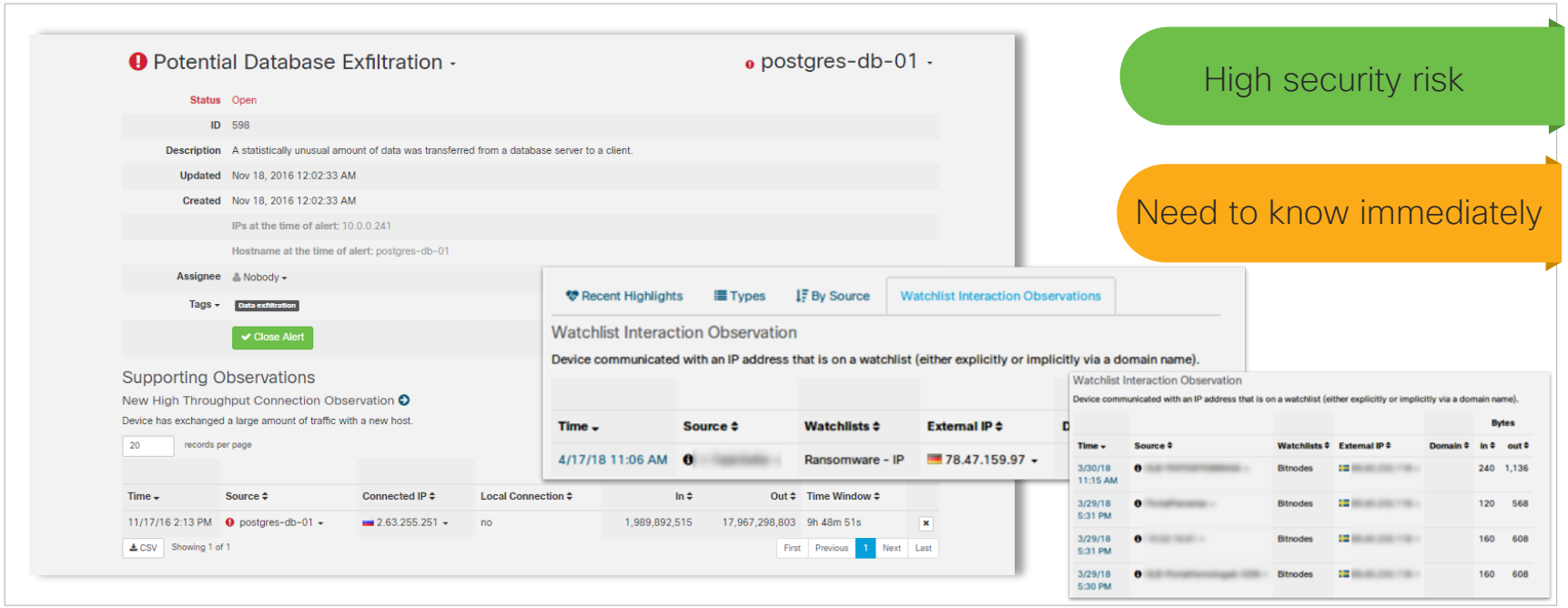
어떻게 동작 하나요? – VPC Flow 로그와 리소스 분석의 학습

- Dynamic Entity Modeling



비정상 행위와 보안 위협 경고 Alert!!

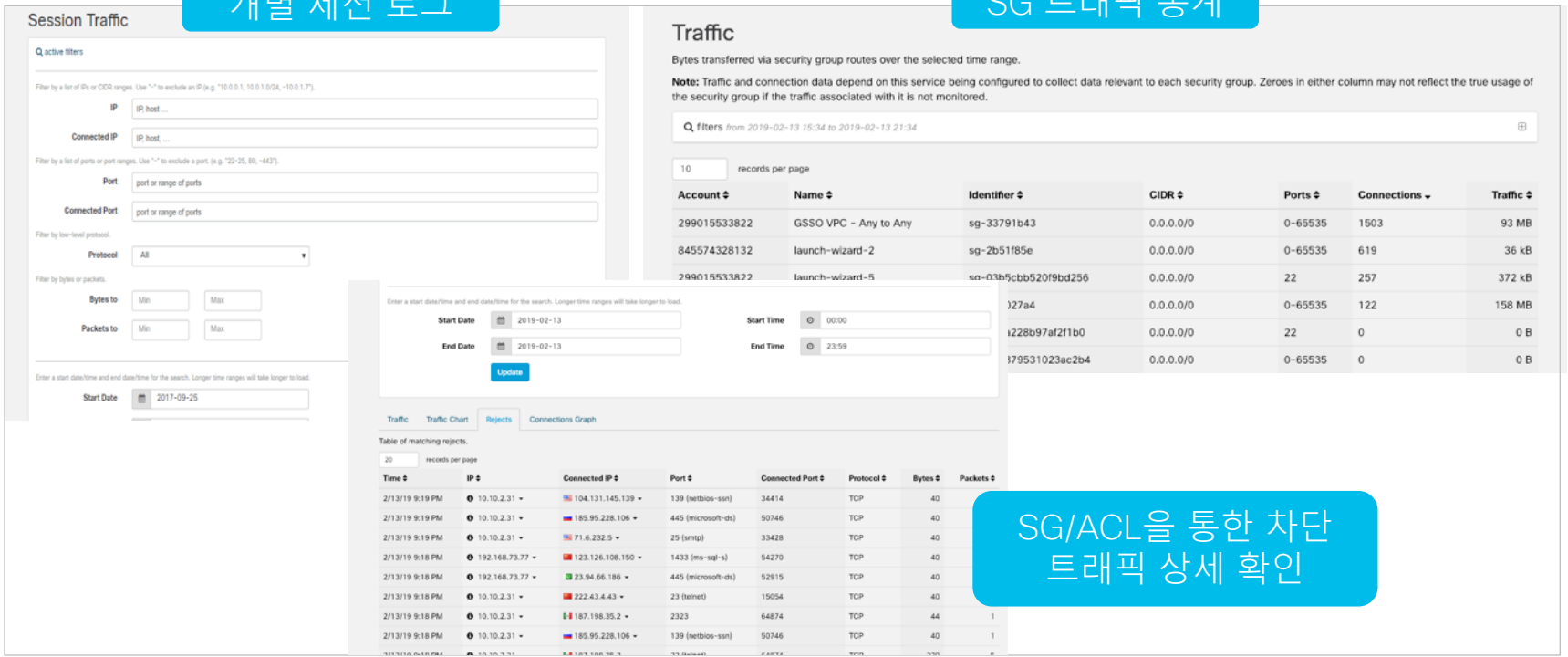
- Automatic security event detection



상세 트래픽 정보 및 SG 정보 제공

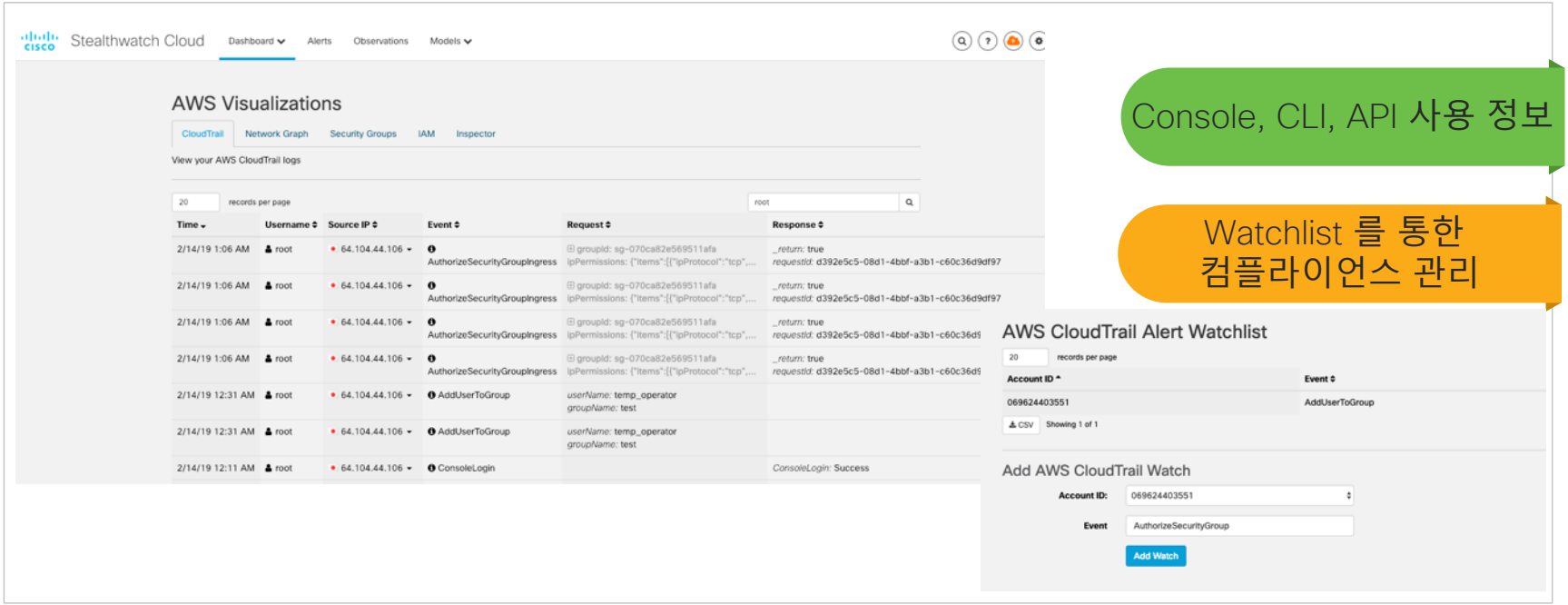
개별 세션 로그

SG 트래픽 통계

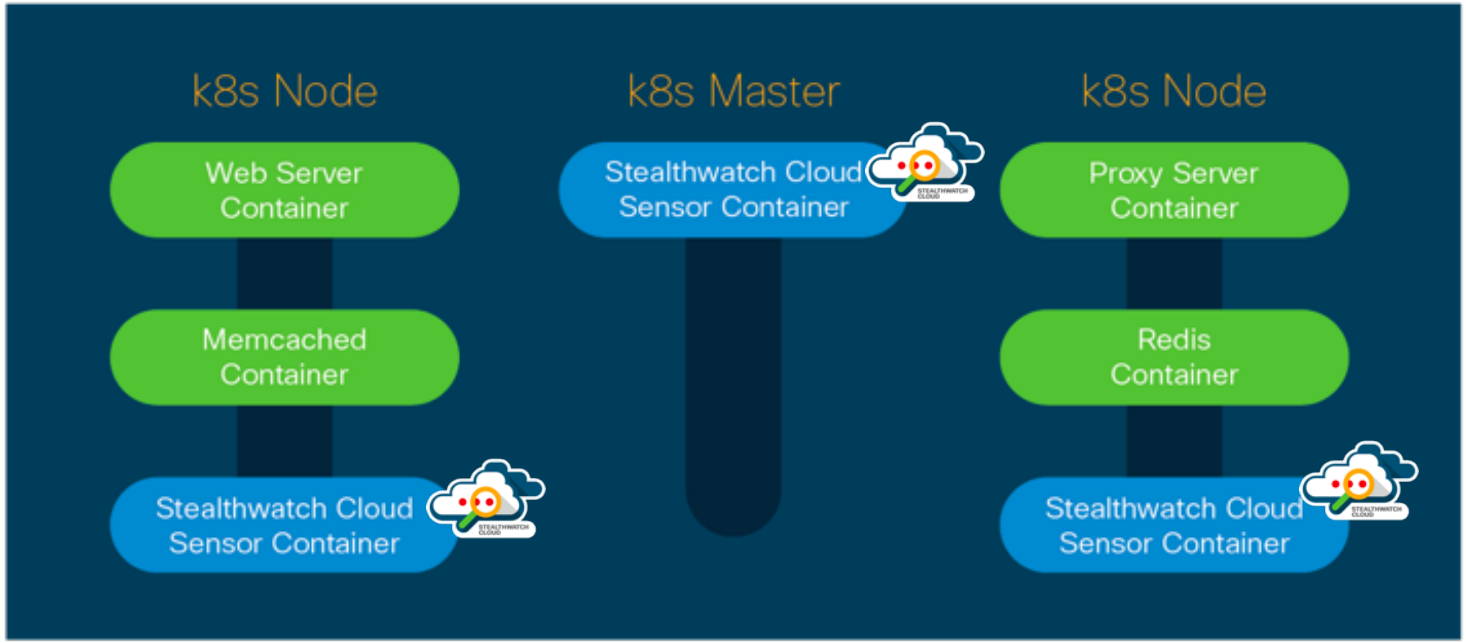


SG/ACL을 통한 차단 트래픽 상세 확인

사용자 컴플라이언스 정보 및 관리



Stealthwatch Cloud for Kubernetes



Daemonset 실행 한번으로 K8S Cluster의 모든 트래픽 가시성 확보!!

Cisco 데모 부스에 방문하셔서 확인하세요!

SK infosec

cisco Partner