The bridge to possible

Detecting Critical Threats
Behavior based detection & response
透過基於行為分析的事件反應調查來偵測關鍵威脅

with Secure Network Analytics/XDR

Derek Chia
XDR Sales Lead, Greater China/ASEAN

Agenda
議程

- Introduction
- Cisco NDR & XDR
- Cisco NDR Solution Overview
- Use Cases
- Demo

Detecting Critical Threats with your Existing Network Elements

使用現有網路機制檢測關鍵威脅

網路和安全維運的挑戰

網路威脅變得更加聰明

Motivated and targeted adversaries

- State sponsored
- Financial/espionage motives
- $1T cybercrime market

Insider Threats

- Compromised credentials
- Disgruntled employees
- Admin/privileged accounts

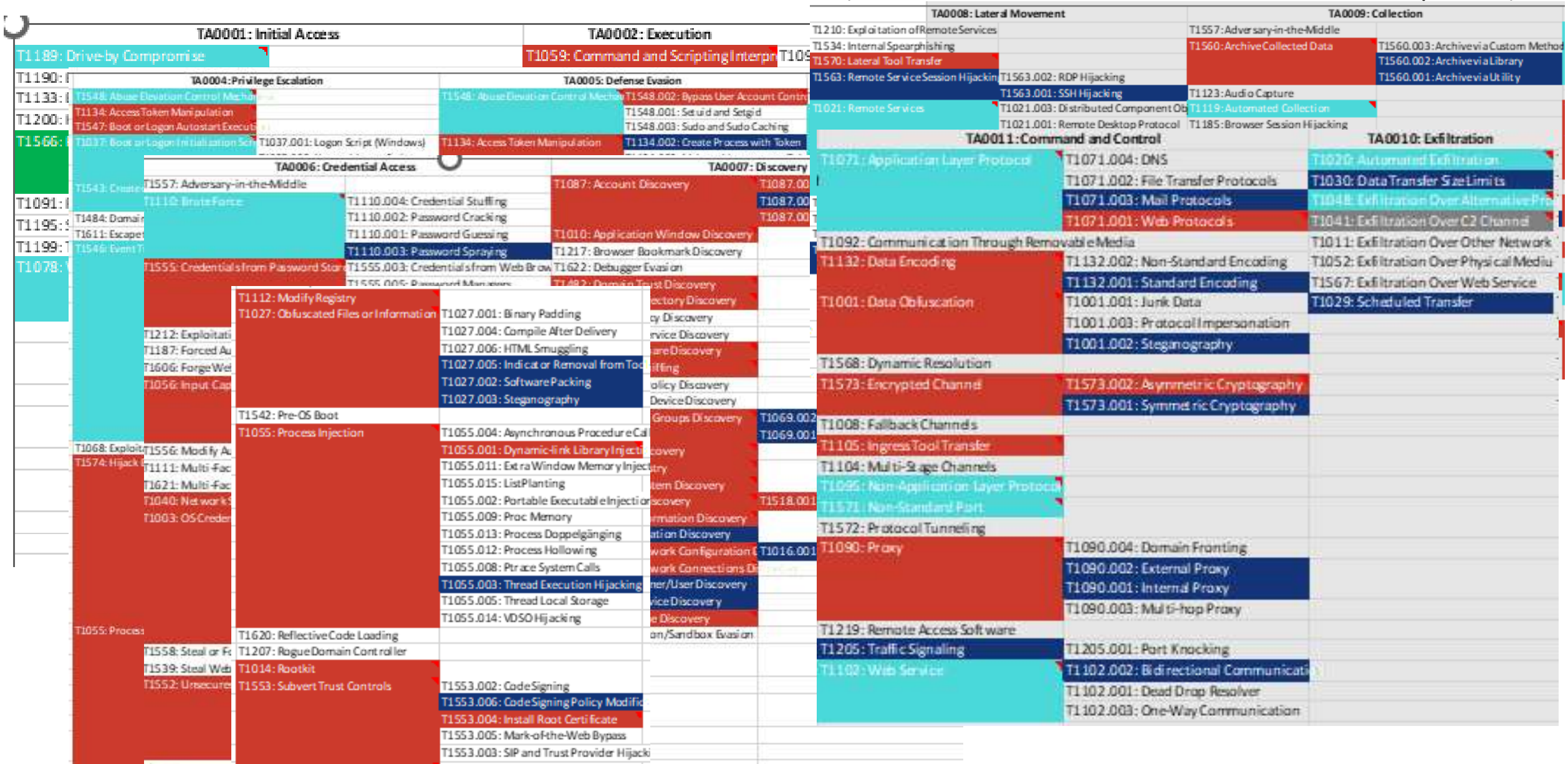
Increased attack sophistication

- Advanced persistent threats
- Encrypted malware
- Zero-day exploits

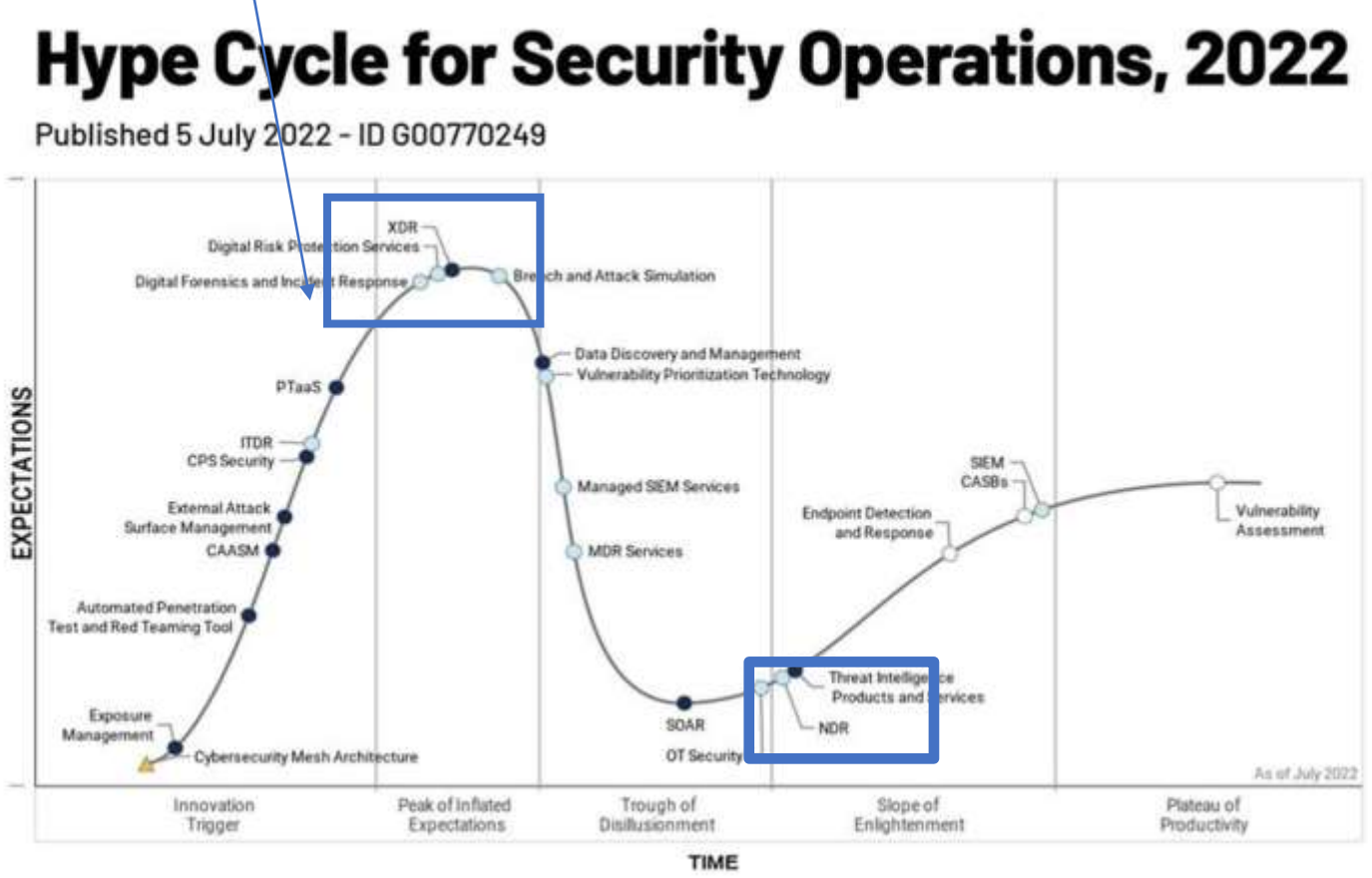
207 DAYS Industry average detection time for a breach → **73 DAYS** Industry average time to contain a breach → **$3.86M** Average cost of a data breach

Source: Ponemon 2020 Cost of a Data Breach Study

How Can We Detect and Respond to All of This
我們如何檢測和應對所有的攻擊分析指標 (MITRE ATT&CK Matrix for Enterprise)?



We Are Here



Gartner

Plateau will be reached:

- <2 yrs.
- 2–5 yrs.
- 5–10 yrs.
- >10 yrs.
- Obsolete before plateau

XDR

Extended detection and response (XDR) is a vendor-specific threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Why This Is Important

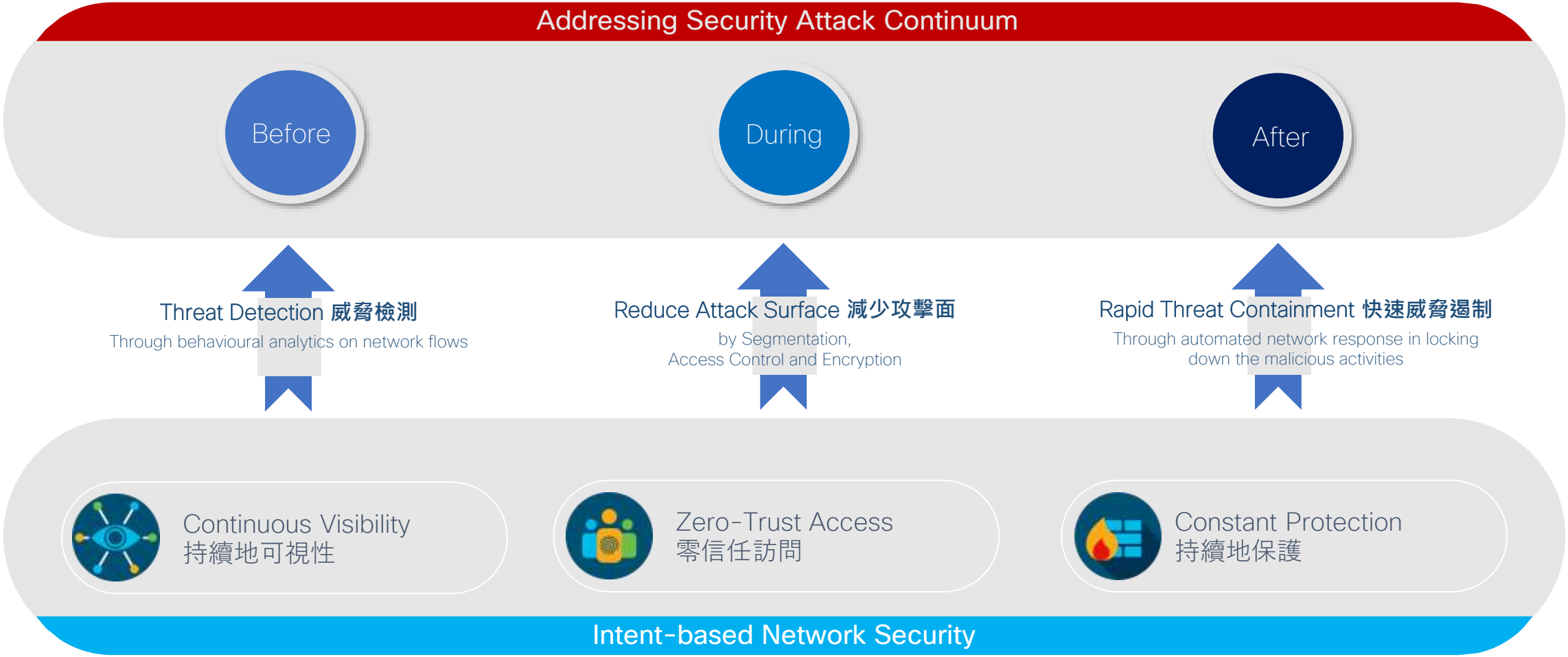
Extended detection and response (XDR) is similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR). However, XDR is differentiated by its level of integration and automation, ease of use, and focus on threat detection and incident response. XDR solution providers must also provide multiple security controls such as EDR, CASB, Firewall, IAM, IDS, directly.

Business Impact

XDR products can reduce the total cost of managing security incidents, improve the productivity of the incident response team and reduce the overall cybersecurity risk posture of the organization.

Intent-Based Network Security 基於意圖的網路安全

Building a Trusted Workplace that aligns and optimise network to security needs



Cisco XDR

Email Security
Cisco Secure Email

EDR (Endpoint Detection & Response)
Cisco Secure Client

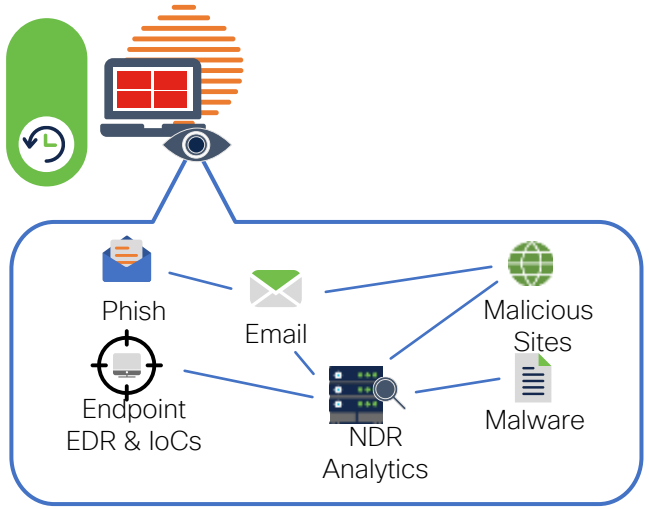
NDR (Network Detection & Response)
Cisco Secure Cloud Analytics
Cisco Secure Network Analytics

ITRM (IT Risk Management)
Cisco Secure Cloud Insights

RBVM (Risk based vulnerability Management)
Cisco Kenna Security

Security platform
Cisco SecureX

SecureX



Unified Visibility
Incident Investigation
Orchestration
Threat Response Automation
Open Integration

What is NDR and Why Do Customers Need It?

[NDR tools] detect suspicious traffic
that other security tools are missing

Benefits:

- Gain comprehensive visibility into network traffic
- Quickly detect advanced attacks and abnormal behavior
- Rapidly respond to and remediate threats found across the network

Use the existing network as a security sensor to find hidden threats, on-prem or in the cloud

使用既有網路設備作為安全偵測工具來發現隱藏在本地或雲端的威脅

未知威脅 Unknown threat Identify suspicious behavior and communications to malicious domains

內部威脅 Insider threat Get alarmed on data hoarding or exfiltration, suspicious lateral movement

加密的惡意軟件 Encrypted malware Use multilayered machine learning to analyze traffic without decryption

違反政策 Policy violation Ensure security and compliance policies set in other tools are enforced

Secure Network Analytics

多層機器學習

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

行為建模

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Global threat intelligence 全球威脅情報

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

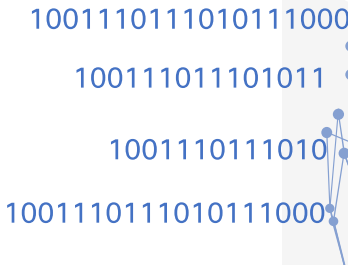
Secure Network Analytics

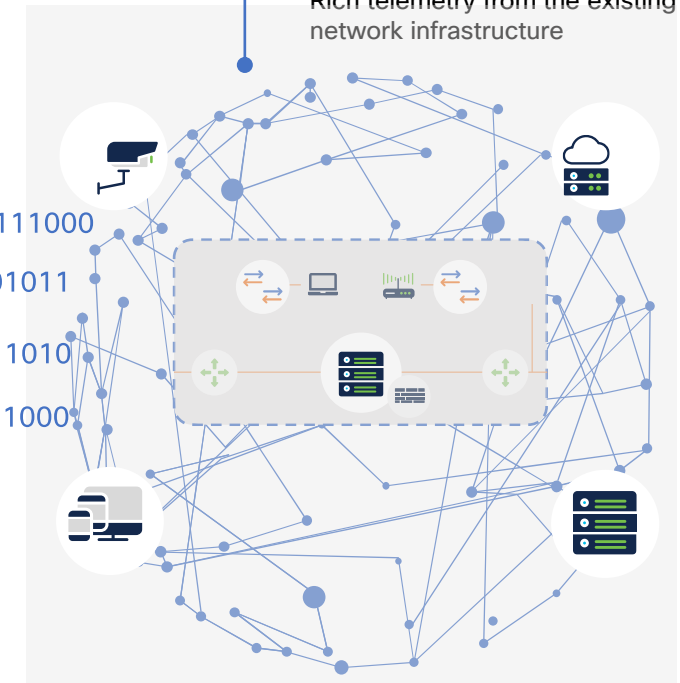
Encrypted traffic analytics 加密流量分析

Malware detection without any decryption using enhanced telemetry from the Cisco devices

Data collection 數據收集

Rich telemetry from the existing network infrastructure

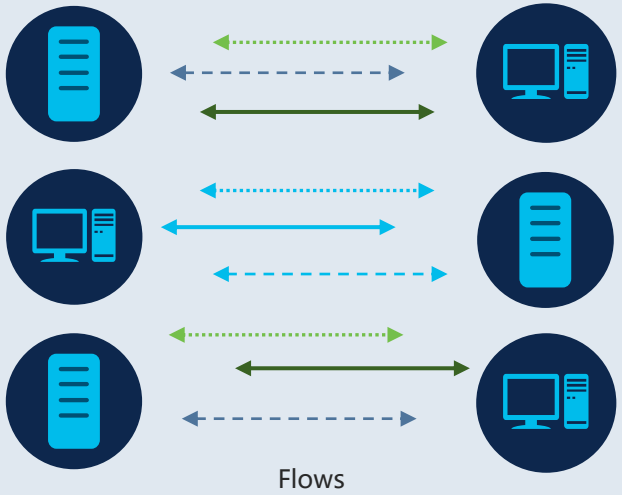




Anomaly Detection Using Behavioral Models
利用行為模型進行異常檢測

Collect & Analyze Data
收集和分析資料

進行數據關聯最佳化並消除重複資料



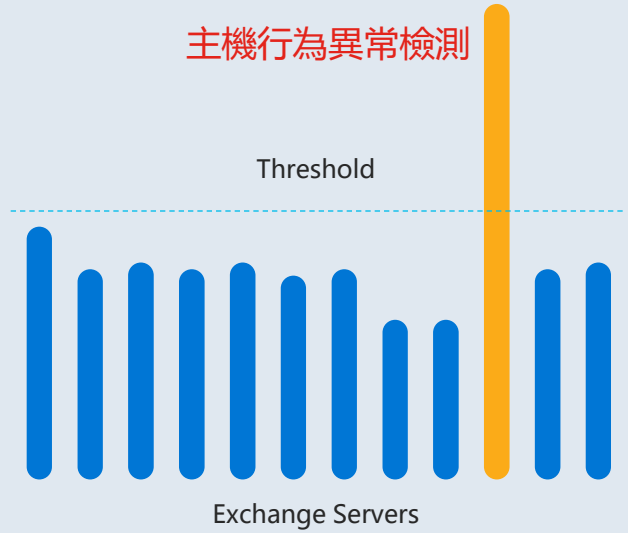
Establish a baseline for normal network behavior為正常網路行為建立基線

檢測異常流量和行為

異常流量和安全事件		
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

Detect abnormal traffic and alert
發現異常網路流量並告警

高風險的告警分類
低誤報告警並提高反應能力



整合全網資訊，實現多雲環境可視化

* Delivered through Advanced Services

Cisco Secure Network Analytics Use Cases
主要使用場景

- Full library of support documentation for gaining visibility, detecting threats, enhancing integration, and increasing your Secure Network Analytics use.
- Use cases are organized by category and across the product lifecycle.
- Find the support you need to customize Secure Network Analytics and integrate it into your security and networking ecosystems.

Compliance
合規

Forensic Investigation
調查取證

Incident Response
事件反應

Network Visibility
網路可視性

Threat Detection
威脅檢測

Cisco Secure Network Analytics 優勢

1. NetFlow deployment for full network visibility, better than only SPAN traffic
2. Combining machine learning, threshold fine tuning and policy customization produces high fidelity results and low false positive
3. Encrypted Traffic Analytics provides malware detection without traffic decryption
4. Working with Cisco Catalyst network switches, Cisco ISE and SecureX provides additional values of enhanced NetFlow for visibility, threat mitigation and response
5. Long term data retention for compliance and forensic (1 year+)

Detection and investigation based on contextual information
基於上下文資訊進行檢測與調查

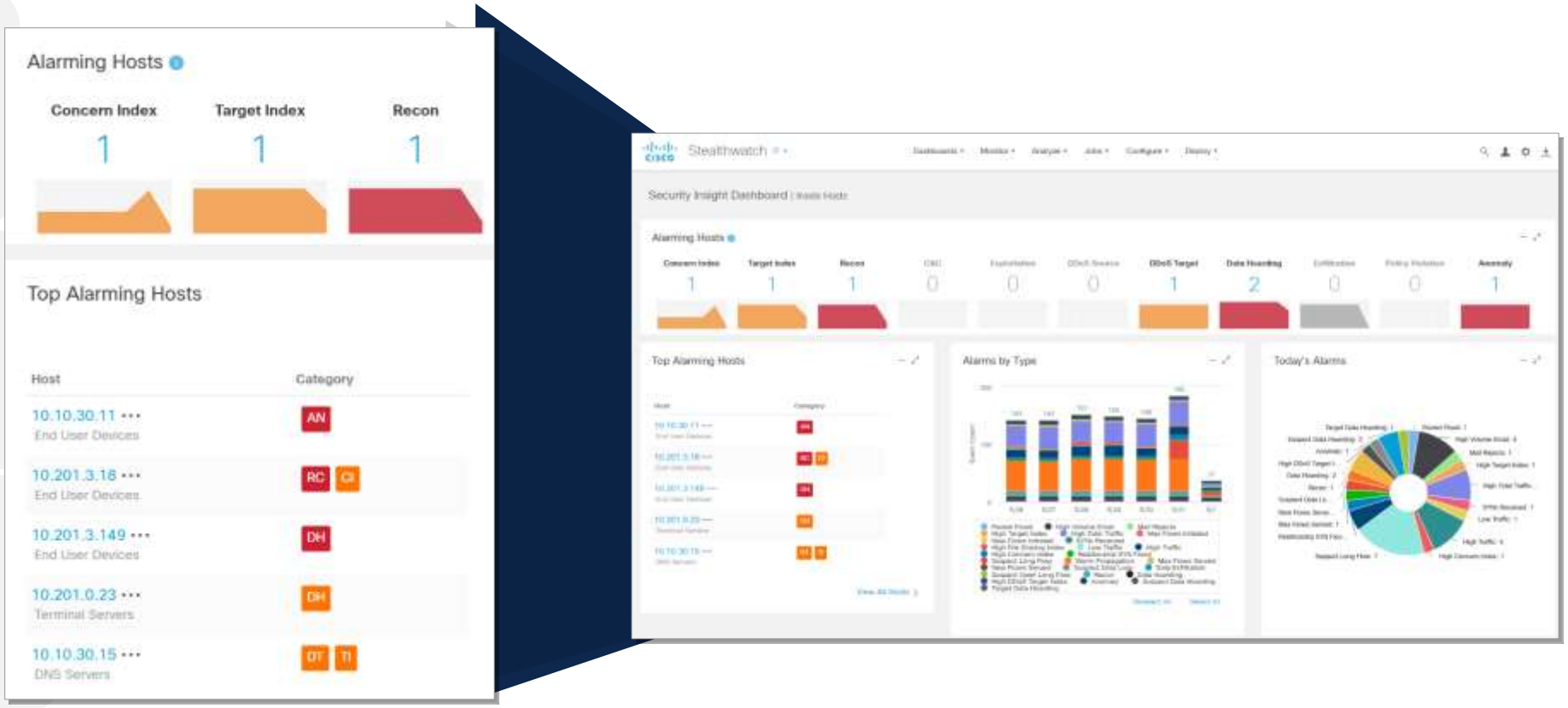
Spot Malicious traffic
快速發現惡意活動報告

information associated with hosts and applications

關聯到主機、應用等上下文信心

Prioritize according to risk

根據風險劃分優先級進行處理



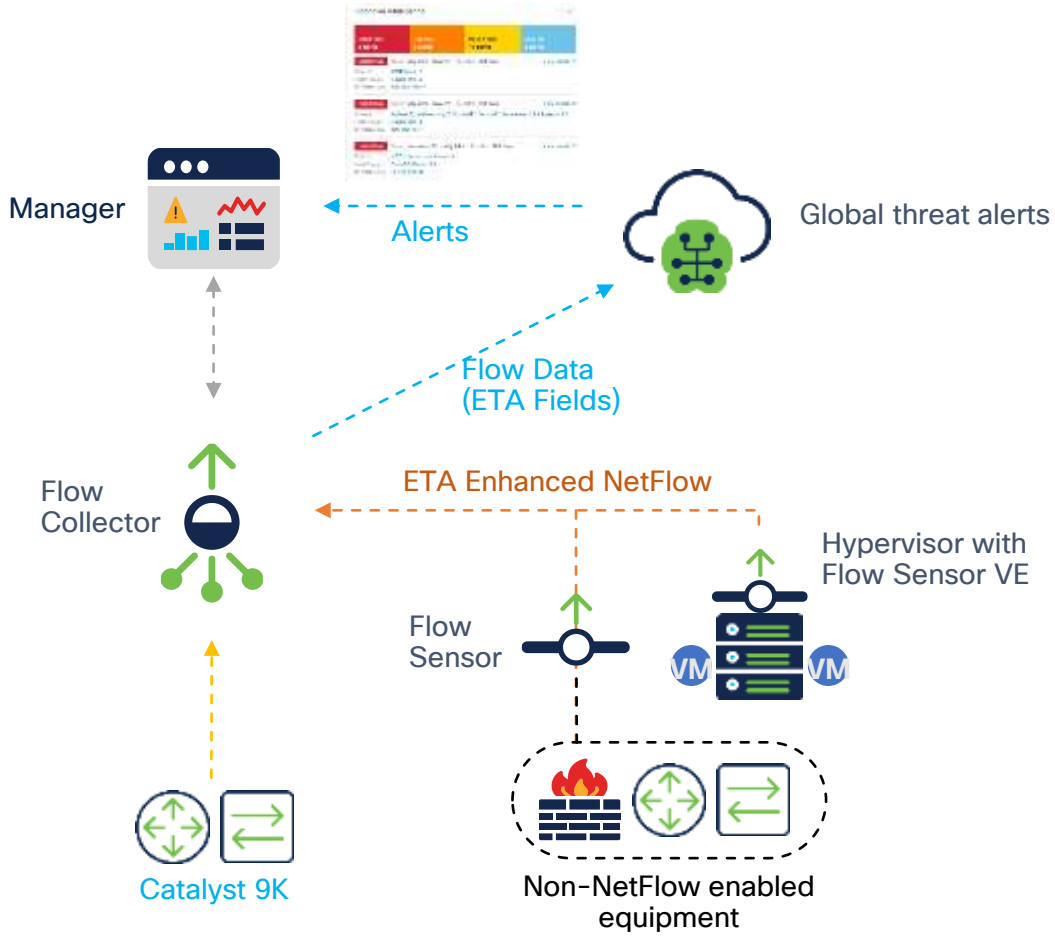
cisco Engage Taipei

Encrypted Traffic Analytics Increases Visibility
加密流量分析提高可視性

Cryptographic Audit

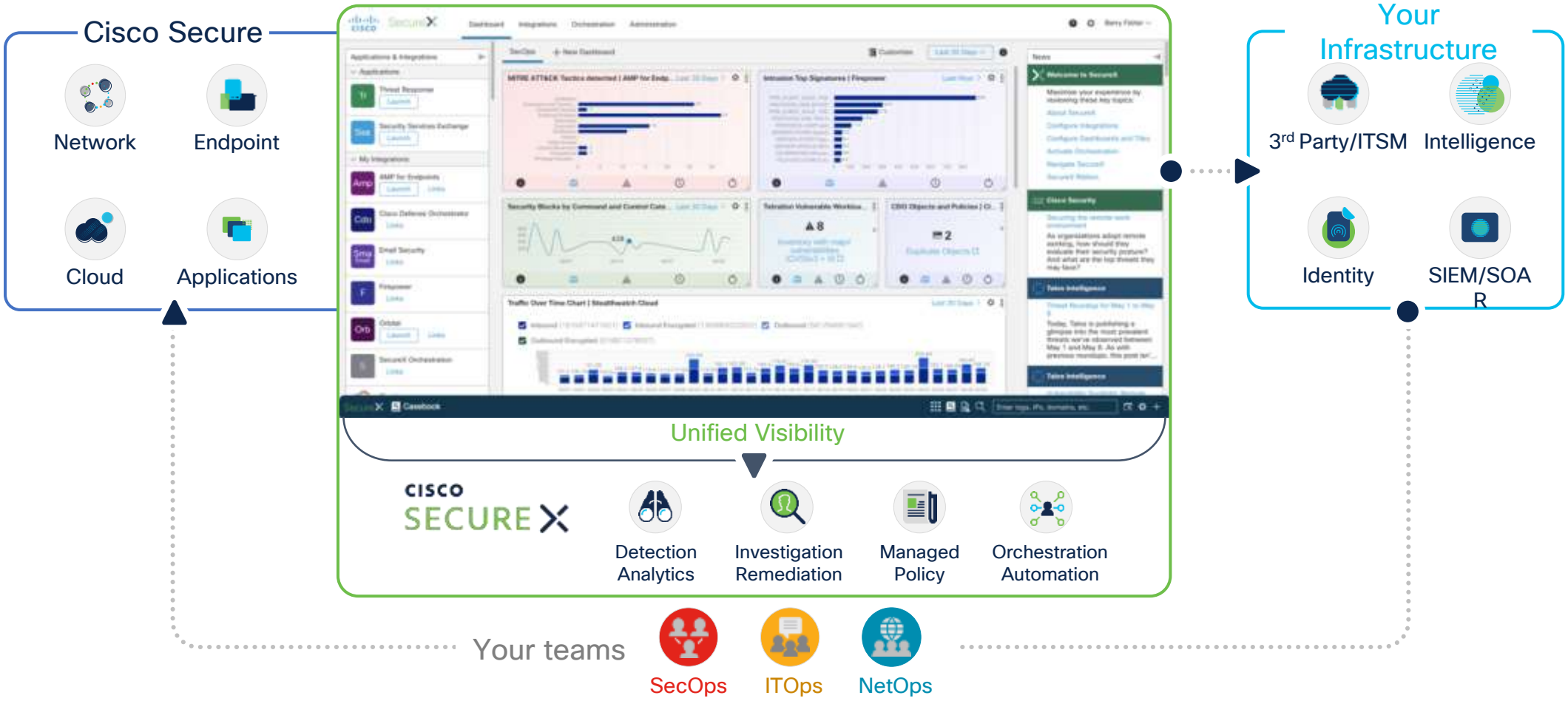
Malware Detection within Encrypted Traffic

- Cisco Catalyst network switches feed enhanced NetFlow to Flow Collector
- Meta data sent to the cloud through a secure channel
- Malware detection analysis is done in the cloud, cryptographic audit is done on-premises



SecureX – XDR

A cloud-native, built-in platform experience within Simplicity, Visibility and Efficiency



Secure Network Analytics & SecureX threat response

End to end visibility

Network anomaly detection

Security analytics

Secure
Network Analytics

Alarms

Security events

Casebook

Investigation

Orchestration

SecureX
threat response

Threat intelligence

File and network IoCs

Investigation

Orchestration

Agentless detection

Secure Network Analytics network-based visibility and security analytics will enrich SecureX threat detection and response with agentless behavioral and anomaly detection capabilities

Correlate, enrich, and resolve

SecureX threat response integrations with other sources of global threat intelligence and internal visibility, will affirm and enrich Secure Network Analytics findings with confirmed threat intel and local sightings. Integrations with Cisco control devices provide two-click mitigation and resolution

Demo - booth


cisco
The bridge to possible
Thank you
cisco Engage Taipei

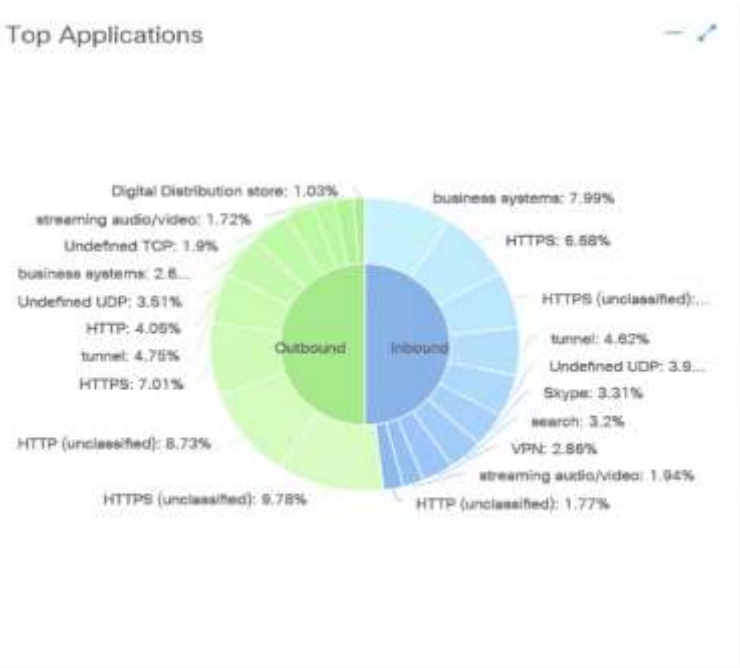
CISCO Engage Taipei

Use Cases Screenshot
主要功能使用場景

一、Monitor and manage traffic by application group

按照應用分組監控和管理流量

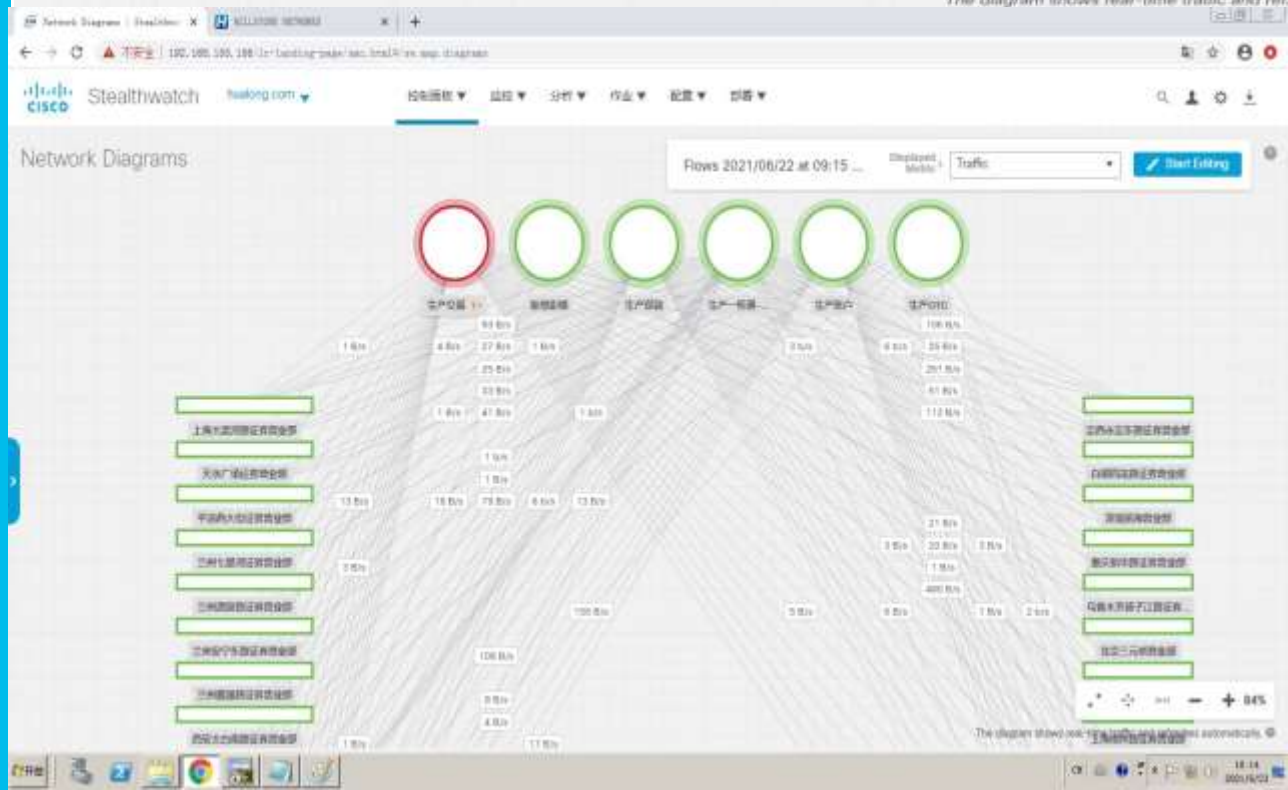
- 根據IP位址範圍定義主機分組，把網路流量關聯到業務和應用
- 按照應用分組可視化呈現
  - 流量分布情況
  - 硬用訪問趨勢
  - 異常流量告警



二、 Application access real-time traffic monitoring view

應用訪問即時流量監控可視圖

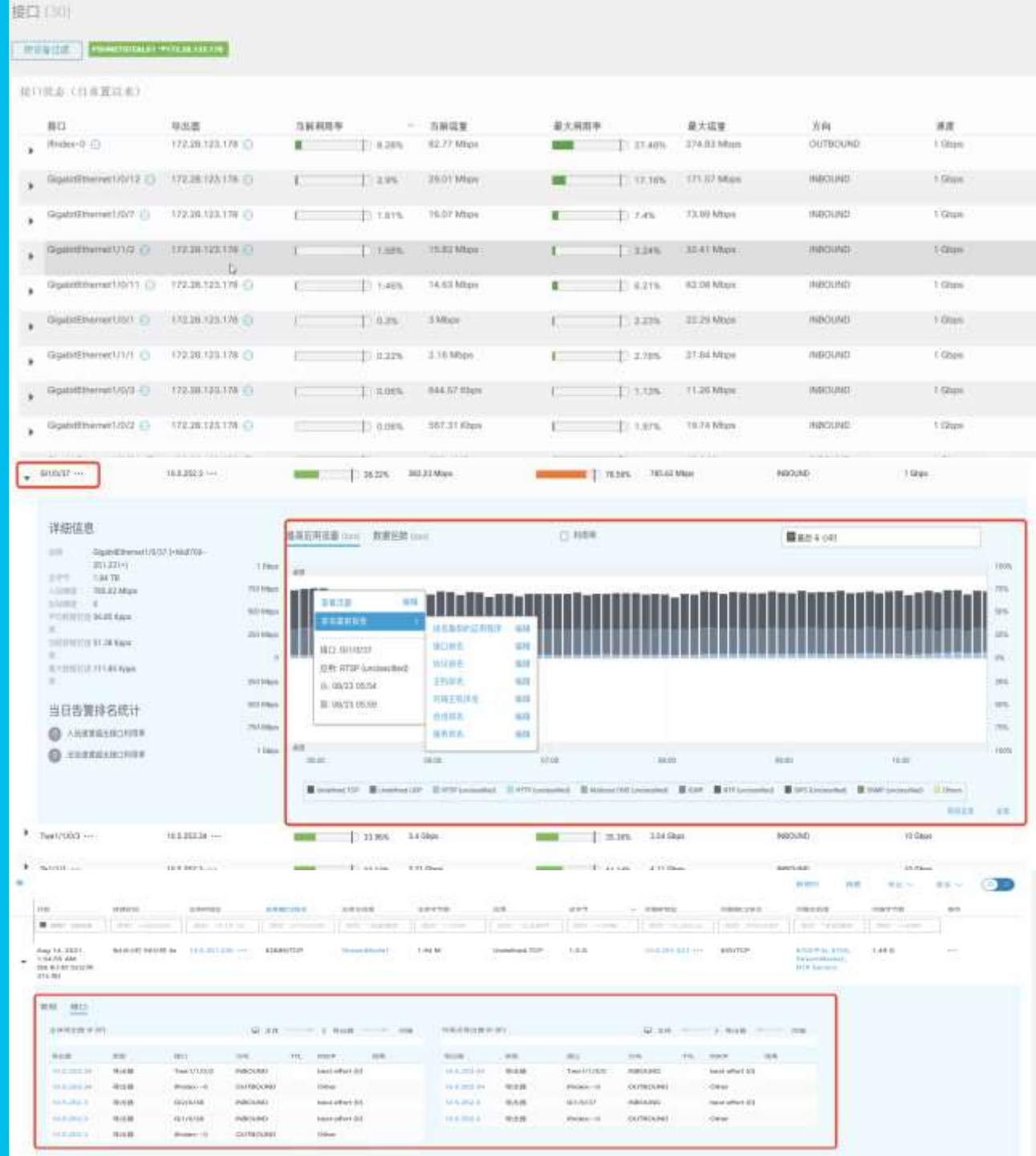
- 根據流量查詢結果，按照需要自動生成應用訪問流量監控可視圖
- 監控可視圖實現
  - 應用分組的訪問關係
  - 即時的流量分布情況
  - 分組之間異常流量發現（機器學習）
  - 快速調查



三、 Network device interface traffic analysis

網路設備接口流量分析和調查

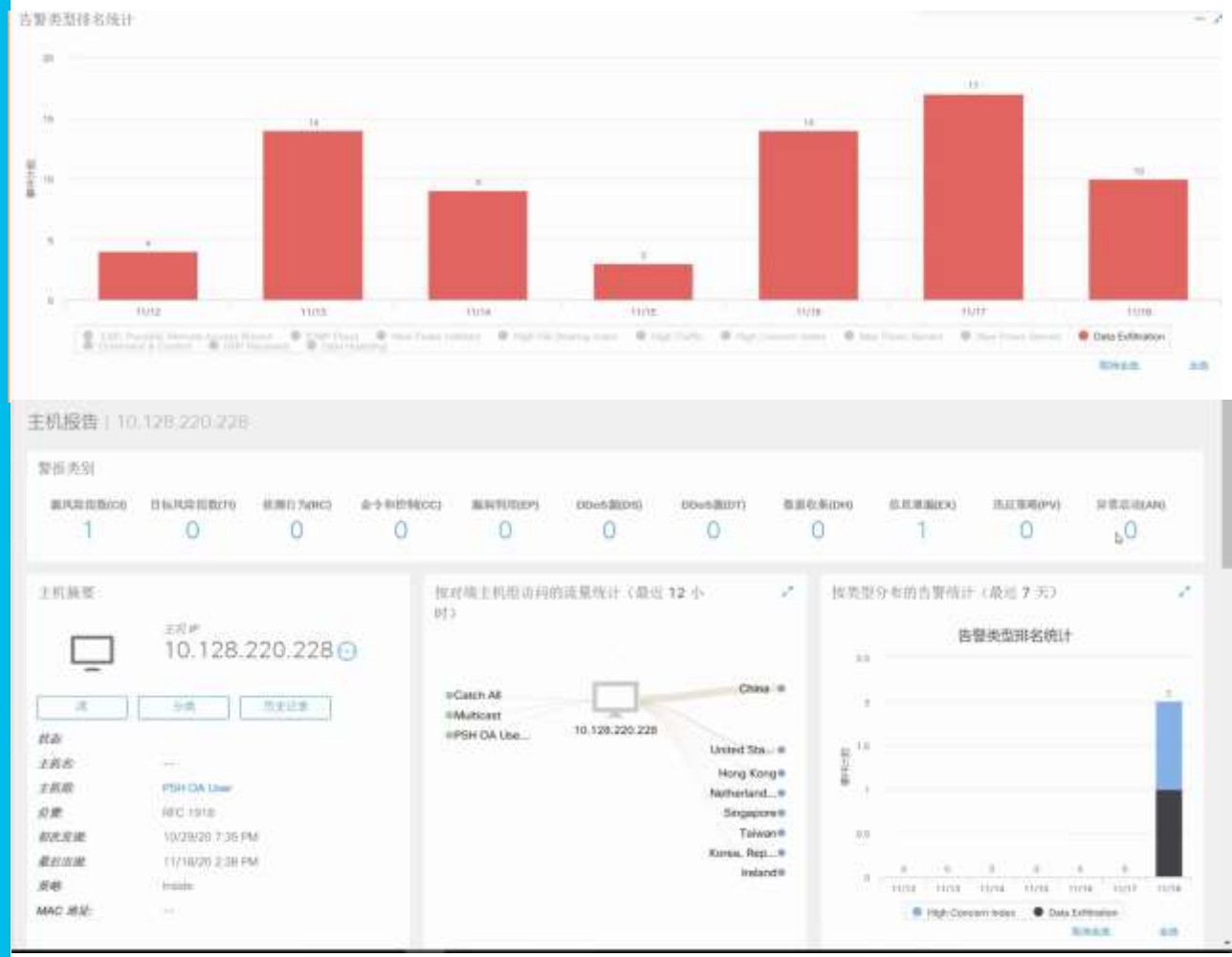
- 設備接口利用率分析（歷史、平均、當前）
- 每個接口流量按照應用類型分布和統計
- 接口流量異常时，快速調查流量Top排名的IP和Session



四、 Early warning and investigation of abnormal network traffic

網路流量異常告警和調查

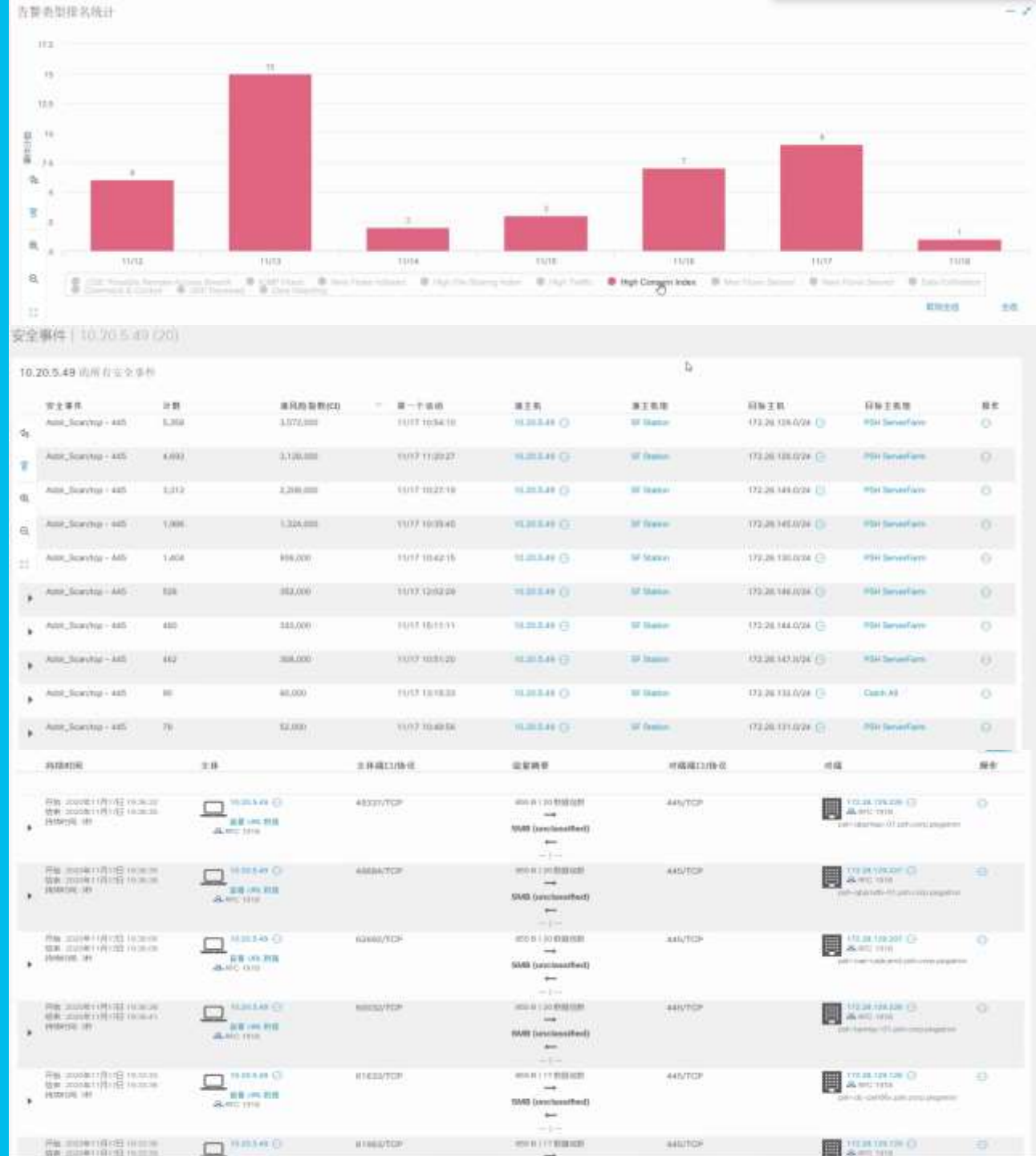
- 主要異常網路流量發現：
  - 大流量告警
  - 資料收集告警
  - 資料外傳告警
- 快速調查分析
  - TOP的IP排名
  - TOP的Session排名
  - TOP的服務、端口排名
  - 關聯到應用分组和網路設備接口



五、 Early warning and investigation of intranet security threats

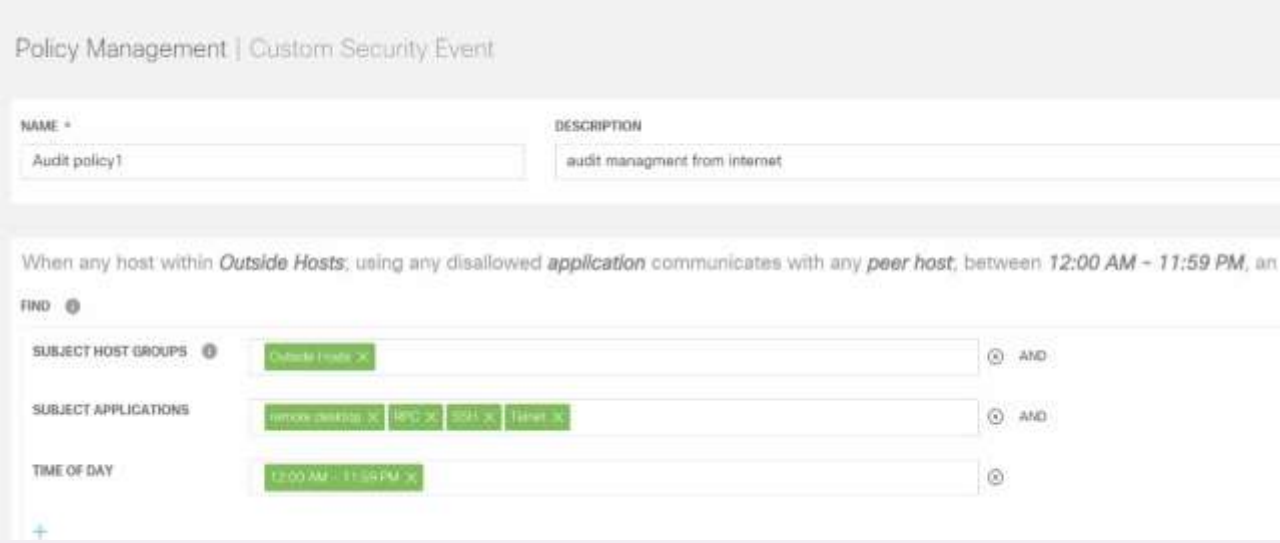
內網安全威脅告警和調查

- 主要安全威脅發現
  - 掃描探測
  - 駭客控制
  - 勒索軟體
  - 資料外洩
  - 違規存取
- 快速調查分析
  - 自動告警
  - 快速定位和追踪IP位址
  - 縮短反應時間



六、Forensics
歷史資料保存、回溯和稽核

- Netflow保存時間長
- 歷史問題回溯和調查
- 合規稽核的要求



Database Storage Statistics

Capacity

	Average	Worst Case
Capacity in Days	482	60
Remaining Days	145	17
Bytes Per Day	4.61G	12.31G

Flow Data Summary

			Rows			Bytes		
Data	Days	Containers	Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	337	377	16.78G	49.8M	137.19M	500.58G	1.49G	4.35G
Flow Interface Details	8	36	812.53M	101.57M	251.3M	24.67G	3.08G	7.69G
Total	337	413	17.59G	151.36M	388.49M	525.24G	4.57G	12.04G

Logical diagrams for monitoring metrics
為重要的監控指標創建邏輯可視監控圖

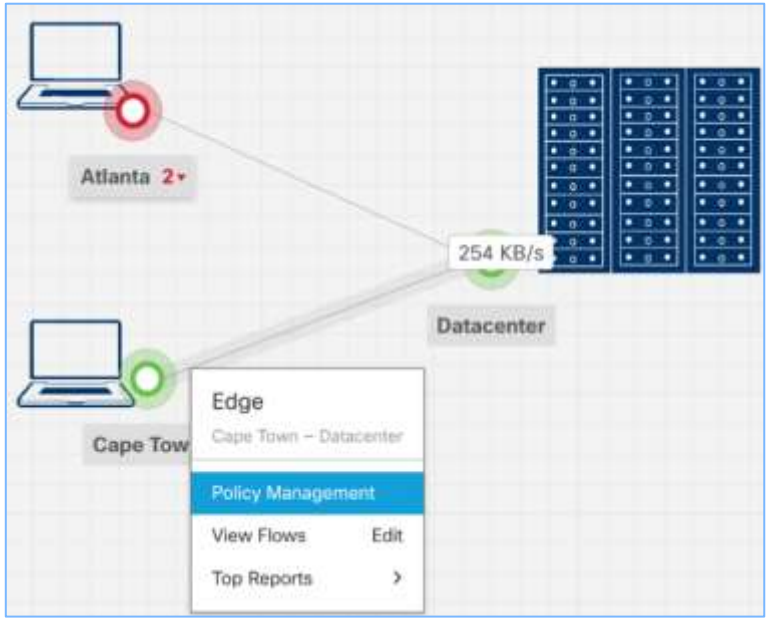
觸發告警

基於主機分組監控異常流量、安全威脅告景，方便調查

網路訪問指標

應用分組流量、頻寬、效能監控

訪問關係策略



圖像化的分組訪問關係策略