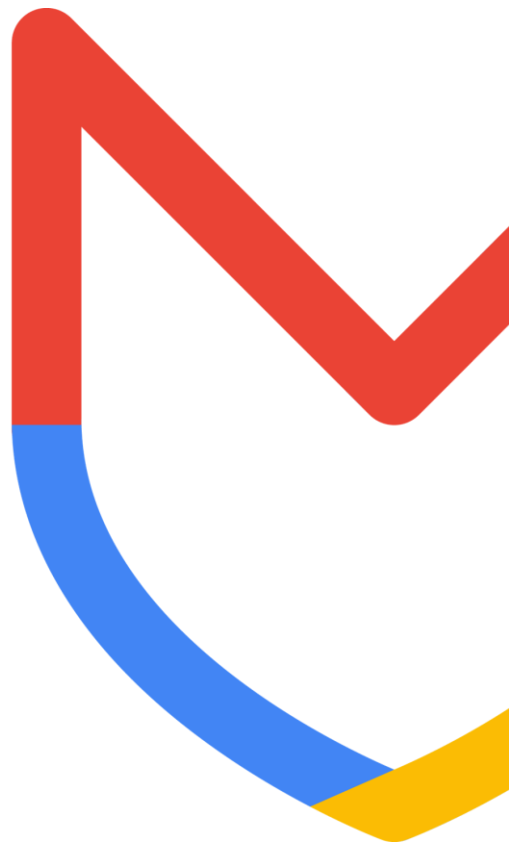




# Google Cloud Security Operations

## 強化數位資安韌性

Patrick Chiu 邱上峯  
Security Architect, Google Cloud Security



# Dwell time 全球停留時間

攻擊者被發現之前存在於受感染環境中的天數。

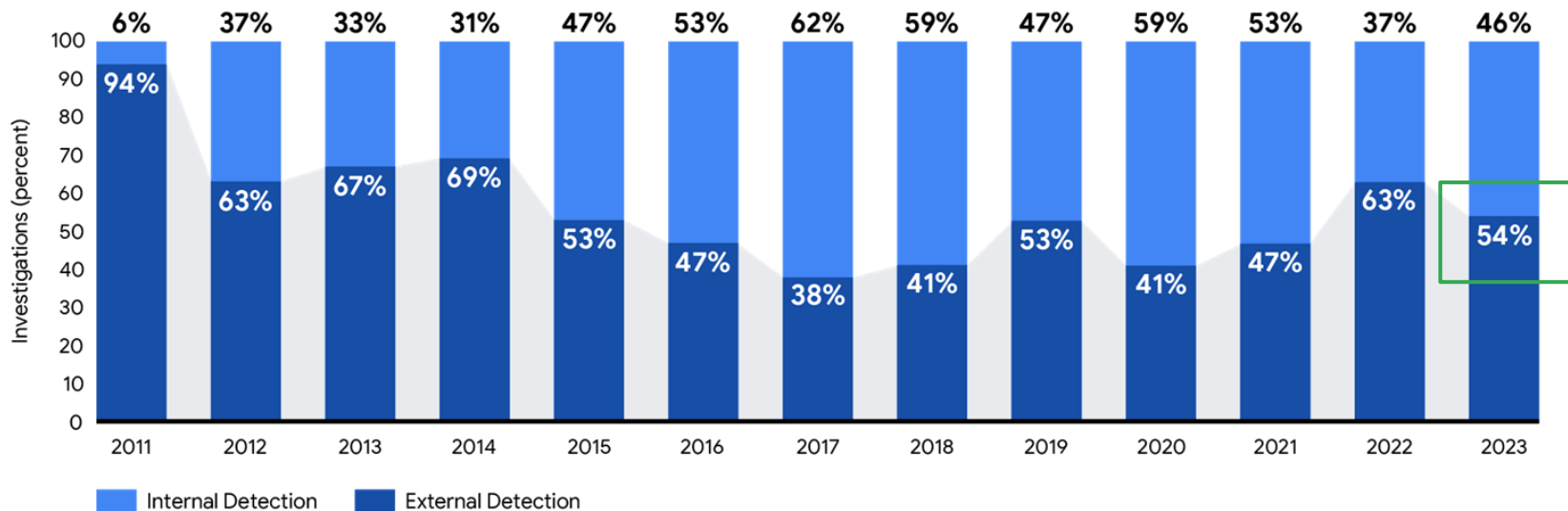
中位數表示按大小排序的資料集中點的值。

**10 days** in 2023

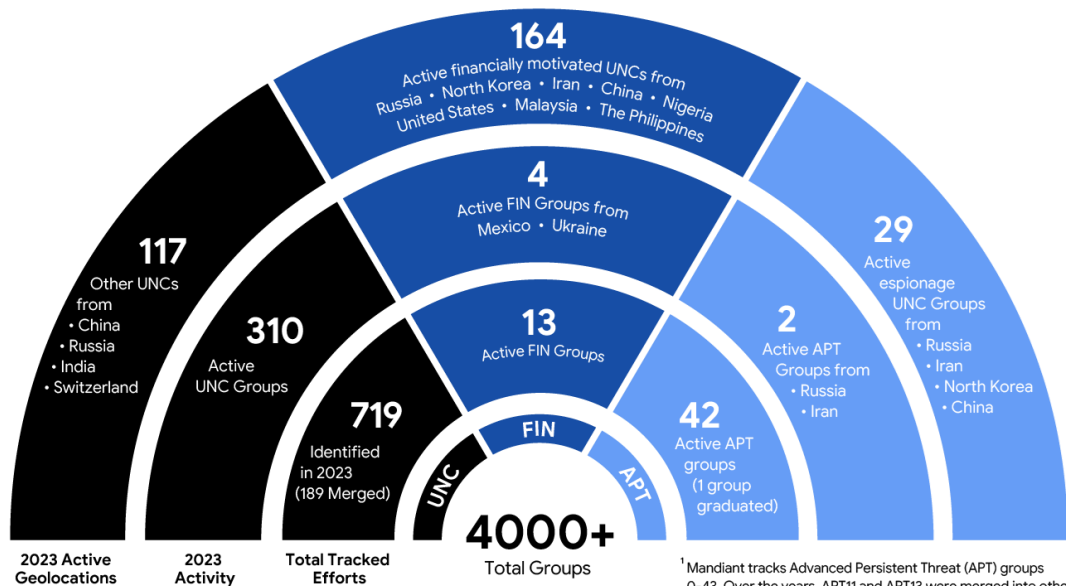
Down from 16 days in 2022

2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
416	243	229	205	146	99	101	78	56	24	21	16	10

# 全球偵測到入侵攻擊的來源分析



# 2023 全球威脅組織活動狀況



<sup>†</sup> Mandiant tracks Advanced Persistent Threat (APT) groups 0-43. Over the years, APT11 and APT13 were merged into other groups and subsequently deprecated resulting in 42 APT groups actively tracked by Mandiant.

**719**

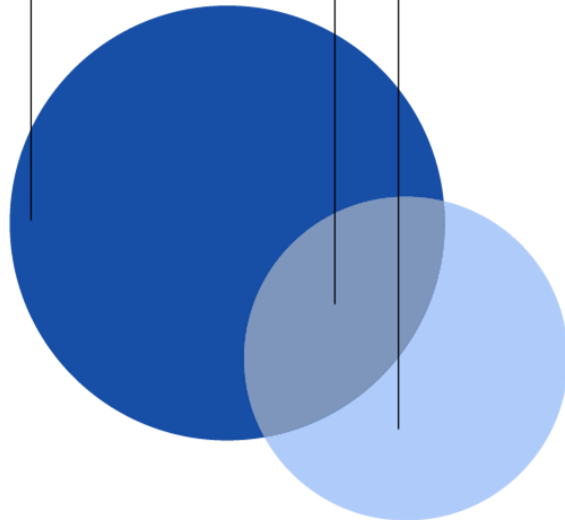
Newly Tracked  
Threat Groups

**316**

Observed  
Threat Groups

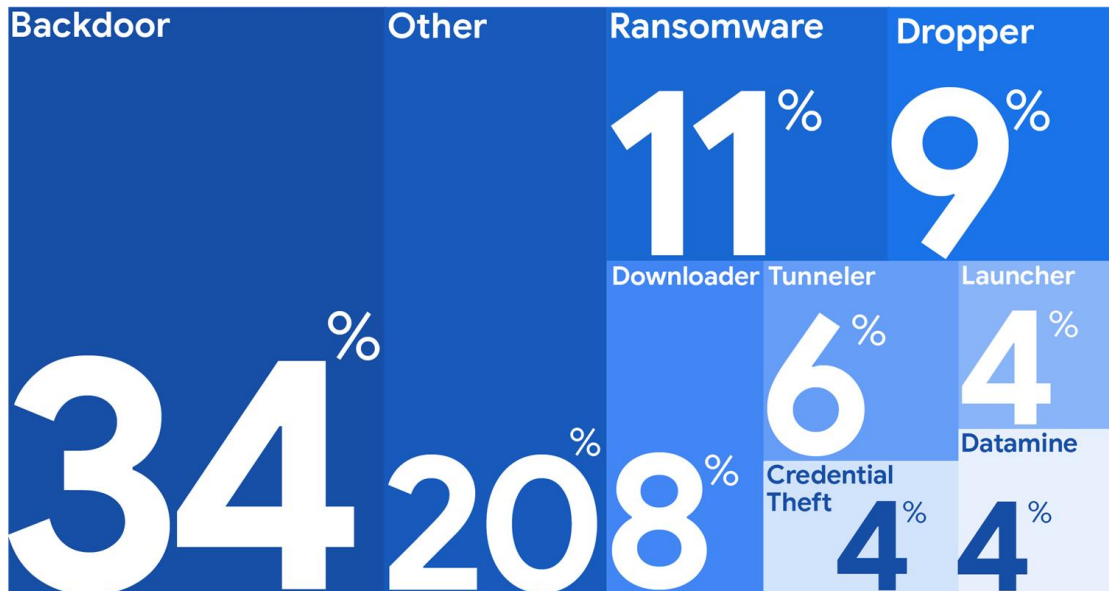
**220**

Newly Tracked and  
Observed Threat Groups



# Malware 分類和家族

Observed Malware Families by Category, 2023



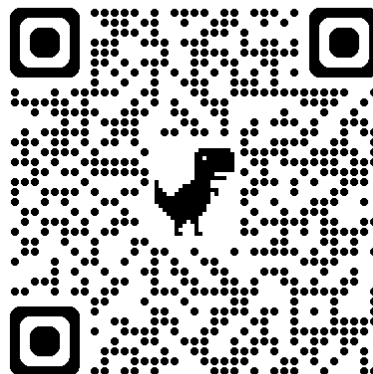
## Most frequently seen malware families:

- BEACON (Backdoor)
- ALPHV (Ransomware)
- LEMERLOOT (Web Shell)
- SYSTEMBC (Tunneler)
- LOCKBIT (Ransomware)

# M-Trends 2024 Special Report

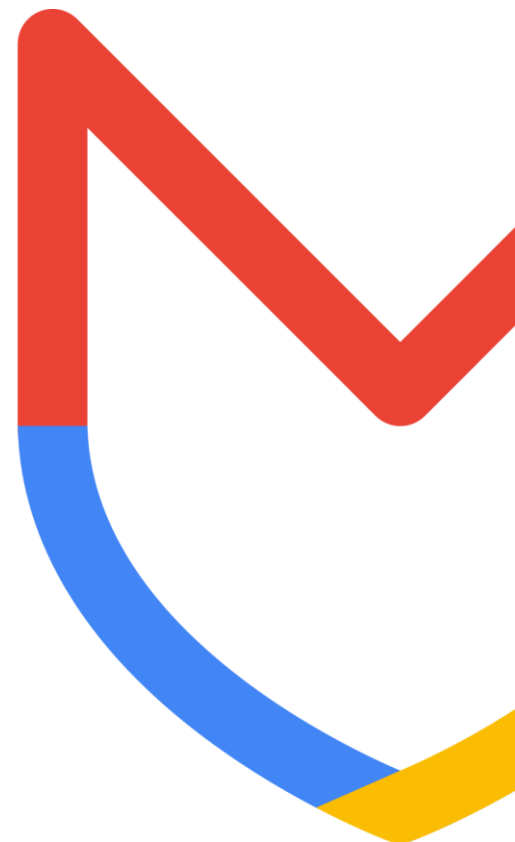
Insights into today's top cybersecurity trends and developments

Executive Briefing Presentation



Google Cloud  
Security

Proprietary & Confidential



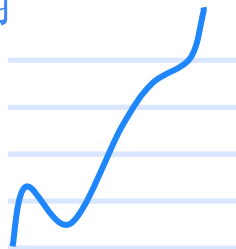
# Cybersecurity today 資訊安全在企業端面臨的挑戰

Proprietary + Confidential

推陳出新

## 新型威脅

資料外洩  
勒索病毒  
DDoS攻擊  
網頁置換  
容器安全  
軟體安全供應鏈



持續增加

## 日常維運

漏洞管理  
系統升級  
規則調校  
事件分析  
基礎設施



供不應求

## 專業資安人員

系統架構  
安全開發  
網路安全  
資安監控  
法遵合規

供應 需求

7x  
increase

781 data breaches in 2012 totaling \$146M. 6,000 last year totaling \$6T. <sup>2</sup>

13x  
increase

2,000 cybersecurity companies in 2012 to 26,000 today. <sup>1</sup>

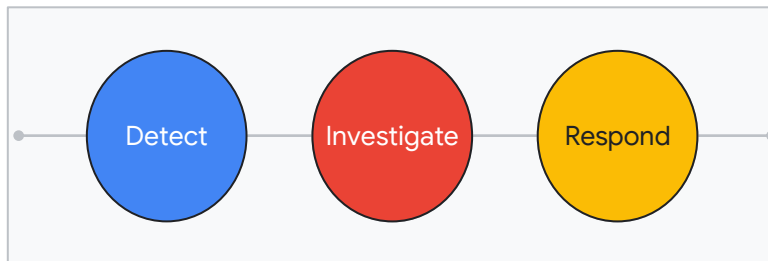
2x  
needed

Up from 1.5M unfilled cybersecurity jobs in 2012 to 3.5 million today. <sup>3</sup>

# 一個人工智能與情報驅動的 威脅檢測、調查與應對 整合的資安管理平台



Google Security Operations Platform



Mandiant  
Managed  
Defense



AI (Gemini + SecLM)



Applied threat intelligence

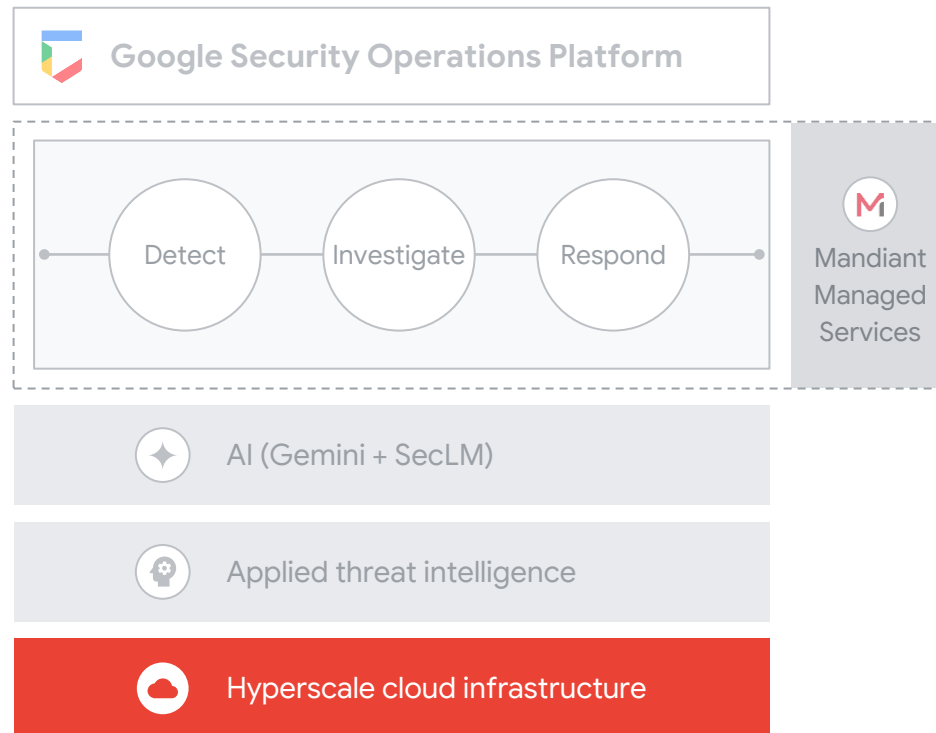


Hyperscale cloud infrastructure



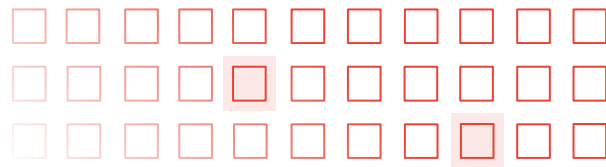
# Hyperscale cloud infrastructure

## 超大規模雲端基礎設施



# 無限制擴展容量

告別傳統的數據量和效能妥協



## Scale infinitely

使用與 **Google 核心服務** 相同的基礎架構搭建的解決方案，分析任意容量的遙測數據。



## Detect more

自動豐富**所有**事件，每個規則支持高達30,000個警報（競品上限的200倍），大幅提升監控覆蓋率。



## Search quickly

跨越 **PB** 級數據的亞秒級、上下文豐富的搜索，搜索結果提升 **25 倍**。



## Retain longer

全部日誌**12個月熱資料**保存，挖掘更多潛在威脅。

**25x**

更多的搜索結果

**200x**

更多的告警  
在單一規則上

**4x**

更長的資料  
保存時間

# 處理日誌的難題...

Proprietary + Confidential

## Palo Alto Networks Firewall

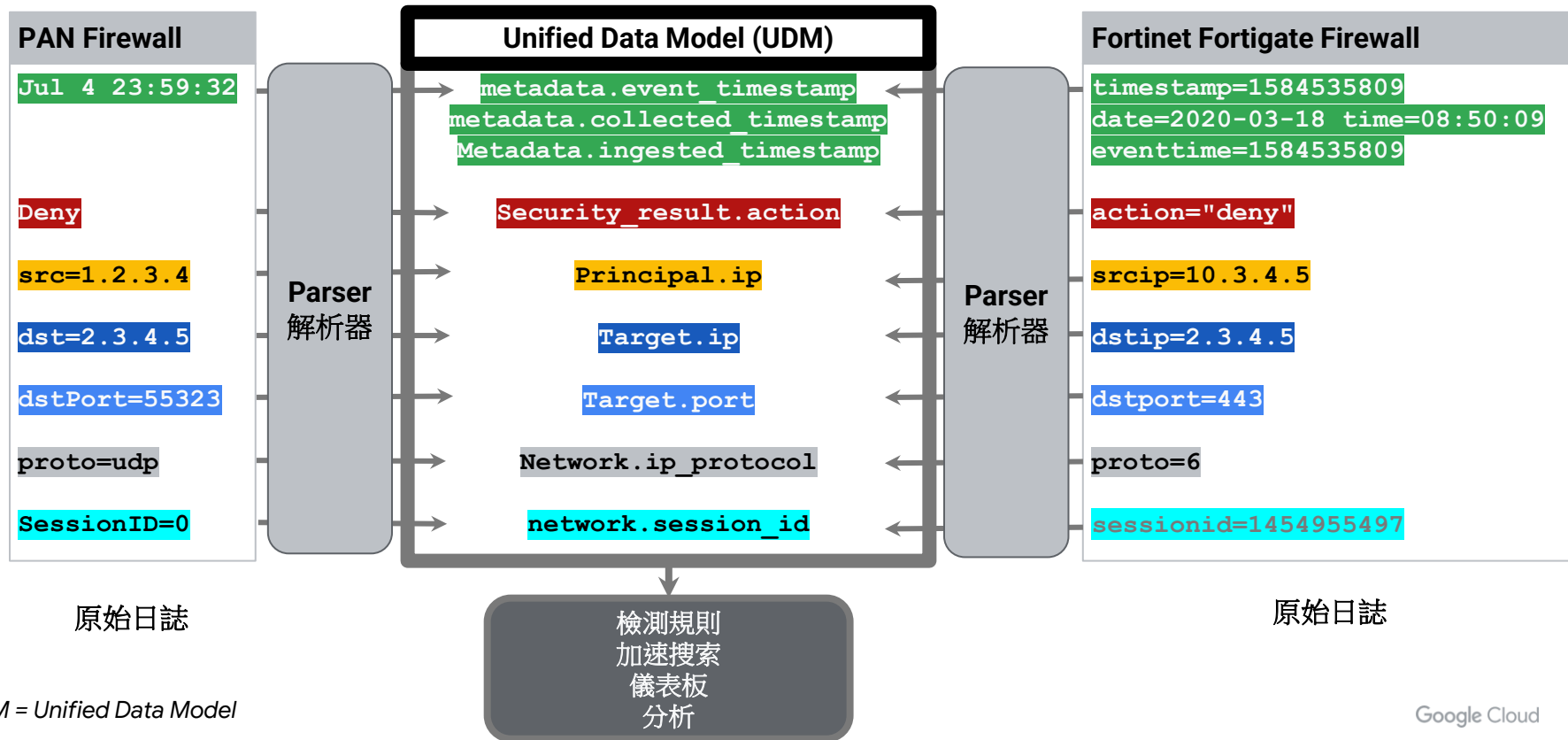
```
<14>Jul 4 23:59:32 ASBC101A005FW04
LEEF:1.0|Palo Alto Networks|PAN-OS Syslog
Integration|4.0|deny|cat=TRAFFIC|src=1.2.3.4|
dst=2.3.4.5|srcPort=389|dstPort=55323|proto=u
dp|usrName=|SerialNumber=642902999105|Type=TR
AFFIC|Subtype=drop|srcPostNAT=10.20.30.46|dst
PostNAT=10.20.30.46|RuleName=interzone-
default|SourceUser=|DestinationUser=|Applicat
ion=not-
applicable|VirtualSystem=vsys1|SourceZone=cor
p|DestinationZone=intlWan|IngressInterface=ae
8.421|EgressInterface=|LogForwardingProfile=W
SI-
Logforwarding|SessionID=0|RepeatCount=1|srcPo
stNATPort=0|dstPostNATPort=0|Flags=0x0|totalB
ytes=255|totalPackets=1|ElapsedTime=0|URLCate
gory=any|dstBytes=0|srcBytes=255|SessionEndRe
ason=policy-
deny|PacketsSent=1|PacketsReceived=0
```

## Fortinet Fortigate Firewall

```
<189>logver=60 timestamp=1584535809
tz=\"UTC-4\" devname=\"ACME_FG800D\"
devid=\"FG800D3916801392\" vd=\"root\"
date=2020-03-18 time=08:50:09
logid=\"0000000013\" type=\"traffic\"
subtype=\"forward\" level=\"notice\"
eventtime=1584535809 srcip=10.3.4.5
srcport=55920 srcintf=\"VLAN220\"
srcintfrole=\"lan\" dstip=2.3.4.5 dstport=443
dstintf=\"wan1\" dstintfrole=\"wan\"
sessionid=1454955497 proto=6 action=\"deny\"
policyid=0 policytype=\"policy\"
service=\"HTTPS\" dstcountry=\"United States\"
srccountry=\"Reserved\" trandisp=\"noop\"
duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0
appcat=\"unscanned\" crscore=30
craction=131072 crlevel=\"high\"
```

防火牆日誌本質是一樣的，但這些日誌事件格式卻大不相同！

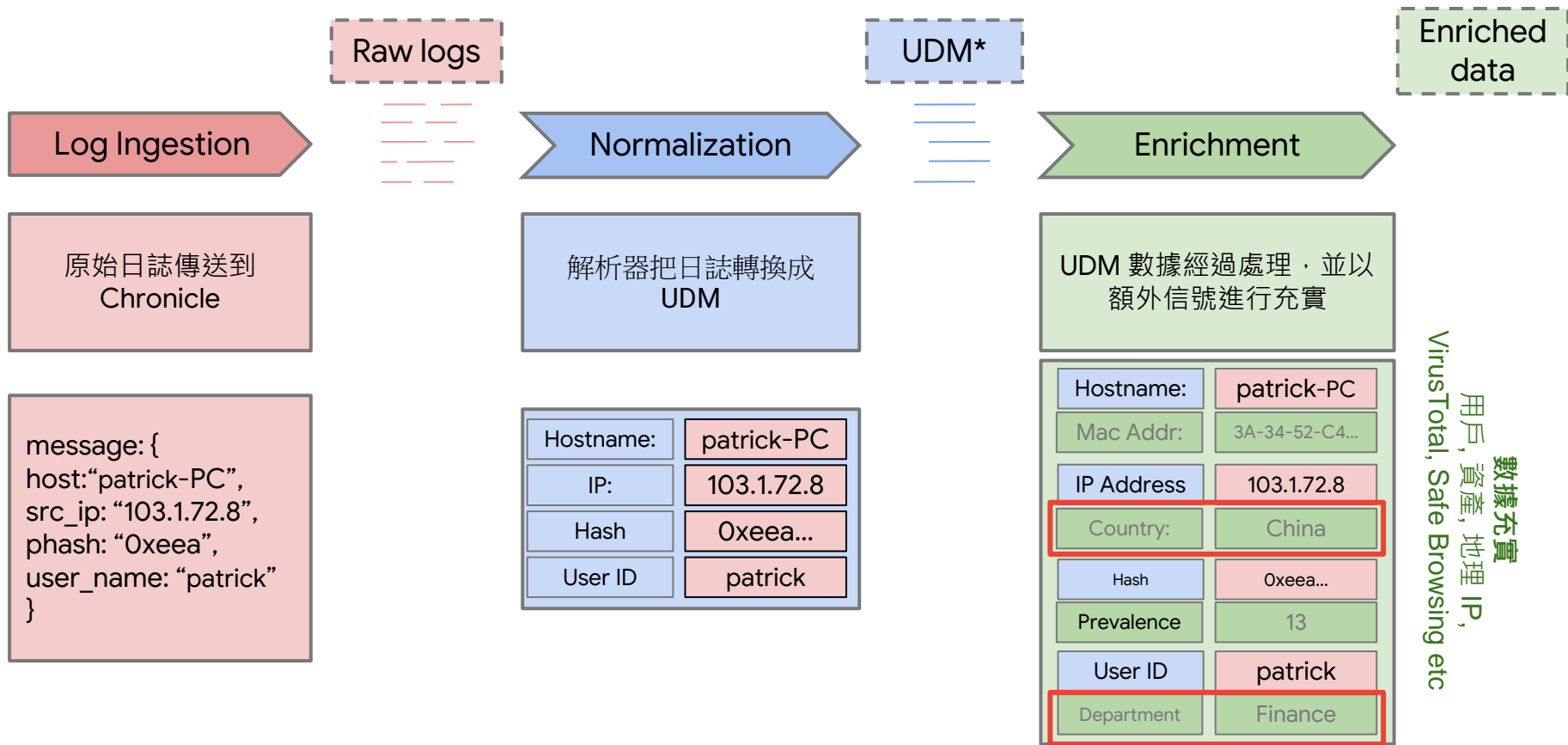
# 正規化



\* UDM = Unified Data Model

# 從原始日誌到深化洞察

Proprietary + Confidential

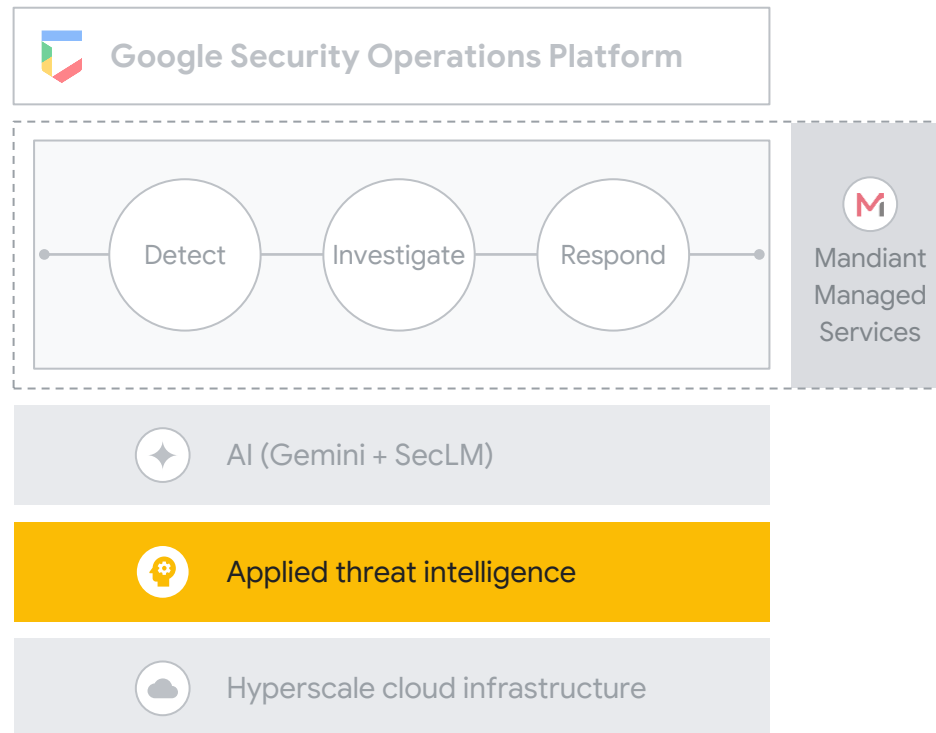


\* UDM = Unified Data Model

# Applied threat intelligence

應用威脅情報

VirusTotal &  
Mandiant TI





# Google Threat Intelligence

領先市場的威脅情資能力

1000次以上

每年IR事件調查次數

3萬份以上

威脅情資報告

430億

每日掃描檔案數量

50億以上

受Google保護的裝置  
數量

+500

資安研究人員和情報分  
析師

20萬小時

每年用於應對攻擊事件  
處理的時數

+300

隨時追蹤威脅行為者

3.6 億

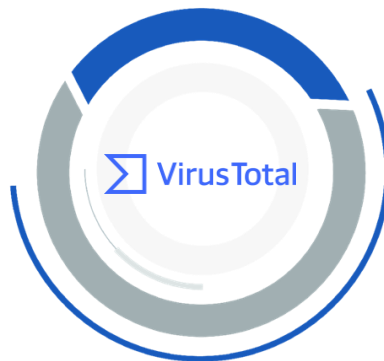
資料集中的文件

20億以上

Gmail 用戶受Google  
保護



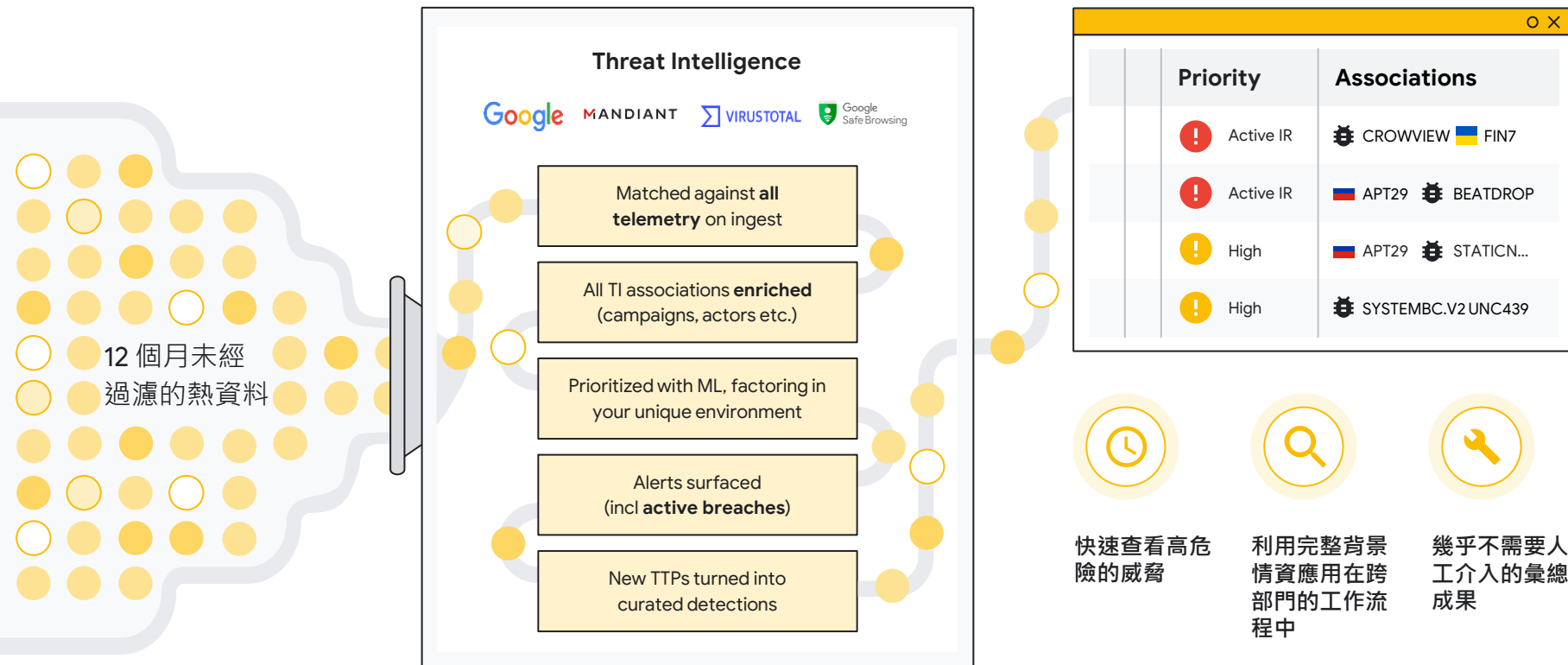
+



+

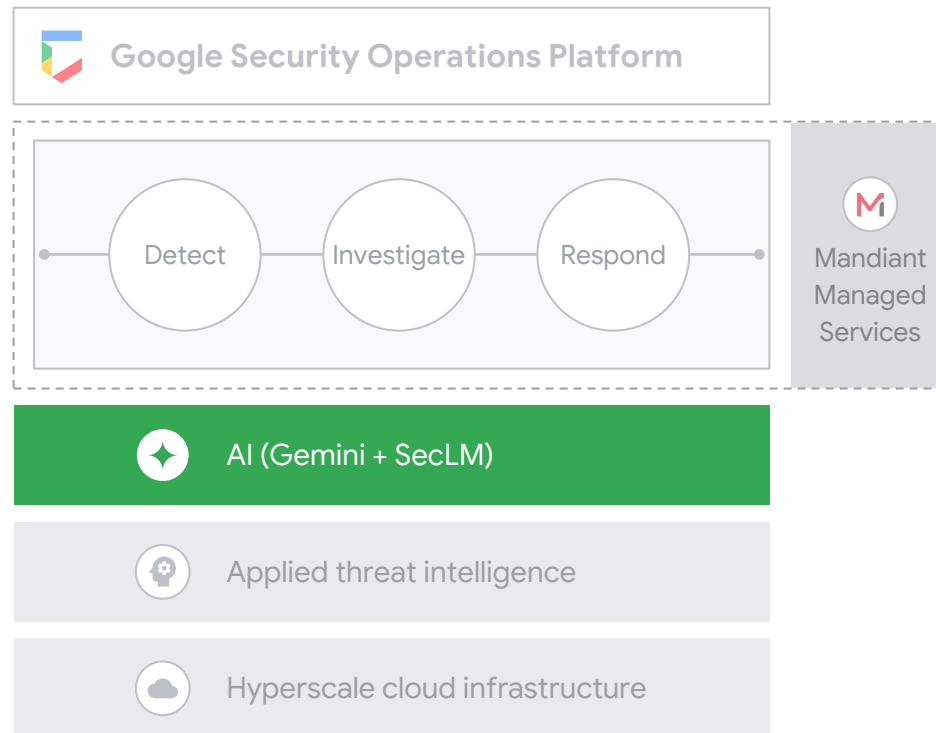


# 威脅情資如何在 Google SecOps 中發揮作用





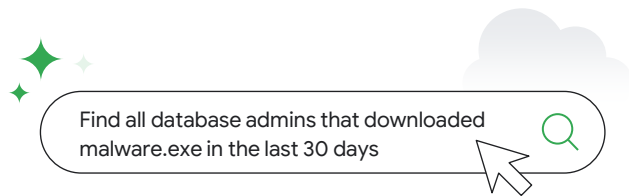
# Generative AI 全面應用生成式 AI



# Gemini in Security Operations

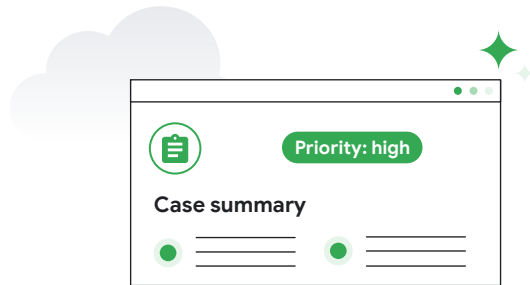
## Investigate 調查

提升您的團隊能力，並透過自然語言搜尋和互動式 AI 聊天機器人快速獲得答案。



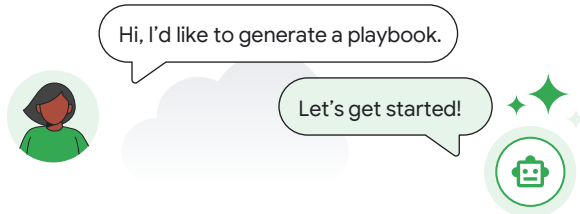
## Summarize 摘要

利用 AI 生成的摘要節省時間，這些摘要包括案件的背景、重要威脅的指導以及回應建議。



## Action 行動

利用 AI 生成檢測規則、建立Playbook並修復威脅。





## SecLM in SecOps

安全營運人員可以使用**中英文混合查詢**；  
**即時生成查詢並進行調整**；  
**無需了解 Yara-L 即可生成規則**並獲得情境化摘要，從而**更快地識別和響應威脅**。



# Gemini in Security Operations

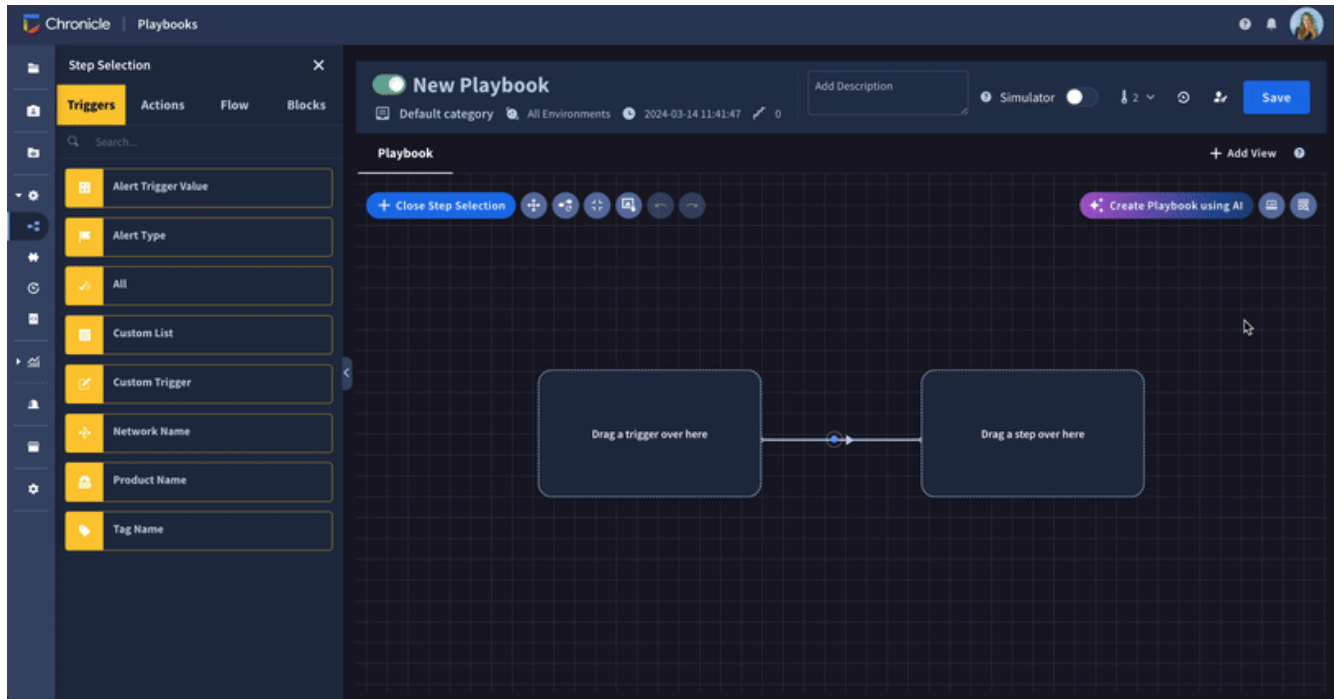
## Gemini in SecOps - Playbook creation



讓SOC分析師能夠使用自然語言輕鬆創建Playbook

減少設計構建劇本所需的時間

減少學習產品的需要  
為經驗不足的SOC初階人員消除學習障礙



# Gemini AI 提供調查結果及建議

Proprietary + Confidential

Cases

218 Cases

Search Case Name

Applied Threat Intelligence...

google\_workspace\_applic...

Applied Threat Intelligence...

Applied Threat Intelligence...

google\_workspace\_user...

chrome\_browser\_safe\_br...

Applied Threat Intelligence...

Applied Threat Intelligence...

SCC: BigQuery Data Ext...

gcti\_benign\_binaries\_c...

google\_workspace\_user...

Cmd.exe Process Extrac...

recon\_environment\_en...

whois\_expired\_domain...

GCP Service API Disable

recon\_environment\_en...

Applied Threat Intelligence IOC Match Rule

ID 2558

SDL

Assessment

2024-03-11 10:55:43

GCTI\_FINDING

Applied Threat Intelli...

Manage Tags

1. APPLIED THREAT INTE...

2. APPLIED THREAT INTE...

3. APPLIED THREAT INTE...

3 Alerts

Overview

AI Investigation

This Case may require a high level of attention

The IP address 38.60.216.78 is associated with the threat actor TEMP.Armageddon.

A network connection was made from 10.128.0.22 to 38.60.216.78 in France.

A file with md5 449088f62868d256dd0547a4bd885b76 was detected by Applied Threat Intelligence IOC Match Rule on 10.128.0.22.

A file with the sha256 hash D6FFD6ED5A5563BD8ABB12E4346C1A732FCC69406F7B934038FE08EA509A71E was detected by the Applied Threat Intelligence IOC Match Rule.

A process was launched on 10.128.0.22 with the file name FGTE.EXE.

Was this helpful?

What Actually Happened?

Based on: 3 Alerts 6 Events 6 Entities

View More

Was this helpful?

The Next Steps You Should Take

Investigate the IP address 38.60.216.78.

Investigate the network connection from 10.128.0.22 to 38.60.216.78.

Investigate the file with md5 449088f62868d256dd0547a4bd885b76 on 10.128.0.22.

Investigate the file with the sha256 hash D6FFD6ED5A5563BD8ABB12E4346C1A732FCC69406F7B934038FE08EA509A71E.

Investigate the process launched on 10.128.0.22 with the file name FGTE.EXE.

Was this helpful?

Write a comment...

Duet AI

+ New chat

Welcome to Duet AI in Security Operations

Ask a question in natural language and get a Unified Data Model (UDM) query. The query is ready to run, or you can quickly refine the query and iterate on results.

Duet AI in Chronicle is in preview. It's a work in progress and might display inaccurate or offensive info that doesn't represent Google's views.

Here are a few ideas to get you started:

Find failed user logins over the last 3 days

Search for network connections to google.com

Show emails to john@example.com with file attachments

Find all cloud service accounts created yesterday

Find all cloud service accounts created yesterday

Here's the query. To refine the query, just ask.

Search Query

metadata.event\_type = "USER\_RESOURCE\_CREATION" AND target.resource.resource\_type = "SERVICE\_ACCOUNT"

Search range: March 10, 01:47 PM - March 11, 01:47 PM (UTC)

Run Search

Edit in Search Page

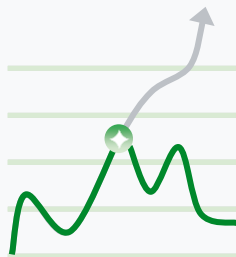
Enter a prompt here

## Generative AI can help

STOPPED

### threats

- ✓ Prevent patient ones



偵測新威脅

LESS

### toil

- ✓ Systems secure themselves

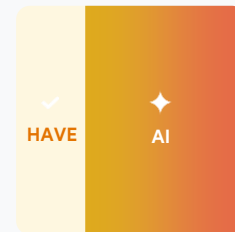


減少操作勞累

SCALED

### talent

- ✓ Democratise security expertise

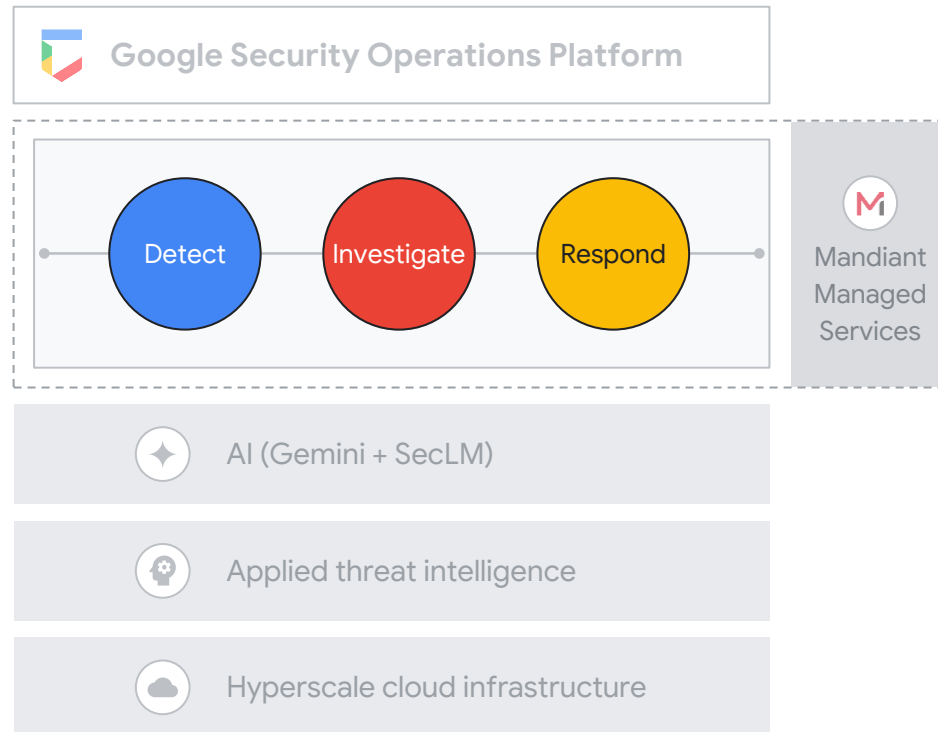


規模化養成人才

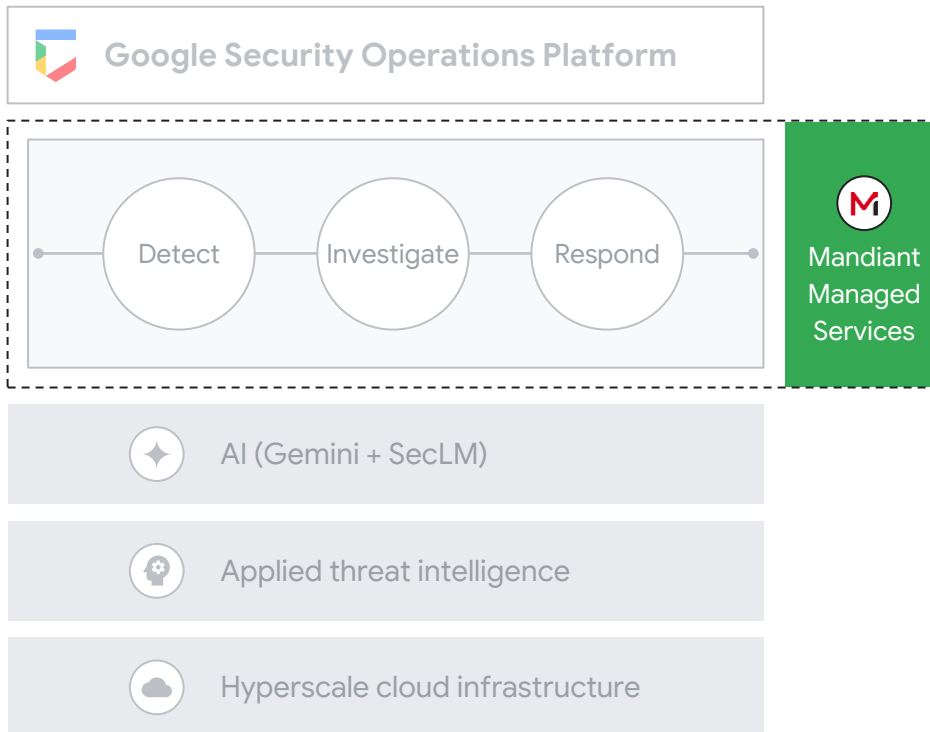
偵測 Detect

調查 Investigate

回應 Respond

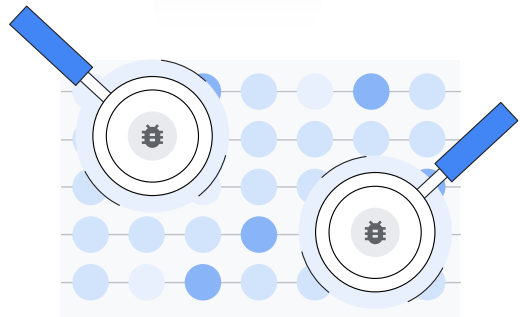


# Expert help 顧問提供協助



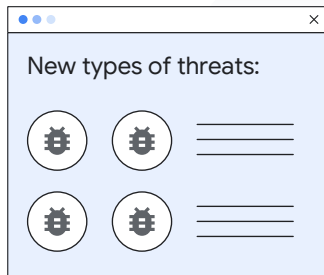


# 以威脅情報為基礎的安全營運平台 Google SecOps Security Operations Platform



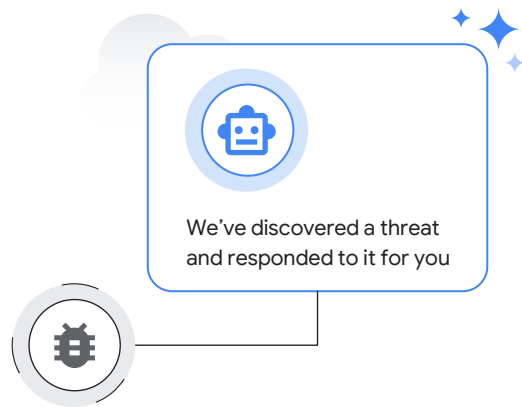
## 無限擴展

以 Google 的規模和速度，  
接收、標準化並分析所有的  
安全遙測數據



## 情報驅動的成果

利用應用威脅情報主動發現並  
防禦最新威脅



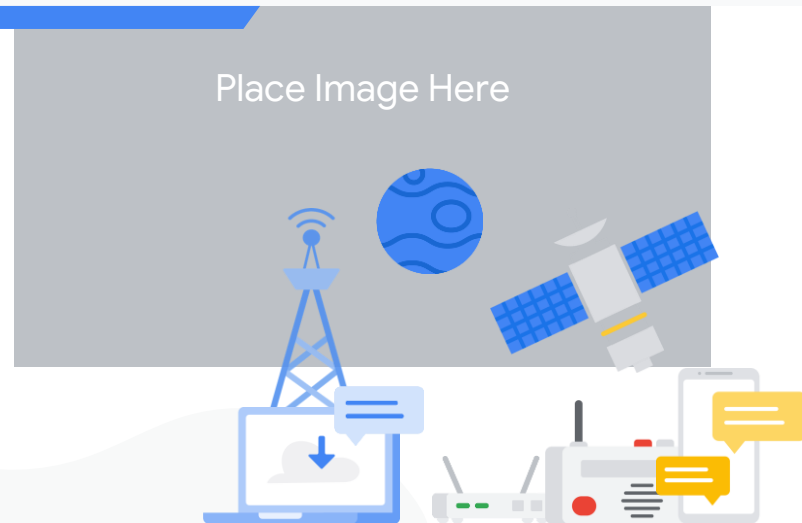
## AI 增強的生產力

透過 AI、自動化和專家協助  
提升技能，讓每個人都能更  
高效地工作

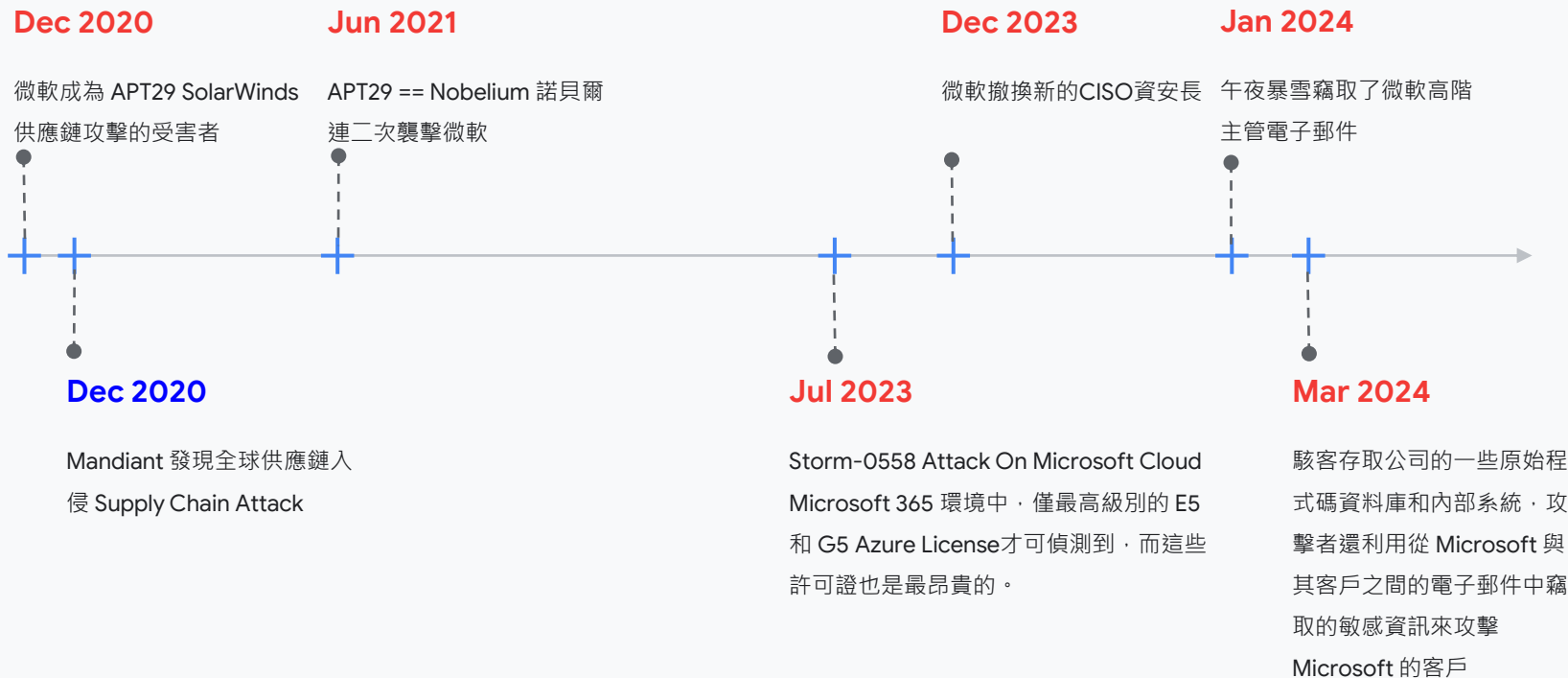
# APT29 (Midnight Blizzard) Attacks On Microsoft Cloud

發生了什麼問題？  
我們怎麼辦？

Place Image Here



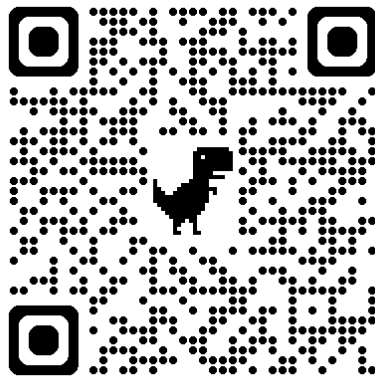
# 微軟在 4 年內 被同一個俄羅斯國家支持的駭客組織入侵 - APT29 2020 年(SolarWinds)、2021 年、2023 年、2024 年。



## APT29 == Nobelium == Midnight Blizzard

## 如何應對 APT29 的影響 Google Cloud Security 對應的服務及解決方案

Mapping solution	Target Point
<b>Incident Response Retainer</b>	for SolarWinds supply chain Investigation
<b>Compromise Assessment</b>	for company environment health check
<b>AD Assessment</b>	for AD health check
<b>Threat Intelligence</b>	for APT29 Actor details
<b>Security Validation</b>	for make sure security defence about APT29 actions
<b>Attack Surface Management</b>	for find out Vulnerabilities
<b>Managed Defence</b>	for EDR consultant services cover security team workload
<b>SecOps Chronicle SIEM/SOAR</b>	for security monitor and Investigation



# Thank you

Visit us at:

[cloud.google.com/security/m-trends](https://cloud.google.com/security/m-trends)

Google Cloud

