

2026 沙崙資安新秀大賽 | 決賽

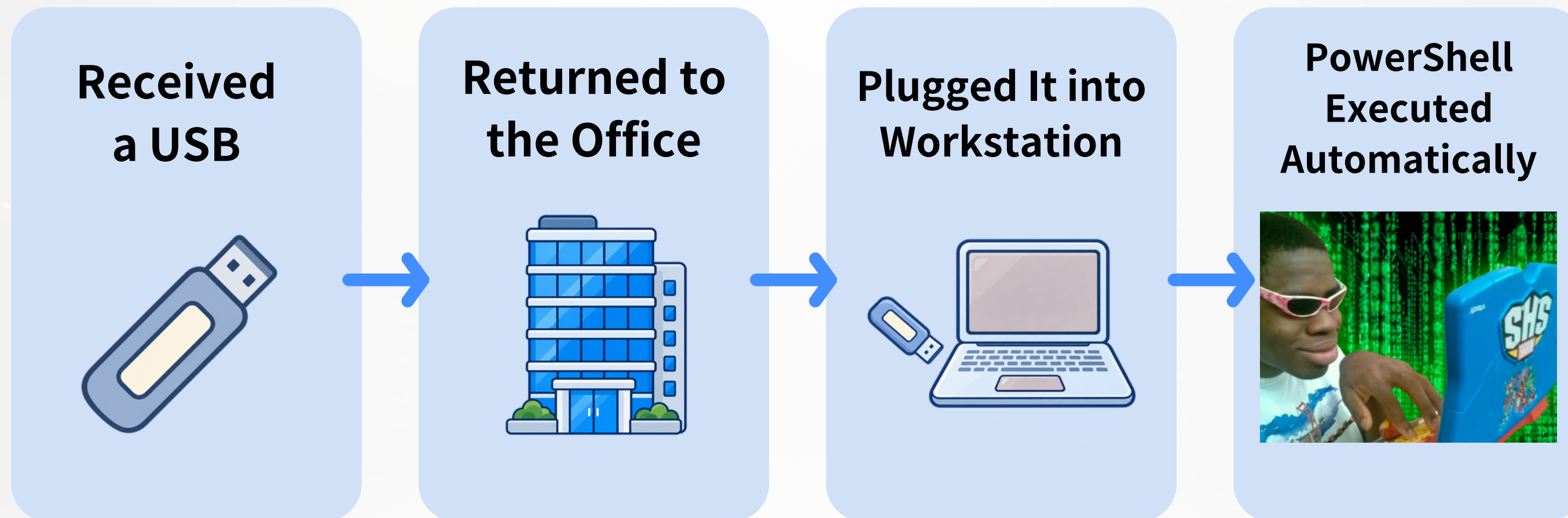
EARLY-WARNING INCIDENT RESPONSE SYSTEM FOR ATTACK CHAINS

Team Members | 鄭宇兩、蔡宇倫、黃煜穎

Advisors | 毛敬豪、黎俊榮

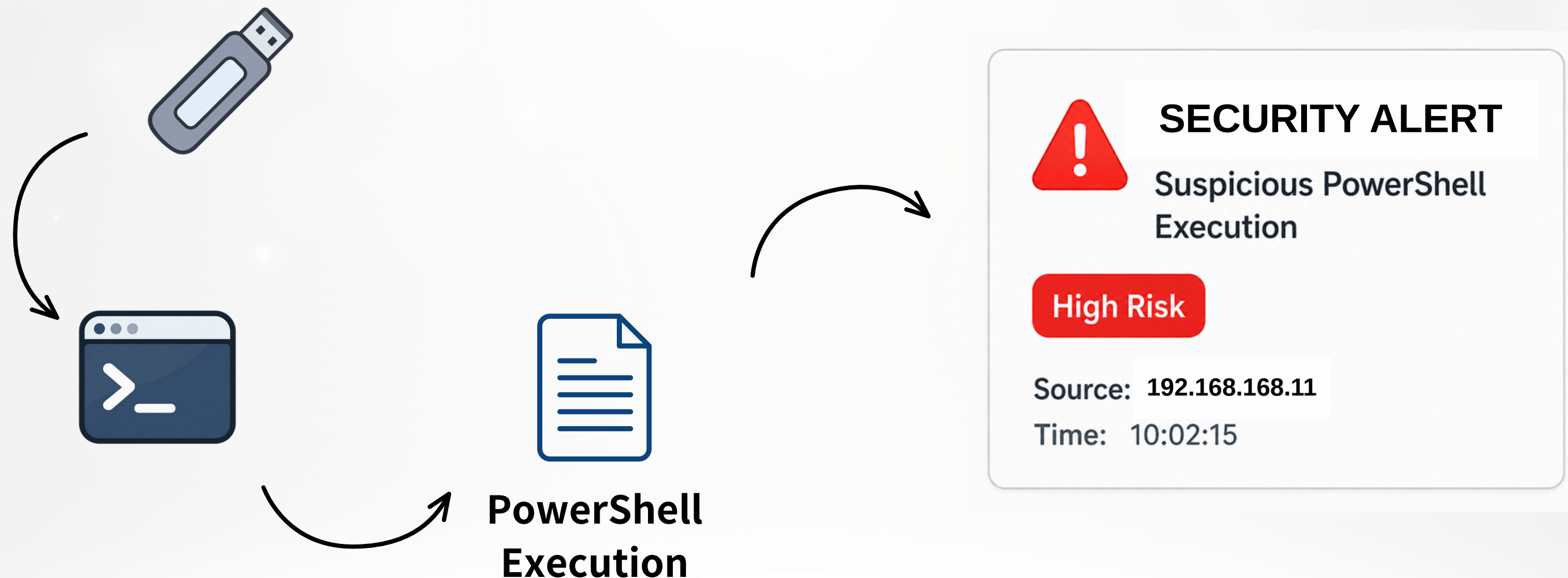
What happened ? → What will happen next ? → What should we do next ?

Started with an USB Drive



RealWorld Case References:
FIN7 / UNC3319 BadUSB

Started Executing Automatically...

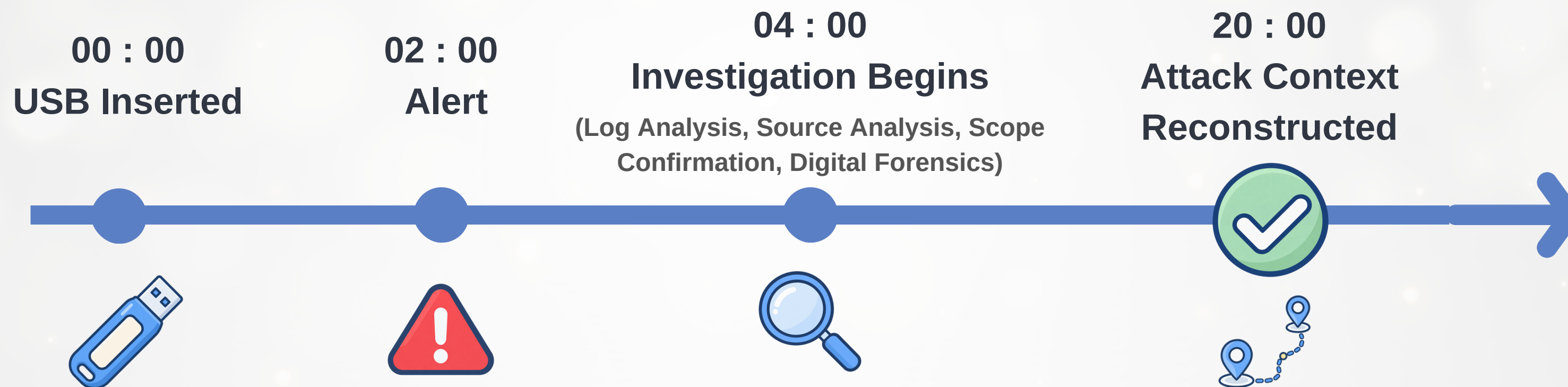


Good News: The Security Appliances **Detected** It
Security Team Immediately Began Investigating...

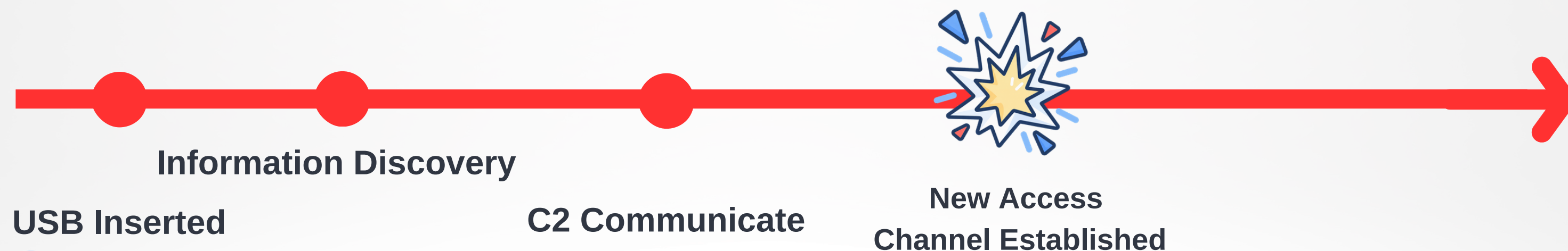


Attack and Investigation Are Racing Against Each Other

Defender



Attacker



But the attacker has **already** completed the next step...

Lack Is Not Detection — but the **Ability to Act** in Time

95%

Confident to Detect Attacks

Detection

≠

17%

Able to Take Timely Preventive Action

Response

Detection Is Faster Than Response
Seeing the Problem ≠ Controlling the Problem

Only Understand an Attack **After It Happens**, Will We Always Be One Step Behind the Attacker?



Can We Predict the **Next Step** Before It Actually Happens?

What Comes Next?

By observing the attack behavior, to understand the attack pattern and predict the next move.



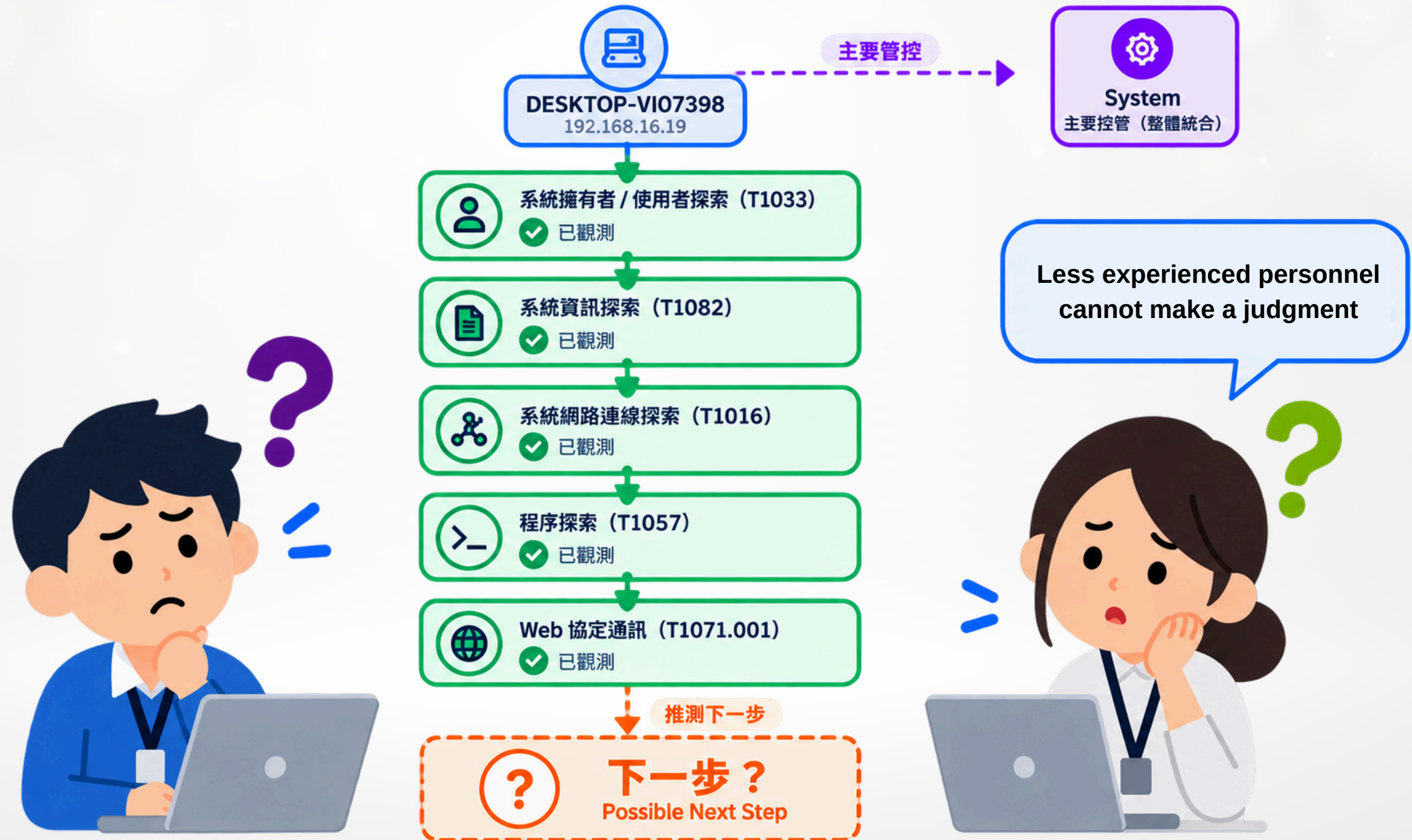
Predicting the Next Step Through Experience

After Log Analysis, Source Analysis, Scope Confirmation, Digital Forensics...



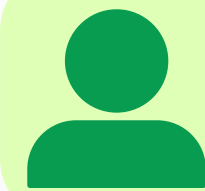
However, not every analyst can make it

Understand what happened, but can not predict next step



Judgment Is **Highly Dependent on Experience**

The problem is not visibility, but that predicting relies on **individual experience**.



Highly Dependent on Individual Experience



Inconsistent Judgment Quality



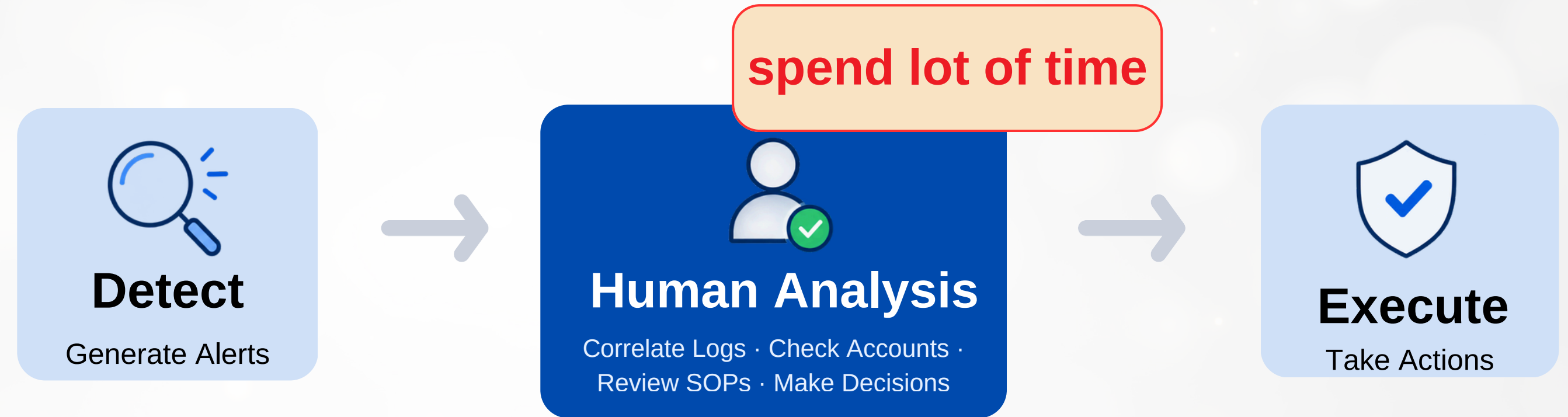
Difficult to Standardize and Scale



Therefore, we aim to systematize the analysis process.

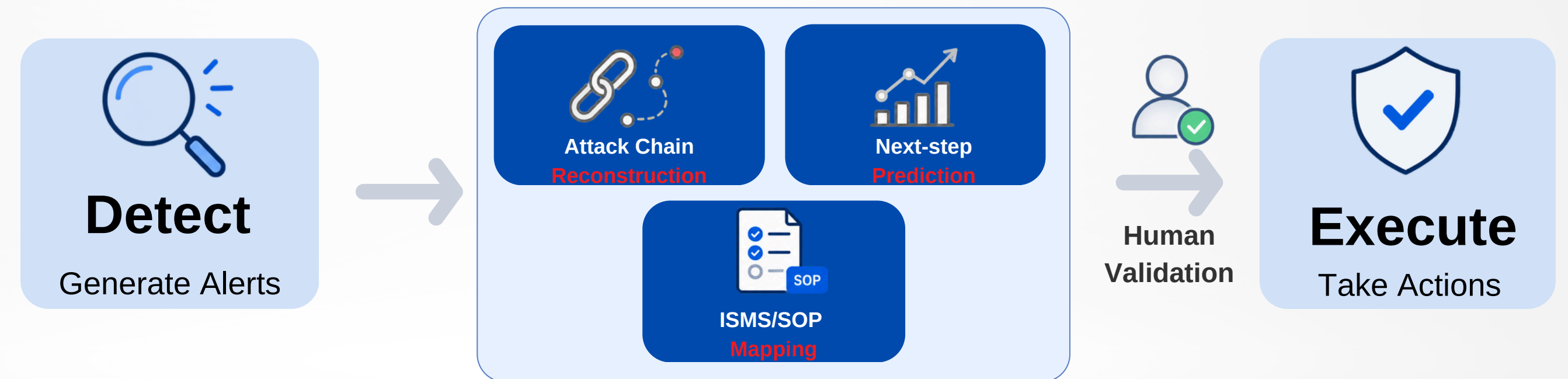
Traditional Workflow

Time Is Spent on **Manual** Analysis and Judgment



Our Workflow

One Black Box
→ Three Explicit Capabilities



Accelerates Analysis, Human Retain Final Decision Authority

Instead of Building Yet Another Detection System, We Focus on:

Core Question ①

What happened?

Understand what did the attacker do?

Core Question ②

What will happen next?

Go beyond understanding the present

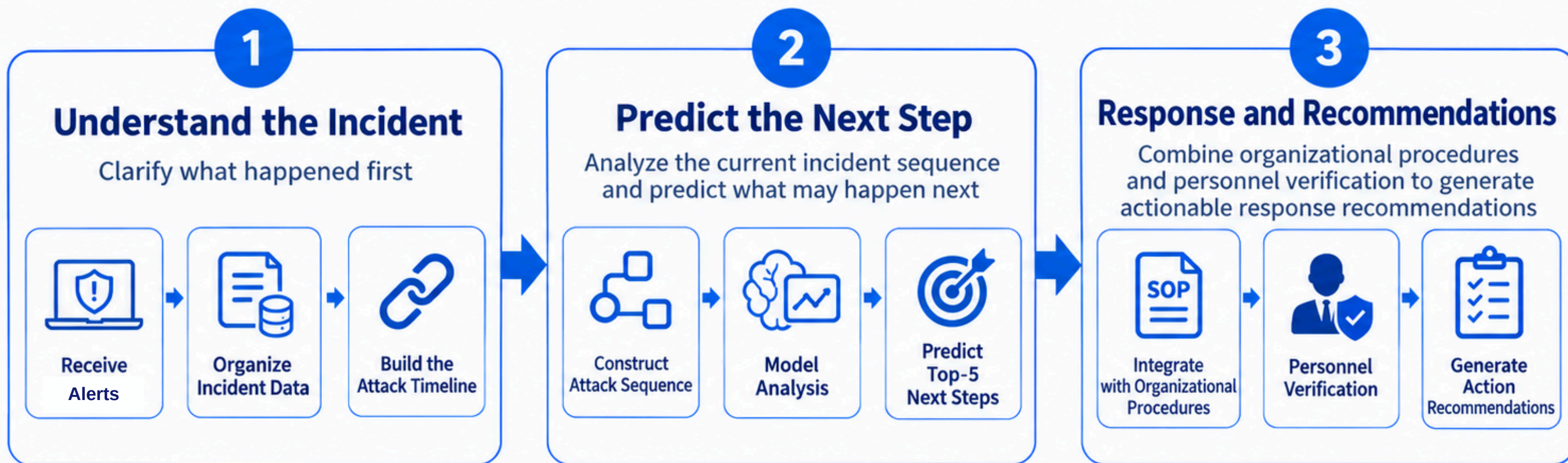
Core Question ③

What should we do next?

what actions should be taken now and after

**AI supports decisions with evidence, procedures, and recommendations
Humans remain in control.**

Complete Workflow in Three Stages



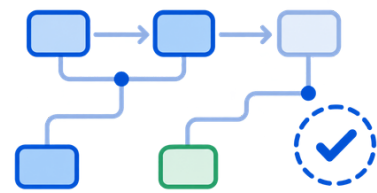
From What happened? → What will happen next? → What should we do next?

DEMO

System Validation

Understand, Predict, and Respond in Time

Episode Correlation



93.3%

Correlation Accuracy

560 / 600 Correctly Correlated Cases
600 Fixed Ground-Truth Cases

Top-5 Prediction



78.5%

Next-Step Top-5 Hit Rate

128 / 163 Predictions Hit
22 Attack Templates
24 Independent Runs

Latency



28.56 s

**Average
Processing Latency**

30 Real EDR Test Runs

P50 20.97s | P90 62.51s

Understand → Predict → Respond in Time

What Makes Our Approach Different



**Built from Real
Operational Needs**



**Integrates with
Existing Operations**



**End-to-End
Alert-to-Action**



**From Detection to
Prediction**



**Organization-Aware
Response Guidance**



Core Question ①

What happened?

What did the attacker do?



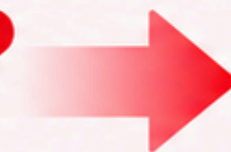
Correlate
scattered information
into an attack chain.



Core Question ②

What will happen next?

What is likely to happen in the future?



Use LSTM and
historical patterns
to predict the attacker's
next move.



Core Question ③

What should we do next?

What actions should we take?

AI does not replace human decision-making,
but provides “evidence + programmatic reasoning + recommendations”
to support security analysts.



Based on organizational
policies and SOPs,
specify concrete
actions to take.



Thanks.



Reference

- [1] Wu, Y., Roesner, F., Kohno, T., Zhang, N., & Iqbal, U. (2025).
IsolateGPT: An Execution Isolation Architecture for LLM-Based Agentic Systems. NDSS 2025.
- [2] Kurniawan, K., Ardian, R. F., Kiesling, E., & Ekelhart, A. (2025).
AgCyRAG: An Agentic Knowledge Graph-based RAG Framework for Automated Security Analysis.
RAGE-KG Workshop, CEUR-WS Vol-4079.
- [3] Yao, S., Zhao, J., Yu, D., Du, N., Shafran, I., Narasimhan, K., & Cao, Y. (2023).
ReAct: Synergizing Reasoning and Acting in Language Models. ICLR 2023.
- [4] Li, S., Dong, F., Xiao, X., Wang, H., Shao, F., Chen, J., Guo, Y., Chen, X., & Li, D. (2024).
NodLink: An Online System for Fine-Grained APT Attack Detection and Investigation. NDSS 2024.
- [5] Meng, Y., Li, S., Gui, J., Jiang, P., & Li, D. (2026).
KnowHow: Automatically Applying High-Level CTI Knowledge for Interpretable and
Accurate Provenance Analysis. NDSS 2026.
- [6] Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H.,
Lewis, M., Yih, W., Rocktäschel, T., Riedel, S., & Kiela, D. (2020).
Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. NeurIPS 2020.
- [7] [FBI Warns FIN7 Campaign Delivers Ransomware via BadUSB](#)

Reference (22 attack template types)

主要類型	代表模板	測試內容
主機與網路探索	host_discovery_scan、network_discovery_to_staging、mixed_discovery_execution	探索主機資訊、使用者、程序、檔案、網路設定及開放服務
帳號與安全環境盤點	account_policy_collection、software_audit_to_archive、service_inventory_web_stage	本機帳號、群組、密碼政策、已安裝軟體、安全軟體與服務盤點
混淆、解碼與命令執行	decode_masquerade_http、web_ingress_decode_execute、training_web_decode_manipulation	模擬腳本混淆、解碼、偽裝、Shell 執行及 HTTP 通訊
資料蒐集、暫存與壓縮	collection_archive_egress、obfuscated_collection_egress	蒐集本機資料、集中暫存、壓縮封裝並準備外傳
盲測組合	blind_host_web_manipulation、blind_security_collection_manipulation、blind_policy_obfuscated_manipulation	使用模型訓練期間未看過的步驟組合，檢查是否只背模板
資料操弄／Impact	training_discovery_collection_manipulation、training_inventory_archive_manipulation 與 6 種 train2_*	從探索、蒐集、下載、壓縮等不同前序行為，最後連接到資料操弄 T1565.001