CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

FINSEC FORUM

FINSEC FORUM

金融資安韌性的實踐與挑戰

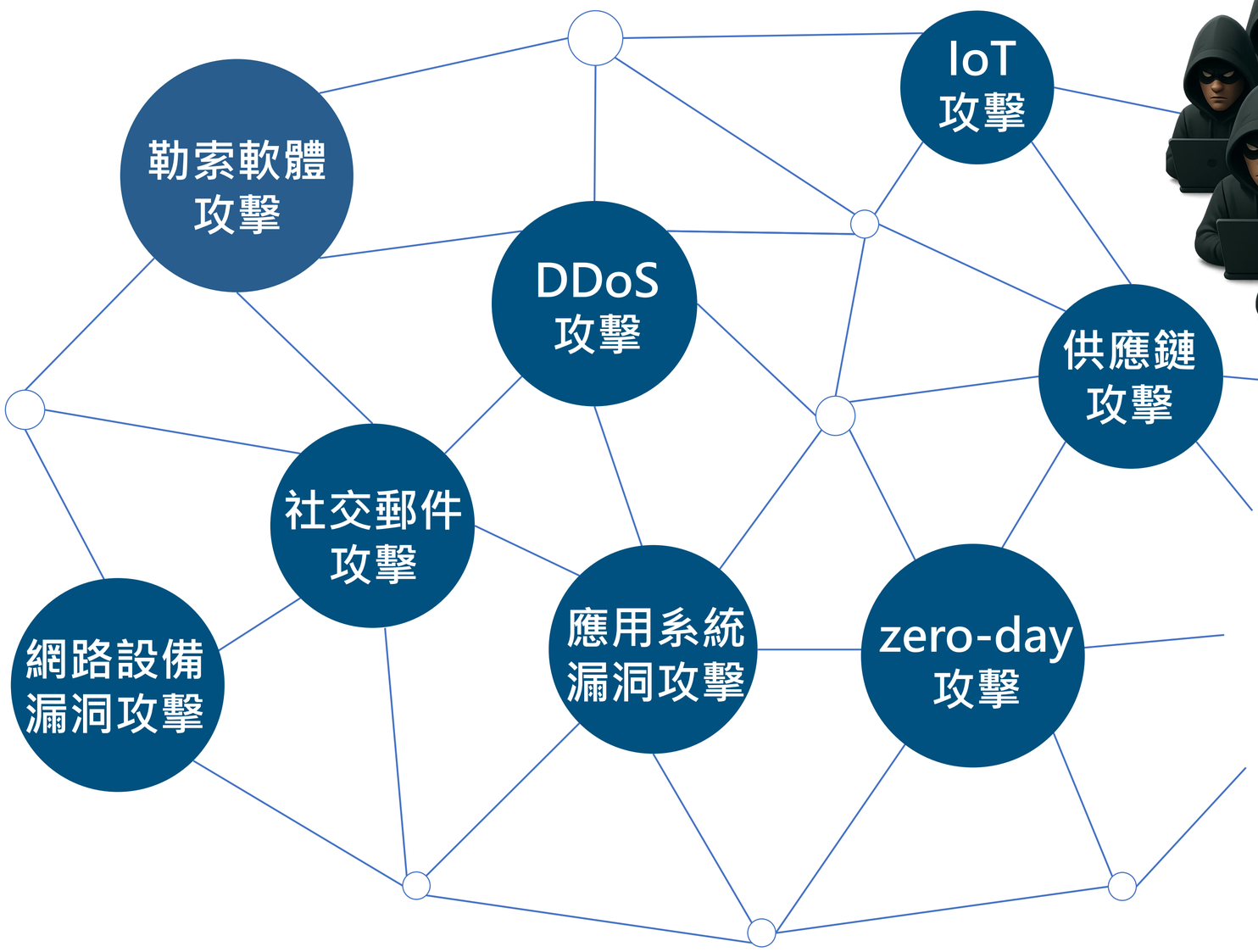
TEAM CYBERSECURITY

林季勳

凱基人壽/資訊安全部

資安長

資安威脅無所不在，我們與駭客的距離!!



地緣政治

- 提高攻擊頻率

生成式AI發展

- 降低攻擊門檻
- 擴大攻擊規模
- 提高攻擊擬真度

數位轉型

- API管理不當風險
- 供應鏈管理風險

面對突如其來的惡勢力，如何因應？

事前 防患未然

ISAC 建立情資處置機制

資安單位

- 資安情資蒐整與發布

資訊單位

- 評估資安情資影響性
- 依評估狀況進行處置

早期預警

金管會

F-ISAC、F-SOC

法務部調查局

壽險公會 …

事中 防微杜漸

SOC 建立資安監控機制

資安單位

- 分析異常警訊
- 建立SOAR機制
- 情資分享F-SOC

資訊單位

- 評估資安情資影響性
- 依評估狀況進行處置

早期預警

持續監控、防禦

外部協力廠商

情資廠商

SOC廠商

原廠、設備維運廠商

事後 降低損害

CERT 建立緊急應變機制

資安單位

- 制定資安應變程序
- 執行資安演練（實兵、程序）
- 資安事件調查

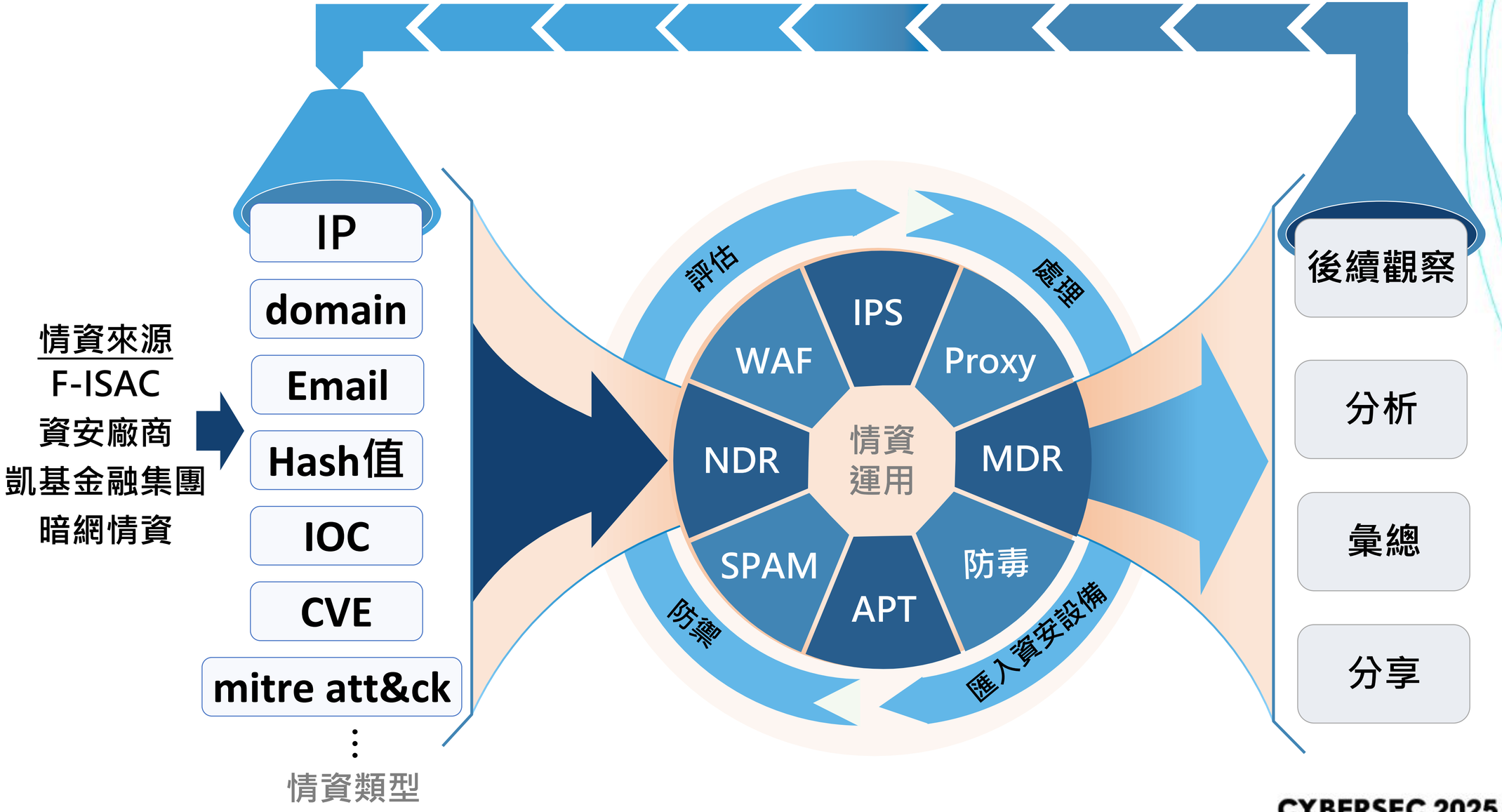
資訊單位

- 資安事件損害控制
- 配合資安相關演練

持續監控、防禦、應變

紅隊廠商、資安顧問公司、驗證組織

面對突如其來的惡勢力，如何因應？



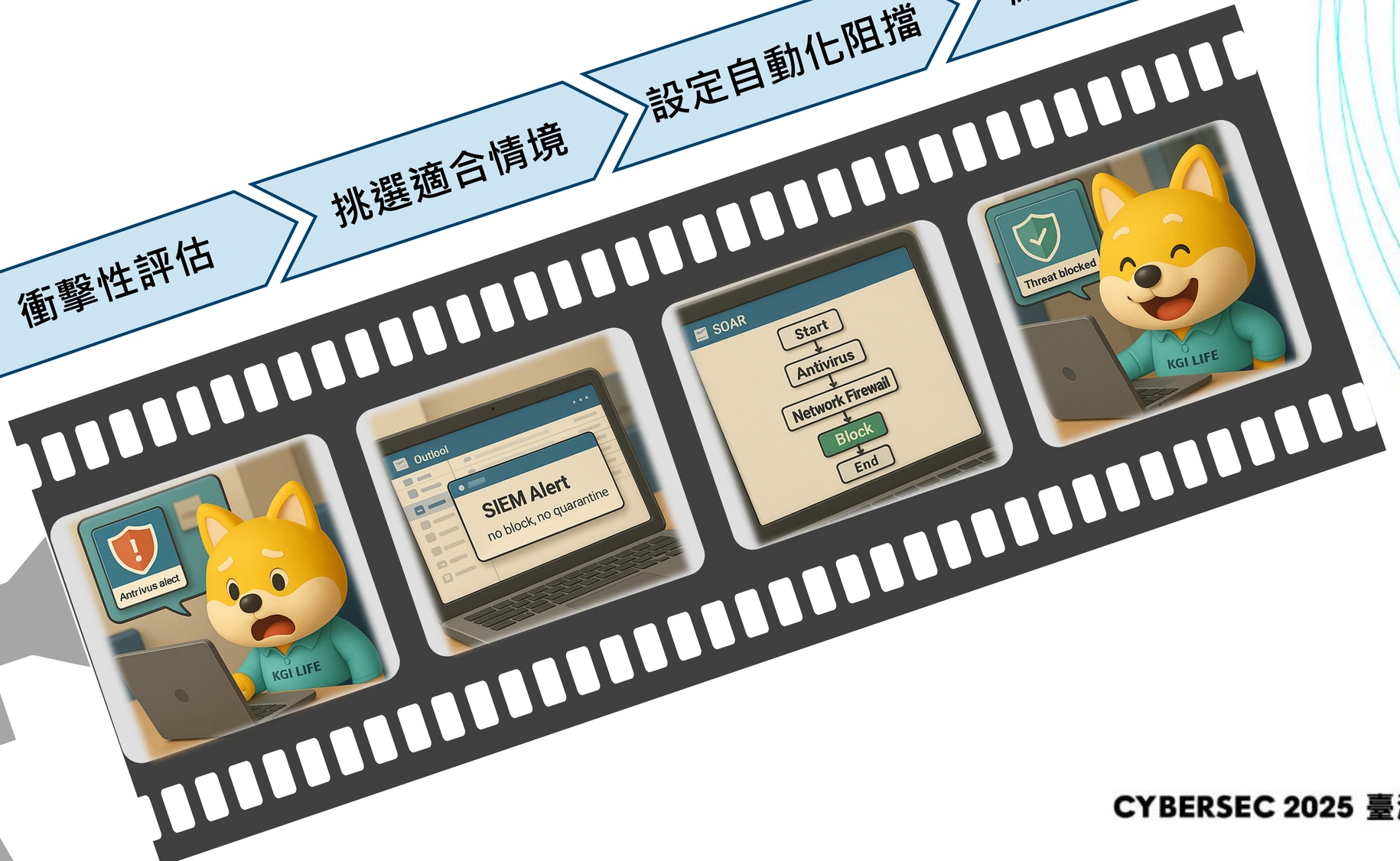
面對突如其來的惡勢力，如何因應？

衝擊性評估

挑選適合情境

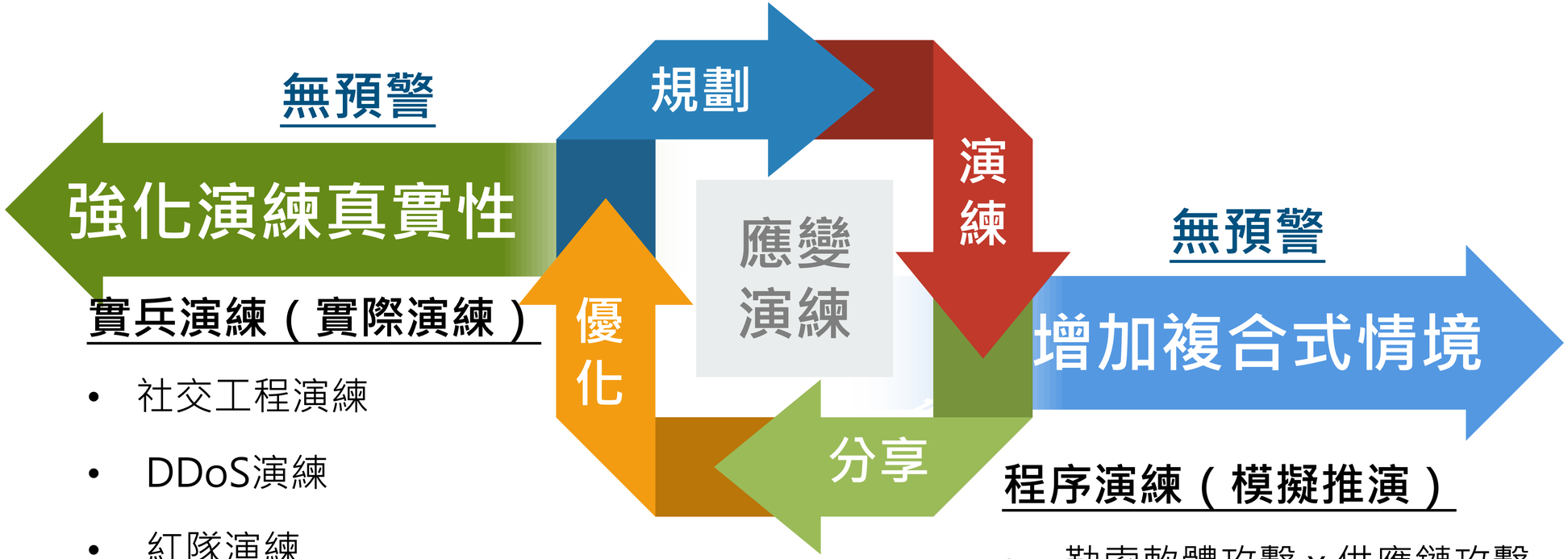
設定自動化阻擋

縮短回應時間



建立
SOAR機制

面對突如其來的惡勢力，如何因應？



實兵演練（實際演練）

- 社交工程演練
- DDoS演練
- 紅隊演練
- BAS演練
- Recovery

程序演練（模擬推演）

- 勒索軟體攻擊 x 供應鏈攻擊
- 網頁置換攻擊 x 應用系統漏洞攻擊
- 勒索軟體攻擊 x 應用系統漏洞攻擊

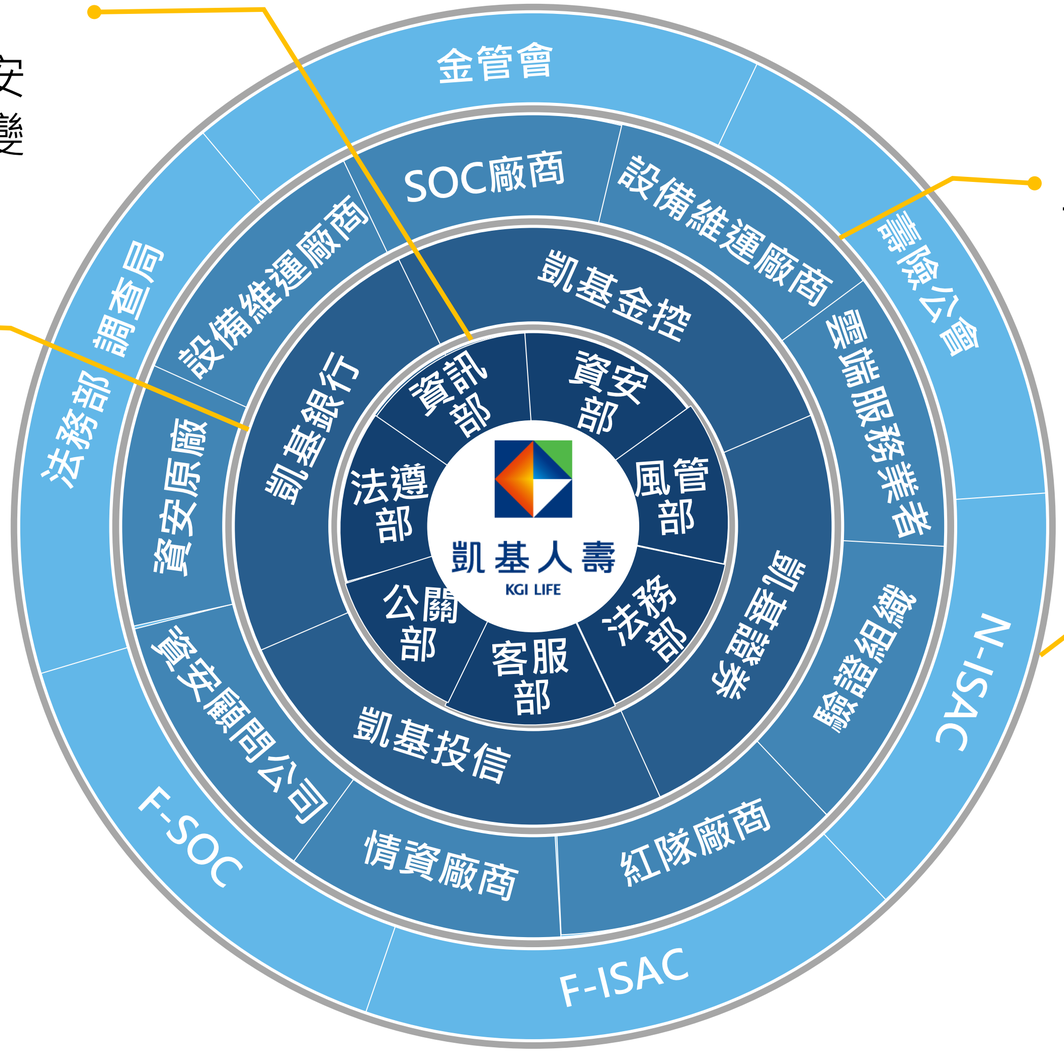
資安聯防團隊的角色與職責

公司相關部門

負責公司整體資安防護、監控與應變

凱基金融集團

集團資安情資分享、資安技術交流



合作之資安廠商

資安情資分享、資安技術支援與交流

合作之公部門

資安情資分享、資安技術支援與交流

透過三大循環機制，持續強化金融資安韌性

善用情報與資源

建立規則自動防禦

強化人員防禦技能
及應變熟練度

情報力
蒐集、整理與分析，
化被動為主動

執行力
提升處理效率

反應力
把握黃金救援/防禦時間

THANK YOU!

TEAM CYBERSECURITY