July 2022

勒索軟體應對之道

蔡 松廷 (TT)

TEAMT5
杜 浦 數 位 安 全
Persistent Cyber Threat Hunters

蔡松廷 Tsai, Sung-ting (TT)

TEAMT5
杜 浦 數 位 安 全

- Founder and CEO, TeamT5
- 18+ years in security industry and hacker community
- Frequent security conference speaker
- Co-founder / chief director / volunteer, HITCON
- Adviser, several Taiwanese government agencies.

Our Team

Persistent Cyber Threat Hunters

- Found in 2017
- Taipei, Taiwan
- Security Experts

TEAMT5

- 300+ IR cases
- 100+ Customers
- 30+ Partners

勒索軟體持續造成鉅額損失

FACT in 2021

- **$6 trillion**: damages from cybercrime (BlackFog)
- **$102.3M** ransomware transactions per month (US Treasury Department)
- **$4.62M** cost of a ransomware breach (IBM)
- **$4.24M** cost of a data breach (IBM)
- **$1.85M** solving a ransomware attack (Sophos)
- Kaseya, Colonial pipeline, Delta Electronics, etc.

Breaches keep happening &
damages keep increasing.

老闆們的惡夢

TEAMT5
杜浦數位安全

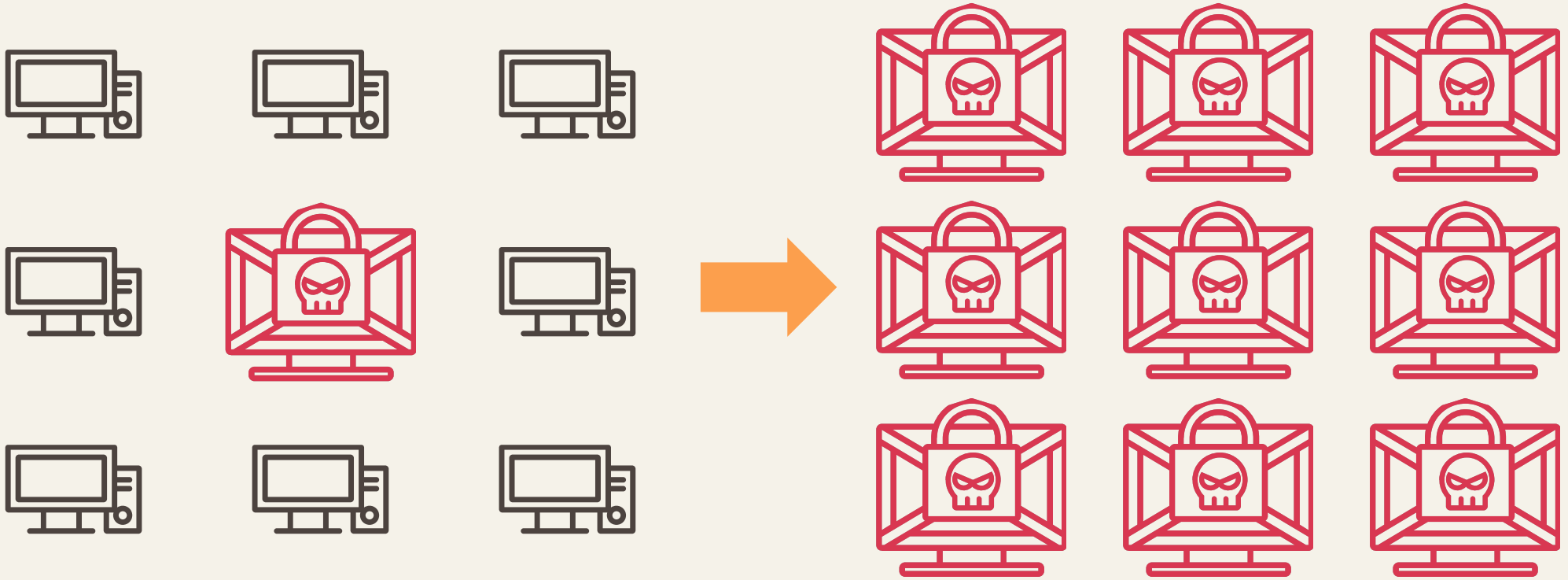
~~他們終於開始在意資安子~~

勒索軟體成為了高層討論的話題

勒索軟體攻擊趨勢 (1)

TEAMT5
杜浦數位安全

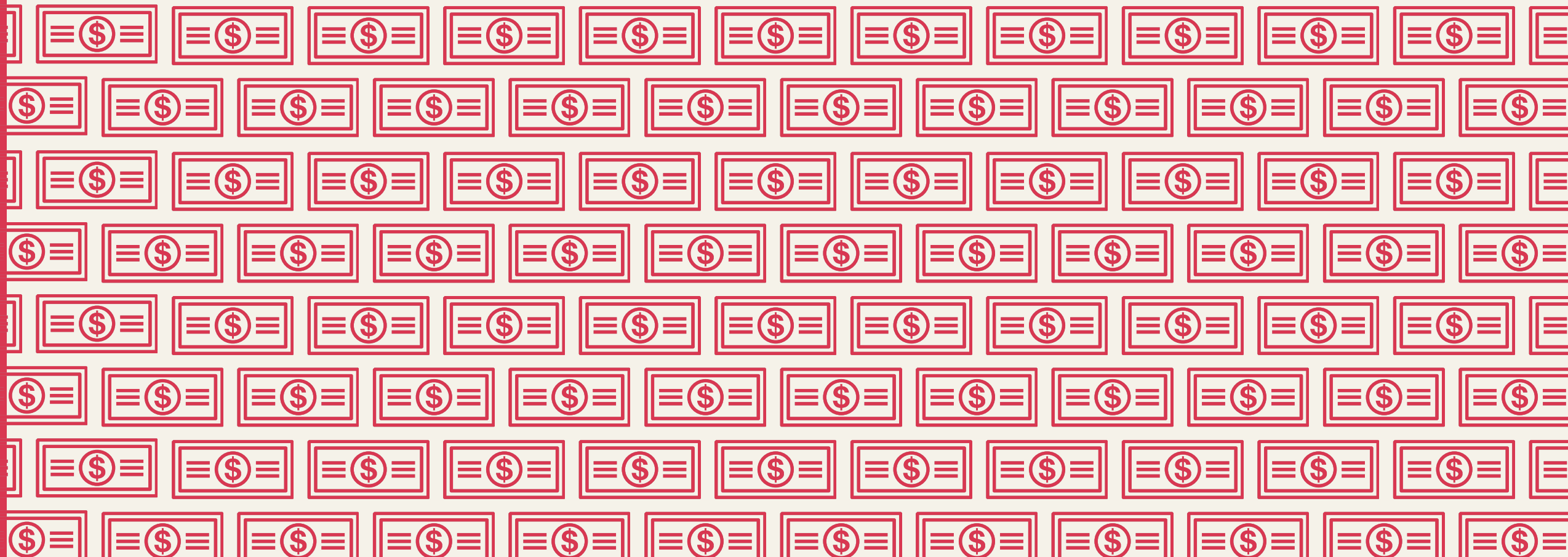
加密單一電腦 → 加密整個組織



勒索軟體攻擊趨勢 (2)

TEAMT5
杜 浦 數 位 安 全

贖金金額來到了 70M (美金)



勒索軟體攻擊趨勢 (3)

TEAMT5
杜浦數位安全

加密速度越來越快，演算法牢不可破

勒索軟體攻擊趨勢 (4)

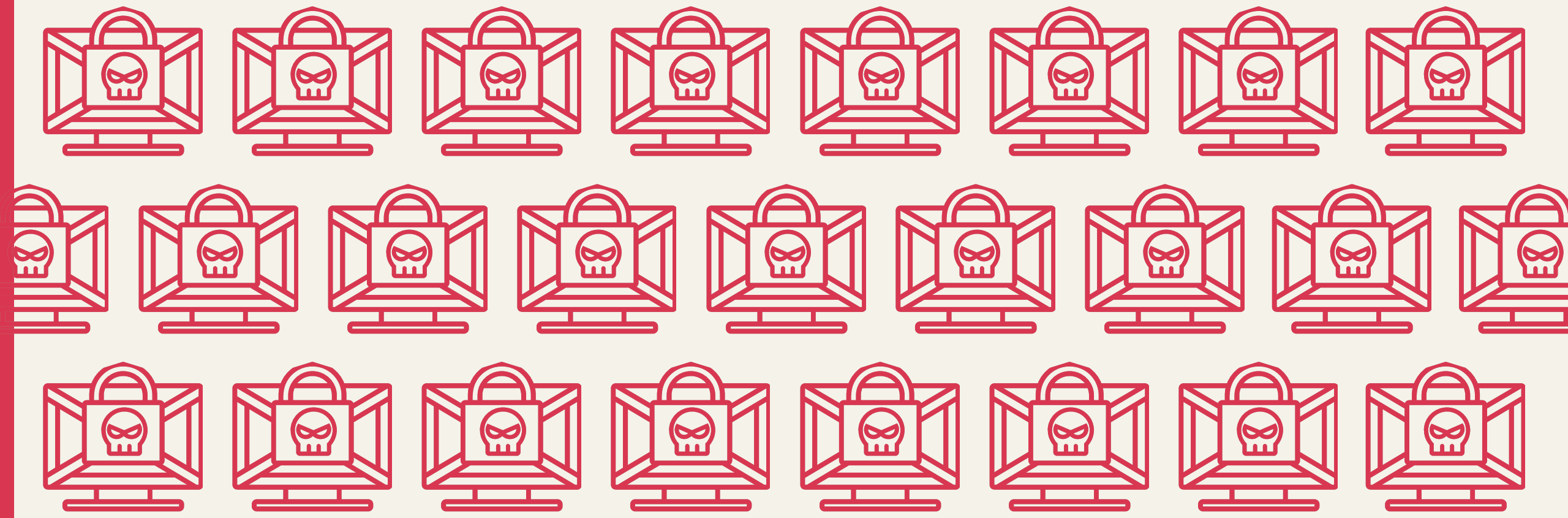
TEAMT5
杜浦數位安全

攻擊目標不侷限特定產業

勒索軟體攻擊趨勢 (5)

TEAMT5
杜浦數位安全

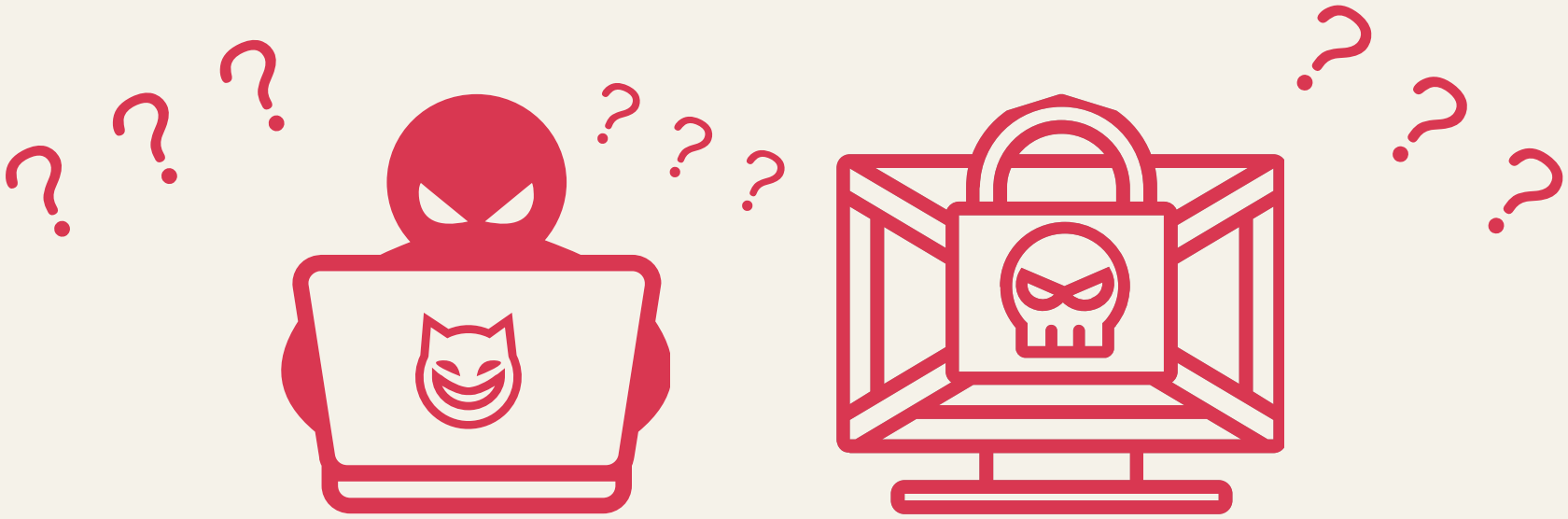
變本加厲的勒索 – 加密網路磁碟 / 破壞備份 / 公開機敏資料



勒索軟體攻擊趨勢 (6)

TEAMT5
杜浦數位安全

APT / 勒索，越來越模糊的界線



勒索軟體攻擊趨勢 (7)

TEAMT5
杜浦數位安全

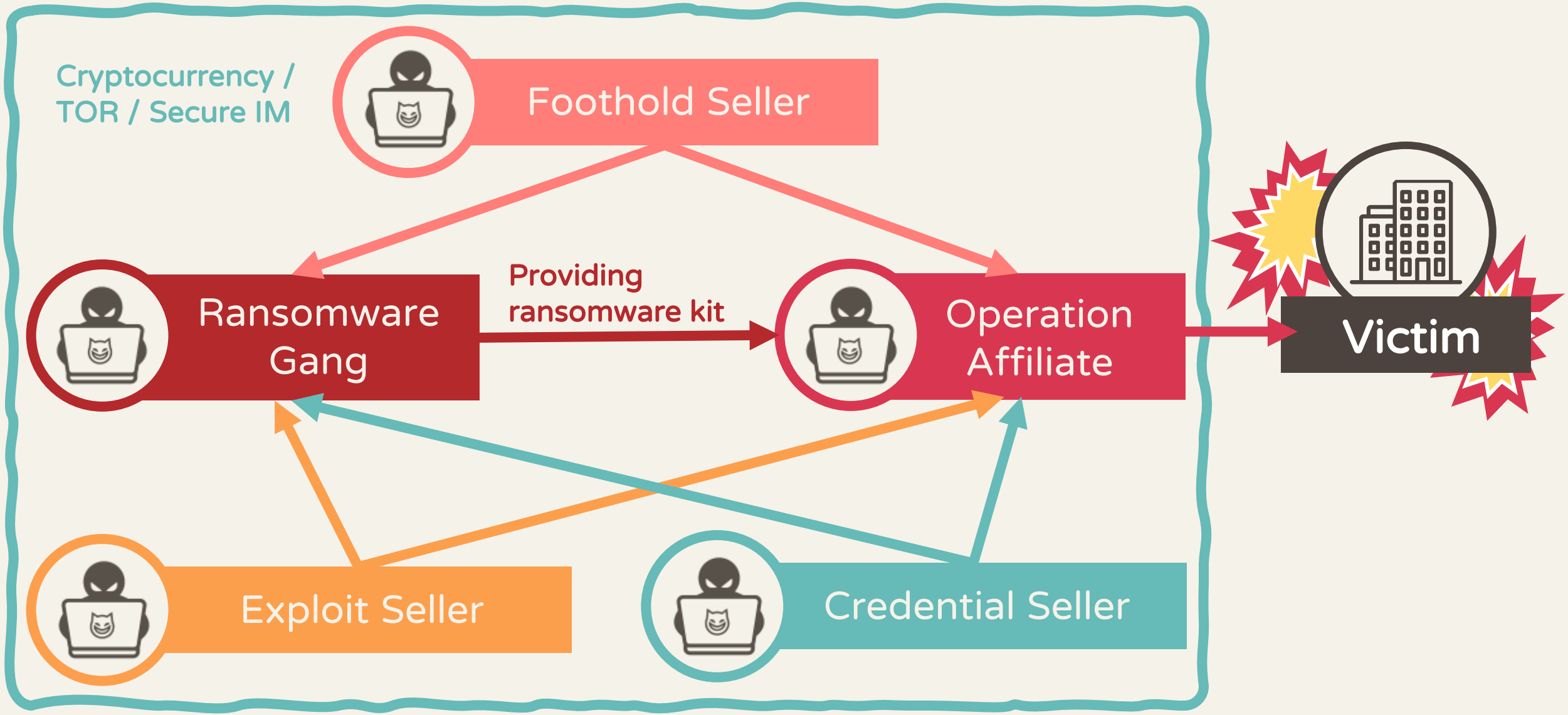
勒索攻擊成為了資安事件的新常態

New Normal

Why is ransomware so difficult to defend?

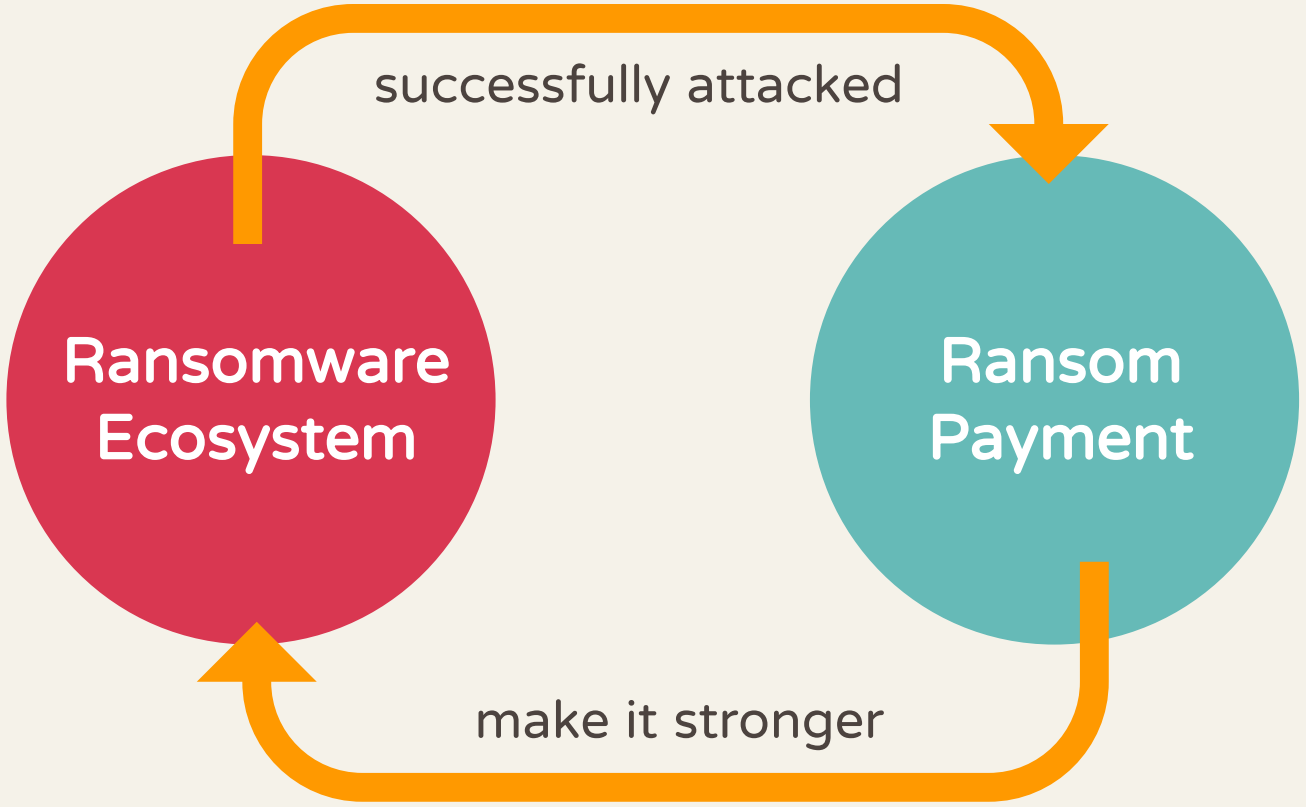
Ransomware Ecosystem

TEAMT5
杜 浦 數 位 安 全



Ransom Cycle

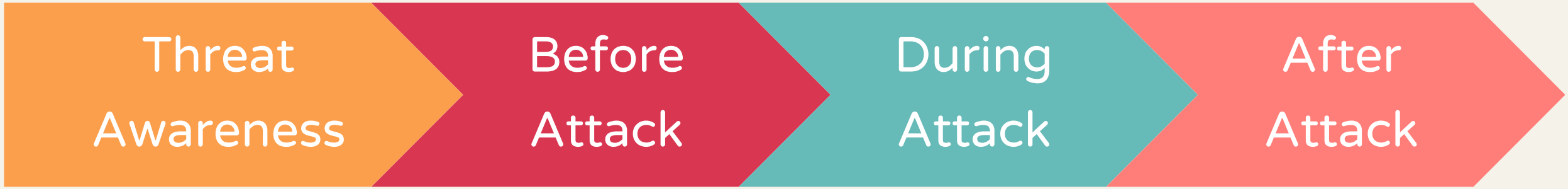
TEAMT5
杜 浦 數 位 安 全



Preparing for a Ransomware Attack

TEAMT5
杜 浦 數 位 安 全

Preparing for a Ransomware Attack



TEAMT5
杜 浦 數 位 安 全

Threat Awareness

TEAMT5
杜 浦 數 位 安 全

Threat Awareness | Before Attack | During Attack | After Attack

Know The Enemies

- Learn from other ransom cases
- Risk assessment and business continuity plan
- Training and drills
- Cyber insurance

Before Attack

TEAMT5
杜 浦 數 位 安 全

Threat Awareness | **Before Attack** | During Attack | After Attack

Assume you will be compromised

- Deploy anti-ransomware solutions
- Deploy latest ransomware IOC
- Patch known vulnerabilities (as many as you can)
- Backup critical data and make it offline
- Retainer arrangement with service partners (Security, Legal, PR)

During Attack

TEAMT5
杜 浦 數 位 安 全

Visibility and response is the key

- Monitoring alerts and be aware of any alerts related to any ransomware groups
- Respond quickly to malicious activities
- Block encryption attempt

After Attack

TEAMT5
杜 浦 數 位 安 全

Threat Awareness | Before Attack | During Attack | After Attack

Containment and Recovery

- Disconnect the attack and quarantine infected area
- Service / Data recovery
- Incident investigation and finding root cause
- PR and legal
- Don’t forget your employees
- Payment negotiation with the actor

Extortion and Cost Consideration

TEAMT5
杜 浦 數 位 安 全

- Revenue lost (per hour/day)
- Service/Data recovery (incl. hardware cost)
- Rollback lost
- Data leakage / disclosure cost (IP, business secret, GDPR, etc)
- External service (Incident Response / Investigation)
- External service (PR / Legal)
- Impact of Reputation and Customer Trust
- Consequences after you paid or not to paid

Preparing for a Ransomware Attack

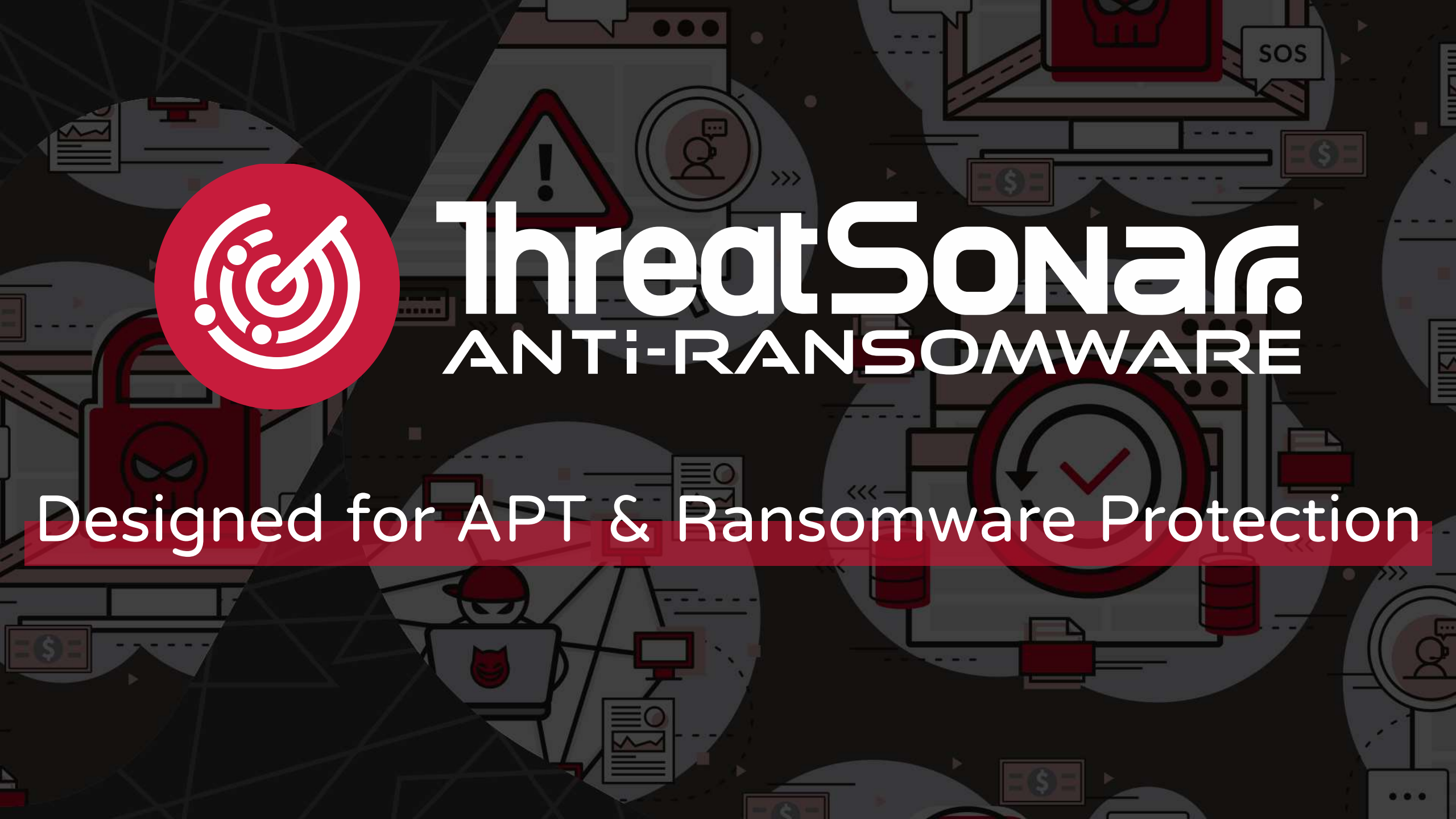
Know The Enemies

Assume you will be compromised

Visibility and response is the key

Containment and Recovery

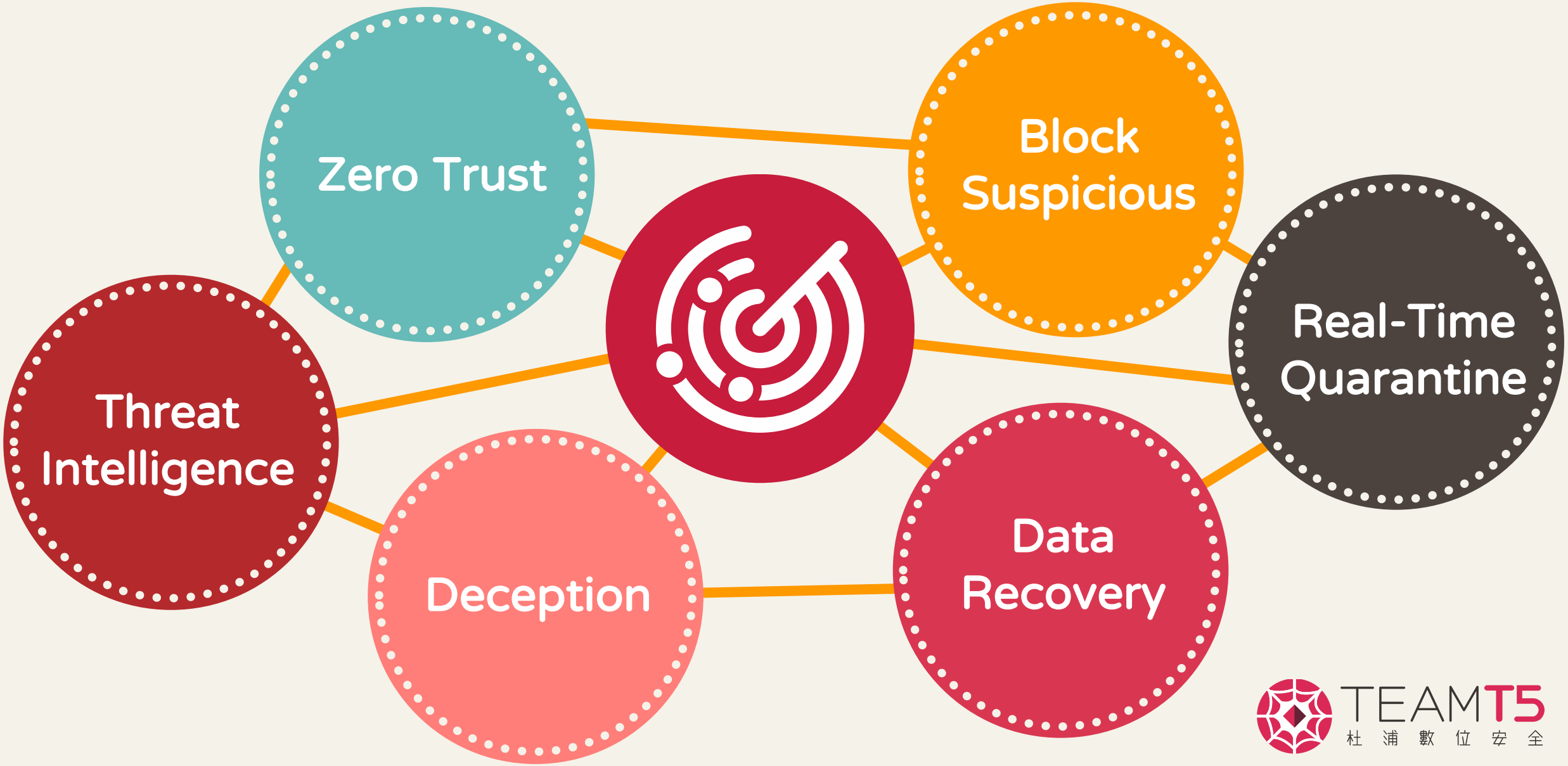
TEAMT5
杜 浦 數 位 安 全



ThreatSonar ANTI-RANSOMWARE

Designed for APT & Ransomware Protection

ThreatSonar Anti-Ransomware



TEAMT5
杜 浦 數 位 安 全

聯絡我們

tt@teamt5.org

Facebook

Twitter

Linkedin

Instagram

TEAMT5

杜 浦 數 位 安 全

Persistent Cyber Threat Hunters