NEITHNET
Accelerate Your Insight

MDR 全面防禦之術

關鍵在地情資，化解遇駭危機

NEITHNET
Accelerate Your Insight

台灣在地原廠

- ✓ 分析師與專業團隊待命，快速回應、即時服務，降低事件造成損失。
- ✓ 自行開發軟體，針對使用者經驗開發，貼近真實事件調查分析

專業資安實驗室

- ✓ 巨量真實攻擊流量分析，最即時攻擊樣本分析
- ✓ 全球情資收集，提供最有效的情資情報
- ✓ 大中華區完整情資佈局，融合全球與在地情資

資深資安團隊

團隊約50人，人員包含各種專業分析能力

- ✓ 資安事件調查專家
- ✓ 網路入侵防禦分析專家
- ✓ 大型網路建置專家
- ✓ 端點安全專家
- ✓ 雲端運算專家
- ✓ AI/ML研究人員

豐富user端實戰處理經驗結合威脅防禦技術開發，提供符合市場需求之解決方案。


Cyber Threats Defense
Active Defense
Passive Defense
Proactive Defense
Responsive Defense

NEITHNET
Accelerate Your Insight

Threat Hunting

-Structured hunting (IoA)

-Unstructured hunting (IoC)

- Mitre ATT&CK

  Adversarial Tactics, Techniques, and Common Knowledge

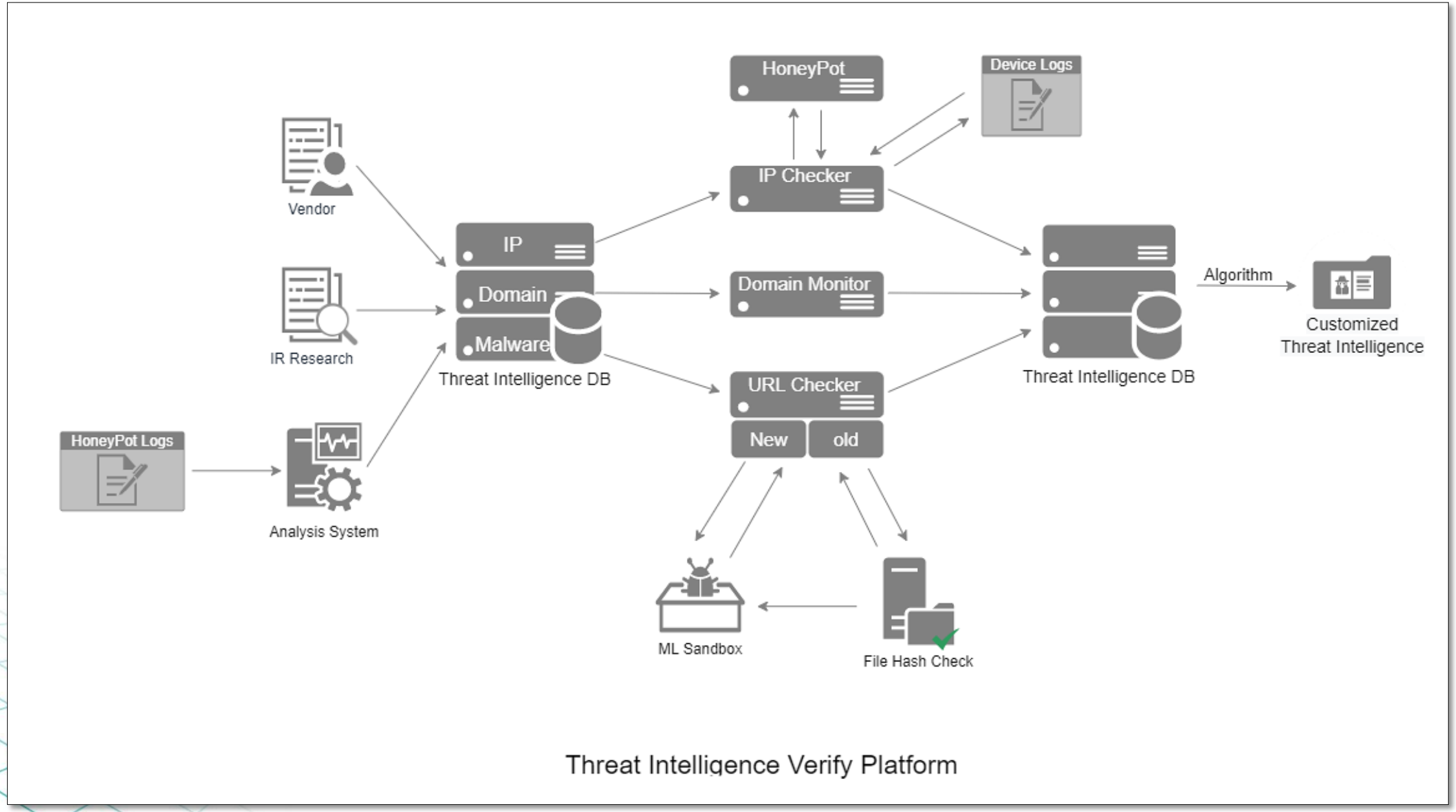
Tactics	• 戰術&策略 • 14
Techniques	• 技術&技巧 • 191 (sub:385)
Data Sources	• 日誌收集 • 39
Mitigations	• 減輕措施 • 43
Group	• APT group • 133
Software	• 軟體&指令 • 680

- Mitre ATT&CK

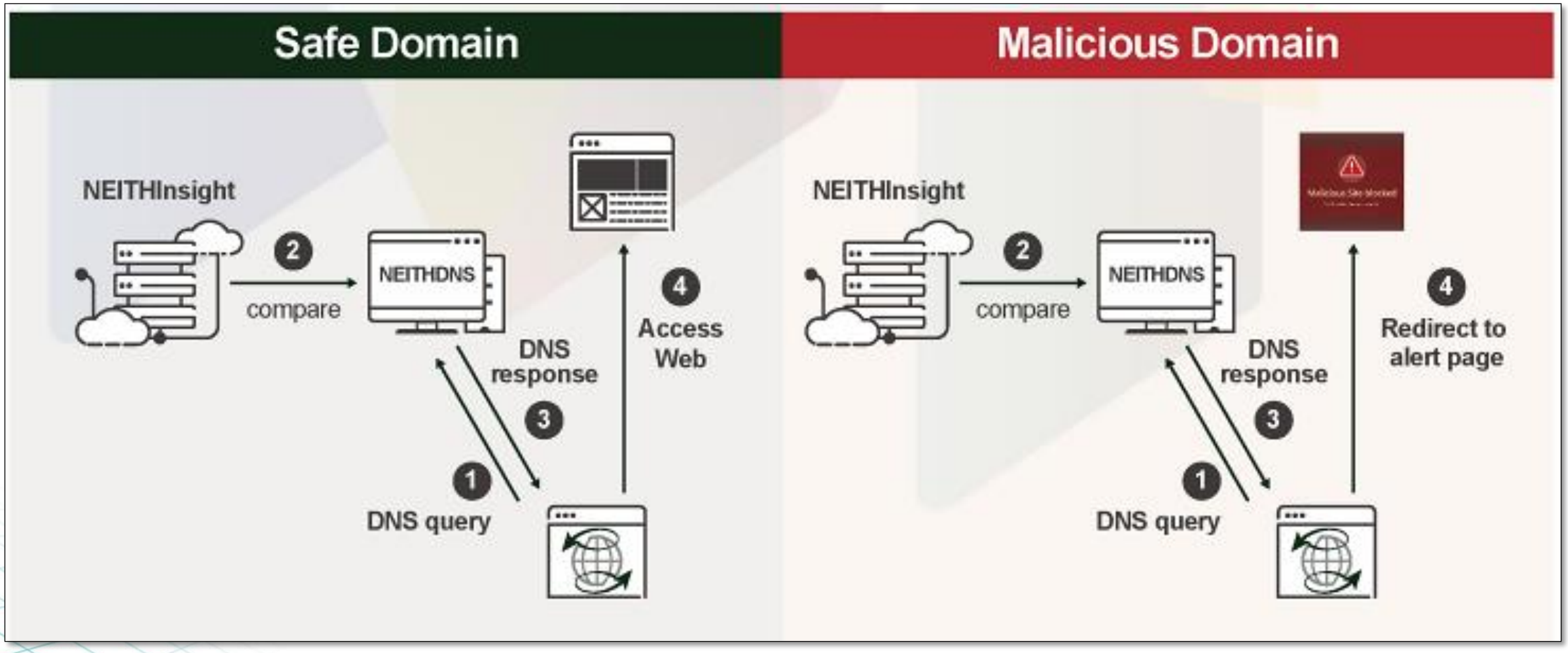
Tactics	• 戰術&策略 • 該階段要達成的目標
Techniques	• 技術&技巧 • 達到階段目標的手法
Procedures	• 過程&程序 • 過程使用軟體或工具


Pyramid of Pain
TTPs
Tough
Tools
攻擊工具
Challenging
Network/Host Artifacts
網路或主機特徵
Annoying
Domain Names
網域名稱
Simple
IP Addresses
IP位址
Easy
Hash Vlues
Hash值
Trivial
IOC
(Indicators of Compromise)
高
情報價值
低

- 客戶的需求是什麼?
- 那些威脅情資對客戶才有用?
- 威脅情資都是威脅?
- 威脅情資該如何維護?



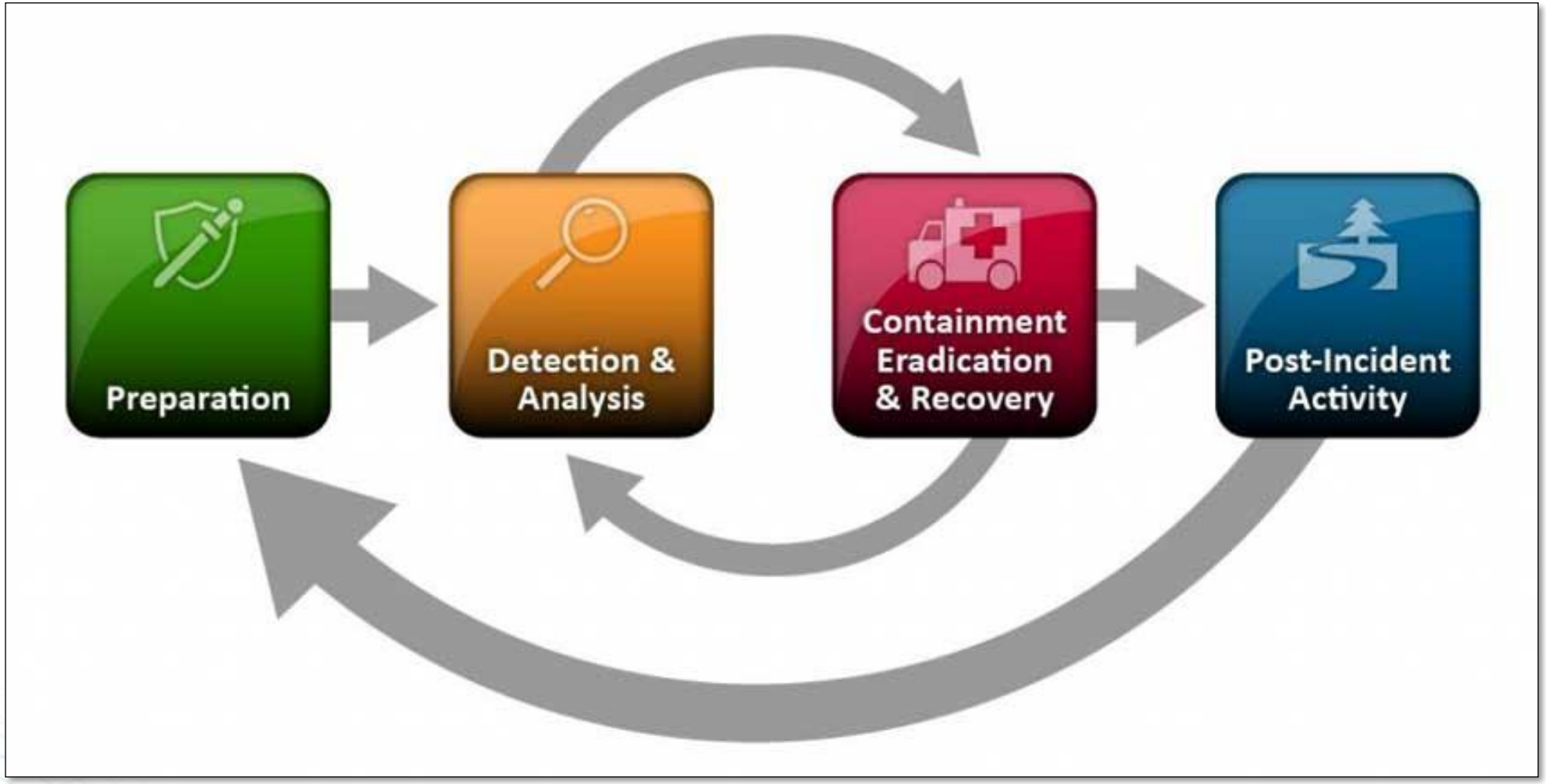
Threat Intelligence Verify Platform


Safe Domain
NEITHInsight
2
compare
NEITHDNS
4
Access
Web
DNS
response
3
1
DNS query
Malicious Domain
NEITHInsight
2
compare
NEITHDNS
4
Redirect to
alert page
DNS
response
3
1
DNS query

7x24 專業團隊協助監控

NEITHNET
Accelerate Your Insight

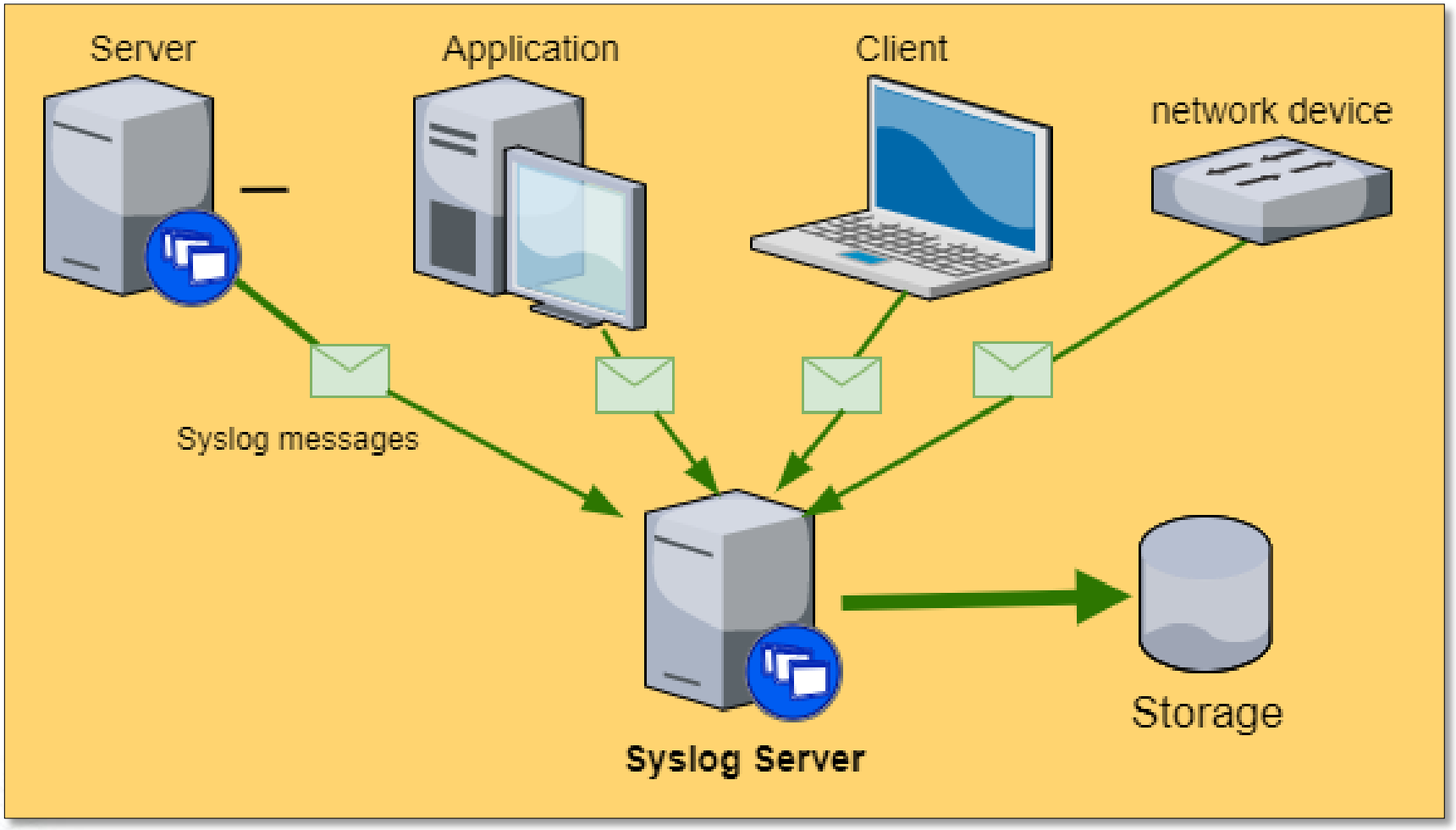
主動威脅獵捕



資安事件協助調查及處理

減少威脅誤判

漏洞管理


Server
Application
Client
network device
Syslog messages
Storage
Syslog Server

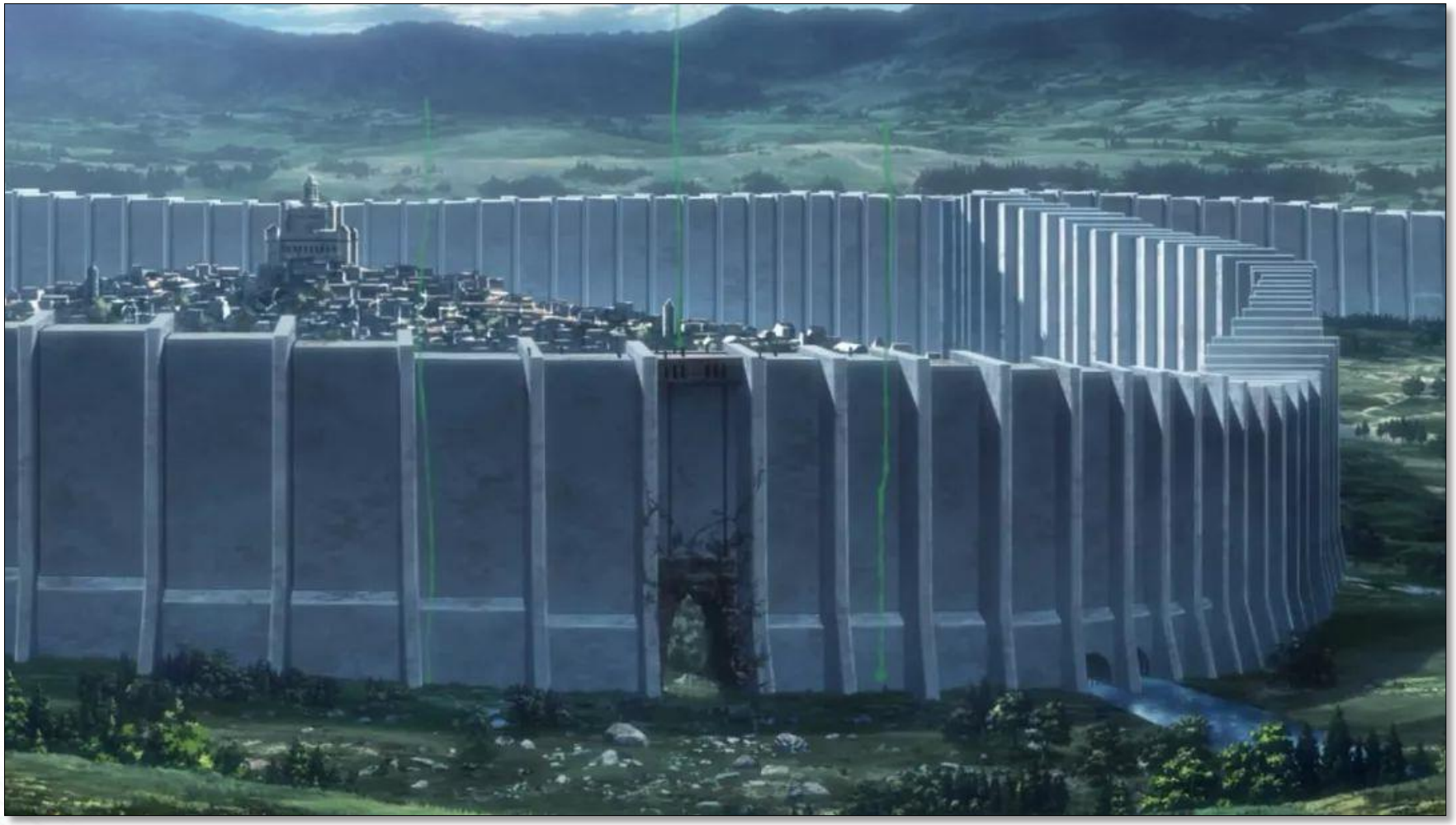
日誌管理

符合規範的報告

低投資、高報酬

Sensitive Data **Loss**

機敏資料外洩



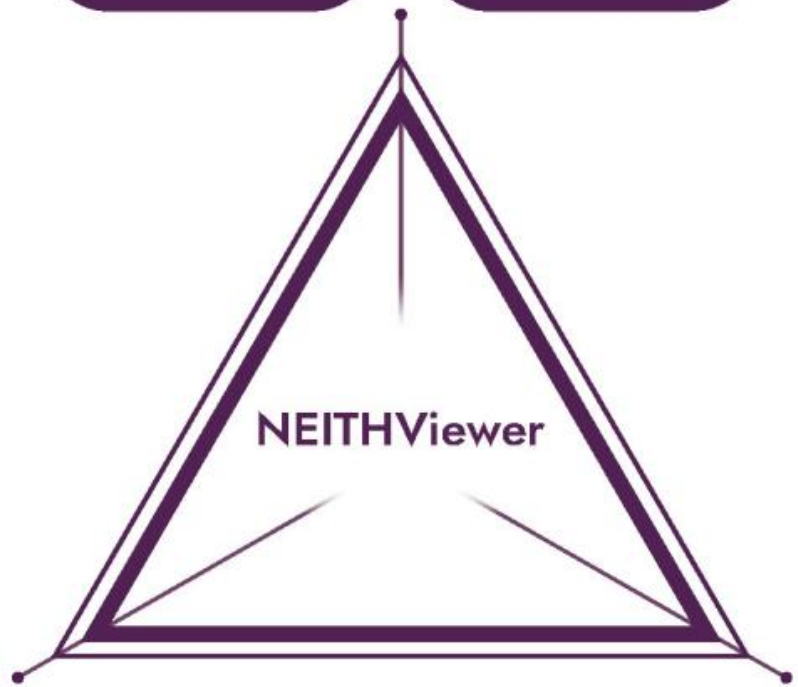
曝露企業資安防護上的弱點


Canon


brother


B Y O D
Bring your own device

惡意連線活動



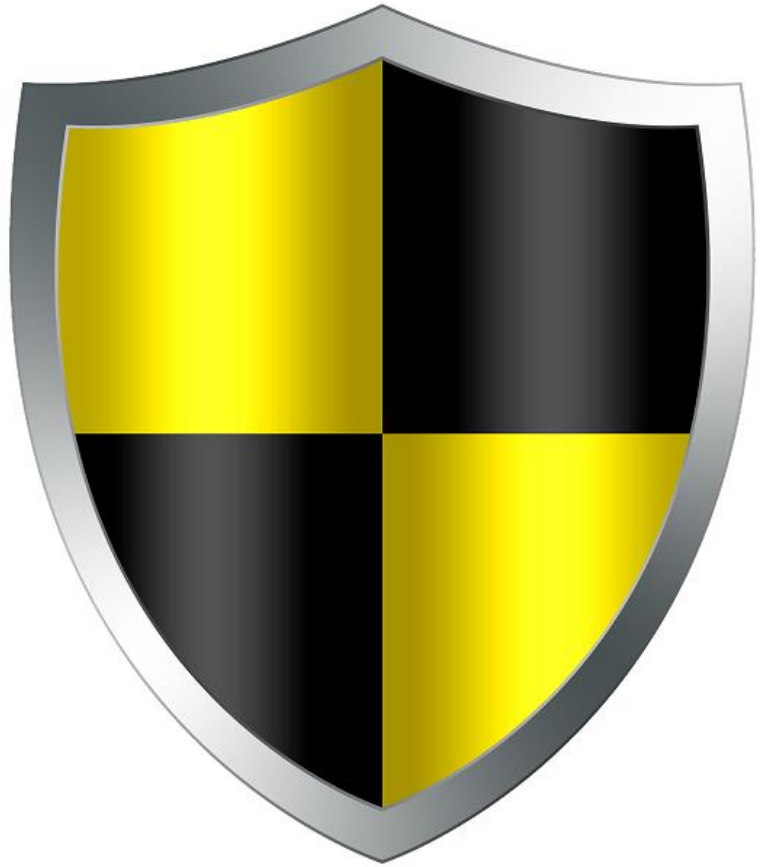
暗樁查找

透過惡意位址與時間回朔
找出曾經連到惡意位址的內網主機

內網擴散

找出內網中異常的
網路行為、流量、連線

NEITHSeeker



NEITHViewer

NEITHInsight

Thank you!

NEITHNET

www.neithnet.com

NEITHNET
Accelerate Your Insight

《議程問卷》

憑填寫完成畫面，於出口處領取精美小禮

關鍵在地情資，化解遇駭危機