數位偵察機

從駭客視角掌握企業資安防線

Kevin Tang 2018/3/1

外部資安防線偵察機 - RiskIQ

#1 Leadership

200+ Enterprise Customers

18k+ Security Analysts

150+ Employees

- 外部數位威脅管理的領導品牌
- 位於舊金山，成立於2009年
- 知名創投
  Summit Partners, Battery Ventures, Georgian Partners, MassMutual Ventures

FORRESTER®
WAVE LEADER 2016
Digital Risk Monitoring

RISKIQ

iSecurity
The Hub of Security Innovations

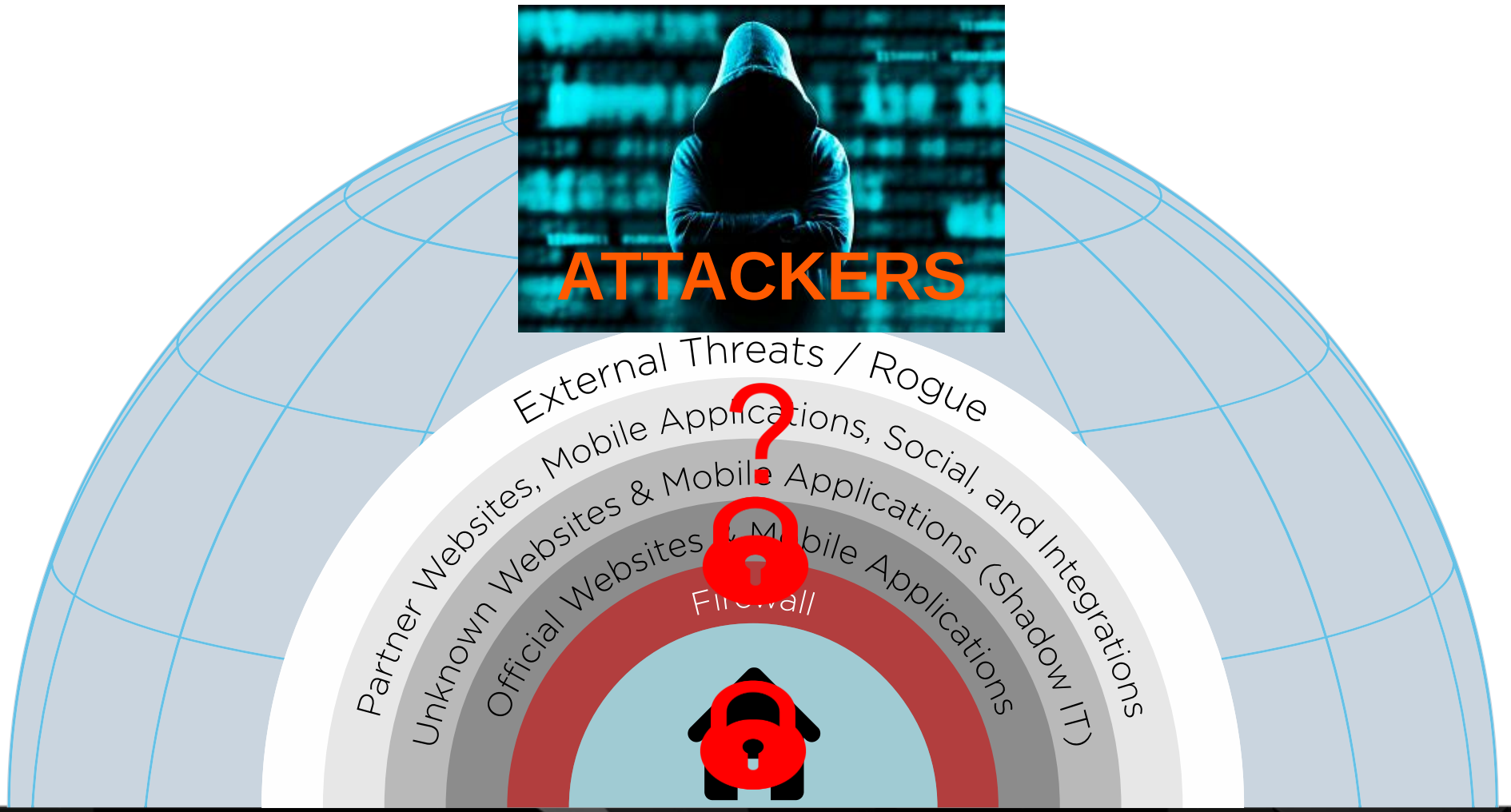

Visibility 能見度

您有多少外部數位資產？

- 據RiskIQ客戶資料統計，導入RiskIQ的服務後，平均發現多出了*30%*的數位資產，這都是在過去確實存在卻不為客戶所知的。

您如何對不知道其存在的資產進行防護？

防火牆有些什麼？


ATTACKERS
External Threats / Rogue
Partner Websites, Mobile Applications, Social, and Integrations
Unknown Websites & Mobile Applications (Shadow IT)
Official Websites & Mobile Applications
Firewall

RiskIQ幫助您...

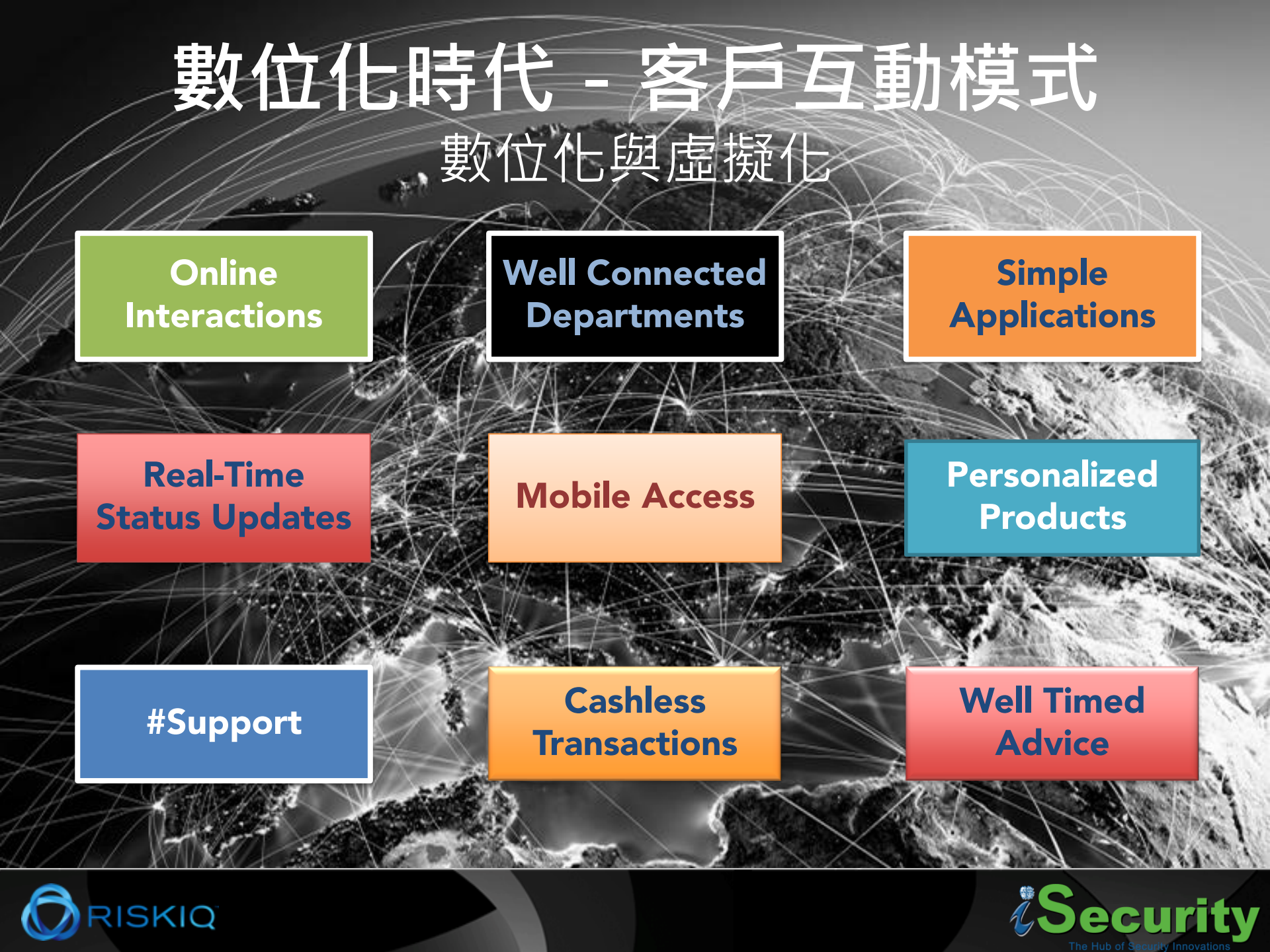
找到茫茫網海中與您相關的數位資產

已知
未知
偽冒

Knowing is the Best Defense.

數位化時代 - 客戶互動模式

數位化與虛擬化



企業開始投入各種數位頻道

Websites　Web Apps　Mobile Apps　Social Profiles

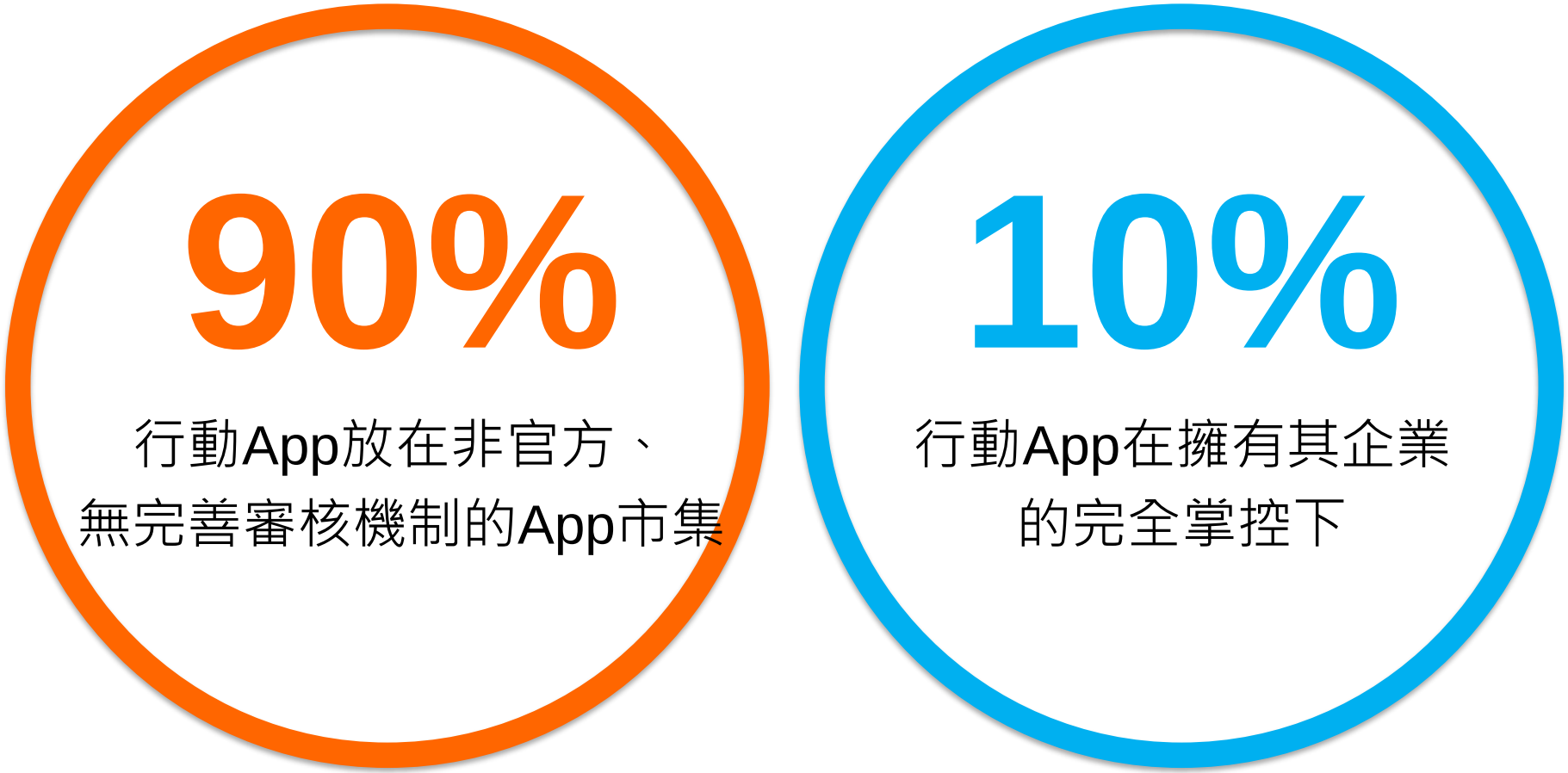
電腦罪犯也是...

勒索軟體	Up 11x y/y
釣魚	155k sites FY16
惡意軟體	2000+ / day Q3-16
品牌濫用	2,754+ cases FY16
流氓App	Up 135% y/y
偽冒社群帳號	83M (Facebook)
惡意廣告	Up 136% y/y

透過未妥善管理的外部數位資產進行入侵；偽冒值得信賴的品牌、商標及社交資訊對用戶進行詐騙

電腦罪犯的新戰場

Easy to Attack **vs.** **Difficult to Attack Directly**

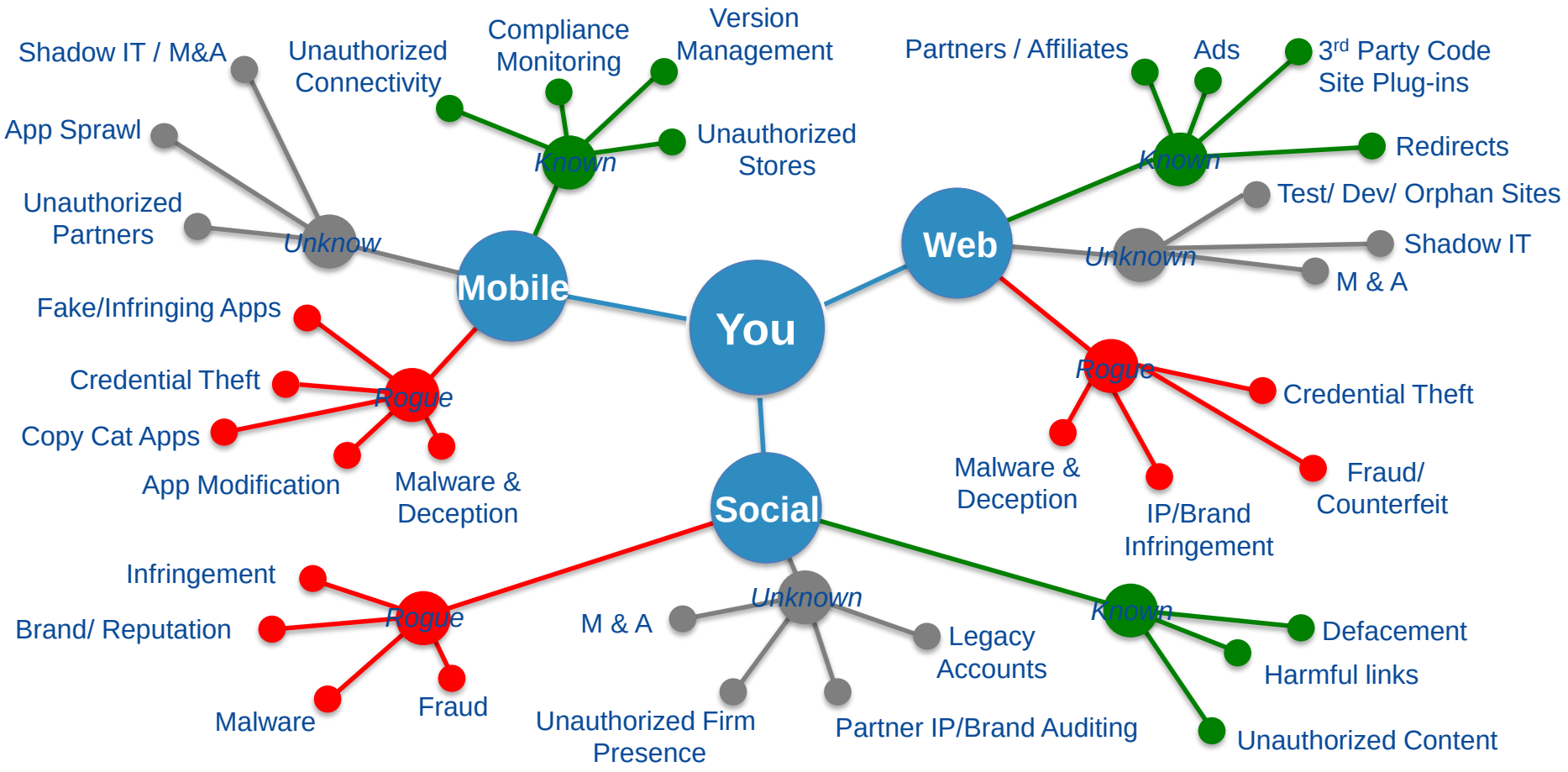


RiskIQ's Q2 2017 Mobile Threat Landscape Report

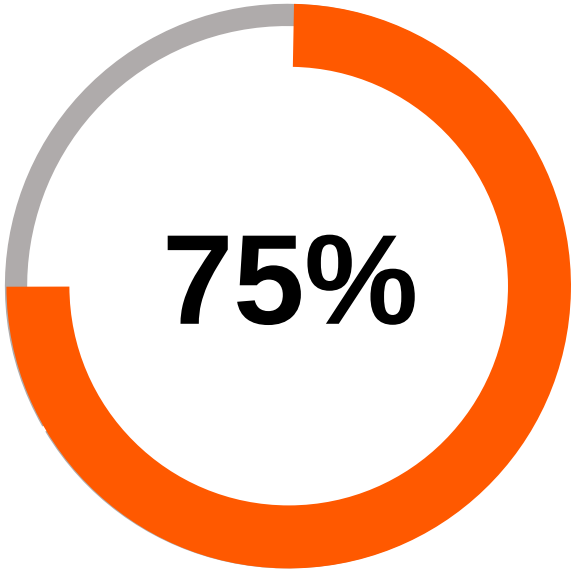
外部戰線持續擴大

- Website, Microsite
- Mobile Apps
- Forgotten, Abandoned Properties
- Test Servers
- Social Media Properties

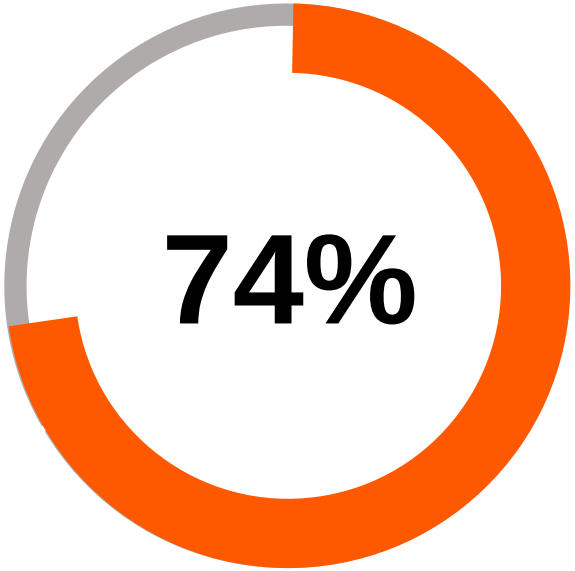
Attack Surface



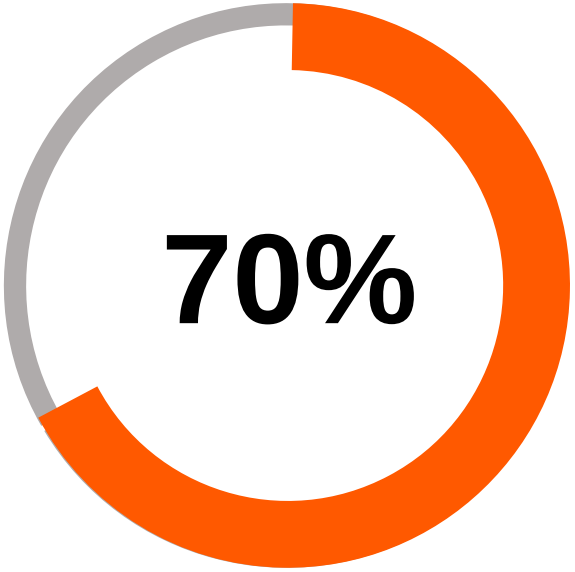
防火牆外的安全議題浮現



資料洩漏的突破口
來自外部威脅



無法找出
發起攻擊的
外部威脅為何



缺乏縮小
受攻擊面(Attack Surface)
的有效方法

Verizon Data Breach Investigations Report (2017)
The SANS Continuous Monitoring Survey (2016)

？攻擊者在忙些什麼？

北韓駭客「水坑式攻擊」　搶劫國際大型銀行

▲北韓如果真的參與去年竊取孟加拉央行案件，就是國家搶銀行。（圖／示意圖／達志影像）

駭客先在金融監管機構網站植入病毒（JavaScript或HTML編碼），當訪客造訪網頁時，就會被引導到另一個偽造的惡意網站，下載惡意軟體的程式。

原文網址: 北韓駭客「水坑式攻擊」搶劫國際大型銀行 | ETtoday國際 | ETtoday新聞雲 https://www.ettoday.net/news/20170328/893559.htm#ixzz54VPYDYrR

？攻擊者在忙些什麼？

新聞

Check Point：駭客大舉掃描網路伺服器安全漏洞，700台伺服器淪為採礦機

Check Point警告一駭客大規模掃描全球30%的網路伺服器，包含PHP、Microsoft IIS與Ruby on Rails等，察探是否存在安全漏洞，藉此植入XMRig採礦程式，目前已有700台伺服器淪陷，成為駭客採礦幫手。

文/ 陳曉莉 | 2018-01-16 發表

？攻擊者在忙些什麼？

【2018關鍵趨勢10：GDPR】歐盟最嚴格個資法規範來了，想跟歐洲做生意都得遵守GDPR

號稱歐盟最嚴格個資法的GDPR，未來只要網站或服務會直接或間接蒐集、處理和利用歐盟民眾個人可識別資料時，都將強制受到GDPR的規範

文/ 黃彥棻 | 2017-12-31 發表

讚 4.6 萬 按讚加入iThome粉絲團 讚 35 分享 G+

？攻擊者在忙些什麼？

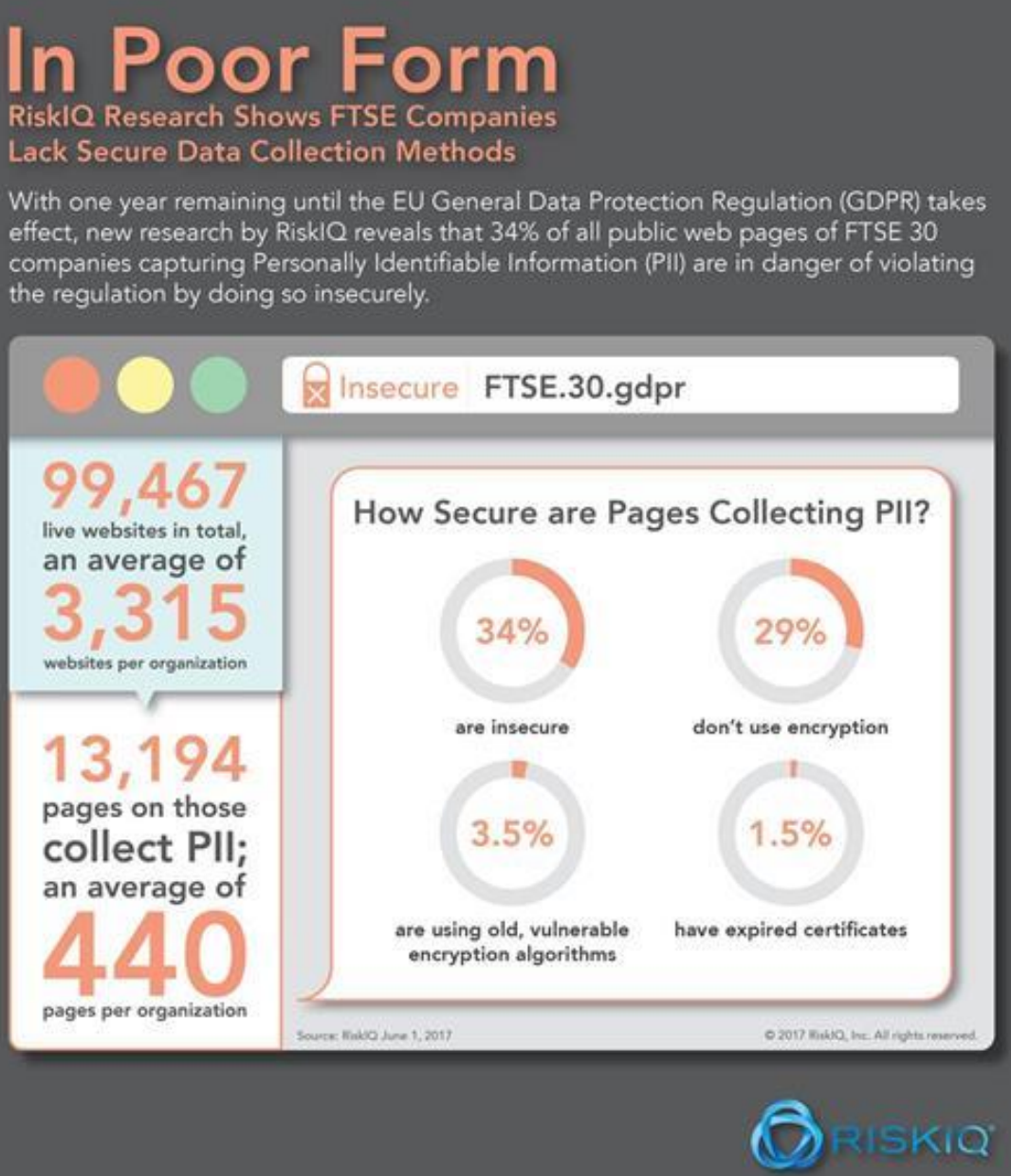
依GDPR規定，企業若未遵循法規要求，主管機關得進行調查，**最重更可裁處企業2,000萬歐元、或該年度全球營業額4%的罰鍰（取其高者）。**

企業必須知道正在蒐集什麼樣的資料和其資料來源

根據RiskIQ去年針對FTSE 30的研究，發現對外蒐集客戶個資的網頁中，有高達三成的網頁是在不安全的狀況下進行個資蒐集。

34%的個資收集網站不安全

29% 沒有加密；
3.5%使用老舊、含有漏洞的加密；
1.5%憑證過期。



更多案例...

2013年5月政府電子公文交換系統遭到駭客入侵，提供該軟體直接下載的網站，被置換成惡意程式，對外連線到不明的中繼網站，預估超過7,000個政府機關受到影響。

- 中華民國交通部觀光局網站被植入惡意連結
- 1111 人力銀行網站被植入惡意程式
- 八大電視台網站又被植入惡意連結
- 佛教慈濟綜合醫院網站又被植入惡意連結
- 台灣達人秀網站被植入病毒下載網址
  (約2500網友受威脅)

……

全盤的掌握您的外部數位資產

SSL 憑證過期、破損?
有多少公司網站頁面使用各類的第三方元件, 如 Facebook Like, tracking code, Open Source Library, iFrame, Widget…?
Web Server的架構、版本是否存在已知漏洞?
網站內哪些login form不安全?
有哪些網站用於蒐集PII相關資訊?
總共有多少個重新導向連結 (redirect) 破損
總共有幾個 Web Sites
今天有任何新註冊的網站掛在公司Domain?
今天有任何公司網站登記email被變更?
今天有任何新網站掛在公司的IP下?
多少公司網站30天內註冊會到期?
有多少公司網站被植入惡意軟體或釣魚網站連結?
有那些公司網站今天Active/Inactive?
重新導向的連結會導向到哪邊網站?
我們能掌握那些重新導向的連結內容有被變更?

新的思維角度

內部防衛了，外部更要掌握

您不能在客戶、Partner 端裝上防火牆或防護軟體，但您還是能做一些事的，例如即時監控、掃描、自動化預警或進一步先移除惡意仿冒資產...等

資安的防護無法僅滿足於內部!

掌握外部的關鍵

Doing the Right Things Right

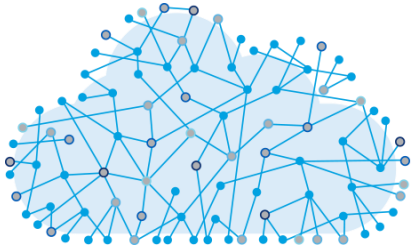
目前狀態

各式不同的情報

各式的工具組

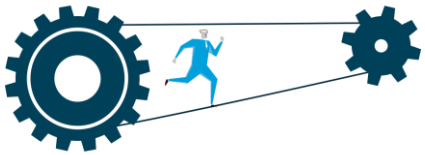
低效率

理想狀態

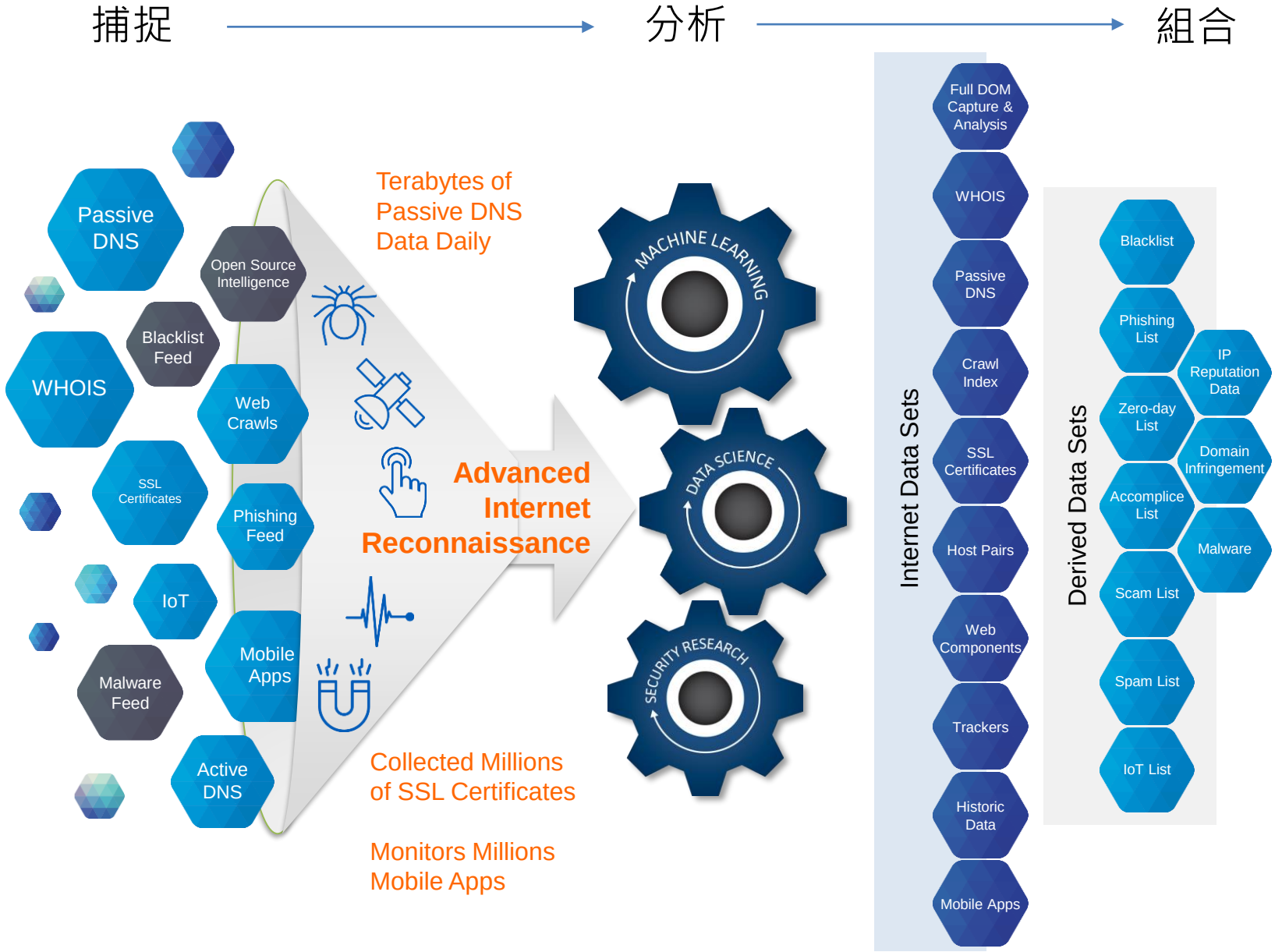


綜整情報
大數據分析

統一的工具組



高效率


捕捉
分析
組合
Passive DNS
Open Source Intelligence
Blacklist Feed
WHOIS
Web Crawls
SSL Certificates
Phishing Feed
IoT
Mobile Apps
Malware Feed
Active DNS
Terabytes of Passive DNS Data Daily
Advanced Internet Reconnaissance
Collected Millions of SSL Certificates
Monitors Millions Mobile Apps
MACHINE LEARNING
DATA SCIENCE
SECURITY RESEARCH
Internet Data Sets
Full DOM Capture & Analysis
WHOIS
Passive DNS
Crawl Index
SSL Certificates
Host Pairs
Web Components
Trackers
Historic Data
Mobile Apps
Derived Data Sets
Blacklist
Phishing List
IP Reputation Data
Zero-day List
Domain Infringement
Accomplice List
Malware
Scam List
Spam List
IoT List

RiskIQ資料收集技術 - Virtual User

防止反偵蒐技術

- 全球地理位置
- 各類流量來源(自用、商用、行動網路)
- 不同時區
- 各瀏覽器、版本、裝置
- 擬人瀏覽行為，滑鼠移動、等待時間、連結點擊、點擊順序、Session長度…等
- 使用者Cookie

大規模數據每日入庫

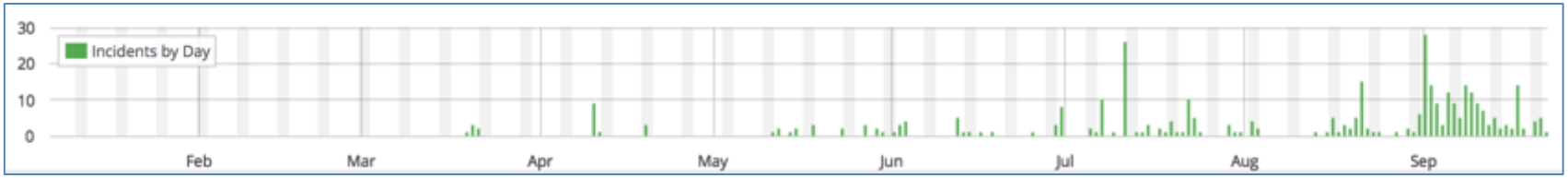
- 1+ TB DNS Data
- 1.8 B web sessions (incl. Doc Object Model)
- 300 M domain records
- 16 Million Mobile Apps

Virtual User實績

2015年9月18日, RiskIQ 偵測到竊取憑證的惡意軟體被植到 jQuery 的下載包中

iFrame on jQuery.com

RiskIQ 的 virtual user 技術偵測到在 jQuery.com 的 DOM 裡面有異常的改變, 於是進一步深入分析該異常連結, 發現有一個 iFrame 會導向連結至攻擊網站 jQuery-cdn.com



Sequence Overview

	Sequence	URL	Ad Network	Cause	Response Code
ℹ	1	http://www.puntdllp.com/punish.phtml?gonext=true&r=	-	topLevelRedirect	302
ℹ	2	http://ierq.alraqdi-museum.com/?PHPSSESID=njrMNruDMh7HApzBKv...	-	redirect	200

思考方向與對策

1. 對外公開的數位資產需做盤點與監控
   - 確實了解組織的受攻擊面
   - 對動態變化的外部資產能同步掌握
   - 了解外部資產可能存在的漏洞及風險

2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
   - 偽冒網站
   - 偽冒手機App
   - 偽冒社交帳號
   - 快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置

3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
   - 能針對可疑IP、Domain、Email快速找出大量關聯資料
   - 資料除當下狀況外，並可追溯過往，拓展調查範圍
   - 與多方鑑識資源連結，節省資訊整合時間
   - 團隊可即時共享調查狀況

思考方向與對策

1. 對外公開的數位資產需做盤點與監控
   - **確實了解組織的受攻擊面**
   - **對動態變化的外部資產能同步掌握**
   - **了解外部資產可能存在的漏洞及風險**

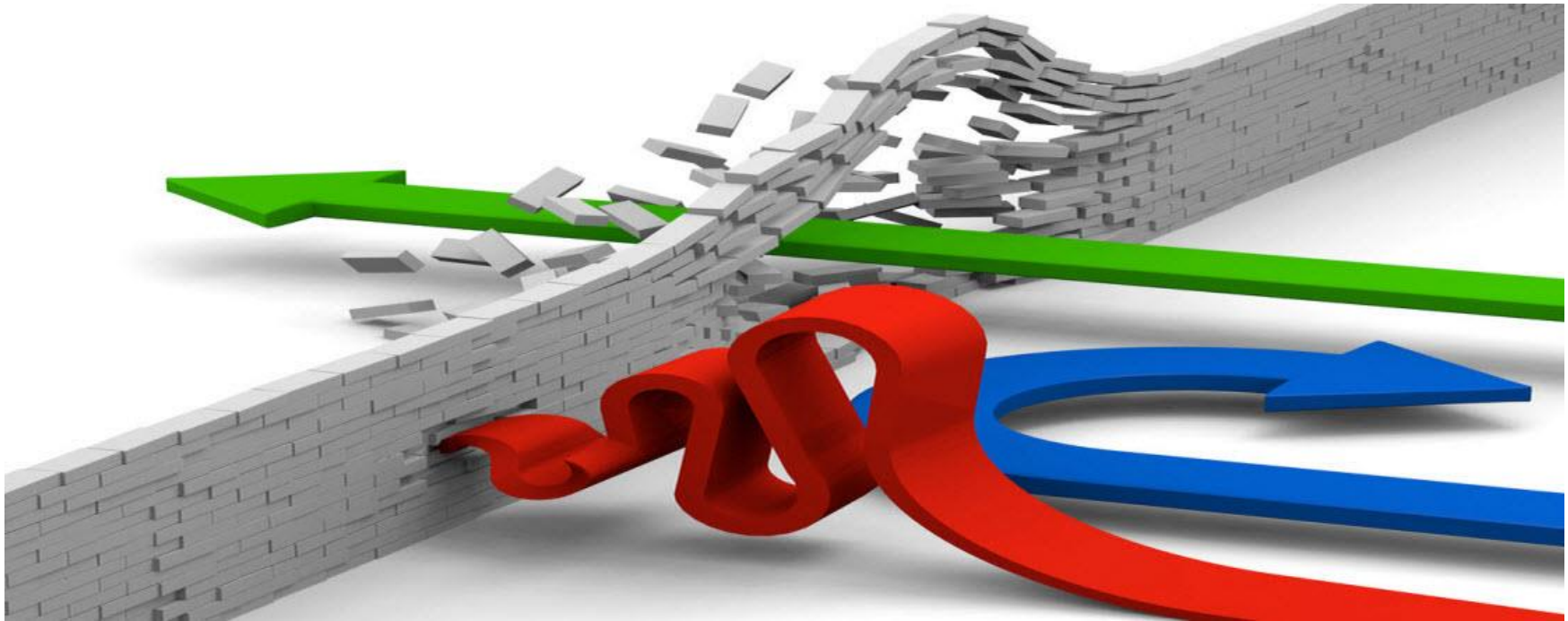
RiskIQ
Digital Footprint

2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
   - 偽冒網站
   - 偽冒手機App
   - 偽冒社交帳號
   - 快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置

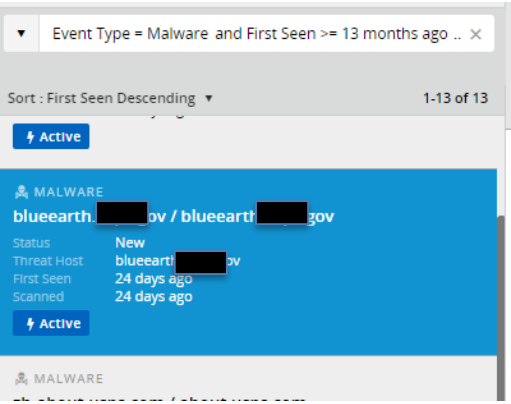
3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
   - 能針對可疑IP、Domain、Email快速找出大量關聯資料
   - 資料除當下狀況外，並可追溯過往，拓展調查範圍
   - 與多方鑑識資源連結，節省資訊整合時間
   - 團隊可即時共享調查狀況

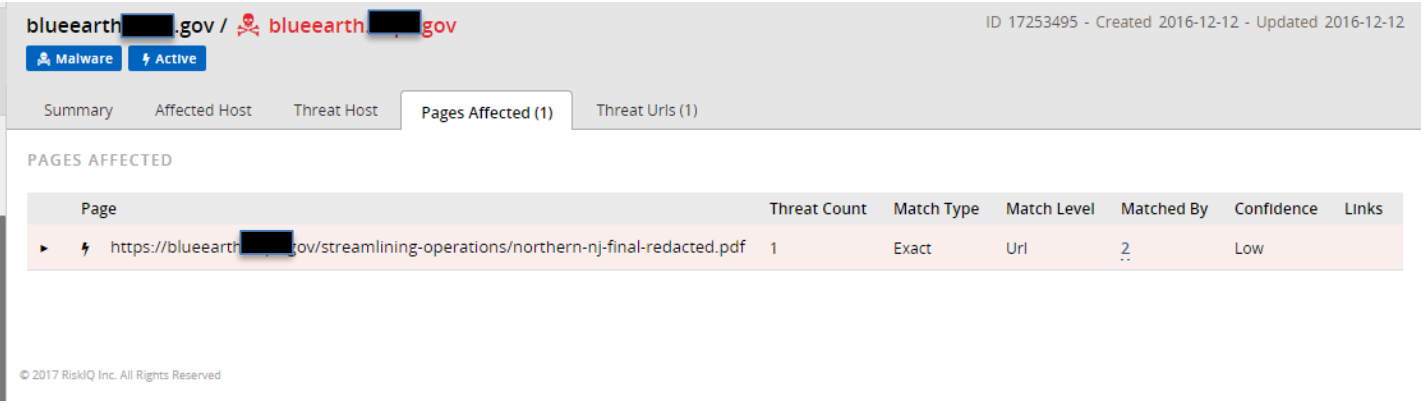
滲透測試不是就夠了嗎?

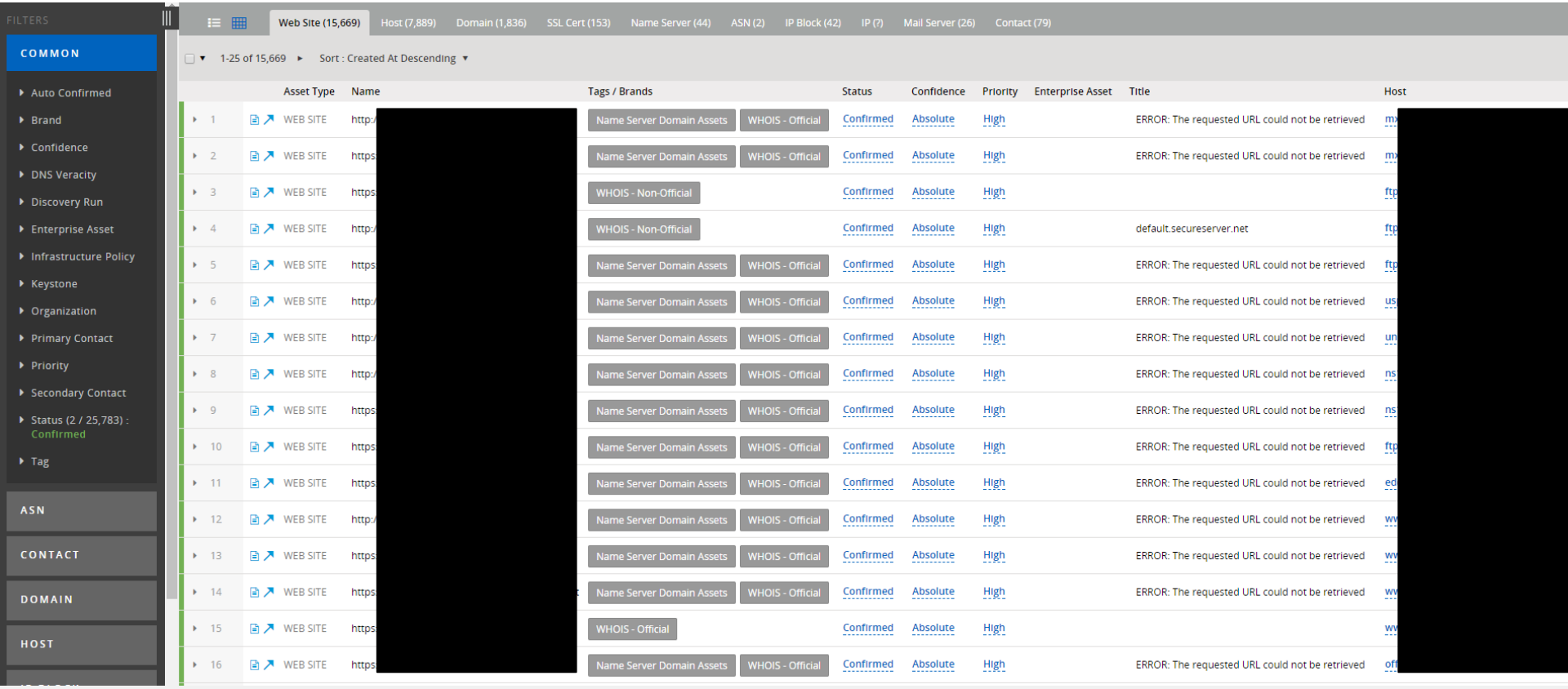
- 得知在測試當下時間點的漏洞，要如何對應這次測試與下次測試之間新發現的漏洞？
- 測試已知給定的範圍，但不知其存在的資產呢？

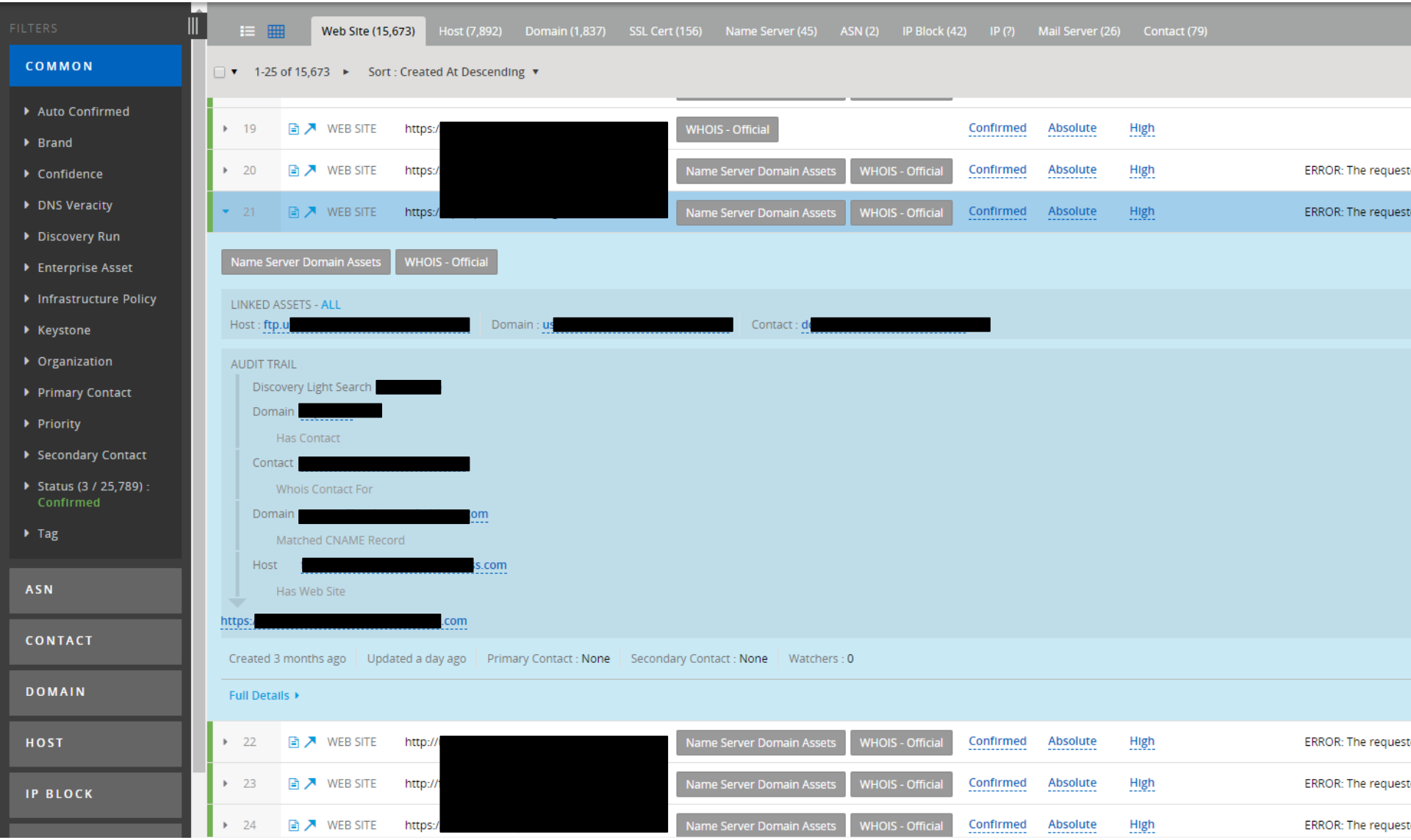


全時監控
才能真正掌握動態變化的數位資產狀態






FILTERS
COMMON
Auto Confirmed
Brand
Confidence
DNS Veracity
Discovery Run
Enterprise Asset
Infrastructure Policy
Keystone
Organization
Primary Contact
Priority
Secondary Contact
Status (2 / 25,783) : Confirmed
Tag
ASN
CONTACT
DOMAIN
HOST
Web Site (15,669)
Host (7,889)
Domain (1,836)
SSL Cert (153)
Name Server (44)
ASN (2)
IP Block (42)
IP (7)
Mail Server (26)
Contact (79)
1-25 of 15,669
Sort : Created At Descending
Asset Type
Name
Tags / Brands
Status
Confidence
Priority
Enterprise Asset
Title
Host
1 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
2 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
3 WEB SITE WHOIS - Non-Official Confirmed Absolute High
4 WEB SITE WHOIS - Non-Official Confirmed Absolute High default.secureserver.net
5 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
6 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
7 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
8 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
9 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
10 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
11 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
12 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
13 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
14 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved
15 WEB SITE WHOIS - Official Confirmed Absolute High
16 WEB SITE Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The requested URL could not be retrieved


FILTERS
COMMON
Auto Confirmed
Brand
Confidence
DNS Veracity
Discovery Run
Enterprise Asset
Infrastructure Policy
Keystone
Organization
Primary Contact
Priority
Secondary Contact
Status (3 / 25,789) : Confirmed
Tag
ASN
CONTACT
DOMAIN
HOST
IP BLOCK
Web Site (15,673)
Host (7,892)
Domain (1,837)
SSL Cert (156)
Name Server (45)
ASN (2)
IP Block (42)
IP (?)
Mail Server (26)
Contact (79)
1-25 of 15,673
Sort : Created At Descending
19 WEB SITE https:/ WHOIS - Official Confirmed Absolute High
20 WEB SITE https:/ Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The request
21 WEB SITE https:/ Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The request
Name Server Domain Assets
WHOIS - Official
LINKED ASSETS - ALL
Host : ftp.u
Domain : us
Contact : d
AUDIT TRAIL
Discovery Light Search
Domain
Has Contact
Contact
Whois Contact For
Domain
om
Matched CNAME Record
Host
s.com
Has Web Site
https:
.com
Created 3 months ago
Updated a day ago
Primary Contact : None
Secondary Contact : None
Watchers : 0
Full Details
22 WEB SITE http:// Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The request
23 WEB SITE http:// Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The request
24 WEB SITE https:/ Name Server Domain Assets WHOIS - Official Confirmed Absolute High ERROR: The request

GLOBAL INVENTORY INSIGHTS

+ ADD INSIGHT

233	Individual IPs with an Open Port IPs seen with at least 1 port open in the last 14 days	24	At Risk Frameworks Sites using at risk frameworks with known vulnerabilities
9	Expired SSL Certs Confirmed Certificates which have expired.	81	At Risk Servers Servers with Operating Systems that have known vulnerabilities
2	Untrusted Certificates WoSign and StartCom Certificates | Symantec-Owned EV Certificates	111	Site Access Login and Signin Pages
6	OpenSSL Sites using OpenSSL potentially susceptible to the Heartbleed vulnerability	90	All Wordpress and Drupal Sites Sites operating on Drupal & Wordpress
27	Broken Redirects Sites that Redirect however the final URL response code is 4xx or 5xx	5	SHA-1 Certs SSL Certificates using SHA-1
58	Test Sites Potential Test Sites		

對策

1. 對外公開的數位資產需做盤點與監控
   - 確實了解組織的受攻擊面
   - 對動態變化的外部資產能同步掌握
   - 了解外部資產可能存在的漏洞及風險

RiskIQ External Threats

2. 如何應對偽冒的惡意攻擊事件，以防止商譽受損
   - **偽冒網站**
   - **偽冒手機App**
   - **偽冒社交帳號**
   - **快速發覺可疑事件，透過足夠資訊做判斷，具備快速的流程做處置**

3. 如何使資安調查團
   - 能針對可疑IP 資料
   - 資料除當下狀
   - 與多方鑑識資
   - 團隊可即時共

對網路釣魚行為的監控

新聞

資安周報第53期：8成釣魚網站快閃詐騙，資安產品難防，強化員工警覺才是對策

根據資安公司Webroot的調查結果發現，今年有84%的釣魚網站存活時間低於24小時，平均存活時間低於15小時，最長存活時間為44小時，最短則只有15分鐘，增加資安公司偵測難度。最常被駭客用來模仿欺騙使用者的網站，今年前4名網站依序是Google、Yahoo、Apple、PayPal和富國銀行

文/ 黃彥棻 | 2016-12-15 發表

資安公司Webroot調查顯示，2016年1月～9月期間，有84%的釣魚網站存活時間短於24小時。

WEB

fullHost

fullDomain

host | domain | tld

url: http://www.irs-tax-settlement-hq.com/…

content

title

responseBody

- **Typosquatting 近似域名**

  domain.com vs. domaiin.com

- **Homoglyphs 同形**

  domain.com vs. dornain.com

- **埋在Domain或Subdomain**

  yourbrand.com vs.

  iswearimnotyourbrand.com

  yourbrand.imnotabadsiteiswear.com

- **Punycode**

  xn--riskiqbnk-ora.com

  riskiqbånk.com  riskiqbank.com

SOCIAL

Profile Name
- Not unique to user
- Changeable with keeping the same username
- *Available field: socialName*

Username
- Unique to user
- Contained in homepage URL
- *Available field: socialUsername*

Description
- *Available field: socialDescription*

Location
- Not currently target-able

Profile Link
- Not unique to user, but limited to 1 per profile
- *Available field: socialProfileLink*

Profile Homepage: https://twitter.com/Wikimedia

Followers
- a.k.a. Likes, Friends, Connections, or Subscribers, etc.
- Not currently target-able

MOBILE

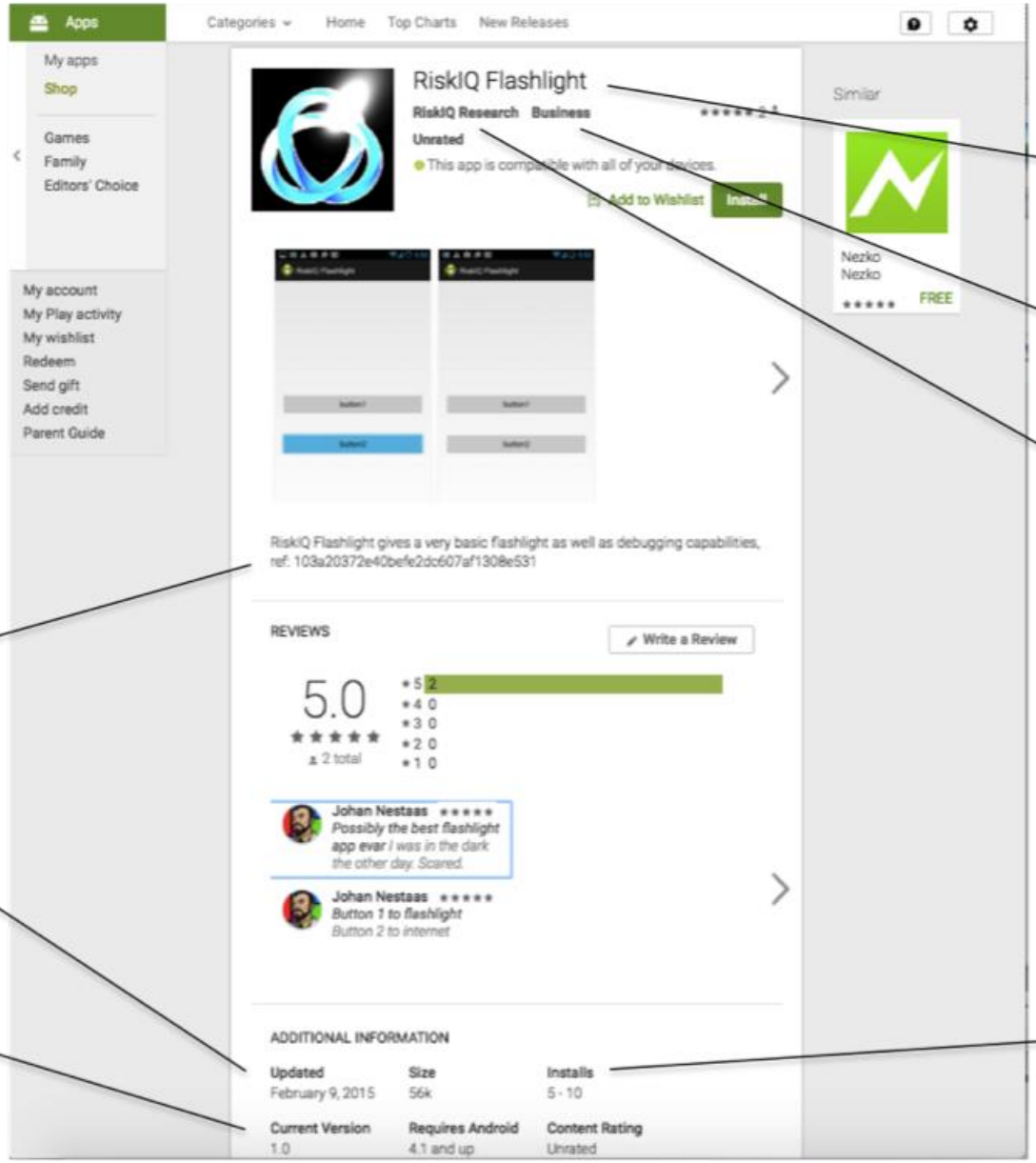
App: https://play.google.com/store/apps/details?id=com.riskiq.riskiqflashlight

App URL

- Contains store name and a unique identifier for the app, such as the title, official ID, or store-specific ID

Package Name/Official ID

- Available field: officialID



App Name

- Available field: title

Category

- Available field: category

Developer

- Available field: developer

App Description

- Available field: description

Date of Publication/Update

- Available field: releaseDate

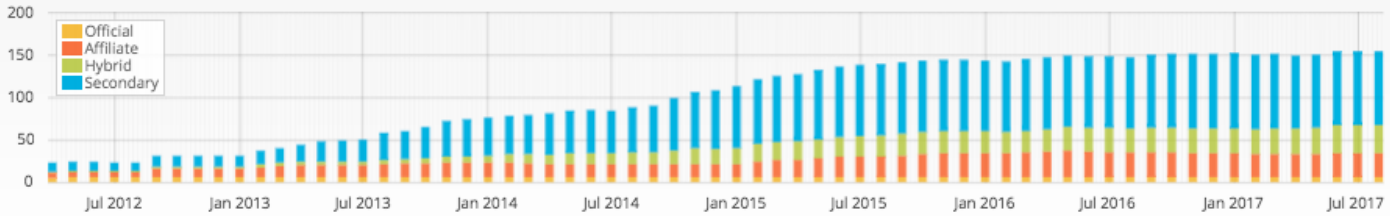
App Version

- Available field: currentVersion

Downloads

- Not currently targetable

23,642,734	188	100	8	9
Active Apps	Stores	Active Stores	Platforms	Languages



CURRENT EVENT STATUS

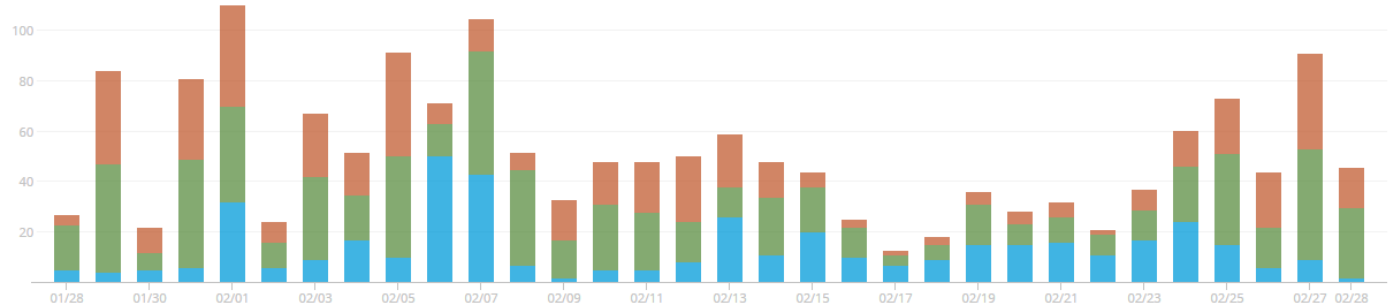
1,424	30	10	1	639	252	309	2,273
New	Review	Confirmed	Enforced	Tenacious	Monitor	Resolved Past Month	Active

CURRENT COUNTS BY TYPE

Malware	3
Phish	6
Domain Infringement	1,006
Rogue Mobile App	72
SSL	217
Web Compliance	56
Content	254
Infrastructure	415
Social	327
All	2,356

HISTORICAL DATA

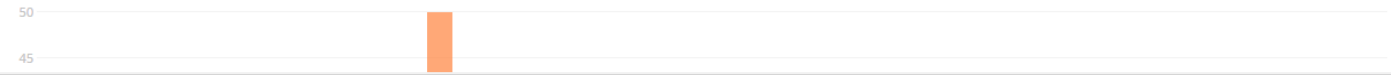
STATUS CHANGES BY DATE



TOTAL STATUS CHANGES

427	New
705	Resolved
508	Tenacious
1,640	All

EVENT CREATION BY DATE



TOTAL EVENT CREATIONS

1	Phish
170	Domain Infringement

對策

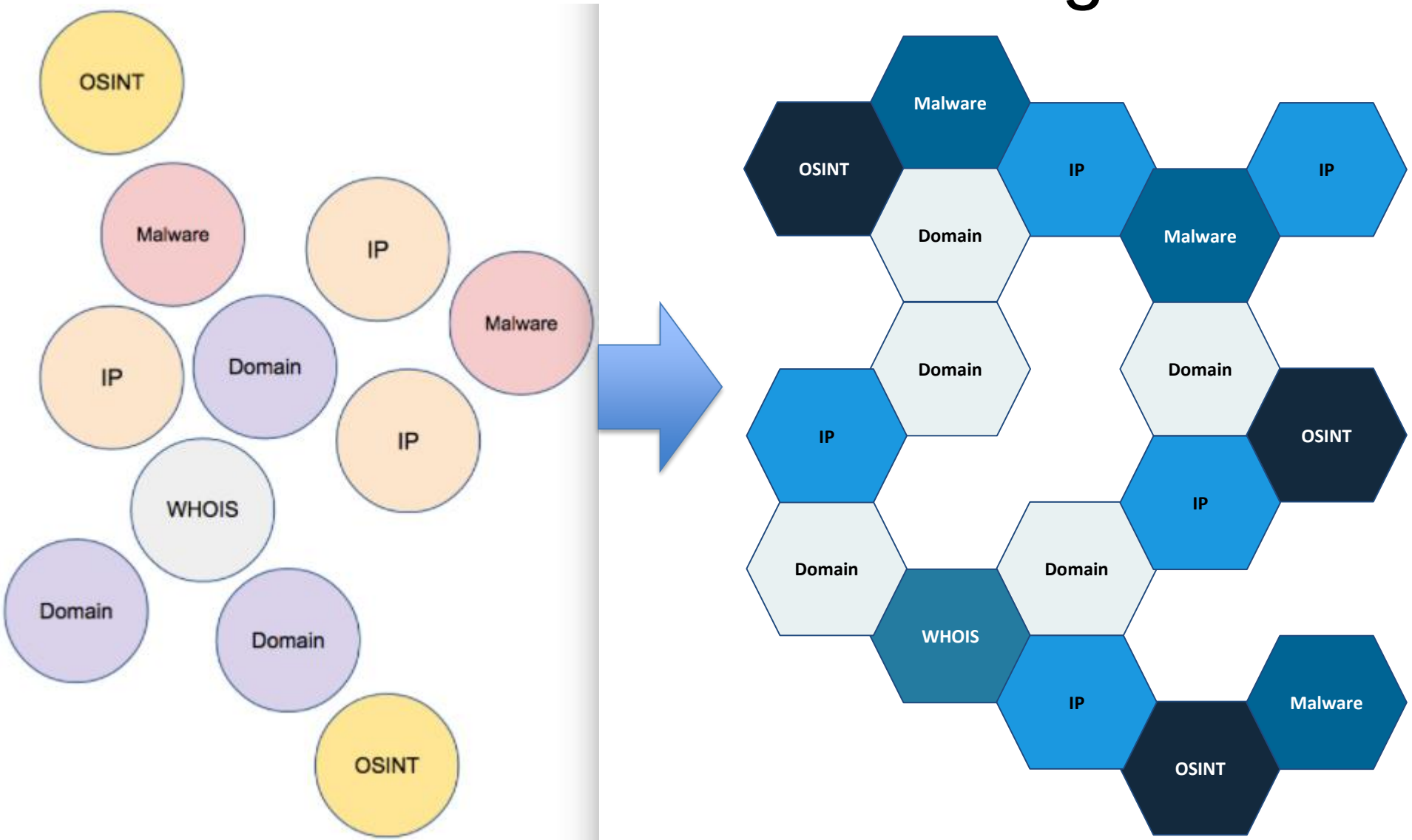
1. 對外公開的數位資產需做盤點與監控
   - 確實了解組織的受攻擊面
   - 對動態變化的外部資產能同步掌握
   - 了解外部資產可能存在的漏洞及風險

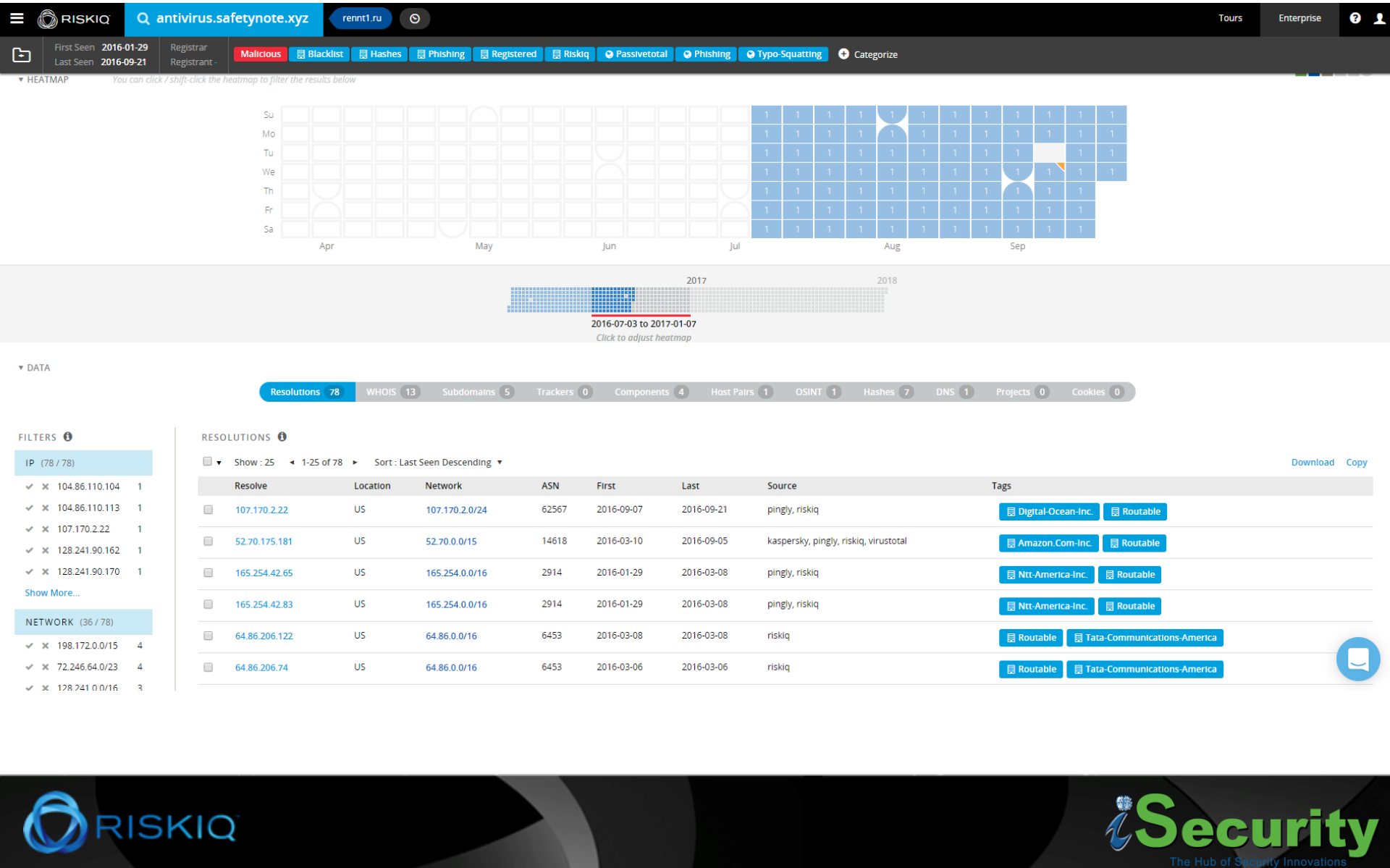
2. 如何應對偽冒的惡意攻擊事件
   - 偽冒網站
   - 偽冒手機App
   - 偽冒社交帳
   - 快速發覺可

RiskIQ
PassiveTotal

3. 如何使資安調查團隊發揮極大效能，主動面對攻擊來源
   - **能針對可疑IP、Domain、Email快速找出大量關聯資料**
   - **資料除當下狀況外，並可追溯過往，拓展調查範圍**
   - **與多方鑑識資源連結，節省資訊整合時間**
   - **團隊可即時共享調查狀況**

Infrastructure Chaining





Passive DNS

- Historical set of records for the resolutions of domains and IP addresses. Reveals patterns of attackers and derives timelines

WHOIS

- Repository of registrant information that can provide leads on connecting different data points together. Sometimes reveals actor patterns

Subdomains

- Any hosts (host.domain.com) that have been seen related to the domain or IP address

OSINT

- Open source intelligence, both long and short form provided by individuals and companies.

Hashes

- PassiveTotal partners with a number of commercial and open source repositories of malware data.

Trackers

- Unique fingerprints identified within web page content that correlates to a single point. Helpful in surfacing abuse such as phishing

Components

- Technology used on websites or on IP addresses. This information can include web server software, operating system, web app frameworks.

Host Pairs

- Sequence data obtained from crawling the internet like a user. Identifies related hosts based on dependencies, linking, or redirection.

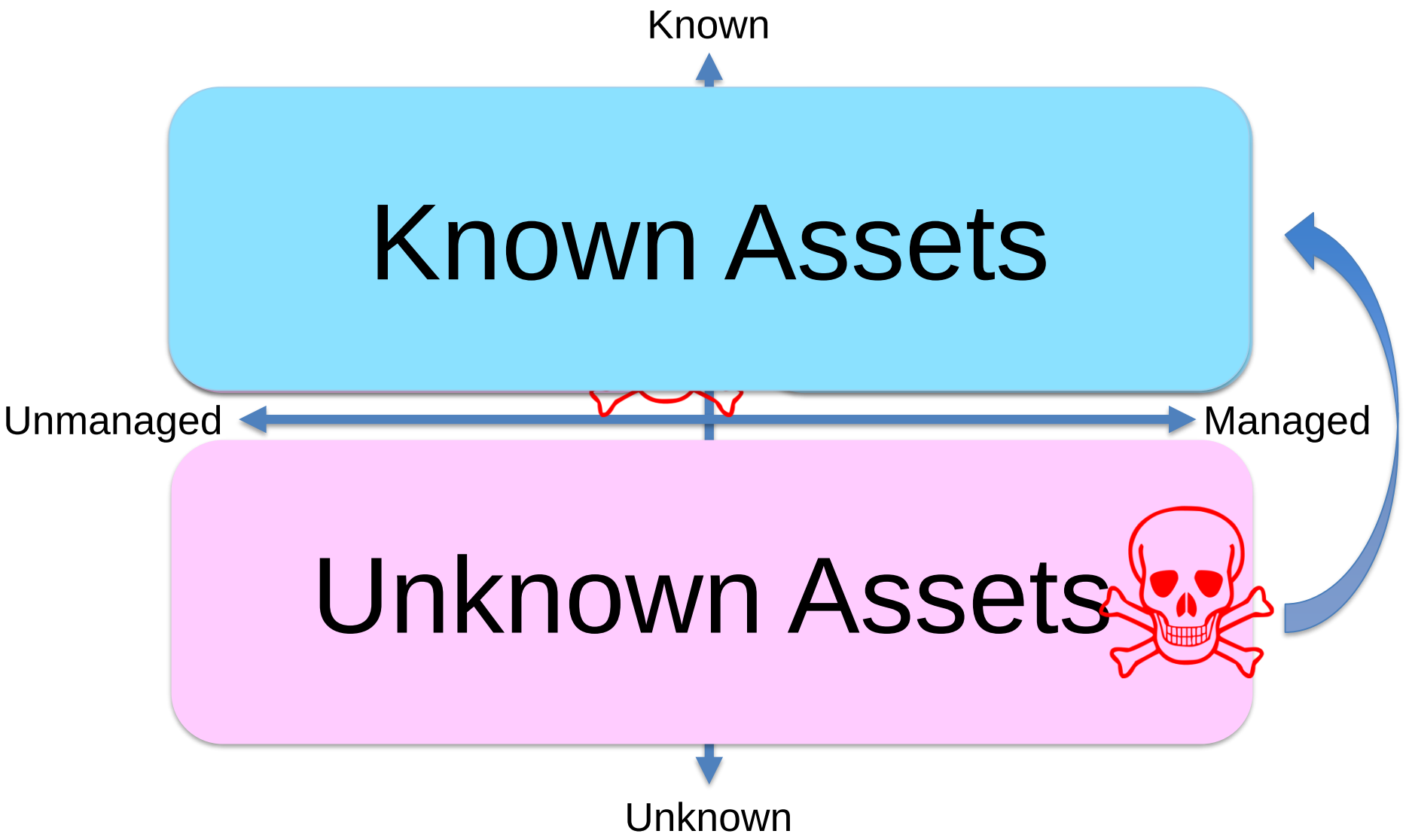
DNS

- MX (mail exchanger), NS (nameserver), TXT (text), SOA (start of authority), CNAME (canonical name) records

您有多少外部數位資產？

您如何對不知道其存在的資產進行防護？

賦予企業對自身外部資產的能見度



KNOWING IS THE BEST DEFENSE™