Openfind™

MAILGATES 郵件防護系統

全方位郵件防護：效能·控管·備援

SEP 社交工程防護模組

網擎資訊

TAIWAN EXCELLENCE 2008

vmware READY

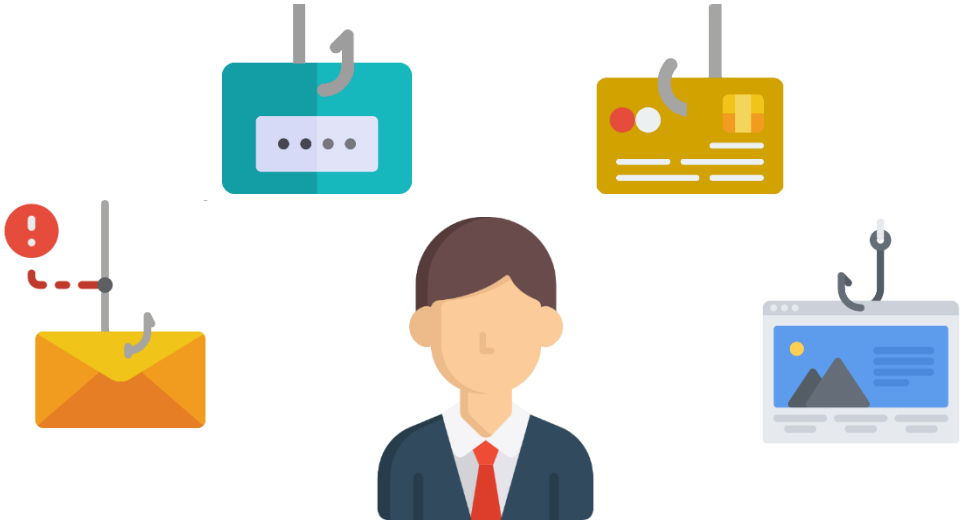
citrix ready

IPv6 READY

Openfind™ Software Engineered for Growth™

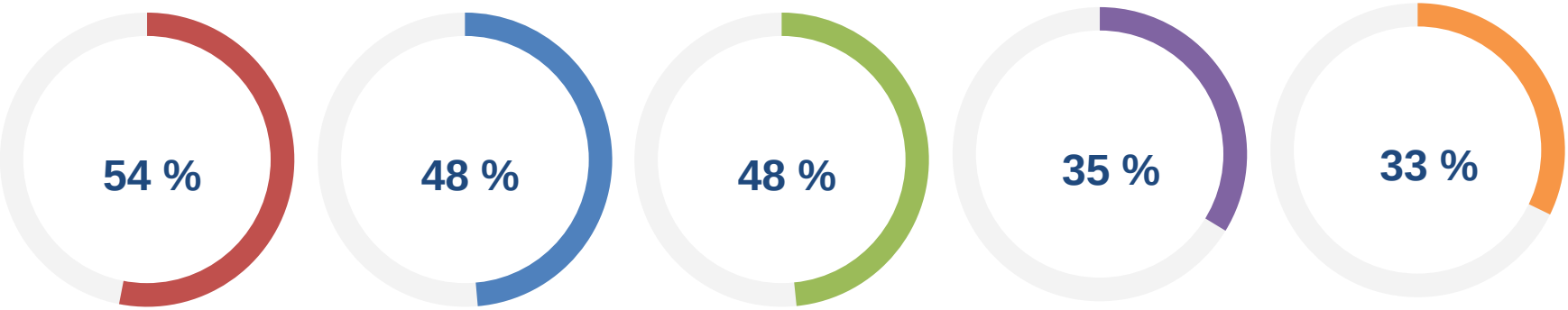
什麼是社交工程攻擊？

社交工程 (Social Engineering) 是利用人性弱點，透過偽冒信件與釣魚連結，以騙取使用者帳號、密碼或機敏資料，進而鎖定目標發動攻擊。



社交工程攻擊的種類

社交工程攻擊的影響



重要資料被竊取

身分驗證資訊外洩

感染勒索病毒

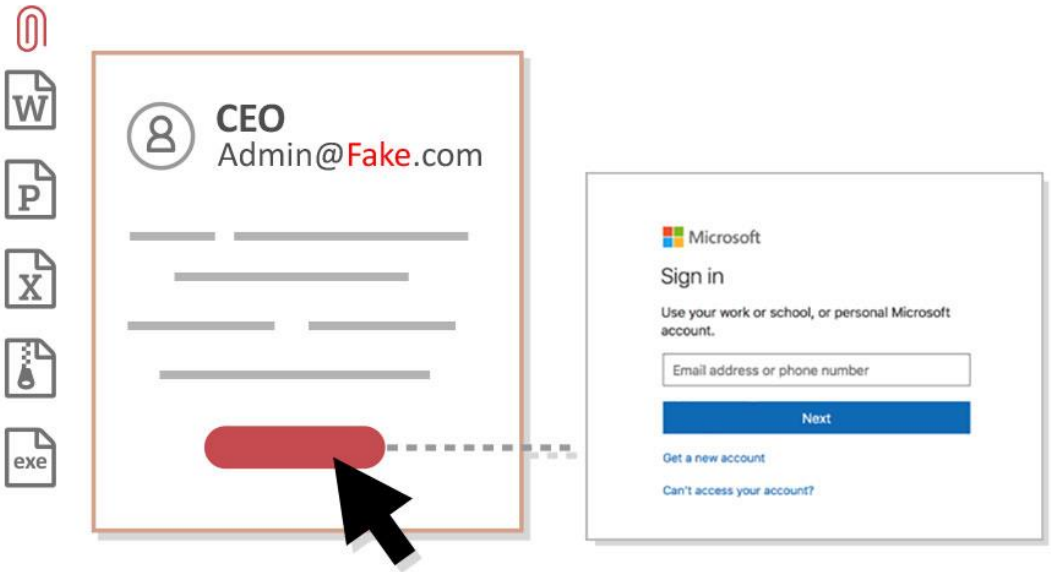
感染惡意程式

財務損失電匯詐騙

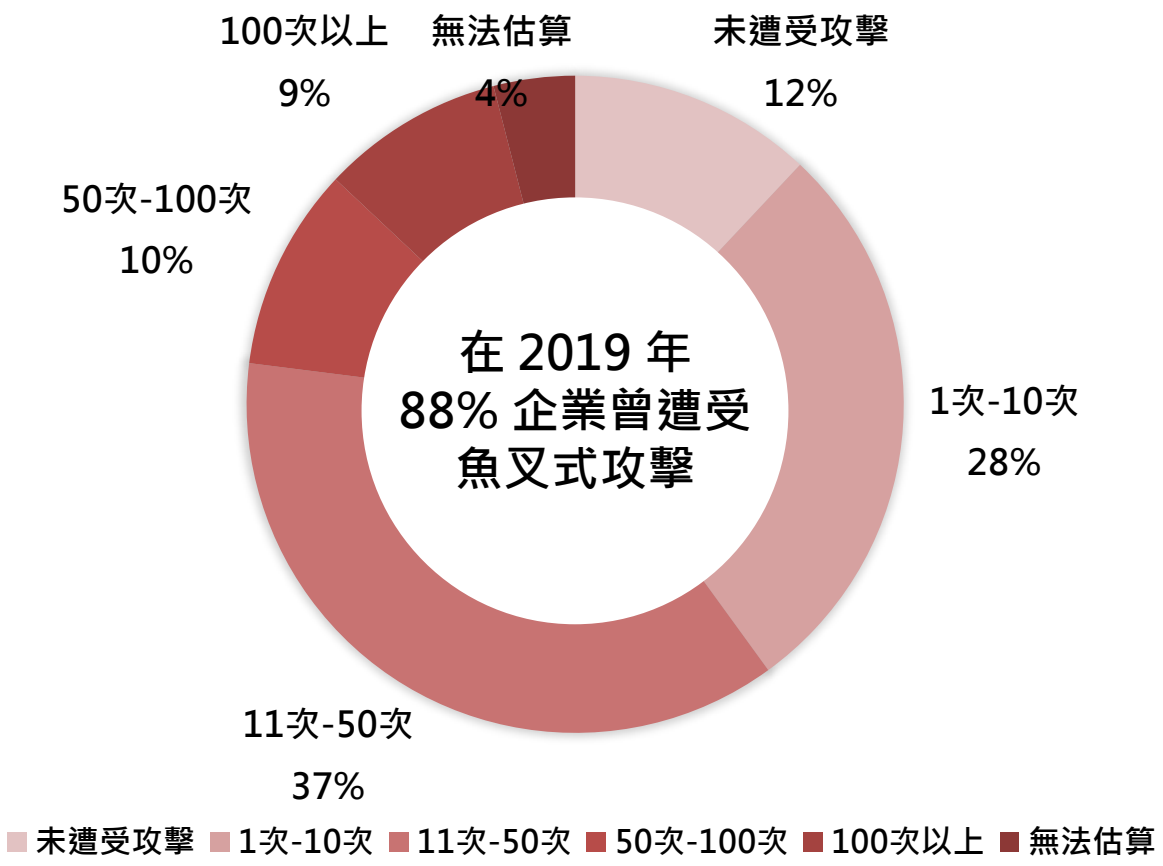
Reference: Proofpoint 2020 State of the Phish

什麼是魚叉式攻擊？

魚叉式網路攻擊（Spear Phishing）是一種社交工程攻擊，也稱作**針對性網路釣魚攻擊**，攻擊者會針對企業組織進行研究，並製作**極為相似的郵件與網站**，進而騙取機敏資訊。



2019 企業遭受魚叉式攻擊統計



Reference: Proofpoint 2020 State of the Phish

如何防範社交工程攻擊？

制定資安政策

資安意識訓練

追蹤紀錄與分析

社交工程防護模組

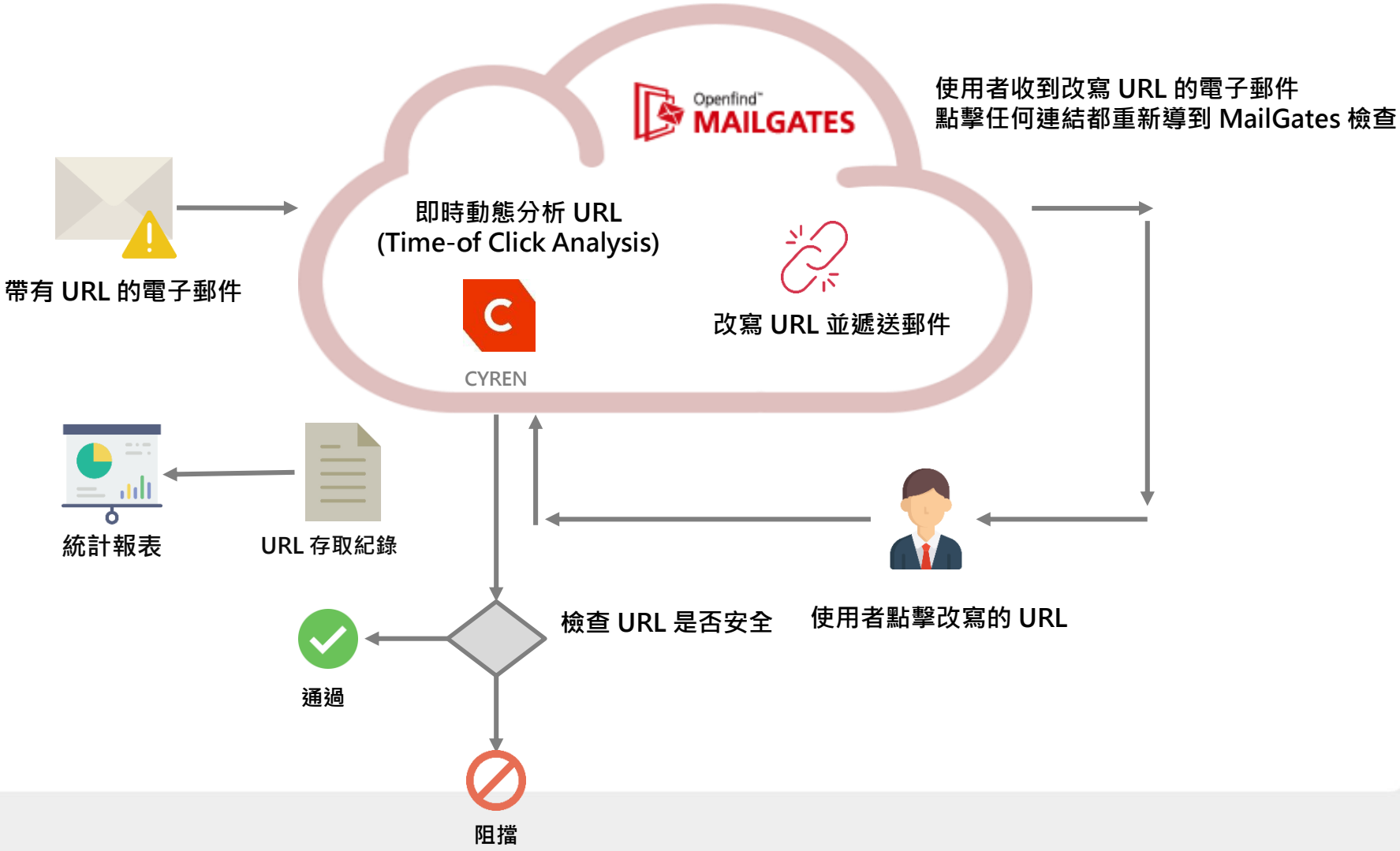
- ✓ URL 改寫政策
- ✓ 網域黑白名單
- ✓ 內文、HTML 檔

- ✓ 完整 URL 日誌
- ✓ 存取紀錄
- ✓ 改寫 URL 追蹤

- ✓ 每日 URL 統計
- ✓ 改寫 URL 統計
- ✓ 最常點擊 URL

- ✓ 釣魚回報機制
- ✓ 即時更新
- ✓ 操作流程簡易

社交工程防護運作


Openfind™ MAILGATES
使用者收到改寫 URL 的電子郵件
點擊任何連結都重新導到 MailGates 檢查
帶有 URL 的電子郵件
即時動態分析 URL
(Time-of Click Analysis)
CYREN
改寫 URL 並遞送郵件
統計報表
URL 存取紀錄
使用者點擊改寫的 URL
檢查 URL 是否安全
通過
阻擋

威脅情資核心 - Cyren (1/2)

Cyren 為以色列資安科技公司，為企業用戶提供安全即服務（SECaaS）和威脅情報（Threat Intelligence）解決方案。服務包含電子郵件安全、Web 安全、反垃圾郵件服務、即時網路釣魚檢測、勒索病毒保護，URL 過濾、電子郵件 IP 信譽、惡意程式攻擊檢測和雲端威脅情資。

每天分析全球	保護全球	每天阻擋
250 億筆	13 億	3 億次
郵件傳輸資訊	企業用戶	威脅攻擊

威脅情資核心 - Cyren (2/2)

Cyren 威脅情資解決方案被 200 多家資安廠商所採用，其中包括 Google、Microsoft、Intel Security (McAfee)、SonicWall、T-Mobile 與 Check Point。

Microsoft Google McAfee Together is power.

SONICWALL T Check Point SOFTWARE TECHNOLOGIES LTD.

社交工程防護政策

Openfind MAILGATES
進階威脅防護 > SEP 社交工程防護政策 > 社交工程防護政策
回到系統管理者模式
本管理者模式目前所在網域： internal.com 切換至： internal.com 切換
記錄追蹤
統計資訊
帳號管理
威脅管理
進階威脅防護
APT 政策與防毒資訊
APT 統計報表
BEC 郵件詐騙防護政策
SEP 社交工程防護政策
SEP 威脅日誌
SEP 統計報表
通知信管理
稽核管理
郵件誤寄防護
URL 重寫政策
重寫信件內文中 URL
純文字格式 HTML 格式
重寫信件附檔中 URL
純文字 (.txt) HTML 檔 (.html)
套用 URL 排外政策
顯示 URL 目的網址
處理動作
允許通過
警告
阻擋
警告頁面主機名稱
套用系統主機名稱: (mg.aaa.aa)
自訂: mg.internal.com

社交工程防護政策

來源: Eims Express <david@kszqtc.com>
收信: [redacted]
標題: Electronic Invoice
日期: Mon, 02 Dec 2019 13:00:56

SF EXPRESS 順豐速運

亲爱的顺丰速运客户:

感谢您选择我们作为您首选的快递服务。
我们已按您的要求向您发出电子发票。 请参阅下面发票的一些细节。
发票编号: 1459327062019
发票日期: 2/12/2019
发票金额: 元128.33

您可以通过以下选项查看或下载发票。

下载发票 <banzogo.top/cgi-bin/SFExpress/?email=[redacted]
查看发票 <banzogo.top/cgi-bin/SFExpress/?email=[redacted]

我们等着收到您的付款。 感谢您选择顺丰速运。

社交工程防護政策

來源: Eims Express <david@kszqtc.com>
收信:
標題: Electronic Invoice
日期: Mon, 02 Dec 2019 13:00:56

SF EXPRESS 順豐速運

亲爱的顺丰速运客户:

感谢您选择我们作为您首选的快递服
我们已按您的要求向您发出电子发票
发票编号: 1459327062019
发票日期: 2/12/2019
发票金额: 元128.33

您可以通过以下选项查看或下载发票

下载发票 <banzogo.top/cgi-bin/SFExpress/?email=
查看发票 <banzogo.top/cgi-bin/SFExpress/?email=

我们等着收到您的付款。 感谢您选择顺丰速运。

Openfind MAILGATES

即將連結至外部網站

https://banzogo.top/cgi-bin/SFExpress/?email=

此網站安全診斷為

危險

我們建議您關閉此網頁，而且不要繼續瀏覽此網站。

按這裡關閉此網頁。

繼續瀏覽此網站(不建議)。

SEP 威脅日誌

adm@system 登出 | 線上說明

進階威脅防護 > SEP 威脅日誌

本管理者模式目前所在網域： **internal.com** 切換至： internal.com 切換

時間: 今日 3日內 7日內 30日內 90日內 其他 2020/01/01 ~ 2020/01/07 搜尋

寄件者: 收件者: URL: 過濾原因:

惡意 URL (17) | 未重寫 URL (0) | 已重寫 URL (28)

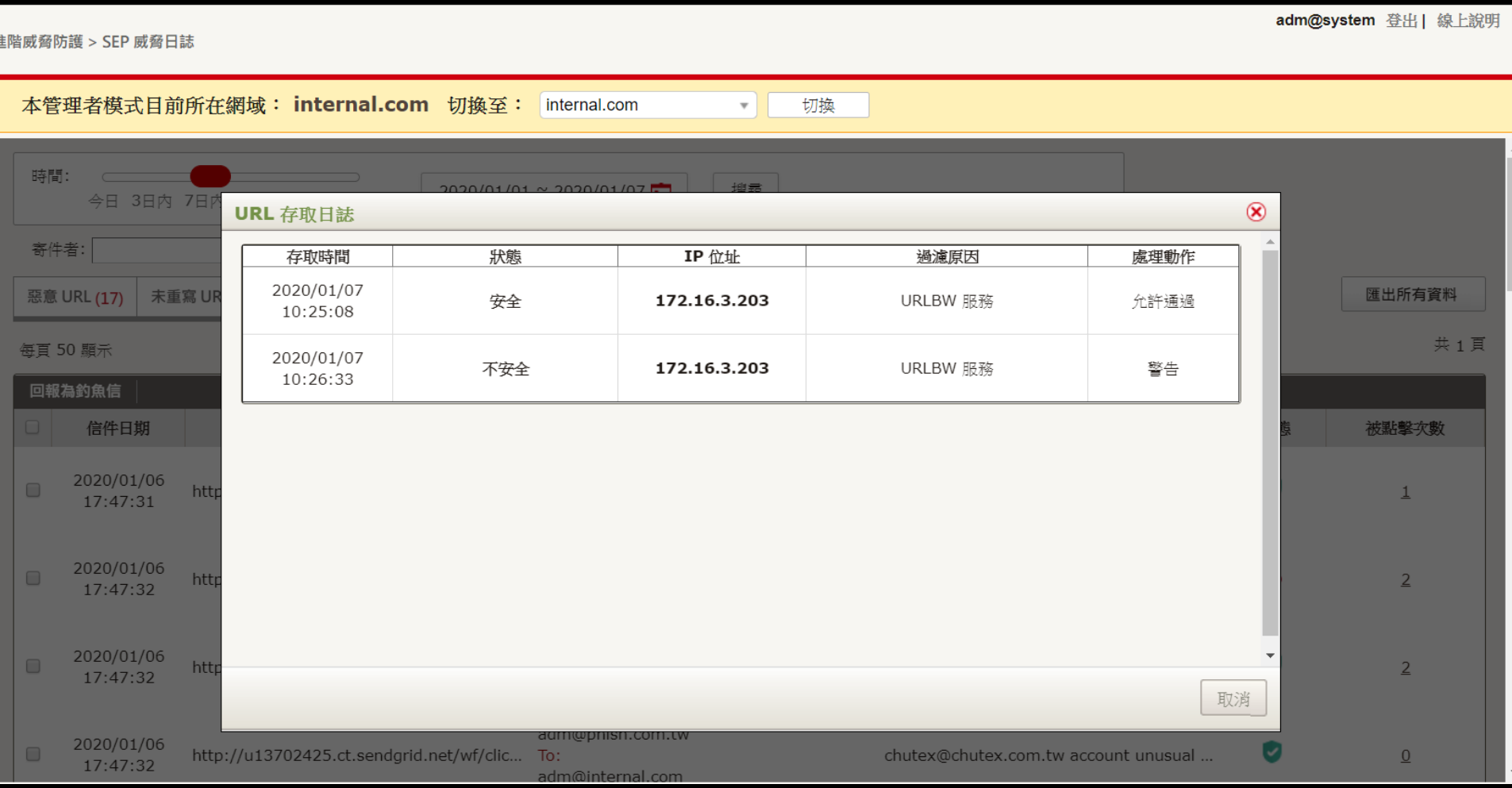
匯出所有資料

每頁 50 顯示 1 共 1 頁

回報為釣魚信

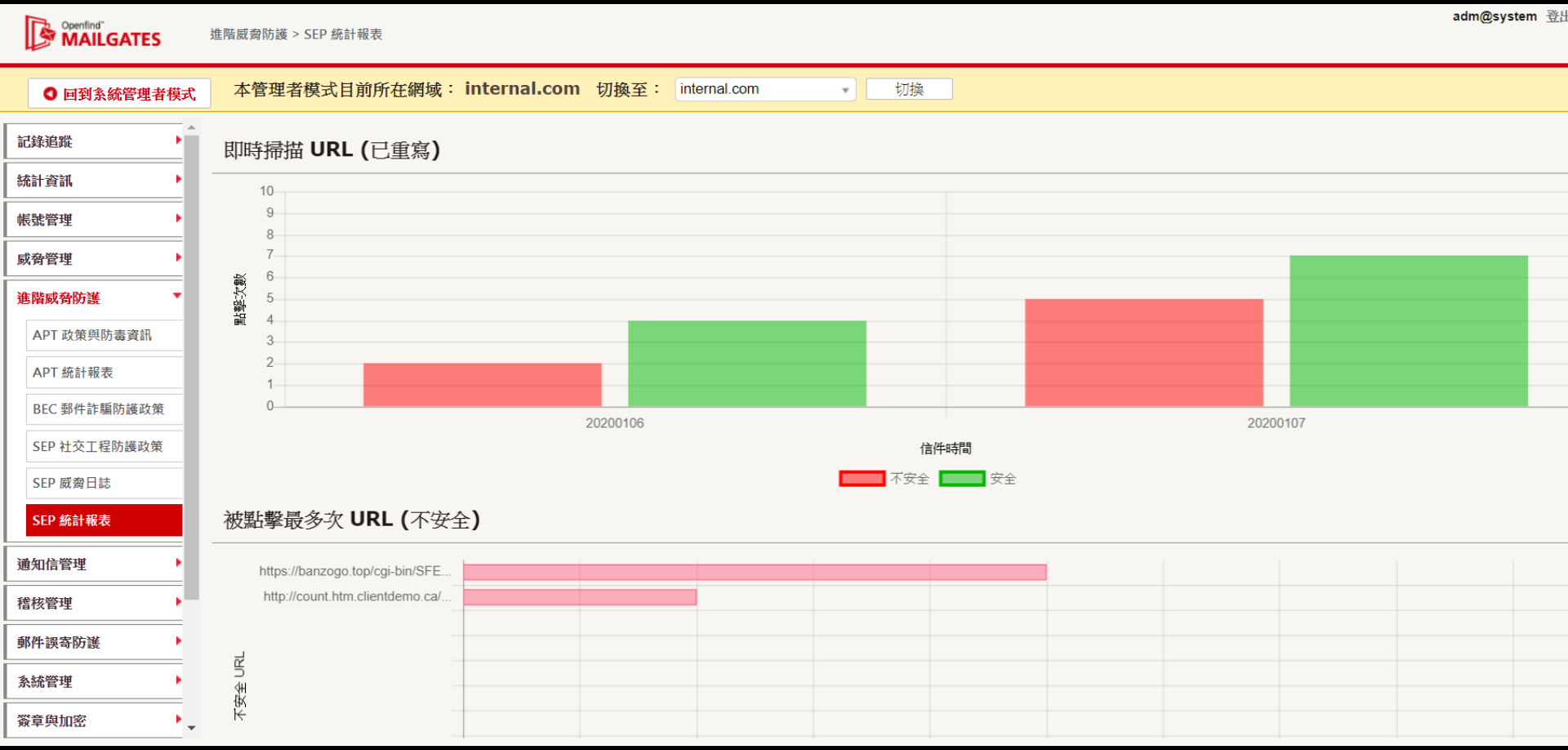
	信件日期	URL	寄件人 / 收件人	信件標題	狀態	被點擊次數
	2020/01/06 17:47:31	https://deref-mail.com/mail/client/bTIBcl...	adm@phish.com.tw To: adm@internal.com	RE: Price and delivery for KPV3000SL		1
	2020/01/06 17:47:32	http://count.htm.clientdemo.ca/yes/ii/?e...	adm@phish.com.tw To: adm@internal.com	Your chutex@chutex.com.tw Will Block in...		2
	2020/01/06 17:47:32	https://u13702425.ct.sendgrid.net/wf/cli...	adm@phish.com.tw To: adm@internal.com	You have 3 pending message(s) in strea...		2
	2020/01/06 17:47:32	http://u13702425.ct.sendgrid.net/wf/clic...	adm@phish.com.tw To: adm@internal.com	chutex@chutex.com.tw account unusual ...		0

SEP 威脅日誌



存取時間	狀態	IP 位址	過濾原因	處理動作
2020/01/07 10:25:08	安全	172.16.3.203	URLBW 服務	允許通過
2020/01/07 10:26:33	不安全	172.16.3.203	URLBW 服務	警告

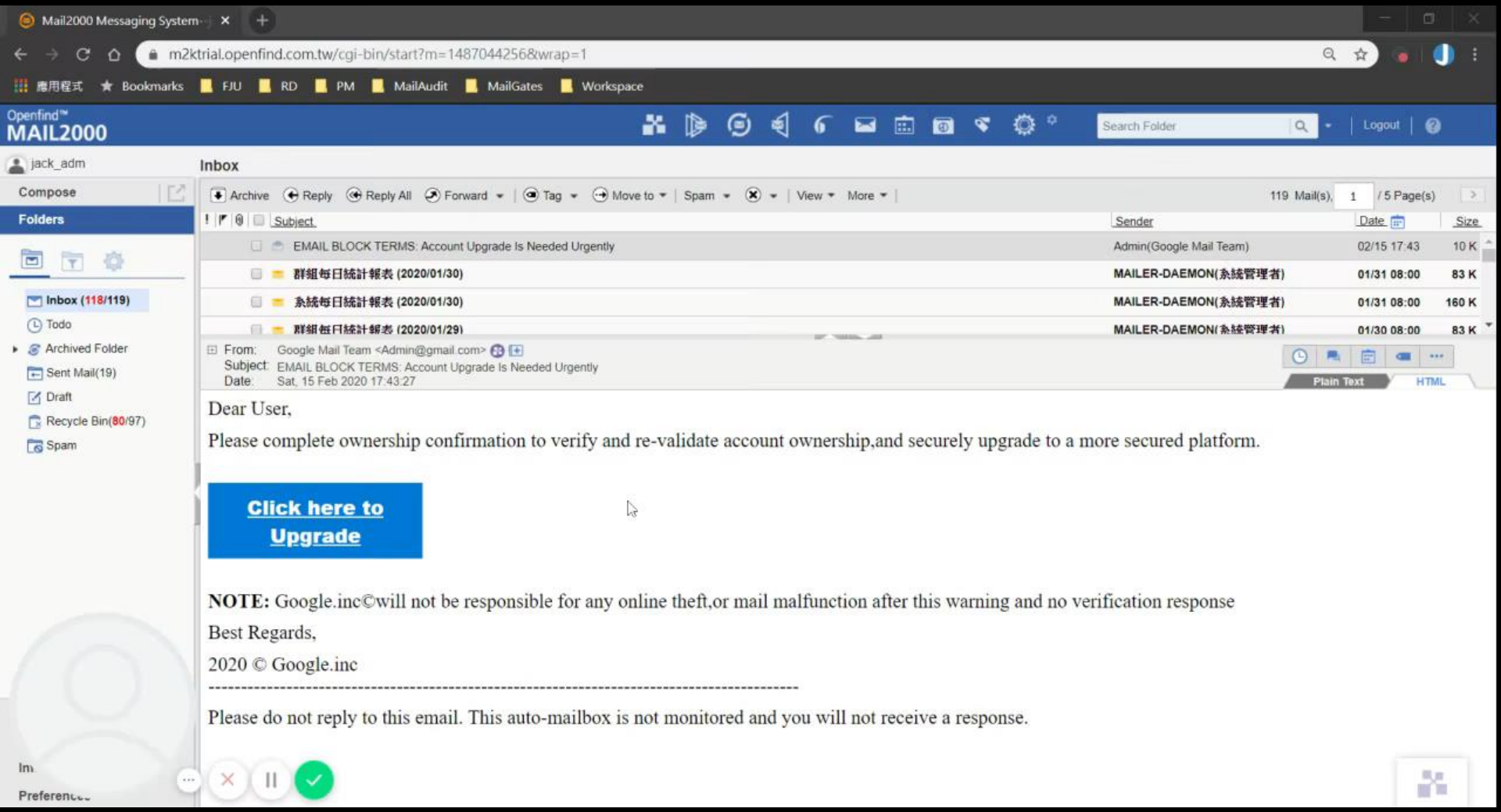
SEP 統計報表


Openfind MAILGATES
進階威脅防護 > SEP 統計報表
adm@system 登出
回到系統管理者模式
本管理者模式目前所在網域： internal.com 切換至： internal.com 切換
記錄追蹤
統計資訊
帳號管理
威脅管理
進階威脅防護
APT 政策與防毒資訊
APT 統計報表
BEC 郵件詐騙防護政策
SEP 社交工程防護政策
SEP 威脅日誌
SEP 統計報表
通知信管理
稽核管理
郵件誤寄防護
系統管理
簽章與加密
即時掃描 URL (已重寫)
點擊次數
10
9
8
7
6
5
4
3
2
1
0
20200106
20200107
信件時間
不安全
安全
被點擊最多次 URL (不安全)
https://banzogo.top/cgi-bin/SFE...
http://count.htm.clientdemo.ca/...
不安全 URL

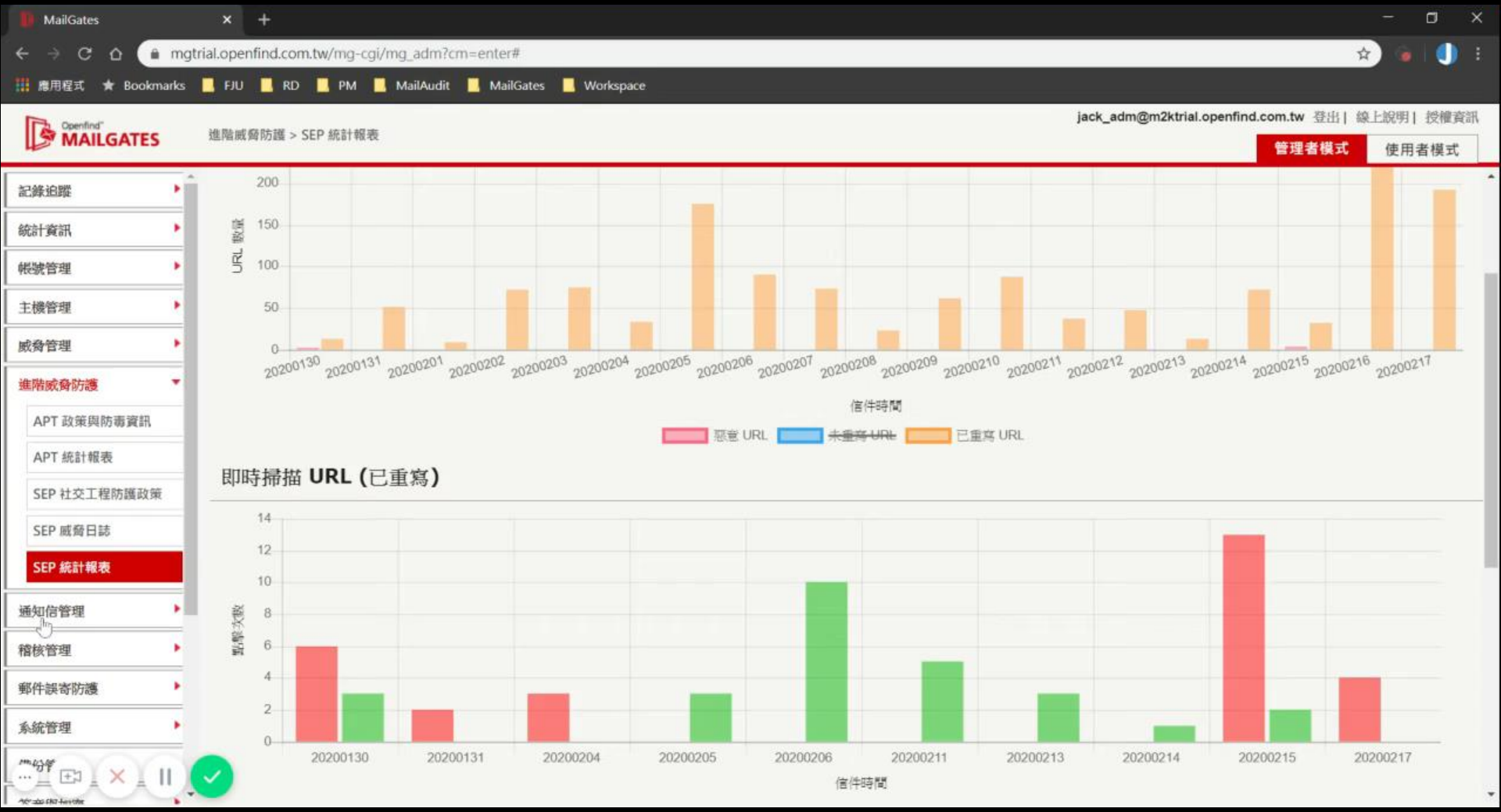
SEP 詳細日誌

	過濾原因	狀態	URL 存取日誌	點擊次數
		安全	存取時間:2020/01/07 10:24:38, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過	1
U	URLBW 服務	不安全	存取時間:2020/01/07 10:25:08, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:允許通過 存取時間:2020/01/07 10:26:33, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告	2
	URLBW 服務	不安全	存取時間:2020/01/06 18:33:29, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告	1
	URLBW 服務	不安全	存取時間:2020/01/06 18:31:28, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告 存取時間:2020/01/07 09:59:25, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告 存取時間:2020/01/07 10:23:49, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告 存取時間:2020/01/07 10:28:09, 狀態:不安全, IP 位址:172.16.3.203, 過濾原因: URLBW 服務 , 處理動作:警告	4
		安全	存取時間:2020/01/06 18:33:12, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過 存取時間:2020/01/07 10:24:41, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過 存取時間:2020/01/07 10:24:52, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過	3
		安全	存取時間:2020/01/07 09:59:10, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過 存取時間:2020/01/07 10:27:03, 狀態:安全, IP 位址:172.16.3.203, 過濾原因: 無 , 處理動作:允許通過	2
		安全		0
		安全		0

導入社交工程防護實際畫面



導入社交工程防護實際畫面



新舊功能比較

功能項目	郵件內容防護	社交工程防護
URL 改寫政策 (URL Rewrite)	信件內文	信件內文 附檔 HTML 白名單政策
惡意 URL 對應政策	阻擋	允許、警告、阻擋
即時點擊分析 (Time-of-Click Analysis)	Web of Trust	Web of Trust CYREN Web Reputation
URL 日誌	X	O
URL 存取紀錄	X	O
URL 統計報表	X	O
釣魚回報機制	X	O

One more thing

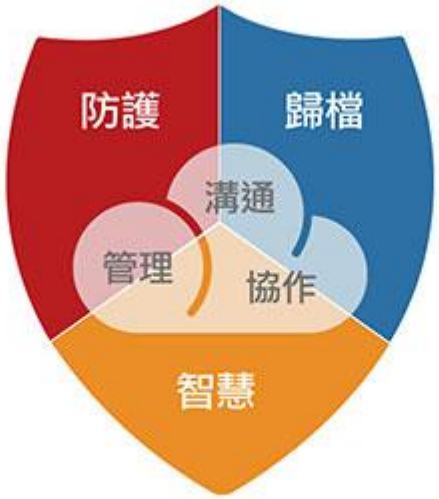
- BEC Phase III
  - 依等級設定
  - 偵測顯示名稱詐騙
  - 詳細統計報表
- 4 月中 release

Openfind™ MailGates 郵件防護系統

Openfind™ Mail2000 電子郵件系統

Openfind™ MailCloud 企業雲端服務

Openfind™ Enterprise Search 企業搜尋探勘系統



Openfind™ Secure 雲端資安服務

Openfind™ MailAudit 郵件稽核系統

Openfind™ MailCloud Messenger 企業溝通平台

Openfind™ ArkEase Pro 雲端儲存服務

Openfind™ MailBase 郵件歸檔管理系統

Q&A

Email: sales@openfind.com
URL: www.openfind.com