

知己知彼 2023網路犯罪威脅報告

Palo Alto Networks 台灣資安顧問

Scottie Wang 王信強





paloalto[®]
NETWORKS



UNIT 42[™]
BY PALO ALTO NETWORKS

網路世界正持續在變化

應用程式正移到雲上



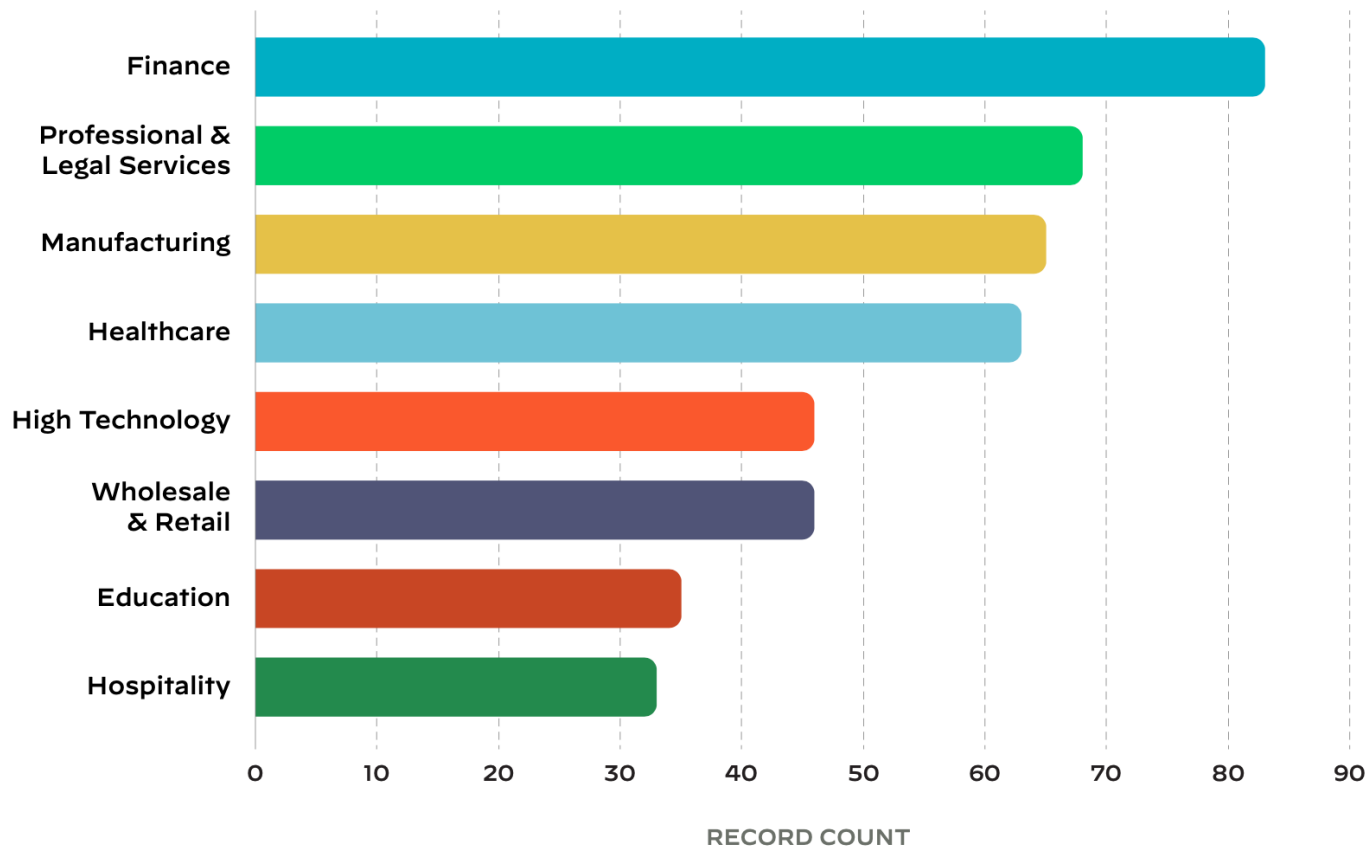
SaaS 應用正爆炸式增長



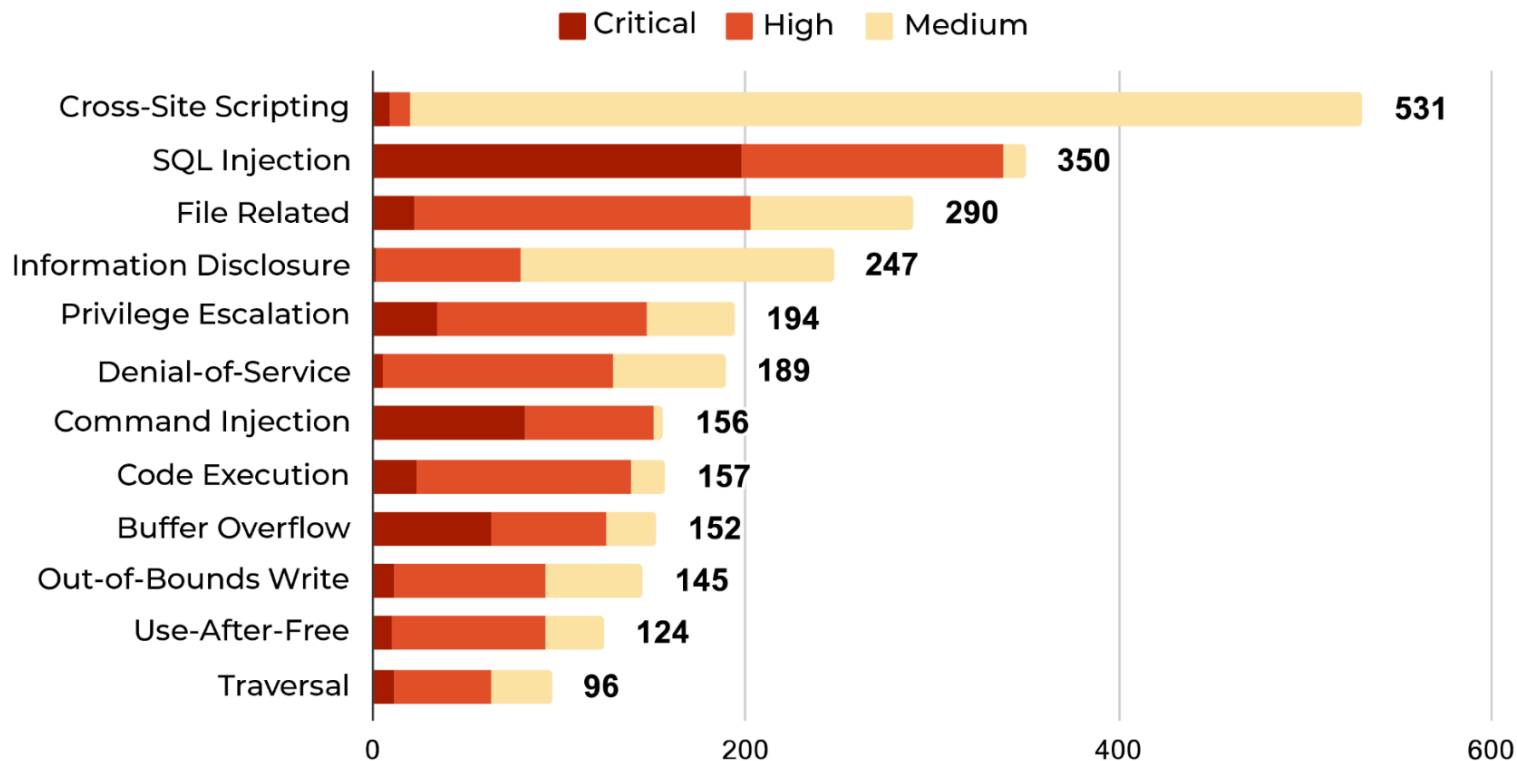
使用者能在任意地方
工作



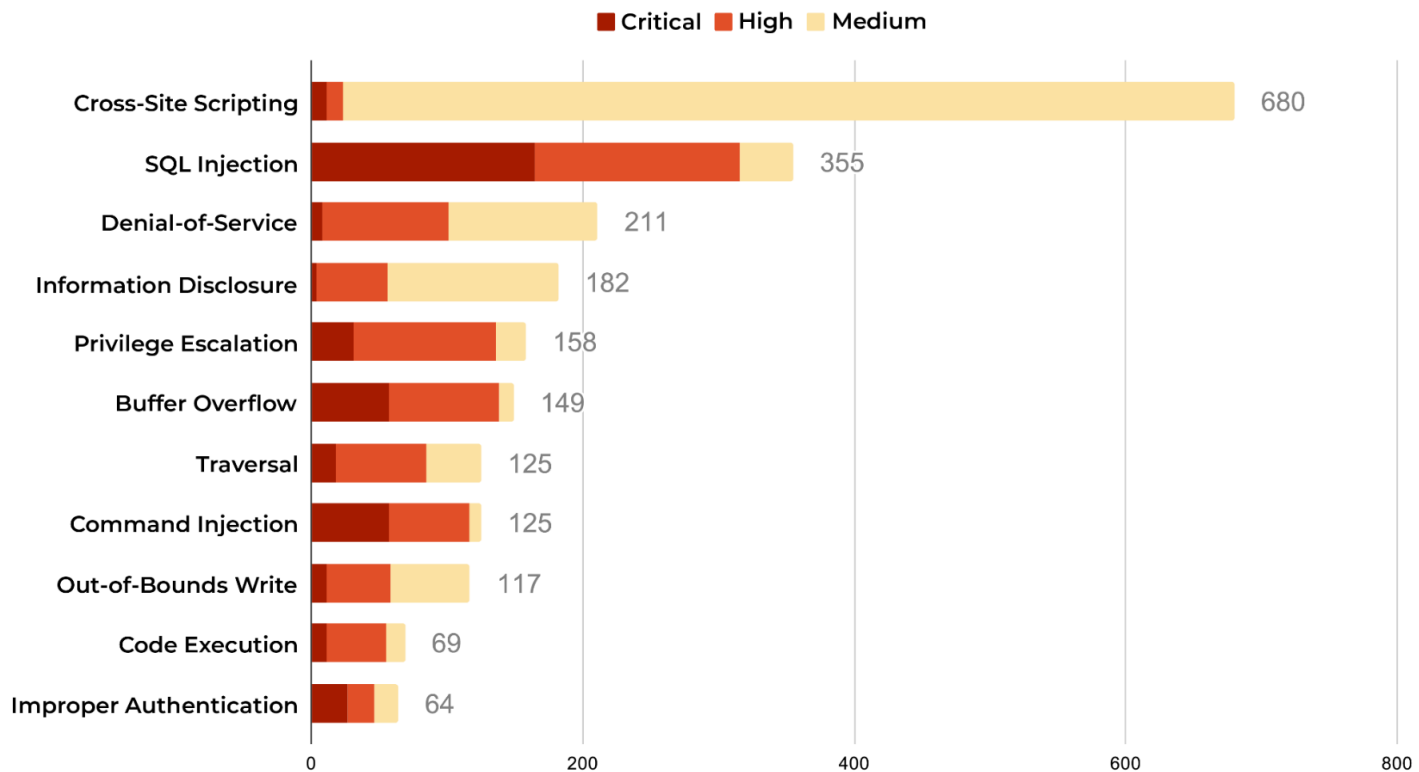
2022最受攻擊的行業別



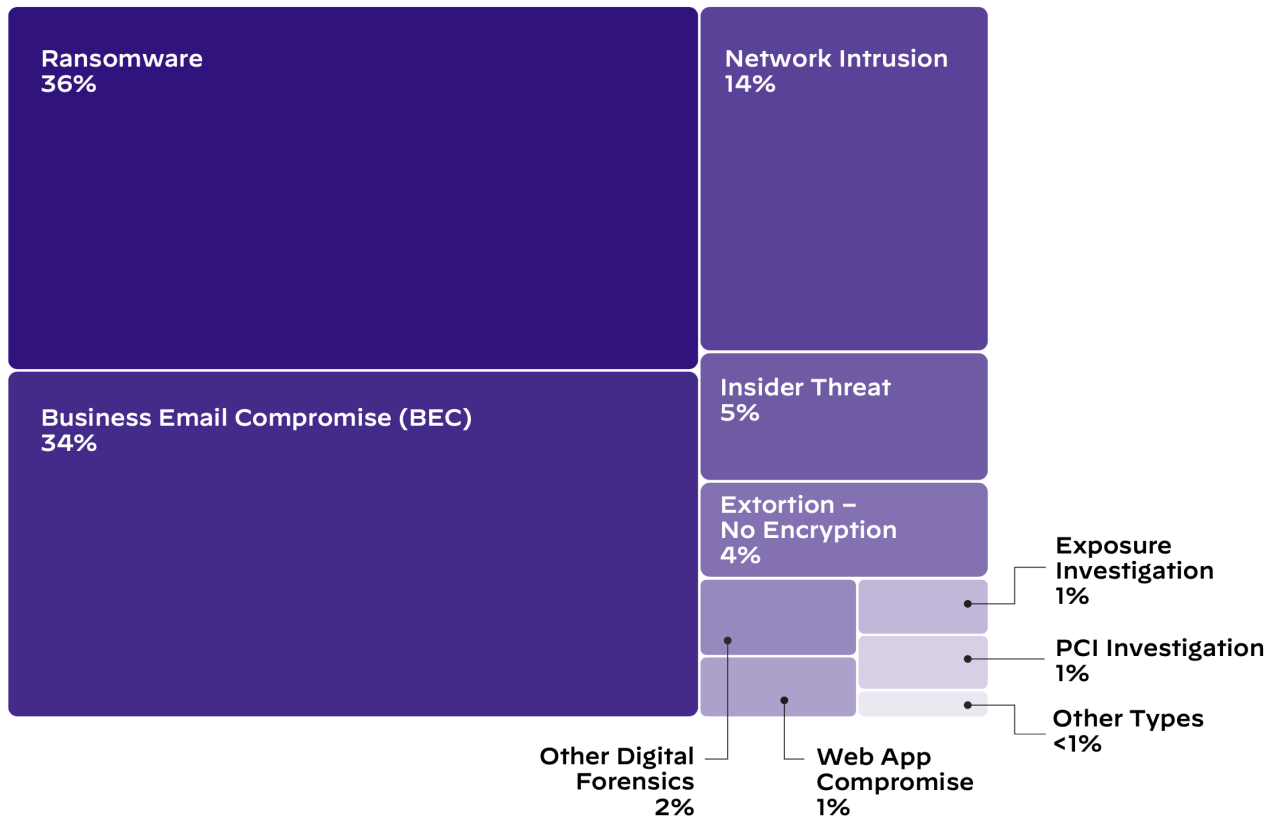
2022/08 ~ 2022/10 CSV漏洞類別分佈



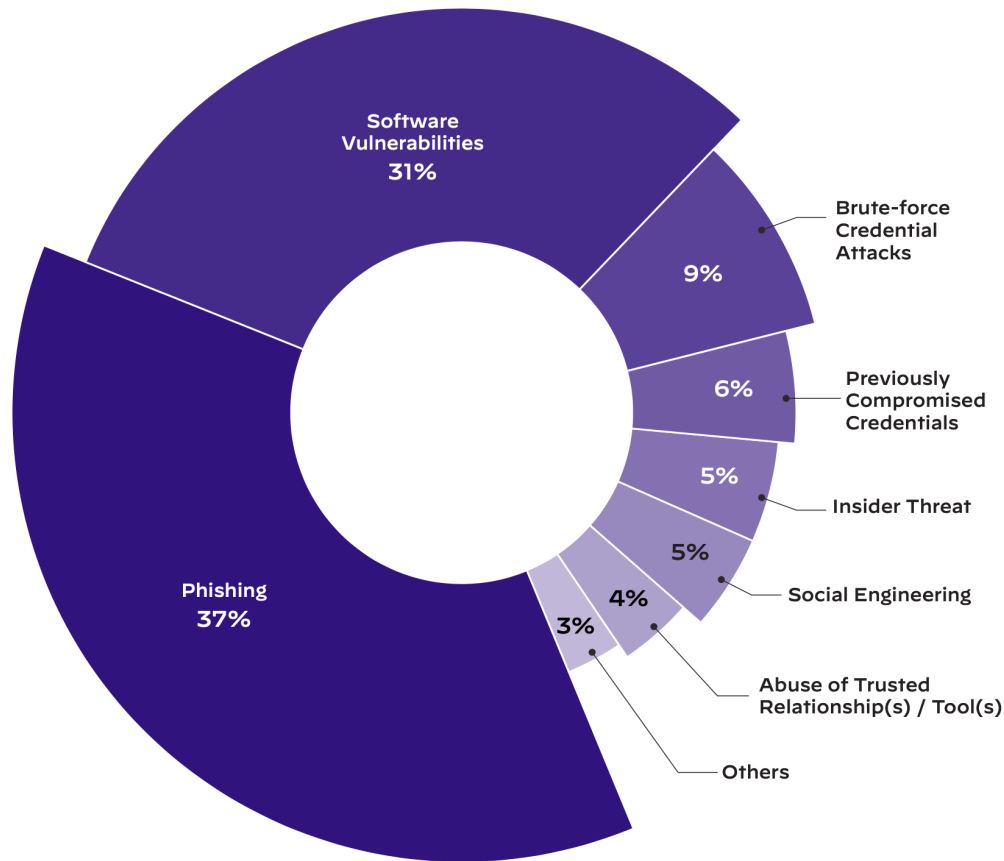
2022/11 ~ 2023/01 CSV漏洞類別分佈



網路犯罪事件類別



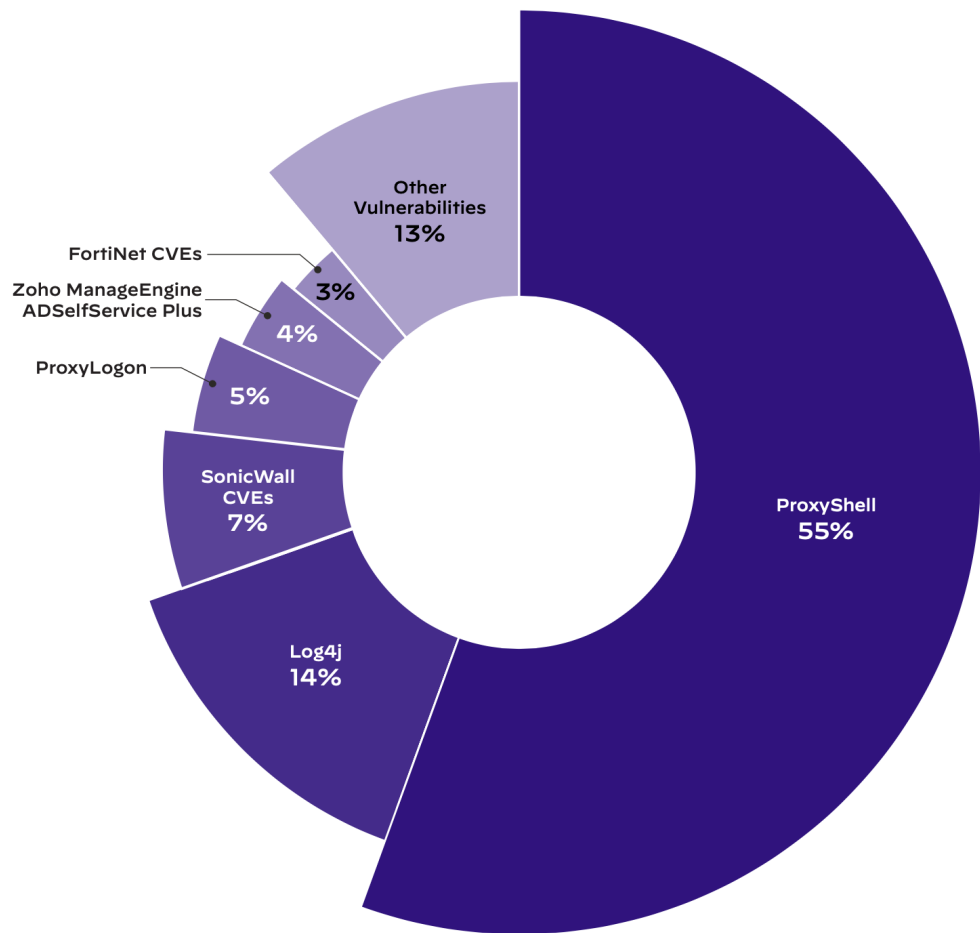
駭客總是尋找最容易的方式滲透



駭客威脅的三大滲透途徑是網絡釣魚、利用已知軟件漏洞和暴力破解攻擊。這些攻擊應用主要集中在遠端桌面協議 (RDP)。這三種滲透途徑佔了77% 以上。

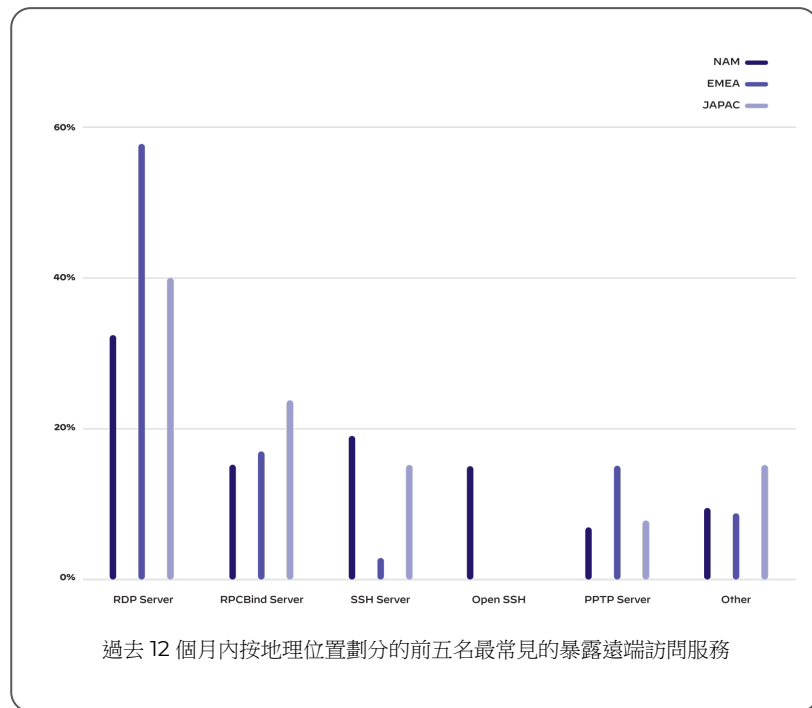
駭客最愛的漏洞應用

- ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)
- Log4j (CVE-2021-45046)
- SonicWall (CVE-2020-5135, CVE-2021-20016)
- ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)
- Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)
- Fortinet (CVE-2023-27997, CVE-2020-12812, CVE-2019-5591, CVE-2018-13379)



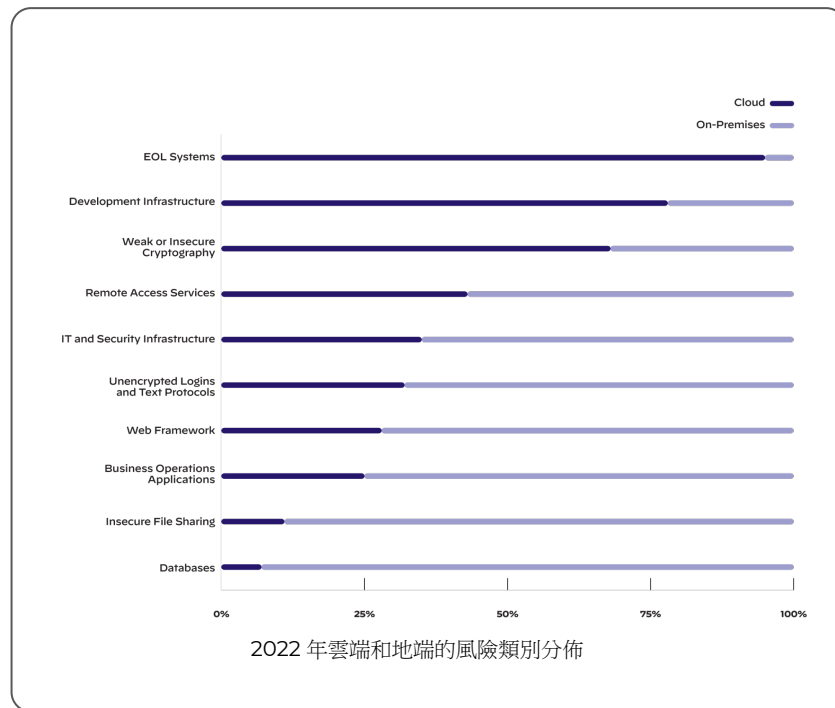
遠端訪問服務在各個行業中持續且頻繁地被發現

- Unit 42 研究的 **9 個行業中**，有 **8 個行業** 在一個月內至少有 25% 的時間於可通過網際網路訪問的 RDP 服務受到暴力攻擊。
- 根據 Unit 42 IR 報告，50% 的目標組織缺乏部署面向網際網路的關鍵系統 (Webmail,VPN...) 使用 MFA，這增加了勒索軟體攻擊成功的可能性。



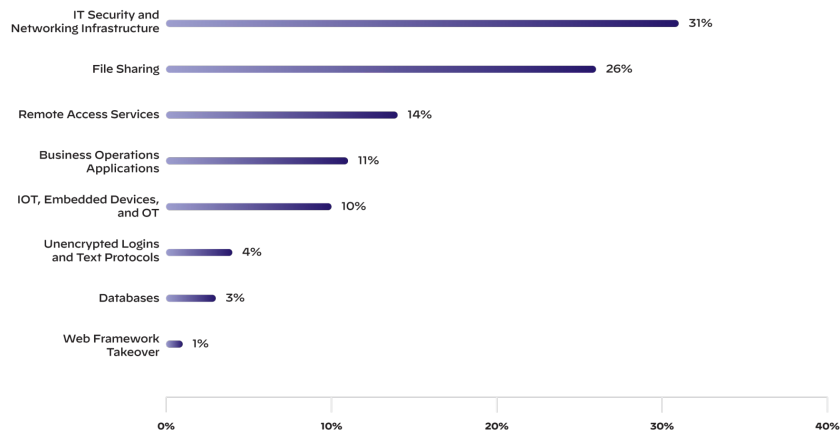
近 95% 暴露在網際網路上的報廢(EoL)軟體系統都存在於雲環境中

- **95%** 已暴露的生命週期終止 (EoL) 軟體系統是在雲環境中發現的，這表明過時的系統可能會在雲中持續存在更長時間。
- 超過 **75%** 已暴露軟體開發基礎設施是基於雲的，這成為攻擊者的主要目標。
- 大量未加密登錄、不安全的文件分享以及主要在地端發現的暴露數據庫；遷移到雲時需要謹慎。



教育機構的風險暴露可能導致嚴重的數據洩露和服務中斷

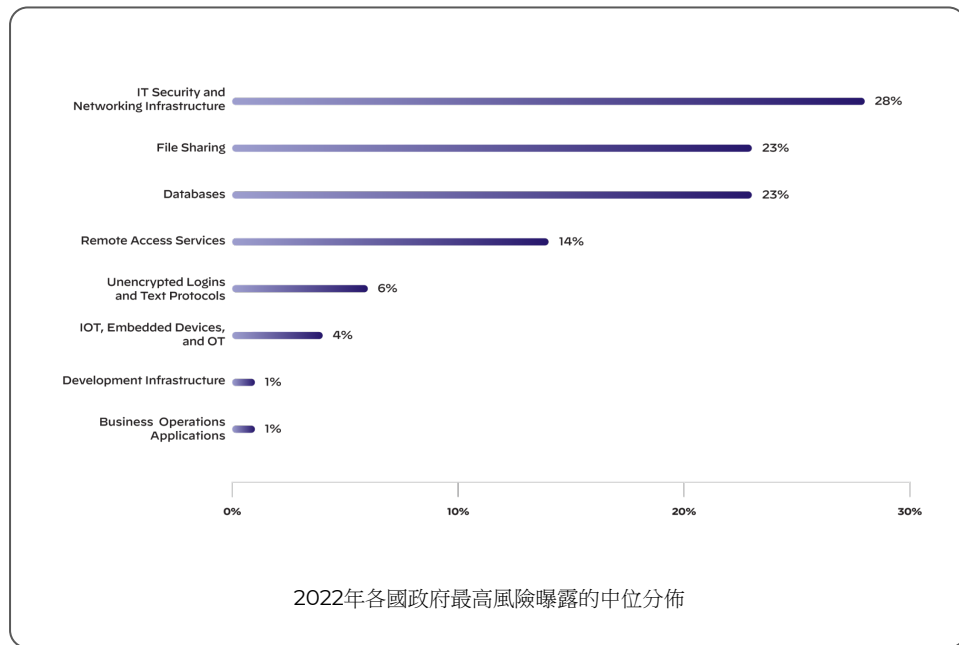
- 最可能暴露 IT、安全和網路基礎設施，從而增加數據洩露的脆弱性。
- 文件共享和遠端訪問服務暴露率較高，存在個人、學術和財務數據被盜的風險。
- 後果包括服務中斷以及調查、恢復和潛在罰款造成的重大財務損失。



2022 年教育組織中最高曝光率的中位分佈

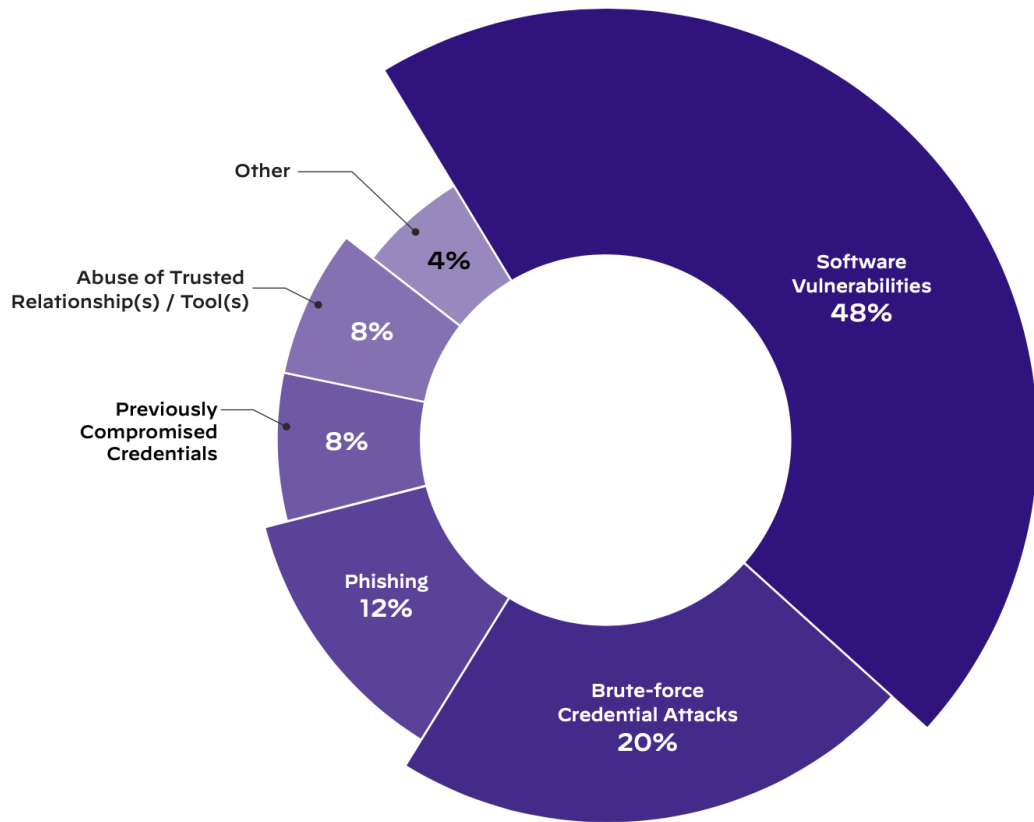
不安全的文件分享和數據庫暴露給各國政府帶來嚴重風險

- 國家政府組織中**超過 46%** 的風險與文件共享和數據庫有關。
- 常見的風險包括 **IT 系統設定錯誤** 以及可通過互聯網訪問的路由器、防火牆和 VPN 的管理頁面。
- 不安全的文件分享和數據庫攻擊**風險高於其他組織**，從而危及國家安全。

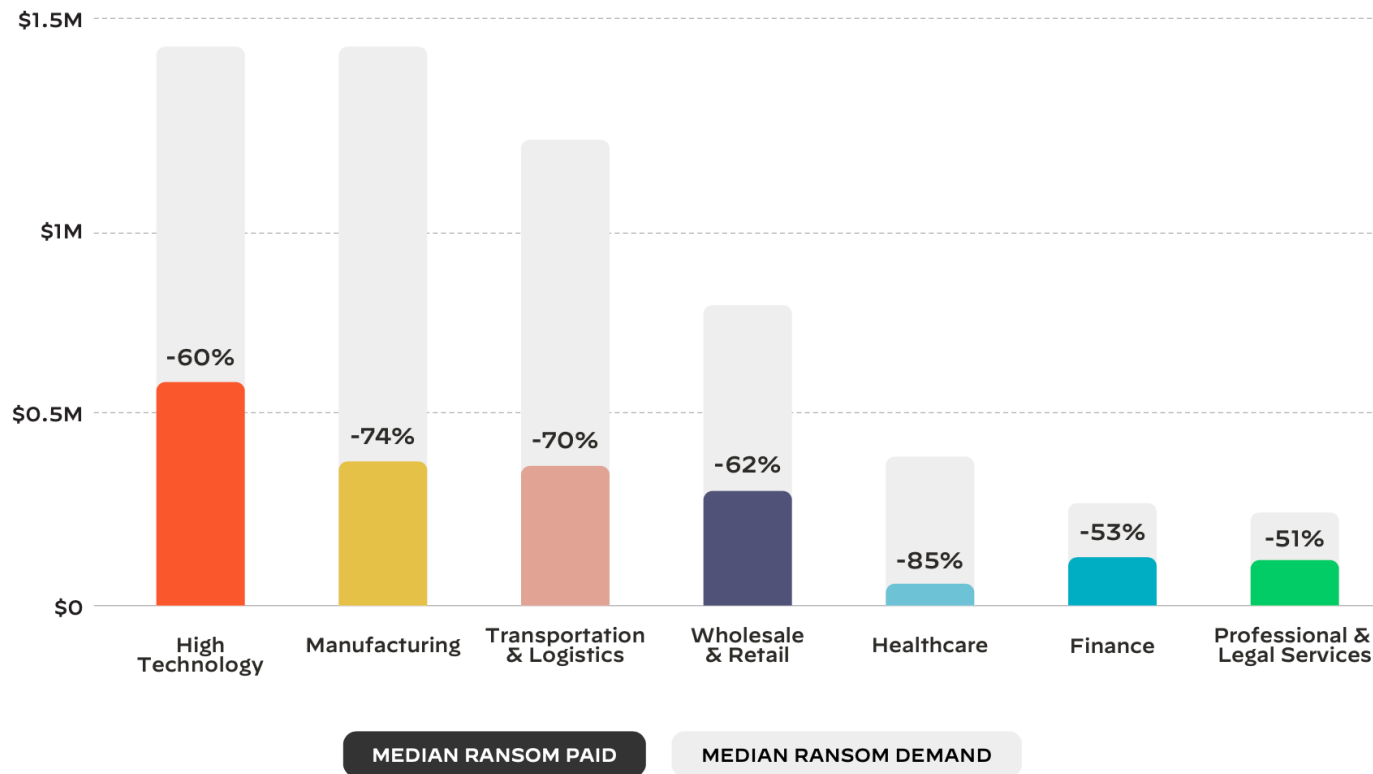


勒索軟體如何攻擊

- 勒索軟體攻擊大量利用軟體漏洞。
- 通常會大規模掃描互聯網，尋找可以重點關注的漏洞和弱點。
- 暴力破解攻擊通常針對 RDP。

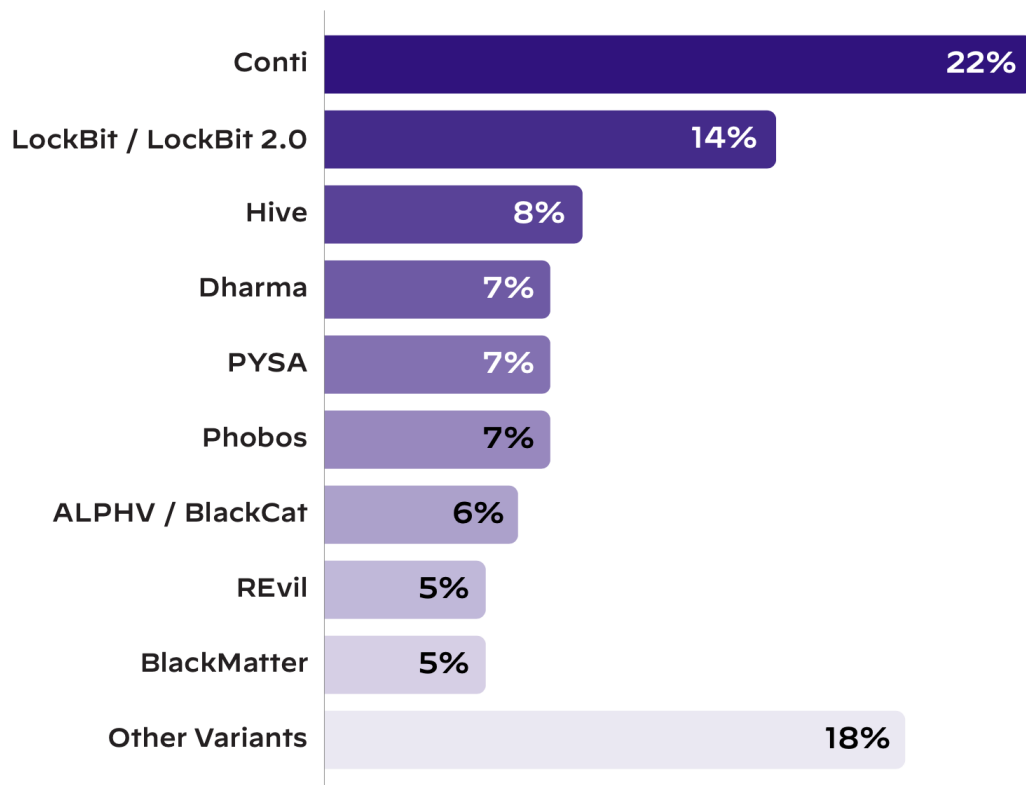


贖金要求與付出贖金



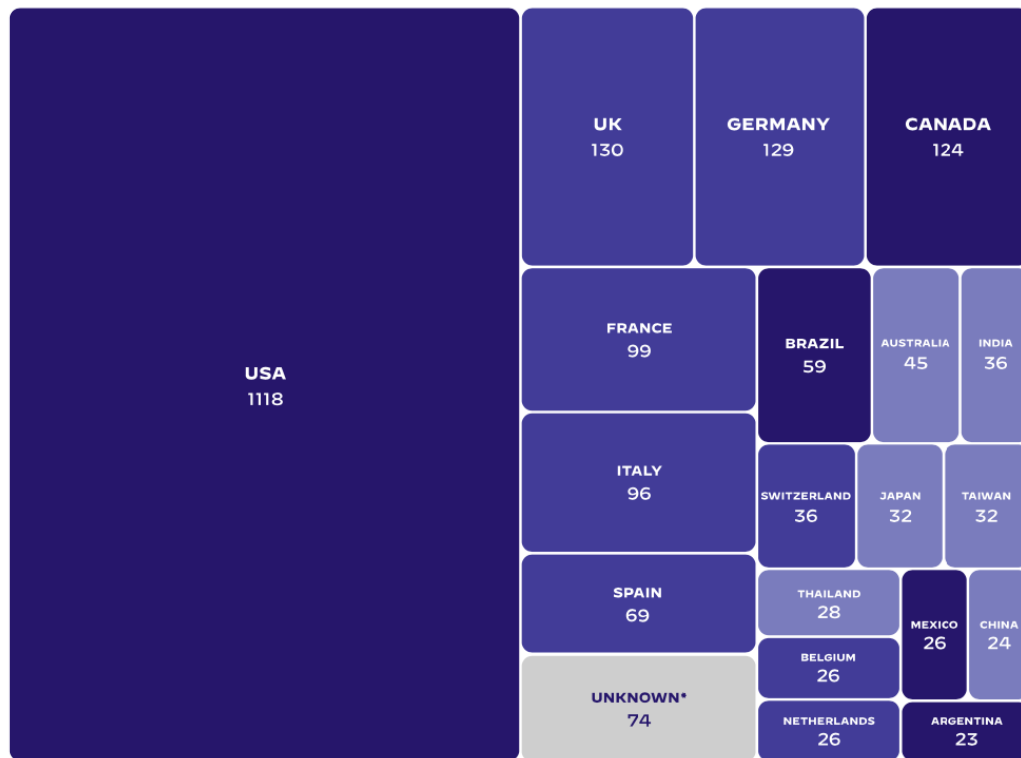
2022年最活躍勒索軟體

- 在我們的事件響應顧問處理的案例中，某些勒索軟體團體表現得特別活躍。
- 勒索軟體團體通常因使用特定的策略、技術和程序而聞名。
- 因此了解哪些團體最活躍和最危險可以幫助您的安全團隊確定將防禦重點放在何處。



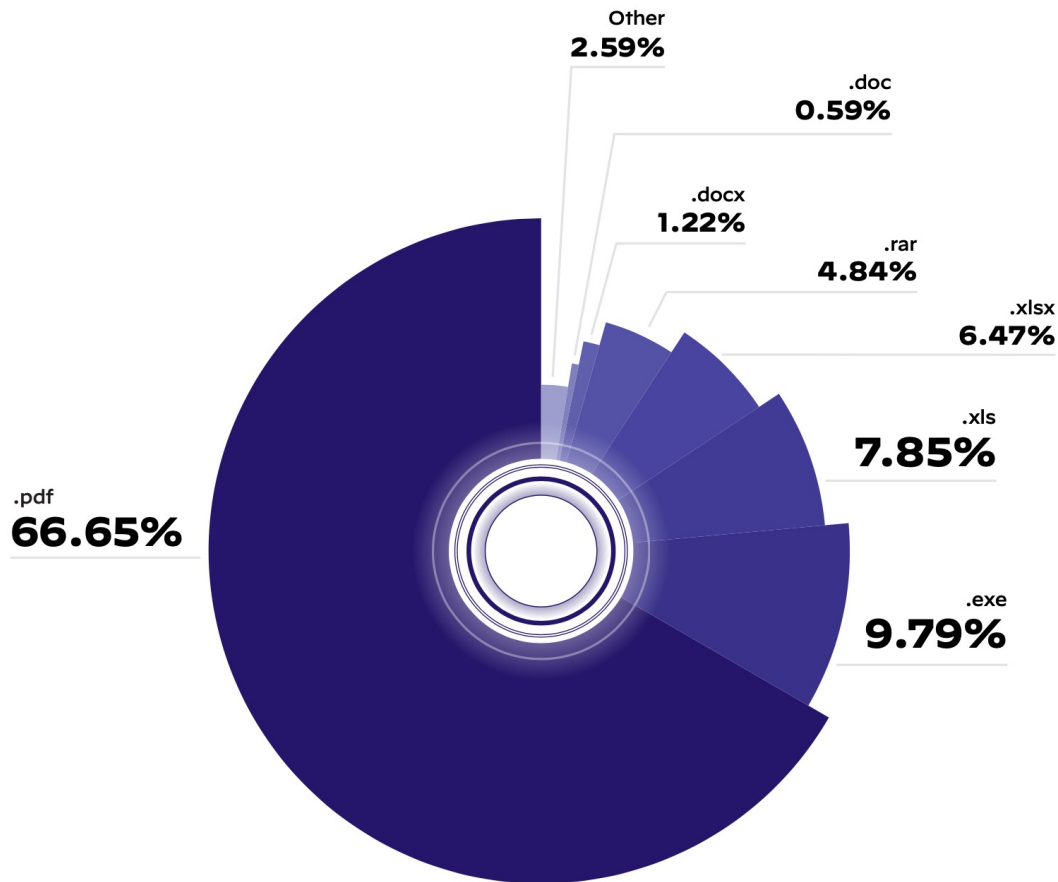
勒索軟體事件地區分佈

- 美國仍然是受影響最嚴重的國家，佔 2022 年觀察到的洩露事件的 42%。



電子郵件作為傳染媒介

- PDF 是主要的惡意電子郵件附件類型，**66%** 的情況下都使用 PDF 來通過電子郵件傳播惡意軟件。
- PDF 文件通常在商業環境中使用，與 EXE 等意外文件類型相比，受害者不太可能對預期文件類型保持警惕。



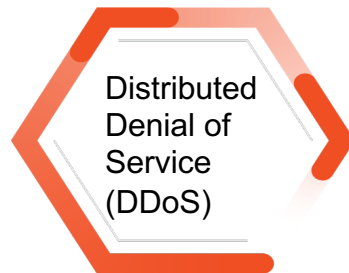
多重勒索



攻擊者要求付款才能恢復對資料的存取，資料加密一直是勒索團體的主要勒索策略。



攻擊者獲取組織的數據並威脅要傳播這些數據至暗網洩露網站，除非他們得到贖金。包含個人身份信息 (PII)、客戶財務數據等。



通過 DDoS 攻擊其他資源為目標，以擾亂運營並引起組織的注意。



威脅行為者可能會致電、發送電子郵件或以其他方式聯繫組織的員工或客戶。

使用勒索軟體的攻擊團體經常利用各種勒索技術（稱為多重勒索）來迫使組織做出支付贖金的艱難決定。

攻擊者不希望您解決的七個問題

1. 多重身份驗證

有50%案例缺乏對面向互聯網的關鍵系統的多重身份驗證

2. EDR/XDR

有44%案例沒有端點檢測和響應(EDR)或擴展檢測和響應(XDR)安全解決方案

3. 更新管理

有28%案例碰到糟糕的更新管理程序提升了攻擊者成功比例

4. 暴力攻擊緩解

有13%案例沒有採取緩解措施來確保帳戶因暴力破解攻擊而被鎖定

5. 安全警報

有11%案例未能審查/採取安全警報

6. 密碼安全

有7%案例因薄弱的密碼安全實踐致使攻擊者進一步實現其目標

7. 設定錯誤

有7%案例系統配置錯誤是導致該事件的一個因素

Paloalto 給您的10項建議

1. 全面了解您的
環境

2. 標準化軟硬體
更新流程

3. 安全最佳實踐
是每個人的責任

4. 部署解密 SSL
以暴露潛在威脅

5. 檢測新註冊的
網域

6. 檢測 PDF 文件中的
網絡釣魚威脅

7. 簡化並鞏固供
應商關係

8. 採用零信任思
維

9. 教育所有員工

10. Paloalto能幫
助您

業界最佳的資安平台

透過次世代資安解決方案協助進行數位轉型



資安維運 (Operation)

A complete suite of analytics and automation solutions to power a modern SOC, including XDR, SOAR, and attack surface management



網路安全 (Networks)

Best-in-class Network Security Platform across hardware, software and SASE - securing hybrid workforces and complex infrastructures of today



雲端安全 (Cloud)

Comprehensive cloud-native application protection platform from development to runtime, across multi-cloud and hybrid environments



端點安全 (Endpoint)

Best performing endpoint protection in 2022 MITRE ATT&CK, with 100% detection



資安情資及事件回應(IR)

Unit 42 brings together world-renowned threat researchers, incident responders, and security consultants to help you proactively manage cyber risk

OUR VISION

**We envision a world
where each day is
safer and more secure
than the one before.**





Cybersecurity
Partner of Choice

THANK YOU

