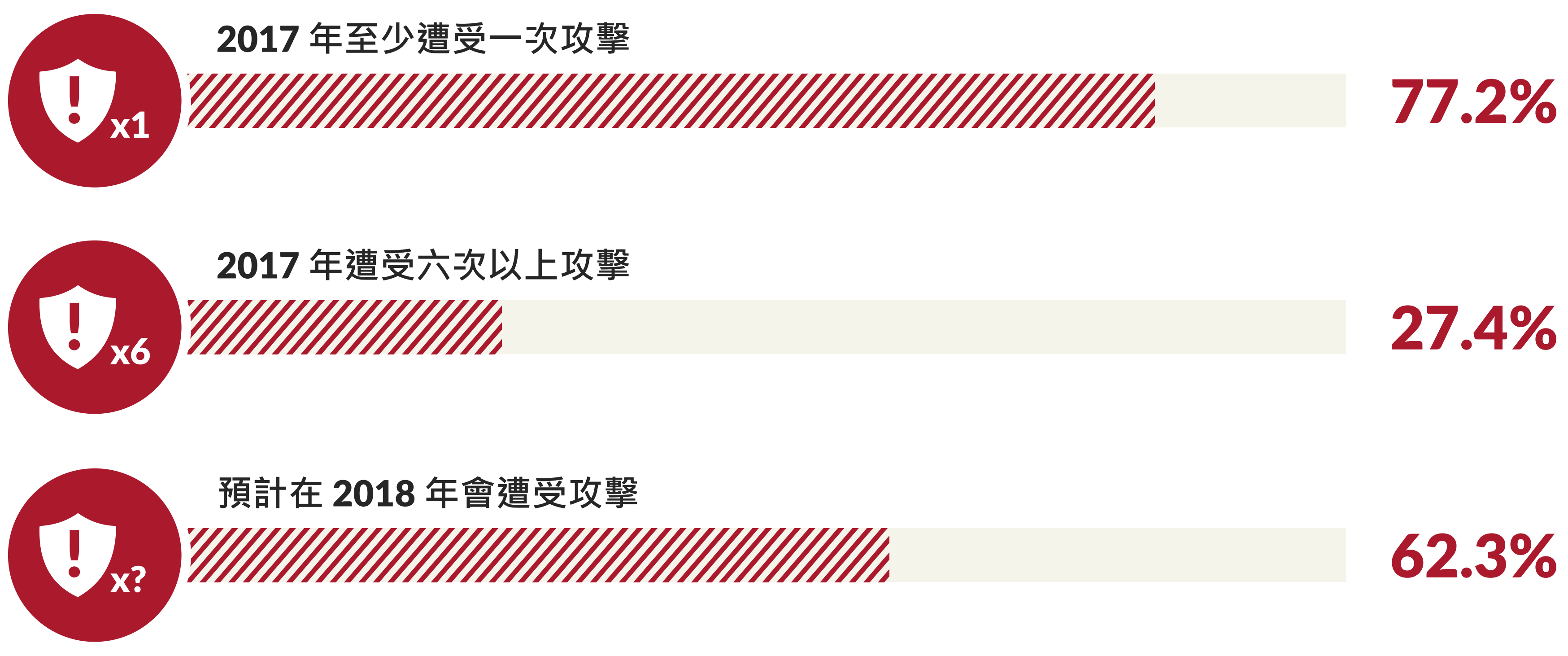
2018 網路威脅防禦報告

CyberEdge Group 的第五個年度網路威脅防禦報告揭示了 IT 安全專家對其組織安全態勢的看法、在建立有效網路安全防禦時面臨的挑戰以及他們必須克服這些挑戰的計畫。繼續閱讀以瞭解今年報告中的一些關鍵發現。

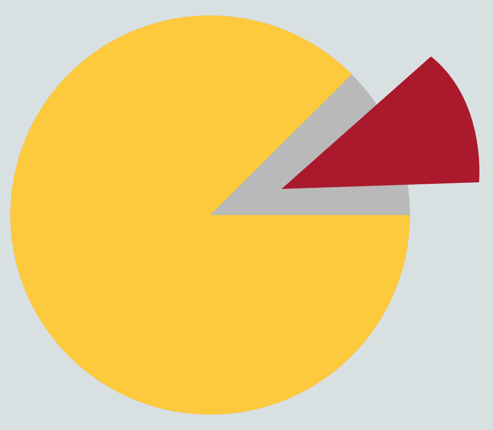
攻擊不可避免

組織正在以驚人的速度成為得逞的網路攻擊的受害者...並且預計未來會遭受越來越多的網路攻擊。



安全預算在增加

根據調查，企業在 2018 年會將其在安全產品、服務和人才方面的支出平均增加 4.7%。



12%
是安全費用占 IT 預算的平均值

但仍然存在很多挑戰

挑戰 1：工作太多

隨著當今企業的技術足跡擴大，必須防禦的攻擊面也越來越多。

基礎結構被認為具有最薄弱的安全態勢

1. 容器
2. 行動裝置
3. 雲端基礎結構

最缺乏的流程/職能

1. 應用程式開發與測試 (SDLC)
2. 減少攻擊面
3. 檢測惡意內部人員/內部人員攻擊

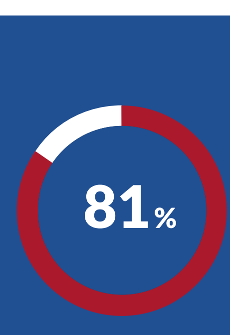
影響效果的主要障礙

要分析的資料太多

挑戰 2：缺少技能人才

當全球都缺少網路安全專家時，在安全上投入更多資金僅是小小安慰。

缺少技能人才被認為是充分防禦網路威脅的最大障礙



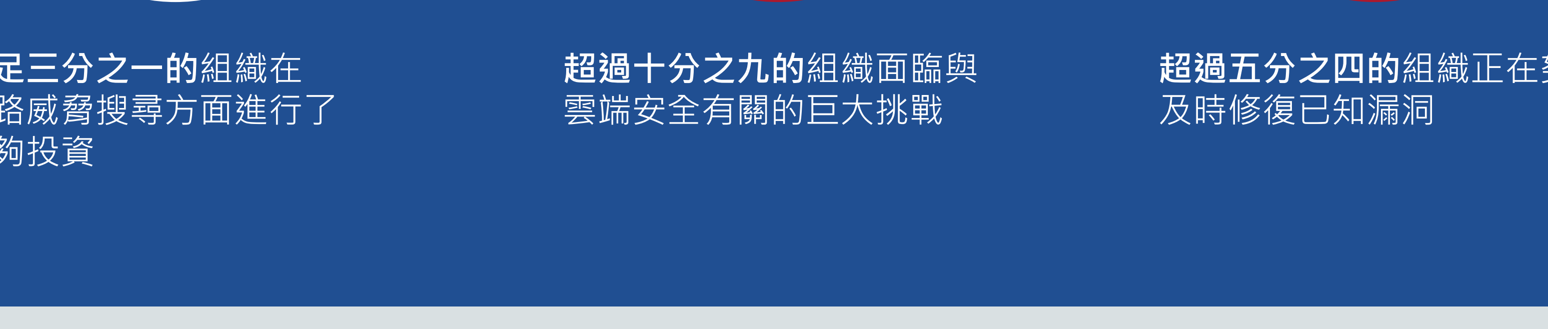
組織正在遭受技能IT 安全人才短缺

教育	87%
技術	85%
製造	82%
金融	81%

遭受 IT 安全技能短缺的垂直行業

挑戰 3：仍在尋找合適的解決方案

在所有正確領域進行足夠的技術投資並盡力充分利用這些投資仍是一些組織尚未解決的難題。



不足三分之一的組織在網路威脅搜尋方面進行了足夠投資

超過十分之九的組織面臨與雲端安全有關的巨大挑戰

超過五分之四的組織正在努力及時修復已知漏洞

繪製前進路線

為了克服 IT 安全挑戰，當今企業需要「能奏效」的網路威脅防禦，例如透過：

1. 提供普遍可見性
2. 分流和簡化安全基礎結構
3. 加速新安全工具的部署和整合
4. 實現協調和自動化

授權給 GIGAMON

若要下載完整報告，請訪問：
www.gigamon.com/cdr2018