埋まらないギャップ

サイバー防御の一歩先を行くサイバー犯罪。打つ手はないのか？

3つのギャップ

サイバー犯罪と対応の関係は複雑です。ハッカーと防御者、戦略と実装、企業の経営と実装者など、複数のレベルのギャップが存在します。

攻撃者 vs 防御者

俊敏で迅速

市場が分散化し、どこからでも瞬時に攻撃ができるようになった。

VS

解消されない煩雑さ

防御者は、面倒な手続きと思い付きの意思決定に振り回されている。

戦略 vs 実装者

90%

90%以上の回答者は、企業にサイバーセキュリティ戦略が実装されていると回答している。

VS

50%未満

戦略を完全に実装している答えた回答者は半分もいない 。

経営陣 vs 実装

独自の視点で結果を評価

サイバー戦略を設計した上級管理者は、効果よりも見た目でセキュリティを評価する。

VS

効き目の薄いセキュリティ

戦略を実際に実装している担当者は、上級管理者との見解の相違に苦しんでいる。

ギャップの状態

企業におけるサイバーセキュリティのリスクは以前よりも高くなっています。リクス管理、チームの認識、攻撃方法と防御策など、複数の断層が存在します。

54%

調査した経営者の54%は、導入されているサイバー対策の効果ではなく、評判に対する影響を気にすると答えている。

76%

76%の回答者は、リスク要因の上位3つにサイバーセキュリティのリスクが入っていると答えている。

83%

83%の回答者は、セキュリティ侵害による被害が止まらないと答えている。

5倍増

サイバーセキュリティに有効な対策はないと答えた回答者が5倍になった。

アイデア/金銭

スマートなサイバー犯罪者はアイデアを盗み、低層の犯罪者は金銭を狙う。

51%

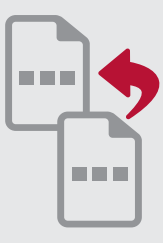
ロシアのIT専門家で正規のIT業界に採用されたのは、わずか51%にすぎない。

42%

42%の脆弱性は、発見後30日以内に悪用されている。

犯罪市場からヒントを掴む

犯罪市場と防御策の類似点

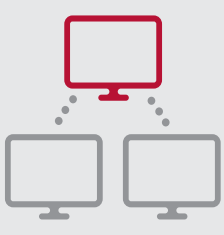


進む可視化

情報共有を進めることで、作業の重複を排除し、防御コストを低減する。セキュリティを大幅に強化する新しい技術とプラクティスを瞬時に展開する。

ギャップを埋める

上位の管理者とオペレーターの間に存在するギャップを最小限に抑えるため、賞やボーナスなどの特典を従業員やマネージャーに送り、適切なセキュリティ対策を実施する。



市場原理の応用

外部委託とオープン契約でコストが削減されたが、競争は激化し、革新的なベストプラクティスも迅速に推進する必要がある。

誰でも簡単に参加

若手や外国のICT専門家など、広範な人材プールでサイバー犯罪に対応する。企業のサイバースキルのギャップを解消し、犯罪市場から人材を取り戻す。

公開する

発見された脆弱性にすばやく対応する。パッチ適用の方法を改善し、古いシステムも迅速に更新する。セキュリティ対策を強化し、攻撃のコストを増大させる。

攻撃者から学び、ギャップを埋めましょう。
生き残りの鍵は適応です。

レポートの完全版は、www.mcafee.com/misalignedをご覧ください。

intel Security

2504_0217_info-misaligned-incentives-cybercriminals-defenders