Gigamon

2018 サイバー脅威 防御レポート

CyberEdge Groupの第5回年間サイバー脅威防御レポートは、ITセキュリティの専門家が、自社のセキュリティへの態勢、効果的なサイバー脅威防御を確立する上で直面する課題、およびこれらの課題を克服するための計画を、いかに把握しているかについて明らかにしています。今年のレポートにおける主要な発見のいくつかについて、考察を進めましょう。

侵入は回避することができない

組織は、驚くべき割合で実際にサイバー攻撃を受けた被害者となっています...
さらにこれ以上のことが今後起きると予測されています。

2017年に少なくとも1回は被害にあった **77.2%**

2017年に6回以上被害にあった **27.4%**

2018年に被害にあう可能性がある **62.3%**

セキュリティ予算の増加

企業からの回答では、企業のセキュリティ関連製品、サービス、人材への消費は、2018年に平均でおよそ4.7%増加しています。

12%
IT予算のうちセキュリティに割り当てられる平均的消費率

しかし、課題の数は依然として変わっていません

課題 No.1:すべきことが多すぎる

今日の企業にとって、テクノロジーの影響範囲の拡大に伴い、防御しなければならない攻撃対象領域が広範になっています。

セキュリティ態勢における インフラストラクチャの順位

1 コンテーナー
2 モバイル機器
3 クラウド・インフラ

最も不完全なプロセス/機能

1 アプリケーション開発とテスト(SDLC)
2 攻撃対象領域の削減
3 内部不正者/内部攻撃の発見

効果的にすべき主要な障壁

膨大な分析データ

課題 No.2:技術を持った人材の不足

セキュリティに費やすための資金追加は、サイバーセキュリティの専門家が世界的に不足している中、わずかな慰めにすぎません。

技術を持った人材の不足は、サイバー脅威の適切な防御への最大の障壁とされました

組織は、ITセキュリティの人材不足を経験しています

縦関係のある業界はITセキュリティの技術不足にあっています

課題 No.3:適切なソリューションの模索中

適切な場所すべてに十分なテクノロジーの投資を行うこと、およびそれらの多くを展開することは、いくつかの組織がこれから解決すべき難問です。

1/3以下の
組織しか、サイバー脅威ハンティングに対して適切に投資していません

10のうち9以上の
組織がクラウドセキュリティに関連した重大な課題を抱えています

5のうち4以上の
組織がタイムリーな方法で既知の脆弱性にパッチを適用することに苦慮しています

今後の進路

今日の企業を悩ませているITセキュリティの課題を克服するには、シンプルに「やるべきことをする」というサイバー脅威防御が必要です。例として：

1 広範の可視化の提供

2 セキュリティ・インフラの負荷軽減と簡素化

3 新しいセキュリティツールの開発および統合の加速

4 オーケストレーションと自動化を可能にする

完全なレポートをこちらからダウンロード：
www.gigamon.com/cdr2018

CYBEREDGE GROUP