Gigamon

2019 サイバー脅威防御レポート

CyberEdge Groupの第6回年間サイバー脅威防御レポートでは、組織のセキュリティ体制サイバー脅威に対する効果的な防御策を確立するうえで直面している課題、それらを克服するための計画について、ITセキュリティ専門家がどのようにして把握しているかを明らかにします。最新のサイバー脅威防御レポートからの重要な所見をご確認ください。

サイバー脅威の包囲網の中で

組織は驚くべき割合でサイバー攻撃の被害を受けています。
そして、今後現状を上回る状況になると予想されます。

- 2018年に少なくとも1回サイバー攻撃を受けた — 78.0%
- 2018年に6回以上サイバー攻撃を受けた — 31.5%
- 2018年にランサムウェアによる被害にあった — 56.1%
- 2019年にサイバー攻撃が予想される — 65.2%

主な課題

近年、ITセキュリティには健全な予算が割り当てられているにもかかわらず、
ほとんどの会社、組織は、サイバー脅威に対する効果的な
脅威防御の実現を妨げるいくつかの重大な課題に直面しています。

効果的な対策に向けた障害のTop1

分析対象データの増大

効果的な対策に向けた障害のTop2

84%

会社、組織内で熟練した
ITセキュリティ人材が不足している

脅威ハンティングの障害のTop1

脅威ハンティングツールを
実装、統合することの難しさ

その他の重大な障害

74%

回答者の3/4近くが、SSL/TLS通信の効率的な検査ができていないことが問題であると示唆

セキュリティ体制は整っている

新たなセキュリティ技術が、セキュリティデータの過負荷による課題を、
ITセキュリティ運用チームが解消するために役立つことを約束していますが...

第1位

セキュリティ分析対策は、
2019年に導入が計画されているTop1のセキュリティ技術
（回答者の46.9%が同意）

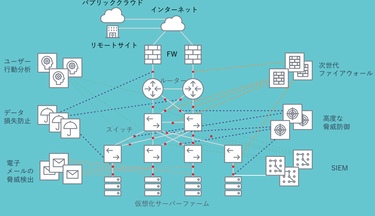
81%

回答者の81%が機械学習と人工知能技術が高度なセキュリティ脅威の解決に役立っていると回答

…現実として、根本的原因には対処できていません。

根本的な問題

長年にわたり、多数のセキュリティツールのレイヤが追加されたことで、
一時的な対策向けのセキュリティアーキテクチャとなっている場合があります。
この設計はセキュリティデータの増大を引き起こすだけでなく、次の欠点があります。



- ネットワークトラフィックへの信頼できないアクセス
- 暗号化トラフィックを効率的に検査できない
- セキュリティスタックの複雑さとコストの増加
- 繰り返し発生する誤検出とアラート
- 新しいセキュリティツールに対する不十分なサポート

解決可能なソリューション

これらの課題を克服するには、広範囲の可視化を実現しながら、
データの配信と検査処理の冗長性、およびその結果として発生する
セキュリティイベントを最小限に抑えることができるソリューションが必要です。
次のように、セキュリティツールと運用チームを翻弄させることなく、
適切な情報とインサイトの両方を提供することが重要です。

1. ツールに最適化されたトラフィックを提供（物理/仮想/クラウド基盤）
2. リソース集約型のプロセス（SSL復号化など）の一元化
3. 新しいセキュリティツールの導入および統合の加速
4. オーケストレーションと自動化の有効化（運用効率を高めるため）

レポートのダウンロードはこちらから：
www.gigamon.com/cdr2019

CYBEREDGE GROUP