LAC

クラウドセキュリティ設定診断 by MVISION Cloud

ラック セキュリティ診断サービス「クラウドセキュリティ設定診断 by MVISION Cloud」

安全なクラウド環境を、使い続けたい!!

クラウド環境を、安全に安心して活用するために。

クラウド環境上にシステムを構築し、運用している企業が急速に増えている一方で、個人情報の漏洩や、マルウェア感染、仮想通貨マニングによる高額請求など、クラウド環境でのセキュリティ事故が後を絶ちません。これらの原因の多くは、クラウド環境の設定不備によるものです。クラウドがもたらす多くのメリットを正しく享受するためには、定期的にクラウド環境の設定を確認し、その都度設定不備を修正していく必要があります。

お困りではありませんか ？

- クラウド環境の構築経験が少ないので心配
- クラウド環境の設定を定期的にチェックしたい
- グローバル基準やベストプラクティスに対応したい

ラックが提供する

「クラウドセキュリティ設定診断 by MVISION Cloud」

1.導入・活用支援
- MVISION Cloud の導入支援、また活用するための操作説明などを支援いたします。

2.診断
- 診断対象のクラウド環境をMVISION Cloudに連携し、CISベンチマーク(※1)やその他のコンプライアンスに沿って診断を実施します。

3.分析
- 年4回、弊社診断員が診断結果をもとにセキュリティ設定上の問題点を洗い出します。

4.結果報告
- 診断結果、分析結果をとりまとめ、診断結果の報告を行います。

5. サポート
- MVISION Cloud の操作方法等に関するご質問への回答。
- 診断結果における脆弱性の脅威、影響、対策方法に関するご質問への回答。（製品ベンダやセキュリティ情報提供サイト等で一般公開されている情報に基づき回答します）

クラウド環境の各種設定を解析し、現状の評価、リスク及びベストプラクティスの提示を行います。

McAfee社の「McAfee MVISION Cloud for IaaS/PaaS」(略称：MVISION Cloud)をお客様環境に導入することで、クラウド(IaaS/PaaS)環境が適切なセキュリティ設定になっているかを常時確認できるように支援します。AWS(Amazon Web Services)、Azure(Microsoft Azure)、GCP(Google Cloud Platform)に対応し、各種設定を解析し、現状の評価、リスク及びベストプラクティスの提示を行います。CISベンチマーク(※1)や各クラウド環境推奨のセキュリティベストプラクティス等に沿った設定・運用がされているかを確認し、結果をレポート形式でご報告します。

リソースのセキュリティ構成監視

- セキュリティ設定を継続的に監視し、ポリシーに準拠していない設定ミスを確認します。
- 設定ミスを正しく修正すると、MVISION Cloudが修正を自動的に確認し、インシデントとしての報告をクローズします。

アクティビティモニターとフォレンジック

- フォレンジック調査のためのアクティビティの監査証跡をキャプチャして分類します。
- 100のアクティビティを13のカテゴリに分類し、簡単にフィルタリング/ナビゲーションを行えるので、フォレンジック調査に役立ちます。

内部犯行・ユーザの乗っ取り・特権ユーザアクセスの脅威を検知

- 信頼できない場所からのログイン試行を解析します。
- 過剰なユーザー権限、非アクティブなユーザ、不適切なアクセス、および権限の不当な特権昇格とユーザーのプロビジョニングを識別します。

(※1)CISベンチマークは米国の政府機関や企業などのセキュリティ専門家の協力を得て、インターネット・セキュリティ標準化に取り組む米国の非営利団体「Center for Internet Security」が提供しているベストプラクティスです。(resource：https://www.cisecurity.org/)

LAC

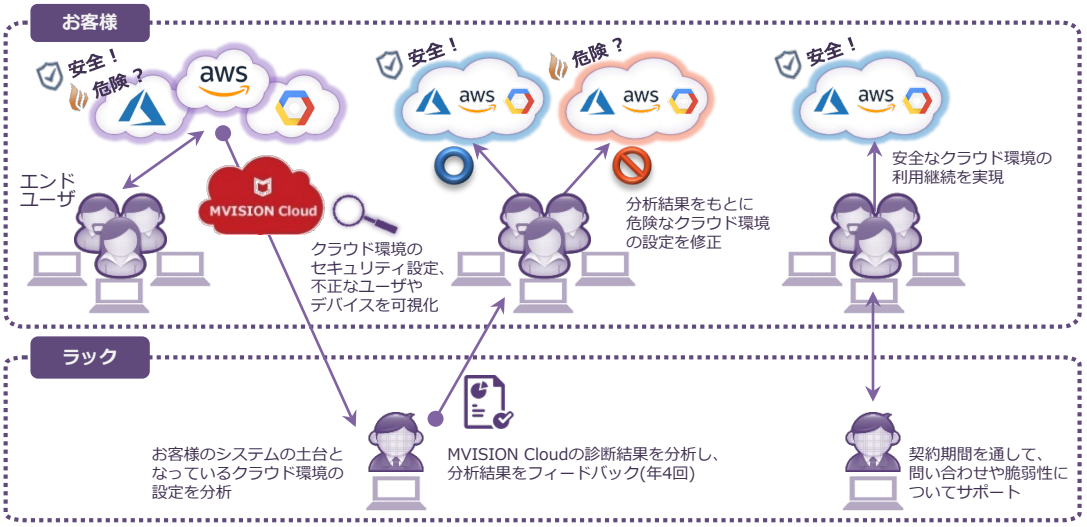
クラウドセキュリティ設定診断 by MVISION Cloud

ラック セキュリティ診断サービス「クラウドセキュリティ設定診断 by MVISION Cloud」

安全なクラウド環境を、使い続けたい!!

「クラウドセキュリティ設定診断 by MVISION Cloud」のサービス提供イメージ

クラウド環境のリスク評価・可視化 ＞ クラウド環境利用のコントロール ＞ 安全なクラウド環境の利用強化



「クラウドセキュリティ設定診断 by MVISION Cloud」の診断項目

AWS(Amazon Web Services)(※2)	
Identity and Access Management	アカウントの保護やパスワードポリシーの設定が適切か診断。
ロギング	ログの取得に関する設定が適切か診断。
モニタリング	ログの監視によるモニタリング設定が適切か診断。
ネットワーク	不要な通信が許可されていない設定であることを診断。
AWS及びMVISION推奨のベストプラクティス	IAM、ロギング、モニタリング、ネットワークの設定がAWS及びMVISION Cloudの推奨する設定であることを診断。
CISベンチマーク項目一部抜粋	
IAM	rootアカウントが利用されていないこと。
ロギング	全リージョンでCloudTrailが有効であること。
モニタリング	不正なAPI呼び出しに対してログメトリックフィルタとアラームが出力されること。
ネットワーク	Security Groupが、0.0.0.0/0 port 22(SSH)への接続を許可しないこと。

(※2)AWSの他、Azure、GCPに対応しています。

Why？ラック　- 豊富な経験と信頼の実績

ラックは、インターネットが普及する前の1995年、いち早くネットワークセキュリティ事業を開始し、2000年には国内初となる24時間体制の「セキュリティ監視センター」を設置、以来リーディングカンパニーとして国内のサイバーセキュリティ対策の普及を牽引しています。

- セキュリティコンサルティング **1,530** ユーザ以上
- セキュリティ診断 **19,000** 件以上
- セキュリティ監視 **940** ユーザ以上
- 緊急対応出動 **3,100** 回以上
- セキュリティアカデミー受講者 **30,000** 人以上

JSOC JAPAN SECURITY OPERATION CENTER　CYBER EMERGENCY CENTER　CYBER GRID JAPAN　LAC Security Academy

LAC
株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー
sales@lac.co.jp　www.lac.co.jp