SRA の技術情報誌
GS LetterNeo
Vol.165　2022 年 4 月

Cavirin の紹介

～セキュリティ/コンプライアンス監視を自動化～

井上 知也

アドバンストクラウドエンジニアリング事業部

はじめに

Cavirin[1] は、AWS、Azure、GCP、コンテナやオンプレミス環境といった、データセンターとクラウド環境について、セキュリティとコンプライアンスの準拠状況を評価し、修正できる製品です。今回、Cavirin の構築、クラウドとオンプレミス環境の評価、そして検出した問題を修正するまでの流れを社内で検証してみましたので、その成果を報告します。

目次

[1] https://cavirin.com/

Cavirin とは？

日々のシステム運用を行う中で、次のような不安や問題はないでしょうか。

- ✓ システムにセキュリティ上の問題はないか、コンプライアンスに準拠しているか調査するよう求められたが、何から手を付けて良いか分からない。
- ✓ システムがコンプライアンスに違反しているということが分かり、対応しなければならないが、方法が分からない。なんとなく対応方法を調べてはみたが、妥当性に不安がある。
- ✓ オンプレミス環境、クラウド環境を複数抱えており、セキュリティポリシーに統一性がない。

マルチクラウドやハイブリッド環境において、Cavirin は、CIS、NIST、PCI DSS 等の主要な規格に求められるセキュリティポリシーやコンプライアンスに準拠しているかを確認する手助けとなる製品です。

まずは動かしてみましょう

百聞は一見に如かず、まずは実際に動かしているところを見てみましょう。

Cavirin は AWS のマーケットプレイスで AMI を公開しています。他に、オンプレミス版として VMware で使用できる仮想マシンのイメージなどもあります。

図 *1 AWS* マーケットプレイス

今回の検証では、AWS 上に Cavirin を展開することにしました。EC2 のイメージですので、事前に VPC やサブネットの用意をしておきます。その後、マーケットプレイスの

Usage に記載されている通りの方法で展開します。Cavirin は基本的に Web UI から操作を行うため、外部から HTTPS で接続できるようにパブリックサブネットへ配置し、セキュリティグループでインターネットからの接続を許可するシンプルな構成にしました。

あとは実際にパブリック IP にアクセスしてライセンスを適用すれば、Cavirin の画面を見ることができます。

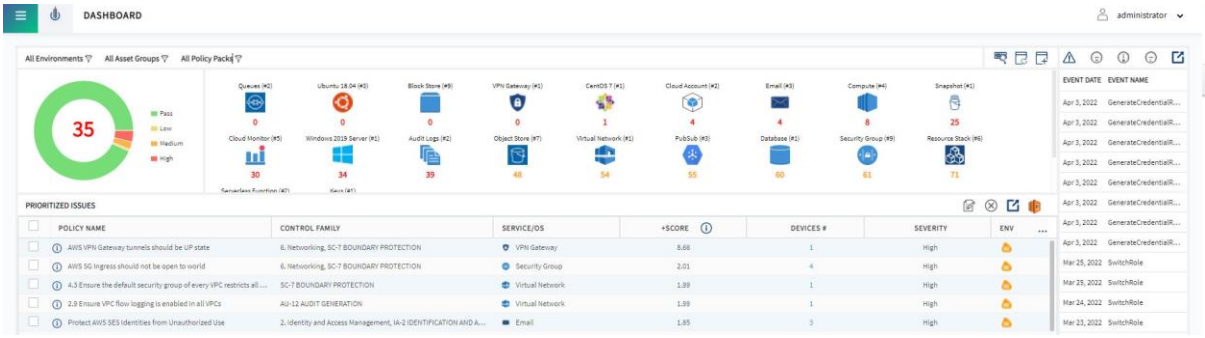

図 *2 Cavirin のダッシュボード*

図 2 は Cavirin のダッシュボード画面ですが、既に AWS や Azure、オンプレミスの評価を行えるよう構成したものです。AWS では S3 や VPC、セキュリティグループといったリソースの設定、オンプレミスではサーバ内の設定ファイルなどについて評価を行うことができます。問題のある評価項目の一覧や、評価結果をスコア化したものがダッシュボードに表示されます。

ポリシーパックによる評価

評価項目の一覧は、ポリシーパックという形で提供されます。例えば、「AWS NIST 800-53r4 Policy Pack」というポリシーパックは、AWS 上で NIST SP 800-53 に準拠するための評価項目を用意しています。

図 *3 AWS NIST 800-53r4 Policy Pack*

Cavirin の大きな特徴として、評価の結果、検知した問題に対しての具体的な対応方法を示してくれるというものがあります。例として、先ほどの「AWS NIST 800-53r4 Policy Pack」内にある「3.11 Ensure S3 buckets have versioning enabled」という項目について見てみましょう。

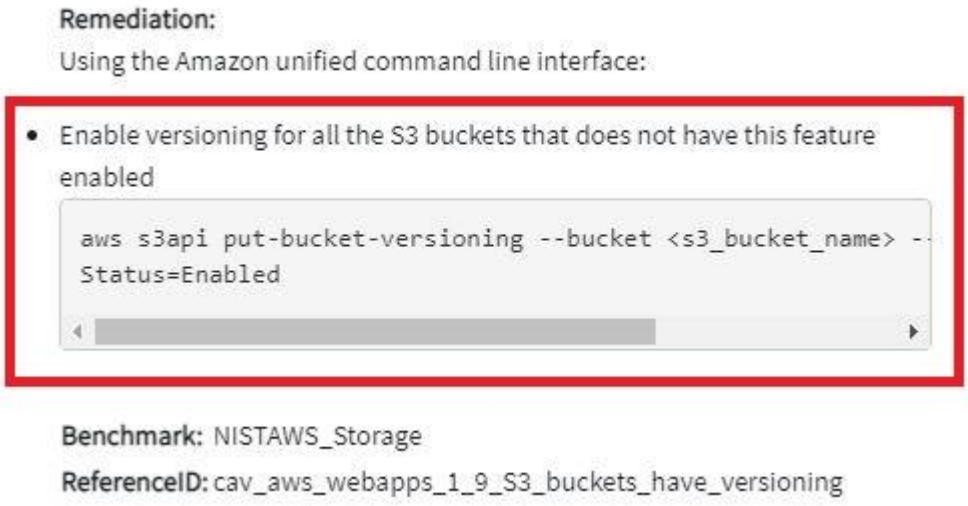

図 4 「*3.11 Ensure S3 buckets have versioning enabled*」の説明(一部抜粋)

説明の中にはオブジェクトストレージである S3 バケットのバージョニング機能を有効化することにより、意図しないオペレーションや障害によるデータ消失からの復旧ができるという修正の必要性などが記載されていますが、特に重要なことは実際に AWS CLI による設定の修正方法も合わせて示されていることです。図 4 の赤枠部分に実際の S3 バケットに対して適用するべきコマンドが表示されています。この情報を用いて手作業での修正を計画することもできますが、設定の適用を Cavirin 上から実施することができます。

Cavirin の修正機能

Cavirin には、Cavirin 上からリソースの修正を行う機能(Remediation)があります。先ほど紹介したポリシーパック、「AWS NIST 800-53r4 Policy Pack」の評価項目の一つである「3.11 Ensure S3 buckets have versioning enabled」に対して、実際に Cavirin 上から S3 を操作し修正できることを確認してみましょう。

AWS 上のリソースに対して Remediation の機能を使用するためには、修正対象となる AWS アカウント上で Lambda、SQS、SNS を展開しておきます。これらは展開用のスクリ

プト(AWS SDK for Python により実装)が提供されます。Cavirin はこれらを経由して AWS リソースの修正を行います。

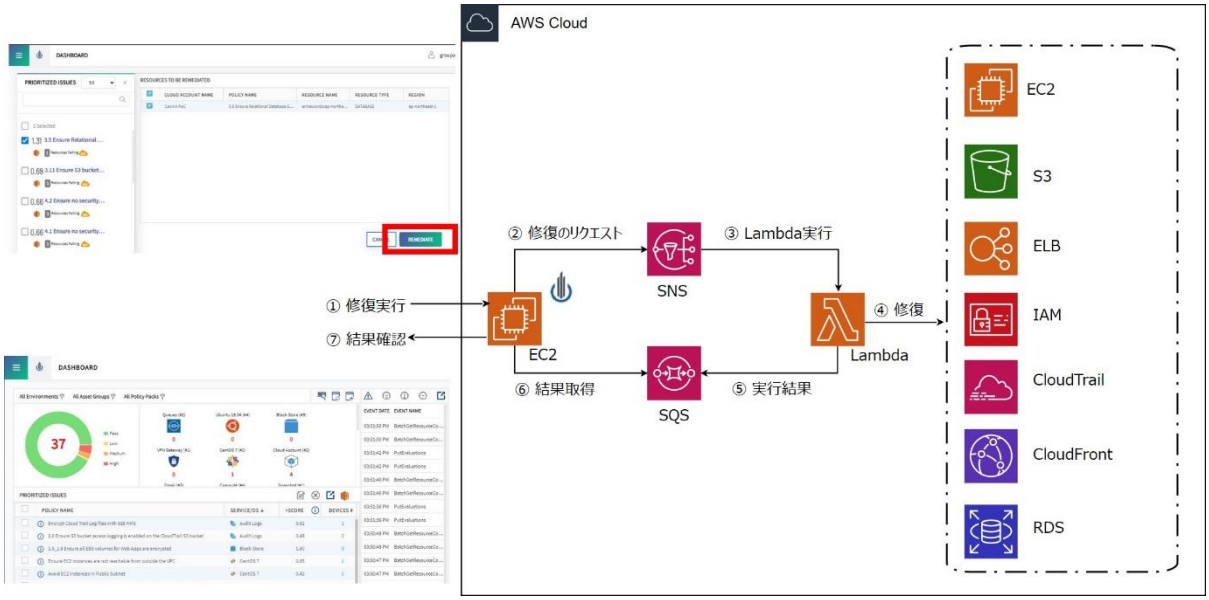

図 *5 Cavirin* の修復機能

検証では、自身の AWS アカウントにあるリソースを修正するために、筆者のアカウント上に展開しました。

では、実際にバージョニングが行われていない適当な S3 バケットを用意します。

図 *6* バージョニングが無効の *S3* バケット

図 6 の赤枠部分で、S3 バケットのバージョニングが無効になっていることが分かります。この状態で「AWS NIST 800-53r4 Policy Pack」による監査を実行し、バケットのバージョニングが無効になっていることを Cavirin に検出させます。

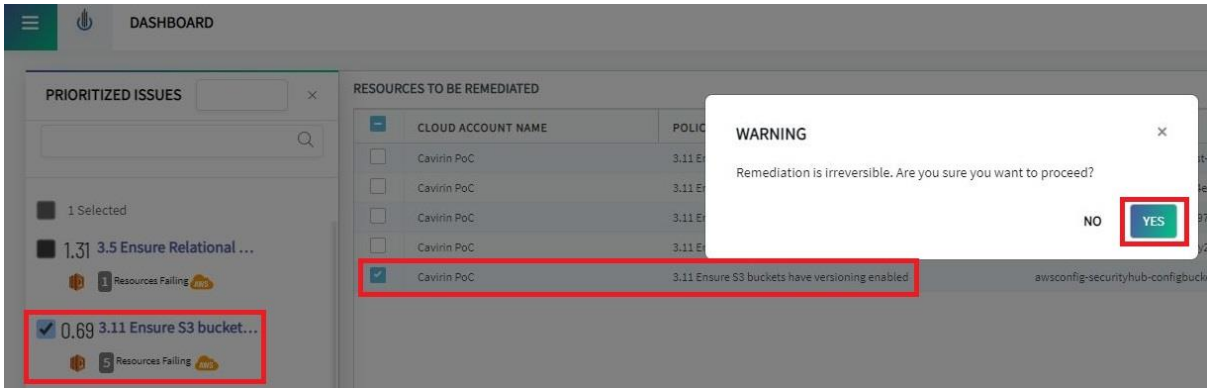

図 *7 Remediation* の実行

そして、Cavirin の Web UI 上から該当の S3 バケットに対して修正を実行します。実行が完了し、改めて対象のバケットを見るとバージョニング機能が有効化されていることが確認できました。

図 *8* バージョニングが有効化された *S3* バケット

本検証では AWS 上のリソースに対して実施しましたが、Azure に対しても同じように修正機能を使用することができます。その場合も、Cavirin で提供されているスクリプトを使用し、Azure 上で事前に Azure Function、Service Bus を構成します。

その他の機能

Cavirin では今回紹介した AWS 以外にも、Azure、GCP、オンプレミス上の Windows や Linux、コンテナ環境である Docker や Kubernetes 用のポリシーパックが用意されています。

また、Slack や Jira などへの通知機能や、AWS CloudTrail をモニタリングしアラートを上げる機能もあります。通知情報のカスタマイズ等ができれば、さらなる利便性の向上も期待されますが、運用者が通常使用しているツールに通知を集約でき、チーム全体への素早い情報共有が可能となります。

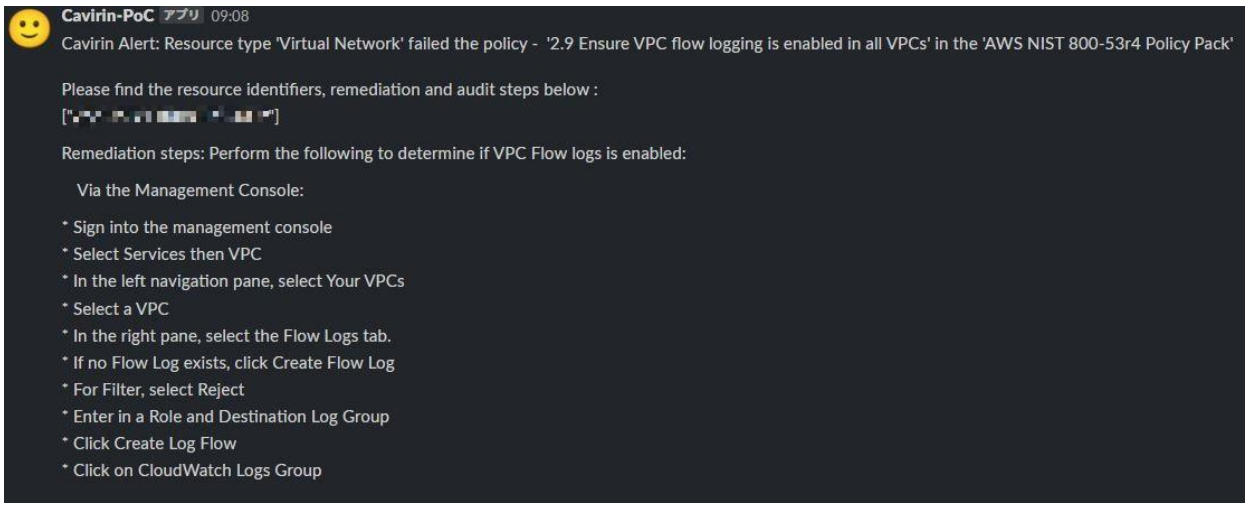

図 *9 Slack* への通知機能

おわりに

今回は Cavirin の主要な機能と、その中でも特に重要な修正機能について、実際に動かして確認しつつどのようなことができる製品であるかを紹介しました。最近ではクラウド側で提供している機能でも多くのセキュリティ対策ができるようになりつつありますが、修正方法までは提示されないため、検知した問題に対してどのように修正すれば良いかを示してくれることにより自身で修正方法の調査を行う手間が省けるだけでなく、Cavirin であれば問題の修正までワンクリックで実行することができる点が便利であると筆者は感じました。Cavirin は Amazon Inspector パートナー[2]になるなどさらにクラウド環境への適応を進めており、今後の機能追加にも期待したいところです。

[2] https://aws.amazon.com/jp/inspector/partners/

GSLetterNeo Vol.165
2022 年 4 月 20 日発行
発行者　株式会社 SRA 技術本部 先端技術研究室

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8

夢を。Yawaraka Innovation
やわらかいのべーしょん