Google Cloud

脆弱性を可視化し脅威検出も可能。対応策の提案機能を有効活用し、統合管理でセキュリティをさらに強化

Classi

Classi株式会社

https://corp.classi.jp
〒163-0415　東京都新宿区西新宿 2-1-1
新宿三井ビルディング 14F

2014 年 4 月、株式会社ベネッセホールディングスとソフトバンク株式会社の合弁会社として設立。「子供の無限の可能性を解き放ち、学びの形を進化させる」というミッションに基づき、教育プラットフォーム「Classi」の開発、および運営を事業として展開。日本全国の高校・中高一貫校 3,000 校以上にサービスを提供。2019 年 1 月、株式会社EDUCOM のグループ会社化により、初等中等領域にも事業を拡大。

インタビュイー

- データAI部 部長 データサイエンティスト　伊藤 徹郎 氏
- データAI部 データプラットフォームチーム データエンジニア　滑川 智也 氏
- データAI部 学習チーム Pythonエンジニア　平田 哲也 氏
- データAI部 学習チーム Pythonエンジニア　工藤 淳真 氏

「まなびをエールする」をコンセプトに、学校向けに特化したクラウド サービス「Classi」を事業として展開する Classi株式会社。新しい機能の開発やデータ分析の基盤として Google Cloud を活用しています。その一環として、さらなるセキュリティの強化を目的に、Security Command Center を採用。セキュリティ対策の取り組みについて、データAI部の担当者 4 名に話を伺いました。

利用している Google Cloud サービス

Security Command Center、BigQuery、Pub/Sub、Cloud Functions

約 3 年前よりデータ分析や新機能開発に Google Cloud を活用

日本全国の高等学校の半分強、高校生の 2 人に 1 人が利用している Classi は、スマートフォンやタブレット端末、PC などのデバイスを活用することで、授業や面談、学校と保護者のコミュニケーションなど、学校現場におけるさまざまなシーンで利用されている教育プラットフォームです。

学校生活の気づきや学びを記録するポートフォリオ、生徒 1 人ひとりに最適な学習コンテンツを提案するアダプティブ ラーニング、Classi の ID 1つで様々なアプリを利用することができるプラットフォーム、任意のグループで利用できるコミュニケーションの 4 つの機能で構成されています。

Classi では、新しい機能の構築、および社内のデータ分析環境に、約 3 年前から Google Cloud を採用しています。

データAI部 部長 データサイエンティストの伊藤さんは、「データ分析基盤として BigQuery を採用した理由は、ハードウェアを気にすることなく、クエリを投げるだけで結果が返ってくるパフォーマンスのよさです。いくつかの選択肢がありましたが、BigQuery にデータを持ってくる方が、機能的にもパフォーマンス的にも価値がありました」と話します。

また、新機能の開発や PoC、大学との共同研究用のデータ提供などにも Google Cloud が利用されています。その一環として、セキュリティの強化に Security Command Center が採用されています。採用の理由を、データAI部 データプラットフォームチーム データエンジニアの滑川さんは、次のように話しています。

「2020 年にセキュリティ インシデントを経験したことから、セキュリティのアセスメントや自動チェックなど、セキュリティの強化を改めて見直す必要性を感じていました。また以前は、新機能の構築やデータ分析など、Google Cloud のプロジェクトごとに、プロジェクト担当者が個別にセキュリティのチェックを行っていましたが、標準的なシステムを導入して、統合管理をしたかったことから、Security Command Center の無償版を利用することにしました。」

（伊藤さん）　（滑川さん）　（工藤さん）　（平田さん）

脆弱性の正確な検知と使い勝手の良さを導入してすぐに実感

Security Command Center の検討は、2020 年 11 月から開始し、まずは、無償版を導入。伊藤さんは、「無償版を 2〜3 か月使ってみて、使い勝手もよく、脆弱性や構成ミスもちゃんと検知できるので好印象でした。今後、Google Cloud 上で動くサービスも増えていくので、クラウドの脆弱性や構成ミスだけでなく、アプリケーション レイヤーやコンテナ レイヤーなど、検知する項目も増えることから、2021 年 2 月に有償版に移行することを決めました」と話します。

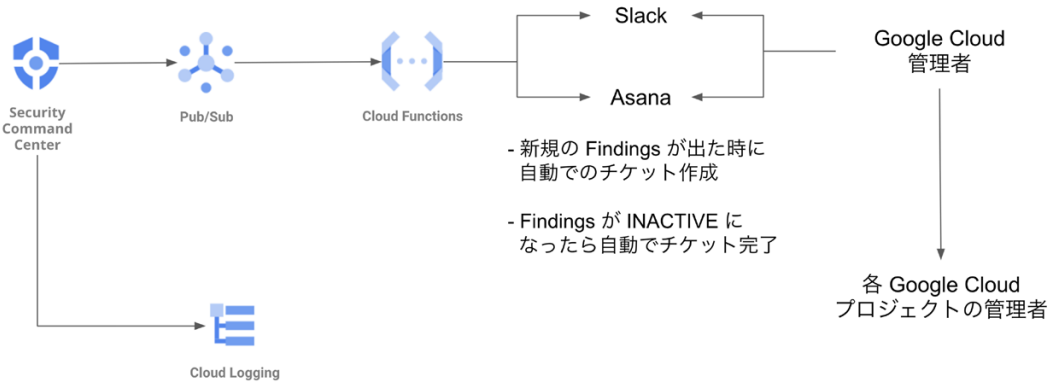
構築されたシステムは、Security Command Center やチケット管理ツール、さらにチャットツールなどを Pub/Sub と Cloud Functions で連携。Security Command Center がスキャンして、脆弱性や構成ミスを検知した瞬間に、チケット管理ツールに自動的に連携され、チケットが登録されます。チケットが自動生成されるとチャットツールで、各プロジェクトの管理者にアラートが通知される仕組みになっています。

Security Command Center のダッシュボードでは、どれくらいのアラートが通知されているかを一覧で確認することが可能。Google Cloud のフォルダ単位やプロジェクト単位に分割して閲覧することもできます。チケット管理ツールに登録されたチケットは、すぐに対応が必要なもの、すぐではないが対応が必要なもの、対応しなくてもいいものの 3 つに分類されて表示されます。

チケットをクリックすると、脆弱性の内容とともに、どのように対応すればよいかが表示され、対応が終了するとチケットが非表示になります。

システム構築時の Google Cloud のサポートについて滑川さんは、「Security Command Center で検知される項目は、重要度の高いものから低いものまでさまざま。そのため、アラートの量やノイズの調整、対応するかしないか、対応する場合、だれが対応するのかなど、システムと運用のすみ分けに苦労しましたが、Google Cloud の担当者のサポートで解決できました」と話します。

また伊藤さんは、次のように話しています。「Google Cloud の担当者からは Security Command Center を紹介してもらって以降、製品のマイルストーンを共有してもらったり、アップデート情報を提供してもらえたり、日々いろいろとサポートしてもらえています。早め早めの情報提供が、巡り巡ってセキュリティ環境のアップデートの助けになっているので、よいサポートだと高く評価しています。」



有償版への移行でスキャン項目が増え、検知項目の対象カバレッジが拡大

Security Command Center の有償版に移行したことで、スキャン項目が増え、検知項目の対象カバレッジが拡大したのは大きなメリットでした。滑川さんは、次のように話します。「広範なセキュリティ スキャンにより脆弱性を可視化でき、それに対して何をすればよいのか、対応方法が明示化されているので知見を蓄積できました。また以前は、プロジェクト担当者が個別にチェックしていたのですが、統一的に脆弱性を可視化できるようになりました。」

また伊藤さんは、「当初、セキュリティスキャンの結果が膨大だったので、どこから手をつけていくか戸惑う状態でした。実際に運用をはじめて対策していくと、スキャン結果を 3 分の 1 程度まで減らすことができたので、それだけセキュリティが強固になったと思っています。Security Command Center がなかったら、担当者の些細な設定ミスや考慮漏れなどの脆弱性が放置されてしまう可能性があったので、その点はよかったです」と話します。

現在、リリースを控えている新しいサービスにおいてもセキュリティ対策が必要でした。データAI部 学習チーム Pythonエンジニアの工藤さんは、「新しいサービスの開発にあたり、Kubernetes を利用しているのですが、Container Threat Detection を使うことで、コンテナ セキュリティや Kubernetes セキュリティで注意すべき点がどこにあるかを理解できました。アプリケーション セキュリティの観点で有益でした」と話します。

また、データAI部 学習チーム Pythonエンジニアの平田さんは、次のように話します。「Web Security Scanner を使用して、アプリケーションへの攻撃を検知し、Security Command Center で確認するための設定も、ボタン操作だけで簡単にできました。普段セキュリティにはあまり関わらないのですが、Security Command Center は容易に利用でき、セキュリティの知見も深められたのでよかったです。」

現在、チケット対応は、チケット管理ツールに自動起票されたチケットを、データAI部のメンバーで対応しています。今後は、チケット管理ツールによる自動アサインや関連チケットの閲覧機能による対応の分散化により、各メンバーが関連するチケットを個別に対応できるようにする計画。システム的に解消できるチケットは、自動で即時対応することで、対応負荷の軽減も目指しています。

伊藤さんは、「セキュリティは、何か 1 つに対応すればよいというものではなく、ずっと付き合い続けていかなければならない取り組みです。またデータAI部だけでなく、全社として習慣づけ、運用への定着を目指すことも必要です。そのためには、脆弱性を常にスキャンをしてくれる Security Command Center のようなツールがあると心強いです。この仕組みをフルに活用することで、より堅牢なサービスを開発、運用していきたいと思っています」と話しています。

Google Cloud を活用することで、ビジネスの将来に注力できるようになります。インフラストラクチャの管理やサーバーのプロビジョニング、ネットワークの構成などに起因する負担を軽減することができます。つまり、イノベーターもプログラマーも、自分の本来の仕事に集中することができます。

お問い合わせはこちらから
https://goo.gl/CCZL78

Google Cloud

Google Cloud の詳細については、右記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。