sysdig

Minna no Ginko

ZERO BANK DESIGN FACTORY

CUSTOMER STORY

個別のセキュリティ運用から脱却、みんなの銀行の守りを固めるSysdigのクラウドネイティブセキュリティ

ゼロバンク・デザインファクトリー株式会社
Architecture Division
Architecture Group　マネージャー
櫻井 拓海 氏（左）

株式会社みんなの銀行
シニアマネージャー　みんなの銀行-CSIRT
CISSP、CCSP、情報処理安全確保支援士
押川 和弘 氏（右）

株式会社みんなの銀行は株式会社ふくおかフィナンシャルグループの100%子会社として2021年5月にサービス提供開始した新しい発想の銀行です。若者をターゲットにスマートフォンひとつでサービスを完結できる銀行としてクラウドを最大限に活用したシステム作りを実践しています。

しかし限られた準備期間とクラウドという新しいプラットフォームに対応することで銀行としての必須なセキュリティ実装においては想定もし得なかった問題に直面してしまいました。2017年ごろから設立準備のための組織が出来て銀行としての機能要件を検討していましたが、当時選択したセキュリティのための製品は機能としては要件を満たしていたものの、実際に運用を行う立場からは課題が多かったと語るのはみんなの銀行のシステム運用を担当するゼロバンク・デザインファクトリー株式会社の櫻井拓海氏です。

「みんなの銀行は『スマートフォン1台で完結する銀行』という方針を持っています。そのためにこれまでの資産を継承するのではなくゼロから作り上げるという選択をしました。最初からクラウドネイティブを指向していましたので、GoogleクラウドのKubernetesサービス、GKEを使っていますし、完全にコンテナベースで全てのアプリケーションが実装されています。これは勘定系から情報系の多岐にわたる多くのアプリケーションを含んでいますので、セキュリティに対する要求も非常に高いものがあります」と櫻井氏は語ります。

株式会社みんなの銀行
ゼロバンク・デザインファクトリー株式会社

事業内容およびサービス内容：

デジタルネイティブ世代の課題・ニーズを反映させたミニマルな銀行サービスを展開

- B2C事業：次世代バンキングシステムを活用して、全国のデジタルネイティブ世代（個人）をターゲットに、スマホを通じた金融サービスを提供
- B2B2X事業：みんなの銀行の金融機能・サービスを、APIを介してパートナー企業（法人）に提供 （金融×非金融の新たな価値共創）
- バンキングシステム提供事業：システム開発/運用業務の内製化を進め、システム・機能自体を提供（販売）（非金融事業者に限らず金融機関も対象）

導入前の課題：

- GUIで個別にしか操作できなかった運用管理
- 自動化のためのIaCツールに未対応
- プロダクトサポートのレスポンス速度と内容

導入効果：

- 統合的に管理できるセキュリティ機能
- 大量に表示される脆弱性アラートを優先順位付け
- インフラストラクチャーアズコード（IaC）の発想でTerraformによる自動化の実現
- 深い知識を持つサポートエンジニアによる充実のサポート

導入前の課題

セキュリティ担当であるみんなの銀行サイバーセキュリティグループシニアマネージャーの押川和弘氏は「実際に詳細に見てみるとここまでの細かい設定が必要なのか？と思うこともありますが、それが銀行のシステムなんです。全てをポリシーによって制御していますが、我々の欲しい細かな設定についてはまだ少しだけ足らないかなと思っています」と語り、毎日のように開発されていく新規のアプリケーションだけではなく銀行の実態に適合したセキュリティ要件を満足するシステム作りに対する難しさを説明しました。

株式会社みんなの銀行
押川 和弘 氏

ゼロバンク・デザインファクトリー株式会社
櫻井 拓海 氏

櫻井氏によれば開発系から準本番、本番システムまでそれぞれが完全に別のクラスターとして隔離されており、みんなの銀行のトップであっても本番システムを触る権限は付与されていないと説明しました。「インフラストラクチャーの構築にはTerraformによるIaCによって自動化されています。アプリケーションの実装もリポジトリからモニタリングまで全て含んで実装できるワークフローが完成しています」と語り、セキュリティに対する要求仕様の高さとクラウドらしい先進的な自動化がなされていることを解説しました。

当初の要求仕様は満足していたベンダーのソリューションでしたが、インフラ担当者とセキュリティ担当者から見れば運用の実態に合ってないソフトウェアだったと言います。それは何故でしょうか？

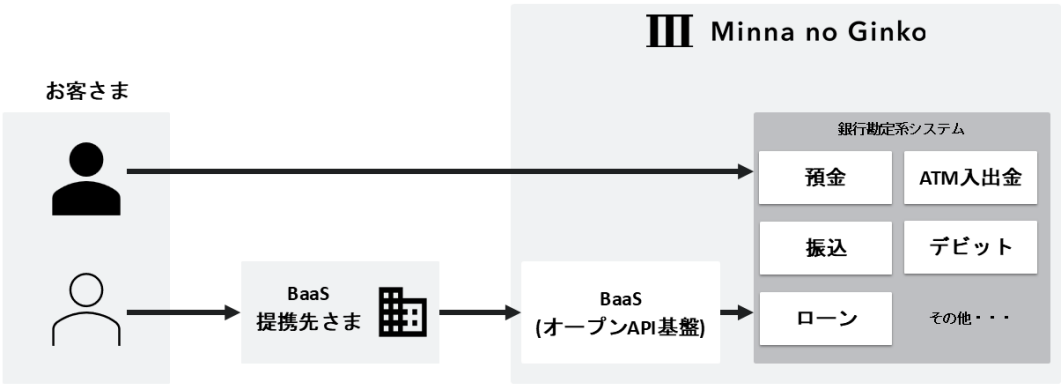
押川氏によれば「当時利用していた製品はクラウド上の様々なアプリケーションに対してカテゴリーごとにセキュリティ機能を適用するソフトウェアでしたが、それぞれの機能がバラバラで運用管理をするのに別々のコンソールからGUIで操作が必要でした」と説明し、セキュリティ担当としての運用コストの高さを指摘しました。またインフラストラクチャーの観点からみんなの銀行はプラットフォーム管理にはTerraformによるIaCを実装しており、GUIではなくコードによる運用自動化を採用していました。そのため機能要件は満たしていたものの運用の観点からは操作のための運用負荷が高いと感じていました。また、サポートの面でも課題がありました。「バグなどに遭遇した際のサポートとして、迅速なスピードで適切に中身を詳しく説明してもらえるサポートが用意されたプロダクトを探していました」と櫻井氏は言います。

ソリューション

そのような課題を抱えていたみんなの銀行が、セキュリティについて変更を検討し始めた時に出てきたのがSysdigでした。セキュリティの観点からは脆弱性の可視化とコンプライアンスチェック、リアルタイムの脅威検出、横断的な統合管理、インフラストラクチャーの観点からはIaCによる自動化、ポリシーによる各種制御などが必要な要件だったと言います。それを全て満足できるのがSysdig Secureだったのです。

みんなの銀行のシステム

- 銀行機能に必要な機能のほとんどを Google Cloud 上に GKE で構築
- 金融機関以外の企業でも決済や与信などの機能を利用できるオープンAPI基盤を提供



「特にGUIに頼らなくてもTerraformから操作できるのが運用面では嬉しいですね」と櫻井氏は説明しました。「以前の製品は個別のツールのGUI使わないと可視化できず、横断的にも見られなかったんですが、Sysdigによってシステムの状況が一つのインターフェースでみられることで運用はずっと楽になりました。脆弱性についても大量にアラートを出すのではなく我々に関連する内容を優先順位を付けて表示してくれるのが良いですね」と語るのはセキュリティ担当の押川氏。

またサポートについては「実際に対応したSysdigのエンジニアが深い知識を持っていることは会話の中ですぐにわかりました。どんな質問を投げてもどんどん深堀りしてくれるし、回答も的確です。『持ち帰って調べます』ということもないのでその場ですぐに問題を解決することができます」と Sysdig Secure への信頼感を櫻井氏は語りました。

これからの展開について「プラットフォームであるGoogleのGKEとSysdigについては満足していますので、稼働率を上げるというよりもセキュアなみんなの銀行のシステムを運用しながらもっとみんなの銀行のユーザーを獲得できる機能を実装していきたいですね」と櫻井氏。押川氏も「生成型AIを使ってセキュリティインシデントの解説をさせるという使い方は良く出来ていますね」と感想を述べました。インシデントについてその影響範囲を生成型AIに解説させることでそれが自社システムにおいてどのような影響を及ぼすのか？を理解するのが早くなったと効果を説明しました。「AIは眠らないし疲れないし文脈を保ったまま何度でも質問できるんです。最後の手段としてサポートエンジニアに問い合わせるにしてもその前の工程が随分と省略できます」とSysdig SageによるAIクラウドセキュリティアナリストの効果を実感していることを教えてくれました。

Minna no Ginko

ZERO BANK
DESIGN FACTORY

GUIによる操作や個別の機能を沢山並べることで機能検討の段階では良く見えても実際にインフラストラクチャー運用を行う部門やセキュリティ担当部門にとっては使いづらい状況が発生してしまう可能性があります。システム運用を継続するために必要な自動化はクラウドネイティブな時代には必須要件とみなすべき時代に既に突入しています。みんなの銀行の経験はそれを教えてくれていると言えるでしょう。

株式会社みんなの銀行
ゼロバンク・デザインファクトリー
株式会社

主な事業内容：
デジタルネイティブ世代の課題・ニーズを反映させたミニマルな銀行サービスを展開

- B2C事業
- B2B2X 事業
- バンキングシステム提供事業

インフラ基盤
Google Cloud

オーケストレーション
Kubernetes

ソリューション
Sysdig secure

Sysdigについて

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

Sysdig. Secure Every Second.

Sysdigの詳細は、sysdig.jp
をご覧ください。

デモを依頼 →

sysdig
CUSTOMER STORY