金融サービス高度化のためのDevSecOps運用の最適化に貢献
蓄積されるも活用されない“ダークデータ”に光を当てる
Splunk Enterprise Security

概要

1999年(平成11年) に設立され、2019年に設立20周年を迎えたauカブコム証券。ネット専業の証券会社として110万以上の顧客口座を擁しており、最近では、証券会社や銀行などに、証券サービスの機能をAPI経由で提供するBtoBtoC事業にも注力しています。

証券プラットフォームとして、同社にとってデータの活用はこれまで以上に大きなテーマです。そこで、これまで可視化、分析してこなかった“ダークデータ”をSplunkによって可視化し、活用することで、インシデント対応の自動化や、DevSecOpsの高度化・自動化をめざす取り組みを2018年以降、本格化しています。

社内CSIRTの体制を見直し、DevSecOpsを確立する必要があった

石川氏によると「セキュリティについては、各種システムやアプリケーションのログは取得していたものの、アラートの自動化や効率的な分析までは着手できていない」状態でした。

そこで、社内CSIRTである「k.CSIRT（ケードットシーサート）」の運用やチームワークを見直すことにしました。k.CSIRTは「kabu.com Cyber Security Incident Readiness Team」の略。一般的には「R」は対応、応答を意味するレスポンス(Response) が当てられますが、同社の場合「普段から継続的に準備をしていく」意味を込めて「Readiness」の頭文字を当てています。

契機となったのが、2017年6月に起きた、DDoS攻撃の事案です。同社のビジターサイトと取引サイトがDDoS攻撃を受け、サイトにアクセスしづらい状況が約30分続いた経験から、石川氏は様々な学びを得ました。その一つが、平時から部門内だけでなく会社全体までコミュニケーション・情報共有を行い「一つのチームになって対応する」ことの重要性です。

様々なログを単一のコンソール画面に統合、分析できる点が決め手

同社は、データ可視化基盤として、マネージドサービスによるSIEMを利用してきました。ベンダーにログデータを渡し、運用をマネージドすることで、インシデントの兆候があった場合、すみやかに通知してくれるものです。

しかし、こうしたマネージドサービスは、データ量が増えれば料金も上がります。また、自分たちで原因やログの相関関係を分析するなどの「可視化」の部分で課題がありました。

石川氏は、構造化データの可視化に「Tableau」を活用してきた経験から、データをモニタリングすることで、問題点が明らかになり、次の改善のアクションが見えてくることを学んだと話します。そこで、非構造化データも扱えるデータ可視化、活用基盤として、金融業界の中でも実績が豊富なSplunkを、2017年に導入しました。

導入当初は無料版を試用しながら特性を掴み、2018年8月には「Splunk Cloud」の利用を開始、さらに2019年5月にはSplunk Enterprise Security（ES）を導入して、本格的に各種ログの取り込み、SIEMとして活用と、DevSecOps確立のために活用することとなりました。

auカブコム証券

業種

- インターネット専業の証券会社

活用事例

- インシデント対応の高度化および、新たな金融サービスを提供していくために、開発と運用が一体となり、セキュリティを自然に組み込むDevSecOpsを確立するためのデータ基盤として活用

課題

- 少人数で、脅威やアラートの検知、分析や自社のセキュリティリスクやビジネスリスクの評価を人力のみで行うには限界があった
- サービスを高速でリリースしていくために、開発と運用が一体化し、サービスリリースの過程に自然とセキュリティが入るDevSecOpsの体制を整備したかった
- 外部の脅威情報をはじめとする膨大なデータとも連携し、インシデント対応を高度化する拡張性のあるデータ基盤が必要だった

導入効果

- Splunkの統合された1画面で脅威やイベントの検知、インシデント分析などがワンストップで行えるため、インシデント対応が迅速に行えるようになった
- サイバーセキュリティ専任の担当者2〜3名という少人数体制でCSIRT運用が行えている
- ダークデータ可視化から、改善と強化実装のサイクルにセキュリティを組み込むDevSecOpsのサイクルが確立された
- ログの取得、モニタリングから改善を繰り返していく意識変革が社内に芽生えつつある

データソース

- Office 365
- Azure AD
- Active Directory
- DNSフォワーダ
- ファイアウォール
- サイバー脅威インテリジェンス
- IT資産管理ソフト

ご利用製品

- Splunk Cloud
- Splunk Enterprise Security（ES）

auカブコム証券株式会社
システムリスク管理室長
石川 陽一氏

Splunk ES採用の決め手として、石川氏は「様々なクラウドサービスのログを、単一のコンソール画面に統合でき、外部の脅威データも取り込むことが可能な点」を挙げます。また、外部にある脅威インテリジェンスなどの「ダークデータ」を取り込むことで、該当するログが自社のログにないか分析できる点も決め手となりました。

データ可視化からはじまるDevSecOpsのサイクルを確立

現在の運用は、システムリスク管理室5名のうち、サイバー専任の2名プラス1名程度の少人数体制でCSIRT運用を行っています。セキュリティ運用の効果として、石川氏は「脅威やイベントの検知、インシデント分析がしやすく、迅速な対応が可能になった」点を挙げます。

統合されたSplunkの画面で分析が行えるため、アプリケーションごとに画面を切り替えて調べる必要がなくなりました。「セキュリティ人材が不足する中で、人材を増やすことが難しいのであれば、人が調べないといけない部分を機械に頼ることは非常に重要だ」ということです。

一方、DevSecOpsの成果としては、粒度の細かいデータの可視化の後、問題点が明らかになり、改善と強化実装のサイクルが確立されました。

つまり、Ops（ビジネスシステム運用のサイクル）を先に、ログからシステムの見える化を支援し、DevSec（改善と強化実装のサイクル）につなげていくのです。こうした「ログのモニタリングから改善を繰り返していくこと」の重要性は徐々に社内にも認識され、石川氏によると「現場から意識改革が芽生えつつある」ということです。

「プロセスマイニング」にSplunkを活用していきたい

今後は、Splunkを金融不正取引の監視や、顧客へのサービス改善などの「攻めの領域」にまで活用していきたいとのことです。また、ビジネスフロー可視化ツールを活用した働き方改革に関する実証実験も始めたところです。

石川氏は、これまでのSplunk活用を通じ、「プロセスマイニング」の重要性を学んだといいます。イベントログデータの蓄積により、プロセスを可視化し、改善ポイントを具体的に特定する手法は、DevSecOpsであれ、サービス改善であれ働き方改革であれ、「すべて同じだ」ということです。

そして、さらなるSplunkの活用のために機能面で要望することは、ハンズオントレーニングやユーザーとのコミュニティなどを「金融などの業種向け、初心者向けなどの内容で実施し、Splunk習熟のコツやユースケースをわかりやすく伝えて欲しい」ということです。そして、さらなる改善のパートナーとして「お互い、前向きなサイクルを作っていきたい」と締めくくってくれました。

20-13888-Splunk-IT-au Kabucom-A4-102-CS-JP