elastic

CASE STUDY

セキュリティ分析

LINE株式会社

インターネットサービス

インシデントの早期発見・解決と効率的な監視を可能に

世界で最も成長しているコミュニケーションアプリである「LINE」。それを支えるシステムやネットワーク、セキュリティ機器が出力する莫大なログからセキュリティ上の脅威を発見しサービスを守るのが、LINE株式会社のセキュリティ室の役割のひとつだ。ここで疑わしい挙動をモニターし、スムーズな状況把握と解決を可能にしたのがElastic Stackによるログの一元管理だ。またX-Packに含まれる Machine Learningで、セキュリティ上の脅威へのプロアクティブな対応も可能に。日々の運用が効率化された。

Elasticsearch　Kibana　Logstash　Beats　X-Pack

40 種類 収集しているログ

3 万+ 収集しているログのソース

20 ノード Elasticsearch クラスター

当時の課題

・システムのさまざまなログが社内に散在していた

・ログが放置され、保存期間も不足

・調査に手間がかかり、収束までに時間がかかっていた

使用の動機

・ログの一元管理と可視化が可能なため

・ログの増加に応じてシームレスに拡張可能なため

・セキュリティエンジニアが容易に作成できる自由度の高いダッシュボードがあるため

使用後の効果

・ログの一元化で、調査の時間を短縮できた

・Kibanaによるログの可視化、ダッシュボードで常に状況を把握

・Machine Learningの導入によって検知精度を高め、誤警告を削減

活用例は次のページへ ▶

バラバラに散在し放置されていたログ

LINEのセキュリティ室が監視するのは、サーバ、ネットワーク機器、および世界中の各拠点で社員が使用するPCなど数万台のデバイス。それらのデバイスから発生するログの管理は、各機器の担当者に任されており、機器内に一定期間蓄積されていた。インシデント発生時にはセキュリティ室から管理者にログのダウンロードを依頼してから受け取る場合もあった。そういったケースではタイムラグが発生し、しかも保存期間が短いために必要なデータが得られないこともあった。

**内外に散在しているログを一元管理することで、
インシデント発生時に必要な調査にかかる時間を
短縮することが課題でした（春木氏）**

集約されたセキュリティ関連のログを自在にダッシュボードで分析できる

2014年からは、ログ管理プラットフォーム「Monolith（モノリス）」の整備をスタートし、ログの分析と可視化にElastic Stackを採用した。

**Elastic Stackを選んだ理由は、
将来的にさまざまなログを扱うことになっても、
データ量の増加に耐えられるスケーラビリティがあったからです（春木氏）**

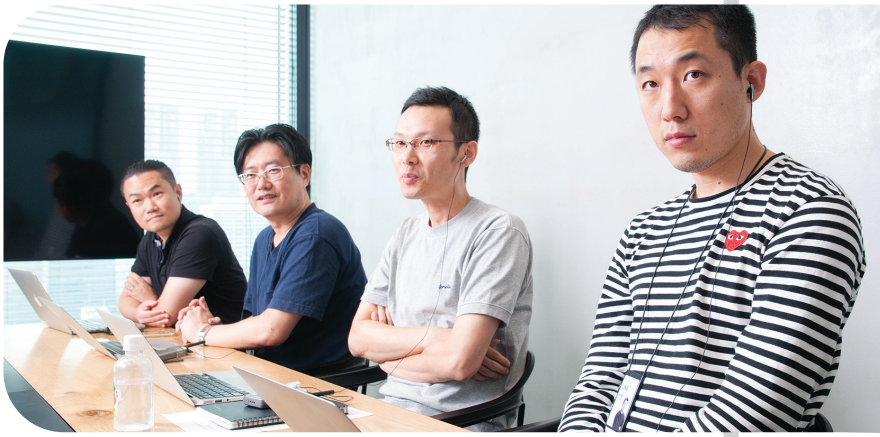
当初は国内のファイアウォール機器とVPNの通信ログが対象だったが、すぐに海外拠点のファイアウォール機器とVPNの通信ログも一元管理するようになった。PCのセキュリティに関連するログについても徐々に追加し、現在では全社員のPCの利用状況、アンチウィルスの検知ログ、システムログインの認証ログなどを収集している。3ノードからスタートしたElasticsearchのノード数は瞬く間に10まで増えた。

**Kibanaによるセキュリティログの分析と可視化は容易で、
インフラセキュリティチームのメンバーがそれぞれ自由に作成しています。
これまで約100個のダッシュボードができましたが、現在アクティブなものは10〜20個ほど。
作成したダッシュボードの中から便利で使いやすいものが自然に共有され、
ノウハウも蓄積されています（春木氏）**

インシデントを解決するまでの時間を大幅に短縮

ダッシュボードでログを可視化することで、調査にかける時間を短縮できるようになった。これまでインシデントの発生時には、複数のログから挙動が疑わしいIPアドレスログをフィルタリングし、これに紐づくPCをひとつずつテキストベースで確認する作業に時間をとられてきたが、Elastic Stackの導入後は、関連するログを検索することで抽出し、全体像を把握できるようになった。

Kibanaでログ検索をすれば、対象の端末が“どういった通信をしていたのか”、“同じ通信先にアクセスする他の端末はどれか”をすぐ洗い出せます（春木氏）



Alerting機能によって、警告をLINEで送信

2016年には、X-Packの機能であるSecurityとAlertingを利用するために、サブスクリプションへと移行した。Elastic Stackの利用者にロールベースのアクセス制御を適用できるようになり、さらにマルウェアを検知したときなどにAlertingを利用してインフラセキュリティチームのLINEグループにメッセージを送ることで、迅速にインシデント対応ができるようになった。バージョン5.0へのアップグレード時には、ログの保存期間と保存対象を増やすために、Elasticsearchを20ノードに増強。今では、サーバ認証系ログ、アンチウィルスやIDS/IPSなどセキュリティソリューションの検知ログ、一部のウェブサービスのアクセスログ、ネットワーク機器やPCの利用状況を一元管理できるようになった。

数カ月分のセキュリティ関連ログをElastic Stackで管理し、分析が可能になりました（春木氏）

elastic

CASE STUDY

セキュリティ分析

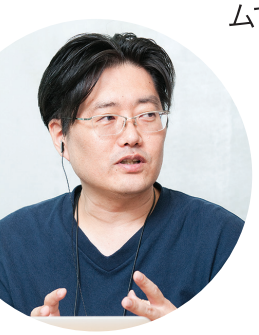
Machine Learningによる自動検知で、調査にかかるリソースを削減

ダッシュボードによる可視化でログ監視は効率化されたが、人の目による異常の発見には限界があると感じた。そこで課題となったのが自動検知だ。異常検知と一言でいっても、曜日・時間帯、システムの種類など、状況によって「正常」の定義は変化するので、単純に閾値を決めて警告すればいいというものではないため、試行錯誤を重ねていた。そんな最中に、ElasticからリリースされたのがMachine Learningのβ版だ。他社の機械学習ソリューションと比較後、2017年5月の正式リリースと同時に導入を決めた。決め手となったのはElastic Stackとシームレスに連携が行えることだった。

Machine Learning を導入したことで、今まで見過ごしていた異常が検知できるようになり、調査にかかるリソースを削減できました（春木氏）

Elasticsearch内のデータをトリガーにした自動化への期待

分散していたログを一元管理することで、インシデント対応にかかる時間を劇的に減らし、セキュリティ監視を効率化した。インフラセキュリティチームでの導入はセキュリティ室の別チームでの導入にも繋がり、他のセキュリティ用途にもElasticの製品群が活用されている。



**今はまだ異常を検知しても、エンジニアが個別に対処する必要があります。
今後はAlertingと連携してすべて自動的に処置できるようになるといいですね
（ インフラセキュリティチーム　マネージャー　朴燦虎氏）**

LINE

所在地 東京都　従業員数 1,716名

COMPANY BACKGROUND

全世界で2億1,700万人超のMAUを誇るコミュニケーションアプリ「LINE」をベースとして、ニュースや音楽、ライブ動画の配信や、ショッピング、決済などのサービスを展開。2017年にはクラウドAIプラットフォーム「Clova」を発表し、音声コミュニケーション分野にも進出。

elastic

Elasticは検索、ログ、セキュリティ、分析などのユースケースで、データをリアルタイムでスケーラブルに利用可能にするソフトウェアを開発しています。2012年に設立されたElasticは、オープンソースのElastic Stack (Elasticsearch、Kibana、Beats、Logstash)、X-Pack (商用機能)、およびElastic Cloud (マネージドサービス)を開発してきました。これらの製品は今日までに累計1億5千万件以上もダウンロードされています。ElasticはBenchmark Capital、Index Ventures、NEAなどから1億ドルを超える資金提供を受けており、600名を超える従業員と共に世界30カ国で事業を展開しています。

その他の事例また活用例に関してはこちらのリンクよりご確認下さい ▶▶▶ www.elastic.co/jp