ウェビナー『次世代ITセキュリティ対策 ～ログ管理とオブザーバビリティ～』

2022年 08月 10日 2:00 pm (EDT)

Webinar | Zoom

Presented by:

ITOCHU Techno-Solutions AMERICA

SYSCOM GLOBAL SOLUTIONS

本日の講師のご紹介

藤原康人

ITOCHU TECHNO-SOLUTIONS AMERICA
ビジネスディベロップメント・マネジャー

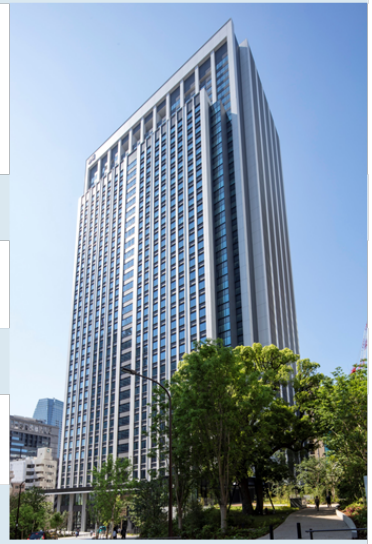
宮本将光

SYSCOM GLOBAL SOLUTIONS INC.
NY営業2部マネジャー

CTCグループのご紹介

2022年4月1日現在

会社名	伊藤忠テクノソリューションズ株式会社（略称 CTC）
英文社名	ITOCHU Techno-Solutions Corporation
本社所在地	〒105-6950　東京都港区虎ノ門4-1-1 神谷町トラストタワー TEL：03-6403-6000（代） URL：http://www.ctc-g.co.jp/
代表者	代表取締役社長　柘植 一郎
創立	1972年（昭和47年）4月1日
設立	1979年（昭和54年）7月11日
資本金	21,763百万円
社員数	単体： 4,718名 連結： 9,695名
事業内容	コンピュータ・ネットワークシステムの販売・保守、ソフトウェア受託開発、情報処理サービス、 科学・工学系情報サービス、サポート、その他



神谷町トラストタワー

SYSCOM のご紹介

会社名：SYSCOM GLOBAL SOLUTIONS INC.

代表者：代表取締役社長　佐藤 誠詞

設立：1990年5月24日

資本金：$3,200,000.00

株主構成：

- 佐藤 誠詞 President & CEO― 199株(66.3%)
- ITOCHU Techno-Solutions America, Inc. ―101株(33.7%)

従業員数：150＋

本社：米国ニューヨーク

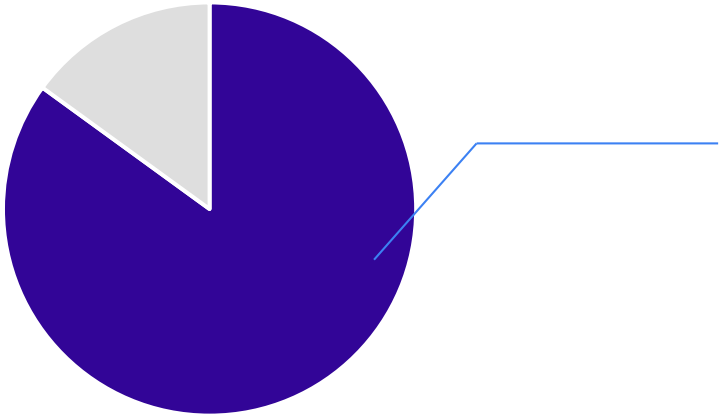
30年以上のUSでの
ITサポート実績

日系企業1000社
以上の取引実績

従業員の7割以上
エンジニア

今回のウェビナーアンケート結果

“御社におけるログ管理・ログ管理ソリューションについて、
あてはまるものにご回答ください。”



85%以上の企業が
“未導入”と回答

ログとは

ログとは
パソコンやシステムの「データ履歴」のことを意味する。

ログの種類:

操作ログ:パソコンやシステムを操作した記録・履歴

認証ログ:パソコンやシステムへのログイン以外に、インターネットのサイトにログインした履歴

イベントログ:パソコンやシステムで起こる特定の現象や動作

通信ログ:インターネットの通信や接続した記録、サーバにアクセスした履歴

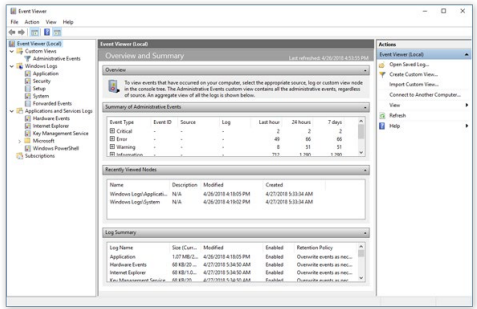
通話ログ、印刷ログ、エラーログ、カメラ映像、入退室記録 etc.

実際にログを見る方法

Windows

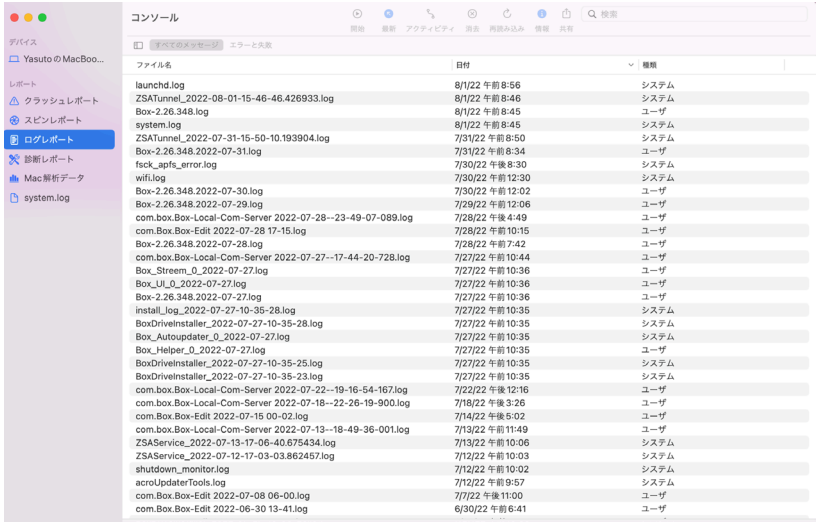
Windows8のログ取得方法
①「スタート」中の「コンピューター」を右クリック、「管理」を選択
②「コンピューターの管理」の中の「イベントビューアー」を選択
③「カスタムビュー」「アプリケーションとサービス」等に並んでいる「Windowsログ」をクリック
④各種選択することでログが表示

Windows10のログ取得方法
①スタート（左下のウィンドマーク）を右クリックし、「イベントビューアー」を選択
②「カスタムビュー」「アプリケーションとサービス」等に並んでいる「Windowsログ」をクリック
③各種ダブルクリックすることでログが表示



Mac

①Finderを開く
②「アプリケーション」を開く
③「ユーティリティ」を開く
④「コンソール」を開く
⑤「ログレポート」を選択



ログ管理によるObservability

システムのクラウドシフトが一層加速し、システムはマルチクラウド、ハイブリッド、オンプレミスが入り組み複雑化。
そのようなシステムを安定稼働させる為にObservability(可観測性)の重要性が高まる。

何故Observabilityが必要なのか

システムの提供する価値が高まり、重要性が向上。
比例して、システムの停止やセキュリティトラブル発生時のコストが上昇。

システム停止のコスト

According to Gartner, the average cost of IT downtime is $5,600 per minute. Because there are so many differences in how businesses operate, downtime, at the low end, can be as much as $140,000 per hour, $300,000 per hour on average, and as much as $540,000 per hour at the higher end.
98% of organizations say a single hour of downtime costs over $100,000. 81% of respondents indicated that 60 minutes of downtime costs their business over $300,000. 33% of those enterprises reported that one hour of downtime costs their firms $1-5 million.

https://www.the20.com/blog/the-cost-of-it-downtime/

セキュリティ障害時のコスト

Colonial Pipeline Company

Darkside
約4.8億円支払い

Revil/Sobinokibi
約81億円支払い

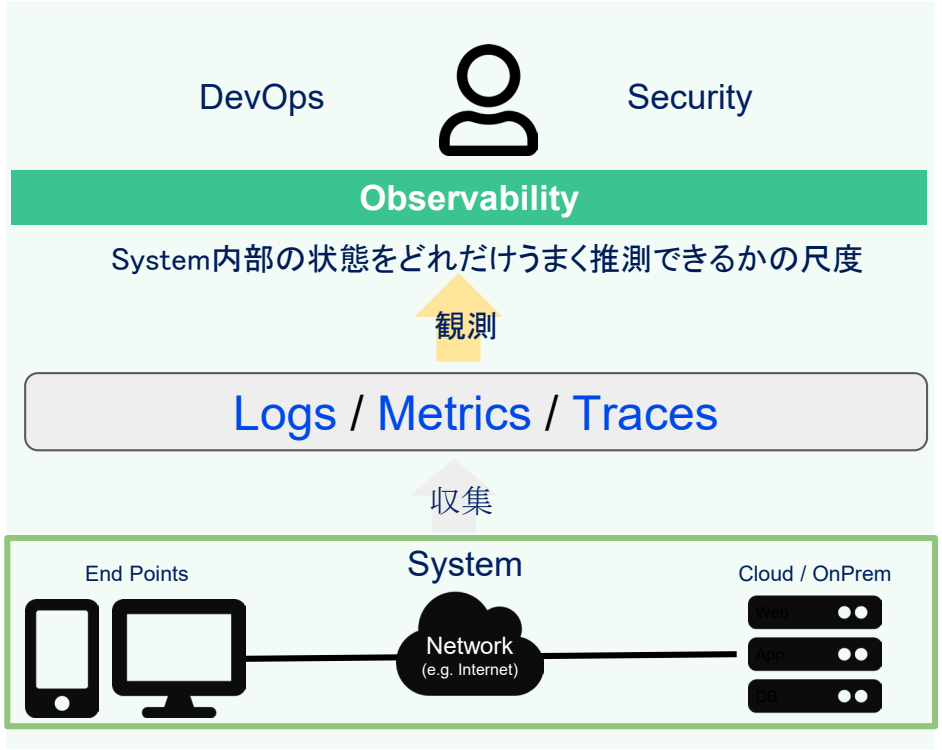
NetWalker
約1.2億円の支払い

sopra steria CONSULTING

Ryuk
約55億円支払い

Observabilityの主要データ

Observability（可観測性）を向上させる際に重要となるデータソースが、Logs / Metrics / Tracesの3つのデータ。



Log

Eventデータとも呼ばれ、人間が読むことが可能なテキスト形式のデータ
利用例：Uberの様なアプリケーションの場合、ユーザー向けに発生した不具合。システムの場合OSへのログインなど全般。

その時、何かが起きたのかを観測

Metrics

時系列毎にその時々の状態を表現する数値形式のデータ
利用例：Uberの様なアプリケーションの場合、地域毎の配車リクエスト数、ドライバー数。システムの場合: CPU使用率など。

時系列での遷移を観測

Trace

主にアプリケーション側での処理時間の内訳をツリー構造表で表す、「スパン」と呼ばれる特別なデータ。
利用例：Uberの様なアプリケーションの場合、Mapなどの3rdパーティアプリとの API連携が遅いかという様な原因やボトルネック解析

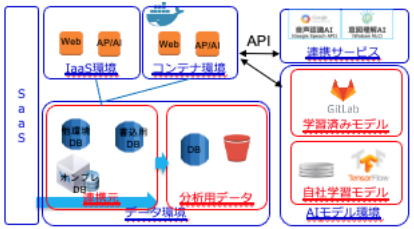
経路上の処理の観測

Observabilityのユースケース

分散化複雑化したシステム環境において、正確な状態の観測は様々な場面で不可欠。

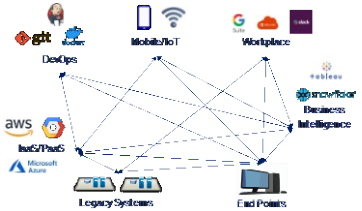
システム運用

旧来のオンプレミス環境から、コンテナ環境などが様々なクラウドに分散するハイブリッドクラウド環境における運用



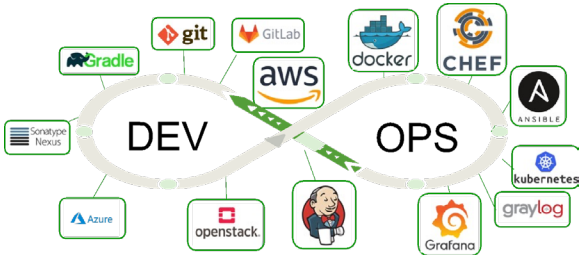
セキュリティ

SaaSを含めたマルチクラウド環境のセキュリティリスクを確実に把握する脅威の検出及び証拠保全



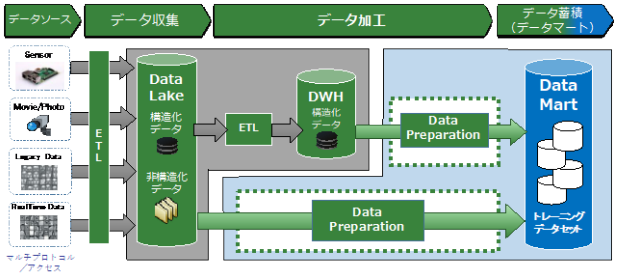
アプリ開発

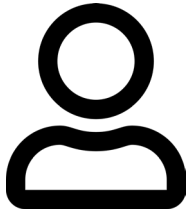
アプリケーションの絶え間ないアップデートの中で、リリース影響を常に観測し、UX等の状況を把握



データ活用

様々なデータソースから収集されるデータの異常値、欠損、鮮度、障害ポイントなどを常に観測し、正しい予測分析を実行



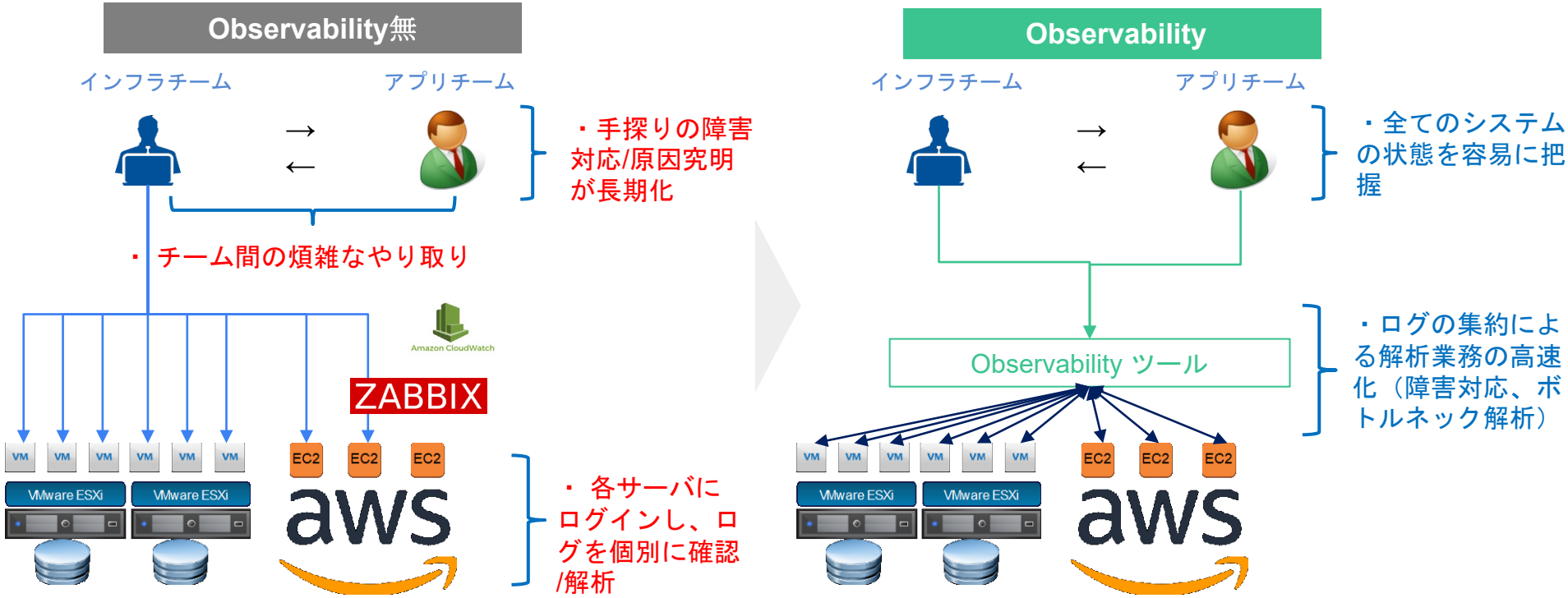


システム運用

セキュリティ

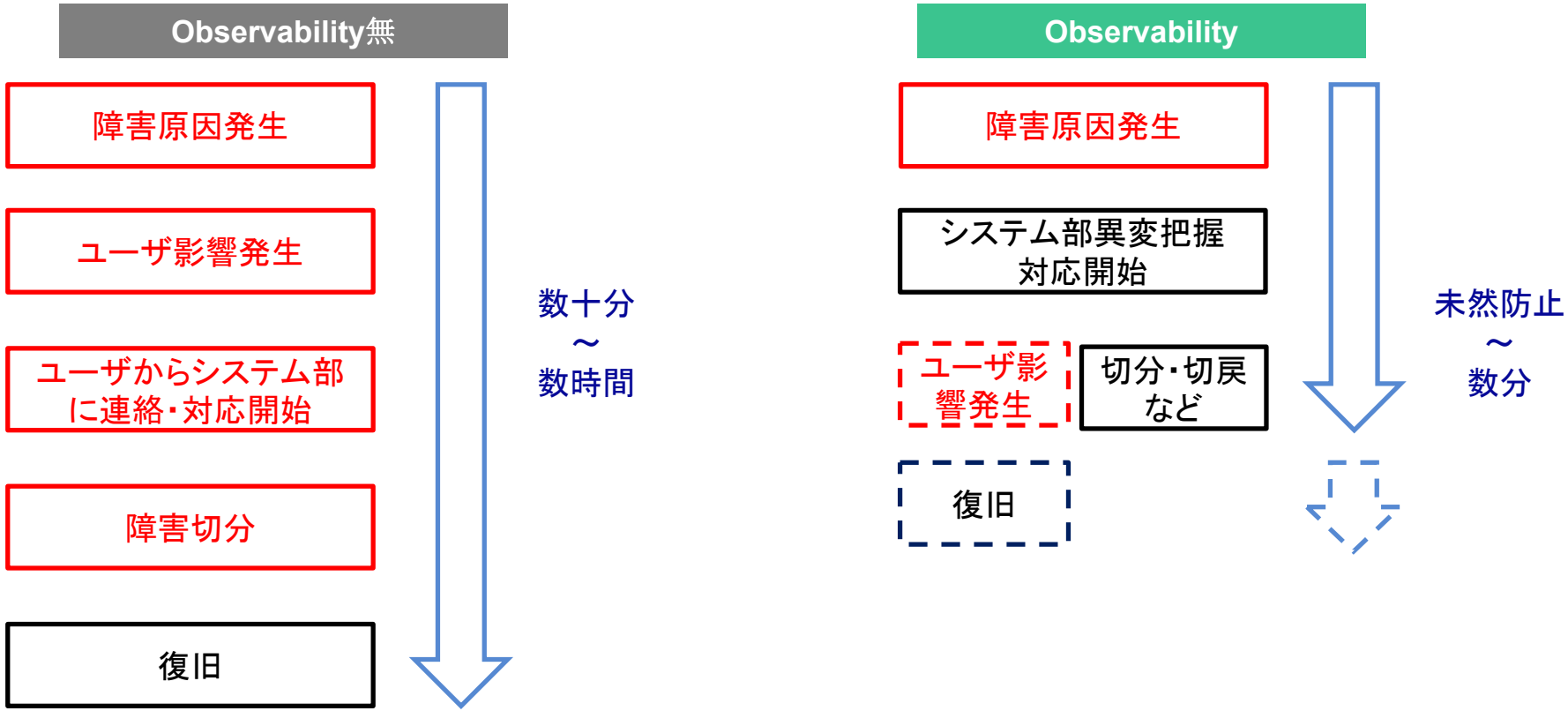
システム運用現場での活用例

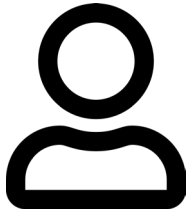
Observabilityツールを導入することで、運用負荷や障害復旧時間の短縮などが可能。



システム運用で起きる変化

Observabilityを導入することで、運用負荷や障害復旧時間の短縮などが可能。



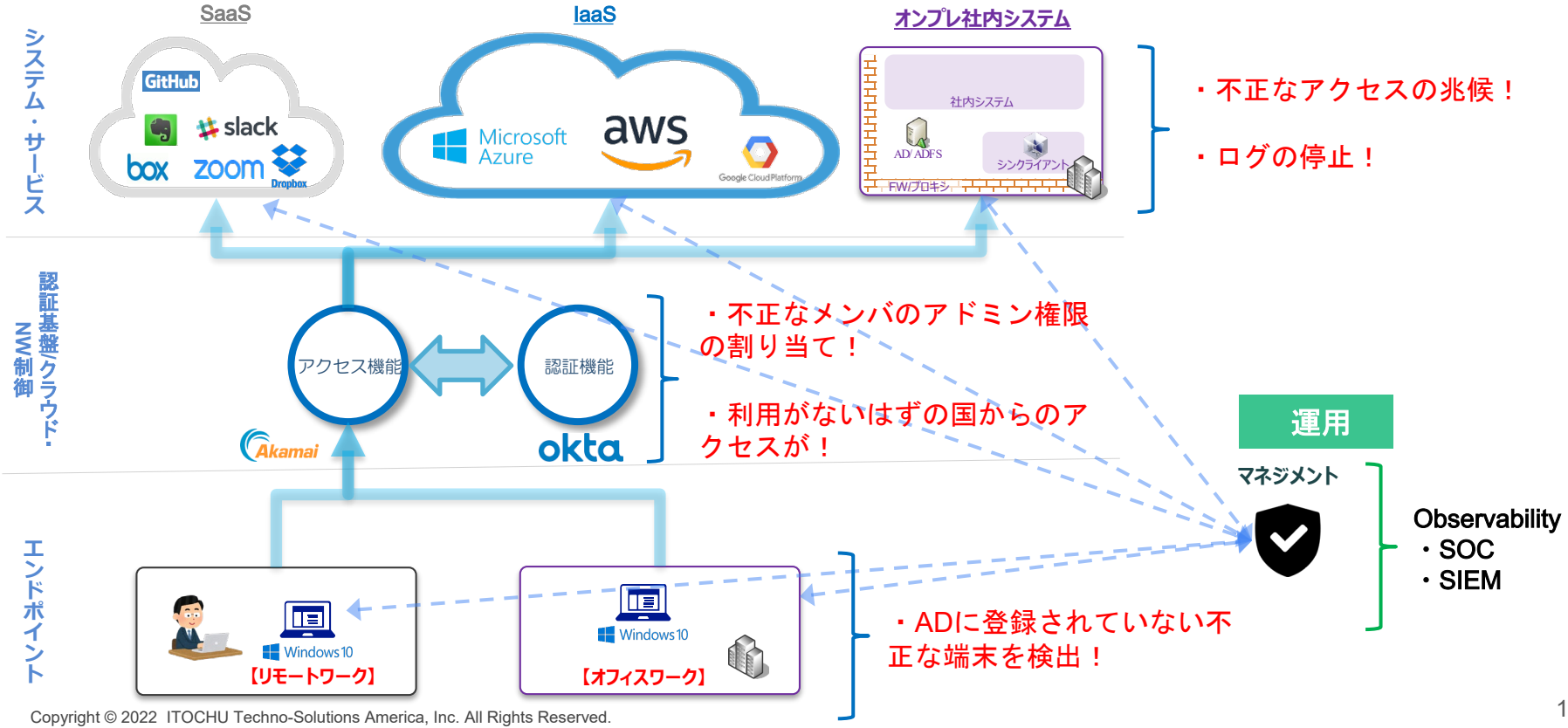


システム運用

セキュリティ

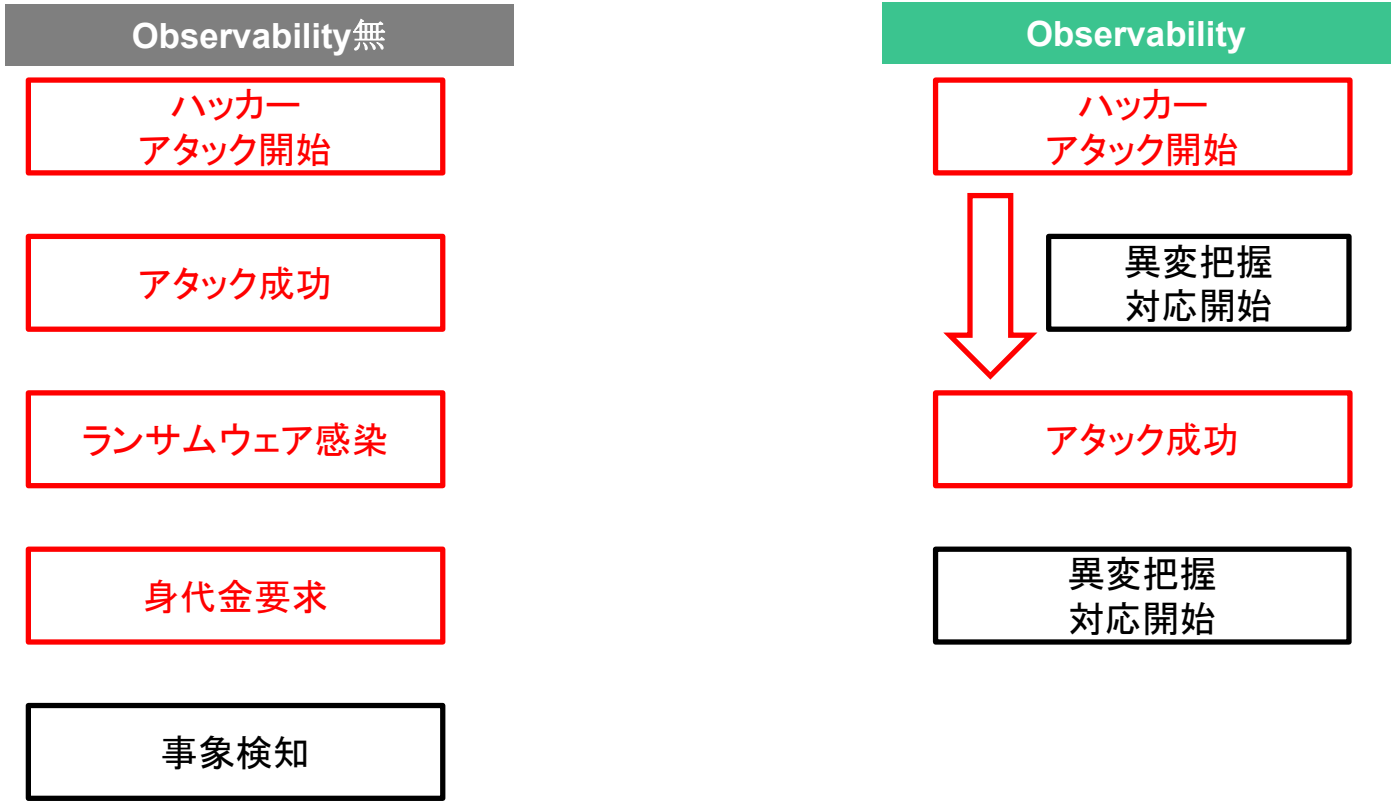
セキュリティ運用での活用例

各コンポーネントに対する不正アクセスなどの検知は Observabilityツールが必須。



セキュリティ運用で起きる変化

各コンポーネントに対する不正アクセスなどの検知は Observabilityツールが必須。



Coralogixの会社概要

独自技術「STREAMA©」を軸にMetrics/Logマネジメント、SIEMをSaas提供する企業。
Saas/FinTech企業や、LufthansaやAdobeなどの大企業も利用。

2015 設立	**2K+** 顧客	**10** Fortune 100顧客	**3M+** イベント数/秒
STREAMA© プラットフォームの 中核技術	**$238M+** 調達	**9.8/10** G2評価	**500K+** アプリでの利用実績

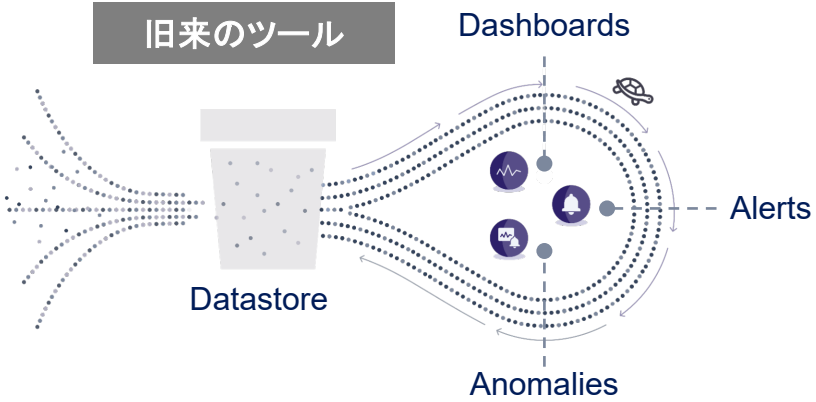
Ariel Assaraf, CEO
イスラエルのセキュリティ精鋭部隊8200出身。その後、Verintでプロダクト開発。

Matt Handler, COO & Pres
Whitehat (NTTが買収), LogLogic, Sumo Logicなど歴任。

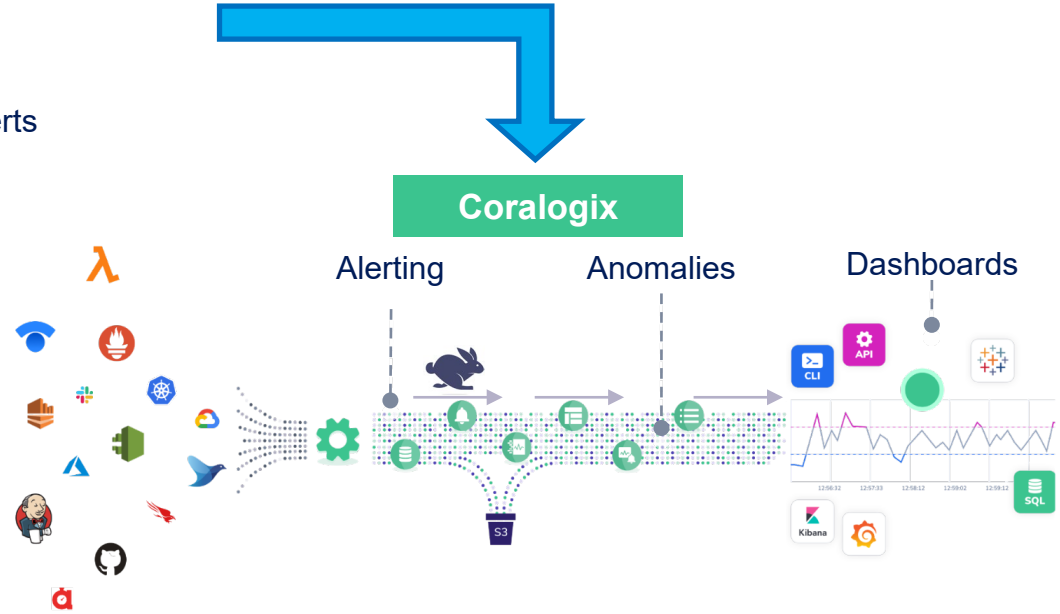
Yoni Farin, CTO
VerintとMotorolaのリードエンジニアリンググループ出身。

従来のツールとの違い

従来のツールと異なり、データをストアする前に分析を可能なテクノロジーを開発。
アラートや異常検知などを高速、安価に実現。



・高いコスト
・データ量の制御や欠損
・活用されないデータ
・長い処理時間
・手動で設定するアラート



Coralogixのメリット

旧来のプロダクトと比べて、以下のメリットをユーザに提供。

旧来のプロダクト

- 全てのデータをINDEX作成して保存 – コスト高
  高い保管コストと過剰なデータ保管量
- INDEX後のデータ分析 – 時間のかかる分析
  リアクティブ, 手動アラート; 長時間の障害調査と復旧
  (MTTI/MTTRの長期化)
- 予測不可能なデータストリームへの課題 – クラウド
  不適閾値超過時のデータの欠落やロスト
- レガシーワークフローに最適化 – DevOps非対応
  CI/CDパイプラインとの不適合
- 製品独自の検索言語を使用 – ベンダ依存
  ベンダーロックインや有識者への依存

最新のObservability

コスト効果

- INDEX作成データの選択
  全データの保管と70%の保管コスト削減の両立

直感性・即時性

- MLベースのリアルタイムなデータ分析
  プロアクティブな監視; 短時間の障害調査と復旧
  (短いMTTI/MTTR)

オートスケール

- お客様環境に応じたオートスケール
  データの欠落やロストの発生を回避

CI/CDへの対応

- クラウドネイティブ時代に必須なCI/CD対応
  プロアクティブな監視によるフィードバックループ構築

オープンソース活用

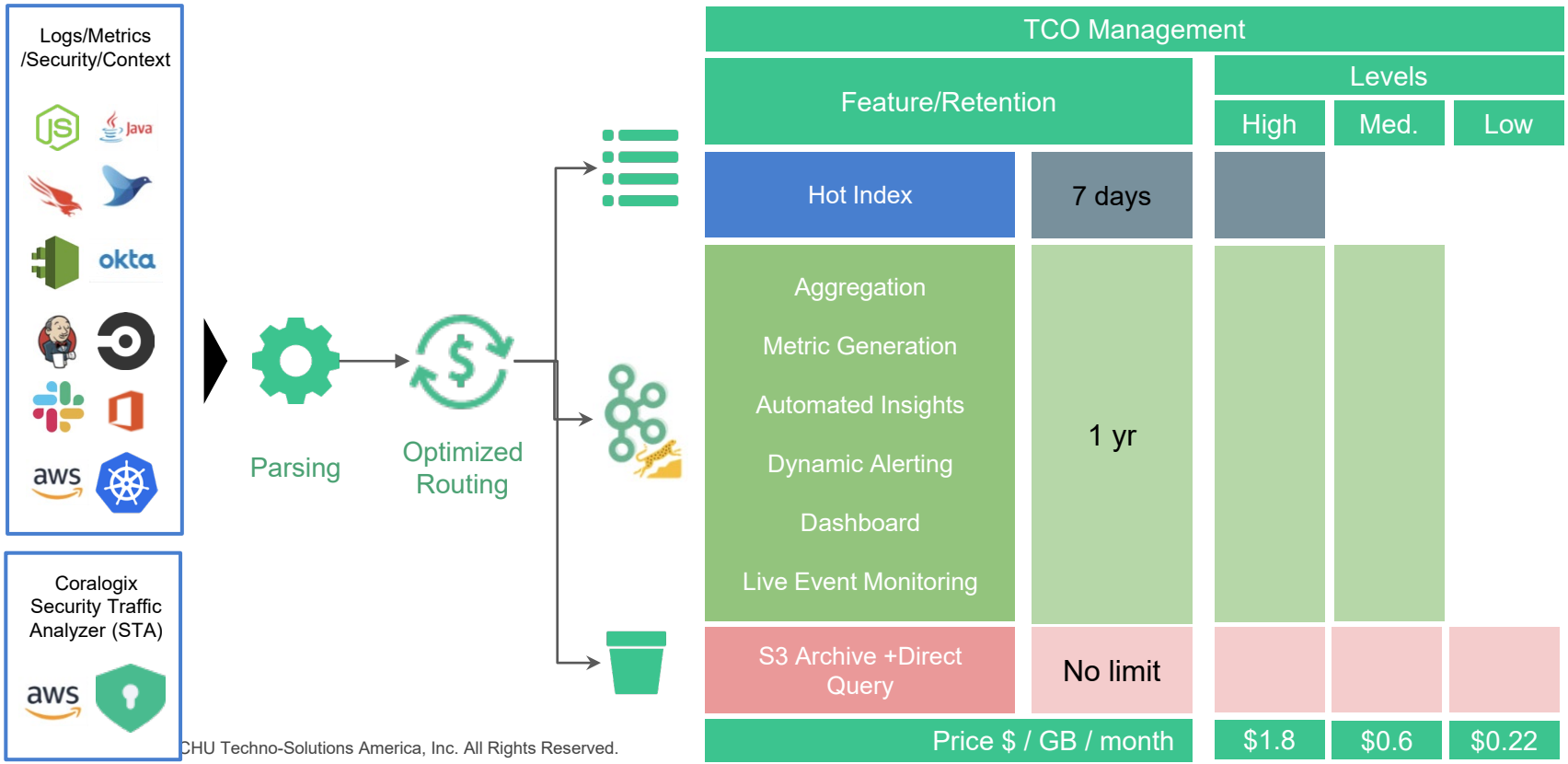
- オープンソースで普及する構文の利用も可能
  ベンダロックインなし, 特定プロダクト有識者も不要

→本日は「安い！」・「うまい！」・「早い！」部分をご紹介

安い！

データの重要性に応じた課金

分析対象、アーカイブ用などデータの利用用途に応じ、単価の異なる取り扱い・保存方式を選択可能。



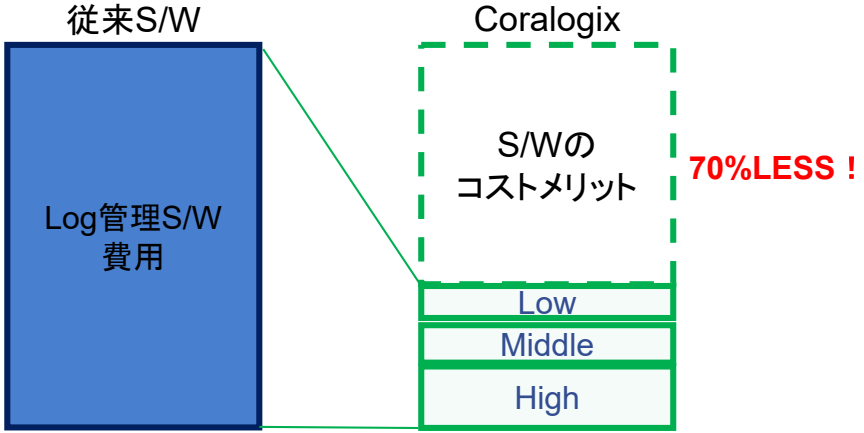
安い！

従来の選択肢とのコスト比較

“STREAMA©”によるコスト削減効果とSaaSにより不要となるコストの相乗効果でコスト抑制を実現。

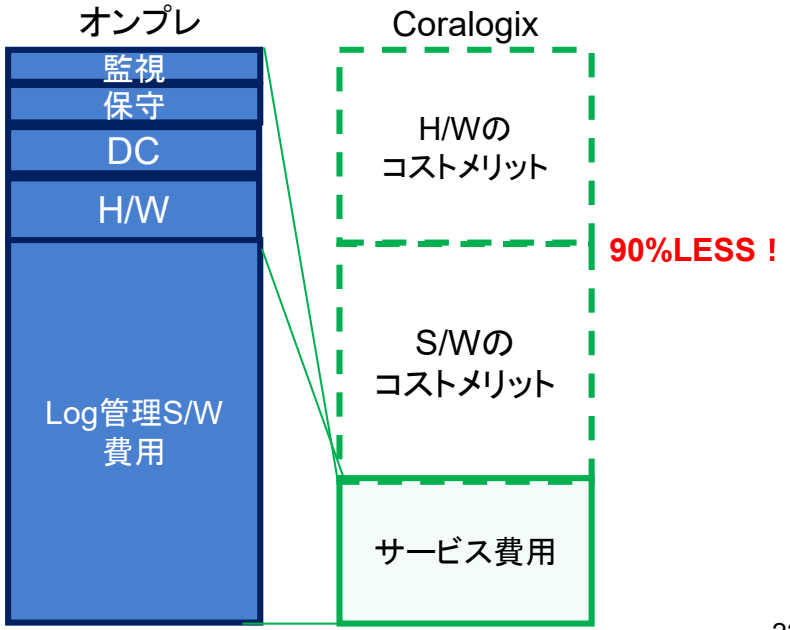
＜S/W比較＞

従来S/Wは全てのデータにIndexを付与する必要があり、不要なデータにもコストが発生していた。
Coralogixは重要性に応じた振り分けが可能かつ、容量単価も安価に設定。



＜H/W比較＞

SaaSであるため、H/W関連コストが不要。



うまい！

優れた操作性

マウス操作による直感的なLog管理を実現し、誰にでもLog運用が可能。
また、Query発行自体もデファクトOSS構文で可能。

＜Coralogixの操作感＞

＜Coralogixのコマンド例＞

使用するQueryの例		
Category	Type	Query
match	full-text	"search better"
multi-match	full-text	key1: "search" key2: "better"
match_phrase	full-text	search better
match_phrase_prefix	full-text	search better
term	term	tasty
exists	term	exists:{ "field":"name" }
range	term	age:{ "gte": 20, "lte":30 }
. . .	. . .	. . .

引用https://coralogix.com/blog/42-elasticsearch-query-examples-hands-on-tutorial/

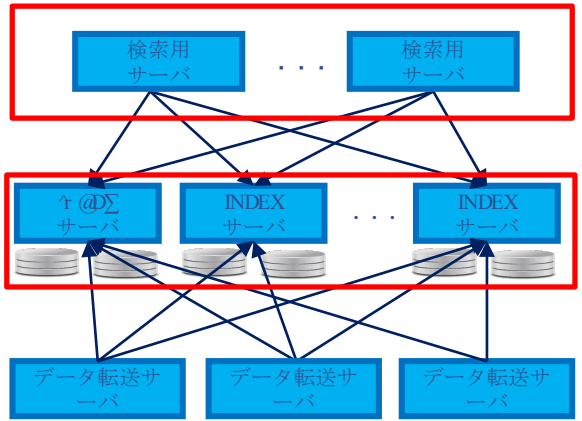
うまい！

障害対応をサポートする豊富な機能

障害対応に必要な様々な機能が用意されており、障害影響が発生する前のプロアクティブな対応や、
迅速な障害解析が可能。

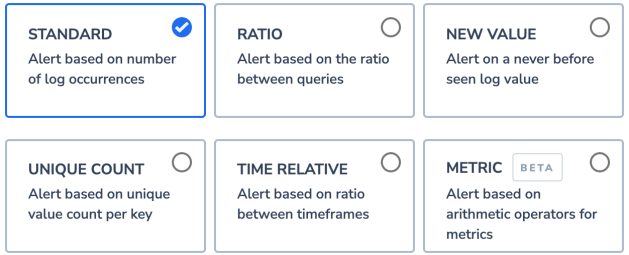
＜リソース不足からの解放＞

CPU不足やディスク不足により、アドホックな
サーチやスケジュールサーチが実行不可となる状況
を回避



＜先進的なアラート＞

一般的なキーワードによる検知だけでなく、新たに出現したログをトリガーとしたアラートや、比率を組み込んだアラートの発報などが可能



＜プリセットテンプレート＞

利用中のサービスに対応したプリセットのアラートやダッシュボードがあり、影響発生前の対応が可能

早い！

迅速な検知

ストアをせずに検知することにより、旧来のプロダクトと比較して検知スピードが向上。

旧来のツール

数分

Coralogix

数秒

対象システム

aws

ログ転送

Observabitly

Coralogix

インシデント管理

Opsgenie

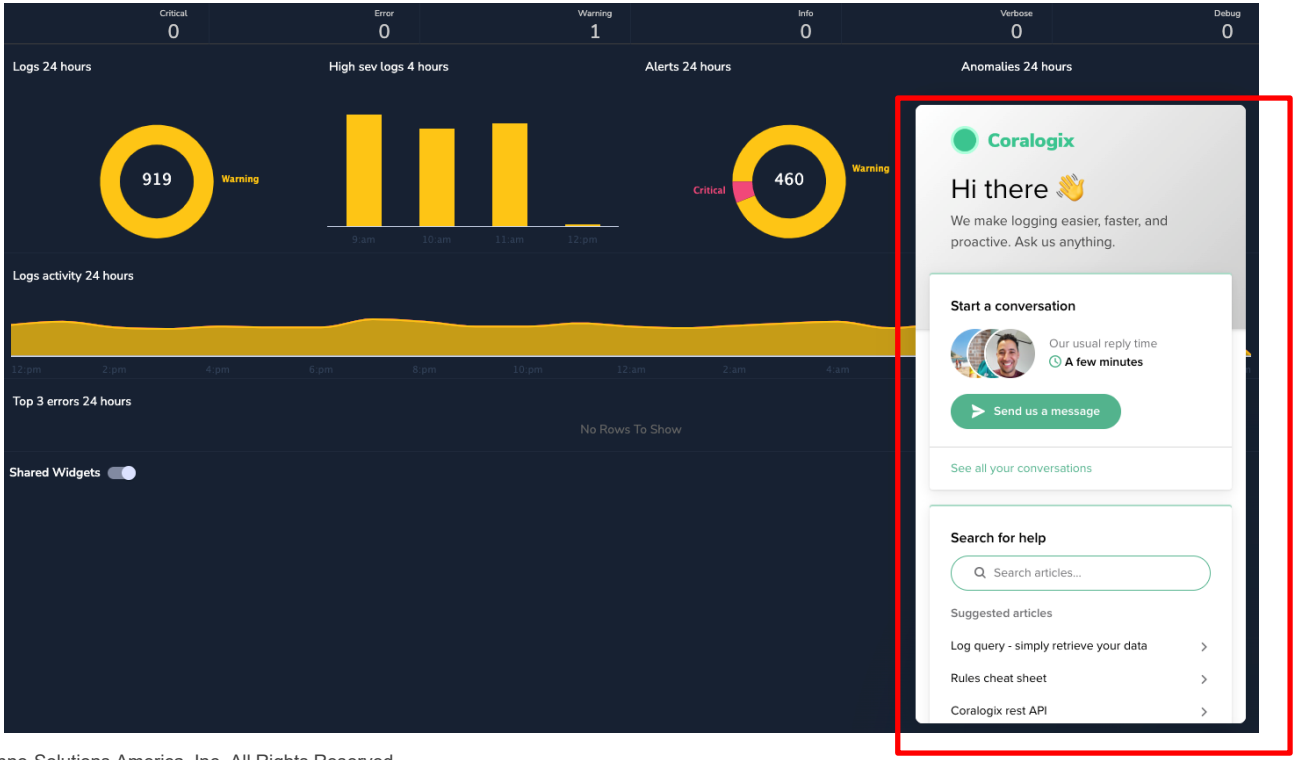
メッセージ

Microsoft Teams

早い！

即時のサポート対応

標準でチャットサポートが提供され、即時のQAが24/365で可能。



導入事例


SONY


VARONIS


Lufthansa


Adobe


Disney+


NICE


moovit


BIOCATCH
Less Friction. Less Fraud.


yotpo.


Capgemini


bookmyshow


monday


Payoneer


fiverr


PayU


ARMIS

導入事例–システム運用–

AGS (American Gaming Systems)

カジノゲーム会社

3倍
ユーザ数
増加率

4.5/5
アプリの
評価

70%
MTTD/MTTR
削減

99%+
エラー比率の
低減

課題:

- 何百万ものログから原因の特定に時間がかかる
- 障害による停止が即座に収益に直結

Coralogixによる改善:

- 何百万のログをMLを活用した集約機能により数十に分類
- MLを活用したアラート機能により異常検知
- 直感的なインターフェースにより、ログ調査時間を50%削減
- エラーログを99%、障害検知・復旧時間を70%削減

導入事例–セキュリティ–

SYSCOM GLOBAL SOLUTIONS

SYSCOM GLOBAL SOLUTIONS INC.

SIer/IT Solution Provider

99%+
エラー比率の
低減

70%
MTTD/MTTR
削減

課題:

- タイムリーな自社のFirewallのログ分析、アラートの検知を実施していなかった。
- 障害による停止が即座にお客様へのユーザー影響に直結する。

Coralogixによる改善:

- 自社Firewallのログ収集、ログ分析、タイムリーなアラート検知が可能となった。
- 直感的なインターフェースにより、ログ調査時間を50%削減
- エラーログを99%、障害検知・復旧時間の大幅な削減

Q & A

Zoom画面下のQAボタンをクリックして、
質問をご記入ください。

Presented by: ITOCHU Techno-Solutions AMERICA

SYSCOM GLOBAL SOLUTIONS