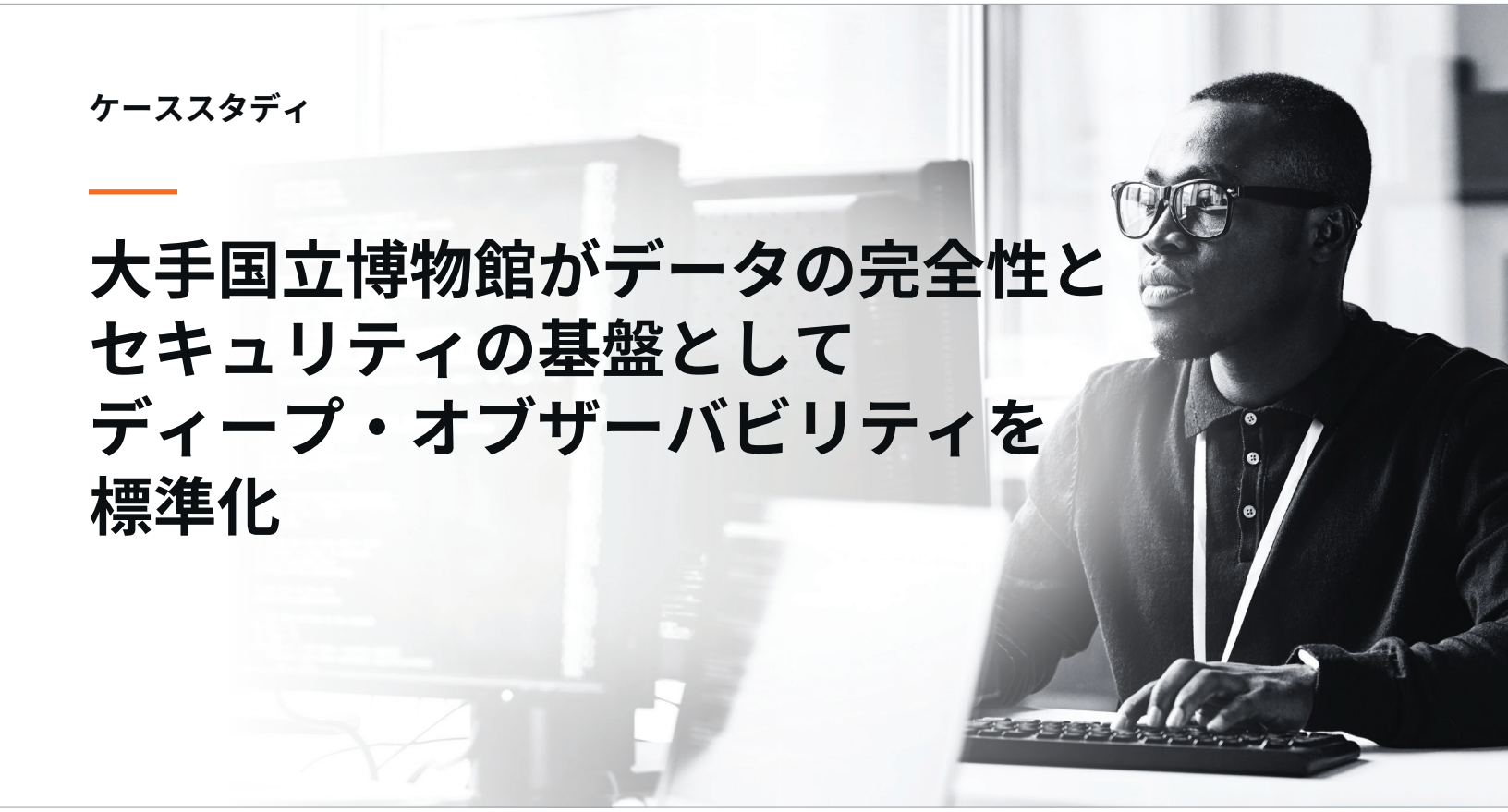
ケーススタディ

大手国立博物館がデータの完全性とセキュリティの基盤としてディープ・オブザーバビリティを標準化



Precryptionテクノロジーにより、Gigamonはセキュリティ業界の10年先を行っています。このテクノロジーは、これまで隠されていた脅威活動を極めて効率的な方法で検出するもので、モノリシックなファイアウォールアーキテクチャや複雑な復号化標準から、パフォーマンスを損なうことなく、当社のサーバーが処理を行う効率的な分散モデルへとシフトすることを可能にします。

MICHAEL TROFI氏
Trofi Security創業者兼CISO

課題

- ハイブリッド・クラウド・インフラ全体におけるディープ・オブザーバリティの欠如
- 悪意のある脅威アクターや国家を後ろ盾とする脅威アクターからの絶え間ない攻撃
- 大量のノイズ、イベントログの誤検出、重複トラフィック

ソリューション

- GigaVUE® Cloud Suite for AWS
- GigaVUE HCシリーズ
- GigaVUE-FM

顧客のメリット

- 改善されたEast-Westトラフィックのオブザーバビリティ
- AWSのネットワーク検知・対応（NDR）システムに流入するトラフィック量を削減
- ノイズを消去された無駄のないデータ
- 同じデータセットを使う既存のツールと簡単に統合し、整合性と予測可能性を高める

Mike Trofi氏による本事例研究で表明された見解は、必ずしも米国ホロコースト記念博物館の公式見解を反映するものではありません。

お客様について

世界中の大量虐殺の残虐行為に関する、7ペタバイトを超える機密性の高い単一ソースの歴史的遺物を保護する任務を担う米国ホロコースト記念博物館は、極めて重要な役割を果たしています。ホロコーストの生きた記念碑としての役割を果たし、世界中の市民や指導者たちに、憎悪に立ち向かい、大量虐殺を防止し、人間の尊厳を促進するよう鼓舞しています。連邦政府の支援により、博物館はワシントンD.C.のナショナル・モールに恒久的な場所を確保しており、その広範な教育プログラムと世界的な影響は、多くの寄付者によって実現されています。

Michael Trofi氏は、ほぼ10年にわたって同館のCISOを務め、貴重なアーカイブの保護を担っています。このプロジェクトで、Trofi氏はGigamonと提携しました。Mike Trofi氏による本事例研究で表明された見解は、必ずしも米国ホロコースト記念博物館の公式見解を反映するものではありません。同氏の会社であるTrofi Securityは、コロラド州ラファイエットに本社を置き、バーチャルCISOおよびセキュリティ・オペレーション・センター（SOC）サービスを提供しています。Trofi氏は、さまざまな業界にまたがる情報技術とサイバーセキュリティの分野で40年以上の経験を持っています。人員確保が継続的な課題となっている中、同氏は人工知能（AI）や機械学習（ML）技術をいち早く導入しており、攻撃を未然に防ぎ、日常的なサイバーセキュリティ業務を自動化し、チームをより効果的に活用するために積極的に取り組んでいます。

経営課題

この博物館は、機密性の高い歴史データを保護するだけでなく、中国におけるウイグル人の扱いなど、現在の残虐行為についても米国国務省に報告しています。このため、博物館はしばしば、世界中の複数の経路から敵対的な攻撃の標的にされます。同時に、博物館にはデータを広く利用可能にするという使命があり、パブリック・クラウドへの移行を加速させている最中ですが、この移行にはセキュリティ面での課題が山積しています。クラウドを活用し、拠点でデータを複製することで、博物館は自身の教育サービスへの世界中からのアクセスを向上させることができます。Trofi氏は、同館のデータは約5年以内にほぼ完全にハイブリッド・クラウドに移行し、オンサイトのデータセンターのフットプリントは最小限に抑えられると見込んでいます。

これまでTrofi氏と彼のチームは、ファイアウォールとポイント・ツー・ポイントVPNを使って顧客のデータを保護してきましたが、Trofi氏は何かが足りないと感じていました。新しいハイブリッドワークフォースモデルでは、VPNはもはやリモート接続の最適なソリューションではなく、セキュリティ境界を拡張するためにはSASE（セキュアアクセスサービスエッジ）ソリューションへの移行が必須です。さらに重要なこととして、Trofi氏はメトリクス、イベント、システムログ、トレースが「答えではない」とも指摘しています。各アプリケーションには独自のデータセットがあり、それらが必ずしも一致しないからです。ノイズや重複トラフィックを処理するのに多くの時間を要し、誤検出も多く見られました。データの整合性の欠如は、Amazon Web Services（AWS）にセキュリティ製品を効果的に供給するチームの能力に悪影響を与えていました。

何が足りなかったのでしょう？それはディープ・オブザーバビリティです。Trofi氏は、次のような質問に答えられるよう、North-SouthトラフィックとEast-Westトラフィックへのより良いオブザーバビリティを求めていました：データはどこへ行くのか？受取人は誰か？それは正当な受取人なのか？彼が指摘するもう1つの問題は、AWSのセキュリティに内在する限界です。AWSがイベントのみを監視し、トラフィックフローを監視しないことです。

「監視対象をトラフィックフローに拡大することは大きなメリットです」と彼は述べています。「パケット、パケット、パケット。パケットは嘘をつきません。ログは重要ではあるが、すべてを語っているわけではありません。ですからパケットレベルまで下りていく必要があったのです。」そこでGigamonの出番となりました。Gigamonは、脅威アクティビティを示している可能性のあるトラフィックの異常を、素早く表面化する能力を備えています。

解決

GigaVUE Cloud Suite™ for AWSが導入され、Trofi氏とそのチームに、博物館のAWS環境に対する強力なオブザーバビリティを提供しました。Gigamonの重複排除とFlow Mapping™機能は、博物館のNDRシステムに向かうトラフィックフローの量を劇的に減らし、質を向上させました。

無駄を排除しノイズを消去されたデータセットにより、チームはセキュリティ・ツールを効果的に統合できるようになりました。「以前は本当にノイズが多かったのです。トラフィックをクリーンにして実際に見えるようにし、ノイズを取り除いたのは大きな進歩でした」とTrofi氏は述べました。

トラフィックを傍受し、集約させ、重複を排除するGigamonの卓越した能力のおかげで、博物館は現在、Fortinet、Check Point、Armis、Forescout Technologiesを含むすべてのセキュリティ・ソリューションの基盤としてGigamonを使用しています。Trofi氏は、Gigamonが博物館に提供しているデータの完全性が最大のメリットだと断言します：「Gigamonは、私たちのすべてのシステムに供給される真実の単一ソースとして機能しています。」

データの完全性が改善されたおかげで、チームはルーティンタスクを自動化できるようになりました。データセットが競合し合う状態では決して実現できなかったことです。「Gigamonのオブザーバビリティにより、私たちはAIと機械学習を活用できるようになりました」とTrofi氏は言います。

新しいクラウドツールとAIツールを使えば、多くのありふれた仕事が自動化され、真に熟練した人材が「本当の問題を追求できる」ようになると彼は指摘します。たとえば、チームの現在の大きなプロジェクトのひとつは、暗号化されていないトラフィックをすべて排除することです。昔のようにログを使用しているだけなら、何年もかかっただろう、とTrofi氏は指摘します。「Gigamonは私たちにとって天の恵みであり、私たちが持つすべてのセキュリティ・ソリューションの基盤です」と同氏は述べます。

Trofi氏は、暗号化されたハイブリッド・クラウド・ネットワークへの移行が、新たな懸念をもたらすことを認めています。「クラウドへの依存度が高まる中、暗号化された通信を検査できるようにすることは、博物館とその資産を脅威アクターから安全かつセキュアに保つ上できわめて重要です。」と同氏は指摘しています。この懸念に対処するため、同氏はGigamon Precryption™テクノロジーを使って、ペイロードが暗号化される前にすべての暗号化された通信を平文で可視化することを模索しています。Trofi氏はこう述べています。「Gigamonは、Precryptionテクノロジーによって、セキュリティ業界の10年先を行っています。これまで隠されていた脅威アクティビティを非常に効率的な方法で検出するテクノロジーのおかげで、モノリシックなファイアウォールアーキテクチャや複雑な復号化標準から、パフォーマンスを損なうことなく、当社のサーバーが処理を行う効率的な分散モデルへとシフトすることができます。Gigamon Precryptionは、セキュリティ業界全体にとって有益であり、クラウドに業務を移行しようとする組織が綿密に評価すべきテクノロジーです。」

メリット

Gigamonは、博物館のセキュリティ体制を改善するだけでなく、ネットワーク・パフォーマンスも改善しました。トラフィックの流れを可視化することで、Gigamonは、ネットワーク・オペレーション・チームがそこに存在すべきでない不正なトラフィックを排除することを可能にしました。「それは、私たちにとってまったく新しい世界を生み出します。私たちは、オブザーバビリティを通じて、ネットワークを『トラフィック形成』することができます。これは20年前には本当に難しかったことです。オブザーバビリティのおかげで容易になったのです」とTrofi氏は主張します。「アプリケーションがどのようにアクセスされるかを可視化してで分析することで、ファイアウォールを通過する経路を最適化することができます。つまり、オブザーバビリティによって、セキュリティの問題だけでなくパフォーマンスの問題にも対処しているのです。そして、それは今後に向けて大きなメリットとなります。」

同氏のチームは、有効な経路が何であるかを知っているので、すべてを敵視する必要はなく、ユーザーにより良い体験を提供できます。Trofi氏は、オブザーバビリティの向上には、さまざまなIT部門が協力的に働くようになるというメリットもあり、それは業界全体にとって一歩前進であると指摘しています。

Gigamon について

Gigamonは、ネットワーク由来の実用的なインテリジェンスを活用し、オブザーバビリティ・ツールを強化するディープ・オブザーバビリティ・パイプラインを提供しています。この強力なコンビネーションを活用すれば IT 組織は、セキュリティとコンプライアンスのガバナンスを維持しながら、パフォーマンスのボトルネックとなる根本原因をすばやく分析し、ハイブリッドおよびマルチクラウドの IT インフラストラクチャ管理に伴う運用コストを削減できます。その結果、現代の企業の完全なクラウド変革を実現できます。Gigamon は世界中で 4,000 社以上の顧客にサービスを提供しています。これには Fortune 100 企業の 80% 以上、10 大モバイルネットワークプロバイダーのうち 9 社、世界中の何百もの政府および教育機関が含まれます。詳しくは、gigamon.comをご覧ください。

Gigamon®

本社
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com