Recorded Future®

ケース
スタディ

# 沖縄科学技術大学院大学
# セキュリティインテリジェンスを活用して教育の卓越性を保護

沖縄県にキャンパスを構える沖縄科学技術大学院大学（OIST）は、教育と研究の優れたモデルとして、世界中の学界で急速に認知度を高めています。

**ユースケース**

- セキュリティ情報 / イベント管理（SIEM）のアラートのトリアージと脅威の検出

**課題**

- リソースの制約と外部の脅威データへのアクセスの制限により、セキュリティ上の盲点が生じている

**ソリューション**

- セキュリティインテリジェンスを IBM® QRadar® Security Information and Event Management（SIEM）に統合

**成果**

- セキュリティ監視の精度と運用効率が 3 ～ 4 倍向上
- QRadar® のオフェンスの誤検出を 25% 低減

## 攻撃者にとって価値の高い高等教育機関

大学は、貴重な研究から重要な医療情報まで、大量の機密データを保持しています。セキュリティ侵害が発生すると、1 つの機関にとどまらず、広範囲に深刻な影響をもたらしかねません。

OIST の最高情報セキュリティ責任者、永瀬啓太氏は「私の主な目標の 1 つは、研究員に柔軟な IT 環境を提供しながら、脅威をリアルタイムで検出して対応することです」と言います。「効果的なセキュリティシステムとスピード、この 2 つを同時に追求することが優先課題です」

永瀬氏のチームは、IBM® QRadar® SIEM システムを利用して、脆弱性管理、ペネトレーションテスト、侵入検知システム、およびその他のツールからなる大学のセキュリティスタック全体のセキュリティイベントのログを検出および関連付けしていましたが、大学を標的にする可能性のある脅威についての外部コンテキストの可視性が欠如していました。

「SIEM で大量のセキュリティイベントが発生していて、どれが重大なリスクを示しているのか判断するのが困難でした」と永瀬氏は振り返ります。**「内部のチームには、関連のある脅威すべてを収集して分析するためのリソースや専門知識がありません。私たちの課題は、脅威検出機能を改善し、高い精度で脅威に優先順位を付けることでした」**

> “Recorded Future のセキュリティインテリジェンスは、今では私たちのセキュリティ運用に不可欠なものになっています。セキュリティ監視の分析の品質を向上させ、情報共有を支援し、インシデントレスポンスのためのインテリジェンスのリポジトリとして機能しています”
>
> 最高情報セキュリティ責任者
> 永瀬啓太氏

Photo: OIST/Kenji Togo

## リアルタイムのセキュリティインテリジェンスで自動化を促進し、リソース制約のバランスを維持

永瀬氏は、Recorded Future の印象と選択した理由について、次のように述べています。
「Recorded Future の機能のなかでも、SIEM のデータのエンリッチメント機能と、クローズドソースやダーク Web のフォーラムにアクセスできることに興味を持ちました」
「しかし、最終的には、情報の品質と高度な自動化機能が決め手となり、マネージドセキュリティ運用サービスではなく Recorded Future のプラットフォームを選びました」

Recorded Future のセキュリティインテリジェンスプラットフォームは、分析と人間の専門知識を組み合わせることで、オープンソース、ダーク Web、技術的なソース、独自の調査からなる、他に類を見ない多様なソースを統合します。QRadar とのシームレスな連携により、OIST のチームは次のことが可能になります。

- QRadar のオフェンスを外部の脅威データと関連付けて強化し、判別にかかる時間を大幅に短縮
- 関連付けのルールに Recorded Future のインテリジェンスを使用し、脅威をプロアクティブにブロック
- IP、ドメイン、ハッシュ、脆弱性のデータをオンデマンドでエンリッチメントし、脅威ハンティング機能を強化
- プロセスを自動化してワークフローを効率化し、チームの効率と自信を向上

## 包括的な可視化、運用の効率化、エグゼクティブレベルのサポート

「Recorded Future のセキュリティインテリジェンスは、今では私たちのセキュリティ運用に不可欠なものになっています。セキュリティ監視の分析の品質を向上させ、情報共有を支援し、インシデントレスポンスのためのインテリジェンスのリポジトリとして機能しています」と永瀬氏は述べています。

> “Recorded Future が提供するさまざまなレポートと、サイバー脅威の詳細情報や分析を活用し、脅威インテリジェンスを実用的なものにできるようになりました。この能力には関係者も感銘を受けています”
>
> 最高情報セキュリティ責任者
> 永瀬啓太氏

また、「以前はツールとリソースの制限によりアクセスできなかった外部の幅広い脅威ソースにも、アクセスできるようになりました。インテリジェンスを既存の IBM® QRadar® のシステムとワークフローに統合し、分析を自動化することで、セキュリティ監視の精度と運用効率が 3 ～ 4 倍向上したと確信しています」とも述べています。

この成果には大学の首脳部も注目しています。「Recorded Future が提供するさまざまなレポートと、サイバー脅威の詳細情報や分析を活用し、脅威インテリジェンスを実用的なものにできるようになりました。この能力には関係者も感銘を受けています」これらのインサイトをもとに、永瀬氏とチームは、同様の攻撃が業界にもたらす影響について報告し、大学がサイバー犯罪者の標的になる可能性を示すダーク Web の傾向を挙げ、確信を持って迅速に攻撃者に対抗することができます。