CSA Japan Summit 2019

クラウド時代に向けて変化するセキュリティ対策・運用

SecureWorks Japan 株式会社
代表取締役　グローバルセキュリティ・エヴァンジェリスト
ジェフ・モルツ

SecureWorks Japan株式会社
山崎景太

May 15, 2019

Classification: //Secureworks/Confidential - Limited External Distribution:

本日の内容

前半：クラウド時代に向けて変化するセキュリティ対策・運用

- セキュアワークスご紹介
- セキュアワークスのサービスポートフォリオ
- クラウドセキュリティ運用の課題
- セキュアワークスのクラウド向けセキュリティサービス

後半：クラウドインシデント対応　Blue＆RedTeamの経験から

- ✓ 後半セッションの資料は非公開となります。
- ✓ また、写真とスライドのＷｅｂ公開ＮＧでお願いいたします。

Classification: //Secureworks/Confidential - Limited External Distribution:

Secureworks ご紹介

インテリジェンス主導のセキュリティ サービス & ソリューション

Counter Threat Unit™ リサーチチーム

- 脅威の兆候を捉える
- 迅速に対応策を講じる

現在の SOC 設置場所

- アトランタ, ジョージア州, 米国
- シカゴ, イリノイ州, 米国
- プロビデンス, ロードアイランド州, 米国
- エジンバラ, スコットランド, 英国
- 川崎市, 日本

- 24時間365日/年中無休
- 三交代のシフトで日本で24時間監視

2,900億
日々処理するサイバーイベント数

4,300+
社のお客様

53
カ国に展開

1,000+
昨年実施したインシデント対応数

2,400+
毎年実施するコンサルティングサービス契約数

2,600
の従業員

独自のカウンタースレッド・プラットフォームを活用
“Counter Threat Platform™”

Classification: //Secureworks/Confidential - Limited External Distribution:

Secureworks のサービス概要

セキュリティ オペレーション & インテリジェンス	セキュリティ、リスク & コンプライアンス ソリューション	セキュリティ テスト	ネットワーク & エンドポイント ソリューション	データ & アプリケーション ソリューション	インシデント対応 & 管理	クラウド セキュリティ ソリューション
SOC 向け アドバイザリ	セキュリティ アドバイス	コンプライアンス・テスト	セキュリティ監視	脆弱性マネジメント	事前の準備 CSIRP	クラウド環境 セキュリティ コンサルティング
世界規模のスレット・インテリジェンスの可視化 / インサイト	フレームワーク毎のリスク・アセスメント	侵入テスト	エンドポイントの脅威検知	脆弱性対応の優先順位付け	緊急のインシデント対応	脆弱性マネジメント（クラウド）
高度なリサーチ・エキスパートの助言	セキュリティ アーキテクチャ評価	実際の攻撃をシュミレーションしたレッドチーム・テスト	標的型攻撃マルウェアからの保護	モバイル、 Web/API アプリの評価	エンドポイント フォレンジック 環境整備	クラウド環境の緊急インシデンド対応
高度な標的型攻撃インテリジェンス / インサイト	全方位のコンプライアンス対応				標的型攻撃ハンティング	

■ セキュリティ・コンサルティング　■ マネージド・セキュリティ　■ インシデント対応 &管理　■ 脅威インテリジェンス

//Secureworks/Confidential - Limited External Distribution
© 2020 Secureworks, Inc.
Classification: //Secureworks/Confidential - Limited External Distribution:

サービスポートフォリオの拡充

クラウド向けセキュリティ戦略＆計画策定
クラウド向け脆弱性診断

仮想ファイアウォール監視
仮想WAF監視
Elastic Server Groups監視
仮想iSensor IPS管理

パブリッククラウド環境における緊急
インシデント対応サービス

クラウドにフォーカス

GRC/SRC
(Governance Security & Risk Consulting)

セキュリティ＆リスク
コンサルティングサービス

MSS
(Managed Security Services)

マネージド
セキュリティサービス

TI
(Threat Intelligence)

セキュリティ上の
脅威情報提供サービス

IMR
(Incident Management Retainer)

インシデント管理対応
サービス

エンドポイントにフォーカス

Red Team Testing
シナリオベース ペネトレーション

AETD Red Cloak
(エンドポイントセキュリティ監視)
CrowdStrike等エンドポイント
3rd Party製品の監視

Target Threat Hunting
標的型攻撃ハンティング
サービス

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウドサービスにおける利用者側の主な課題

- 乱立するクラウドサービス（無法地帯）の利用
- 「責任共有モデル」における利用者側の責任範囲
- 可視化の必要性
- インシデント対応

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウドサービス向けセキュリティ・サービス・ポートフォリオ

セキュリティ対策状況を知る	事故・事件の発生に気付く	事故・事件に対応する

現状把握

- ✓クラウドサービス利用計画策定 &アセスメント
- ✓クラウドサービス評価
- ✓サーバ診断
- ✓Webアプリケーション診断

セキュリティ監視

aws
- ✓仮想ファイアウォール監視
- ✓仮想WAF監視
- ✓Elastic Server Groups監視

Office 365
- ✓Exchange監視
- ✓SharePoint監視
- ✓Azure AD監視

Azure
- ✓仮想ファイアウォール監視
- ✓仮想WAF監視
- ✓Security Center Alert監視

フォレンジック

aws

Azure

Office 365

Cloud Platform-非依存

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウド監視

For Multiple Clouds

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

Microsoft Partner

- ✓SecureWorksのSOCが24時間365日、対象クラウド環境を監視し、不審な兆候を早期検知
- ✓早期検知によりインシデント対応を迅速化

aws

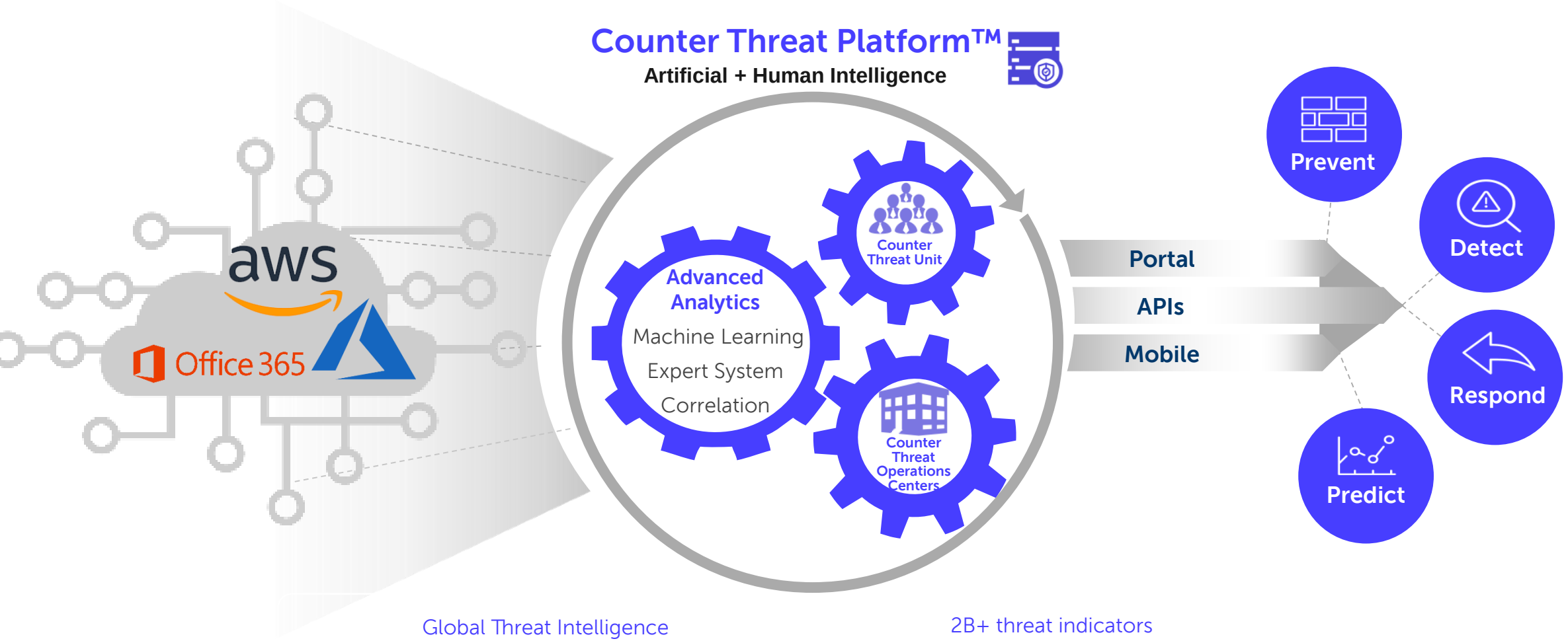
Office 365

Azure

Classification: //Secureworks/Confidential - Limited External Distribution:

インシデント管理システムの一元化

オンプレミス環境及びクラウド環境の不審な活動を独自プラットフォームにて一元的に解析



Global Threat Intelligence

16+ years of attack & threat actor group data

2B+ threat indicators

Applied intelligence based on industry/business

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウド監視

For Amazon Web Services

Leverages AWS標準サービスの監視

CloudWatch Logs

OS and Application Logs

CloudTrail

Record of all API calls

VPC Flow Logs

Record of network connection activity

EC2/Server

Logical Device

AWS上のサードパーティ製品をサポート

Firewall

WAF

お客様からのコメント

"*SecureWorks is a partner we trust to keep our AWS cloud infrastructure secure as we evolve and expand our banking customer base and ensure valuable financial data is protected.*"

-- Banking Sector, Senior Vice President of IT

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウド監視

For the Microsoft Cloud

Office 365

Microsoft Partner

Office 365環境のログを解析することにより、不審な活動を早期に検知、迅速に通知します。

Azure Active Directory

SharePoint

Exchange

検知パターン例

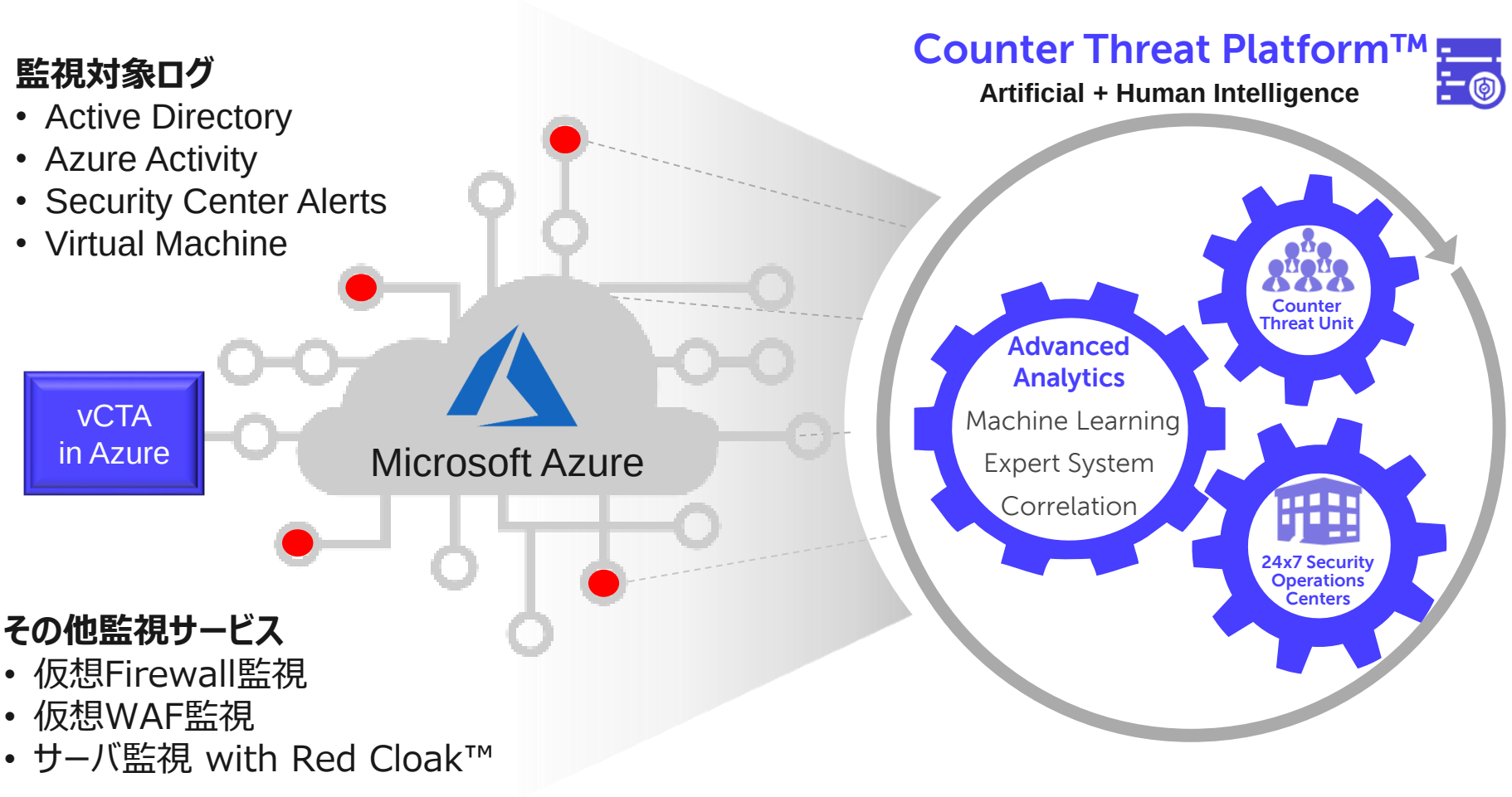
- ログインの失敗
- 異なる国からのログイン
- ユーザの追加／削除
- その他、閾値による検知

Classification: //Secureworks/Confidential - Limited External Distribution:

クラウド監視 for Azure

Azure上の監視対象ログ、その他アプリケーションのログを24時間365日監視し、不審な挙動を検知・通知します。

監視対象ログ
- Active Directory
- Azure Activity
- Security Center Alerts
- Virtual Machine



検知パターン例
- 異常なサインイン
- 特定設定の変更
- パーミッションの変更
- ライセンスの変更
- 特定ユーザ/グループへの操作
- パスワードの変更
- 閾値ベースのアラート
- ストレージアカウントへの操作

その他監視サービス
- 仮想Firewall監視
- 仮想WAF監視
- サーバ監視 with Red Cloak™

Classification: //Secureworks/Confidential - Limited External Distribution:

CSA Japan Summit 2019

クラウドインシデント対応
Blue＆RedTeamの経験から

Secureworks

SecureWorks Japan株式会社
山崎景太

2019/5/15

Classification: //Secureworks/Confidential - Limited External Distribution:

途中、スライド非公開につきご容赦ください

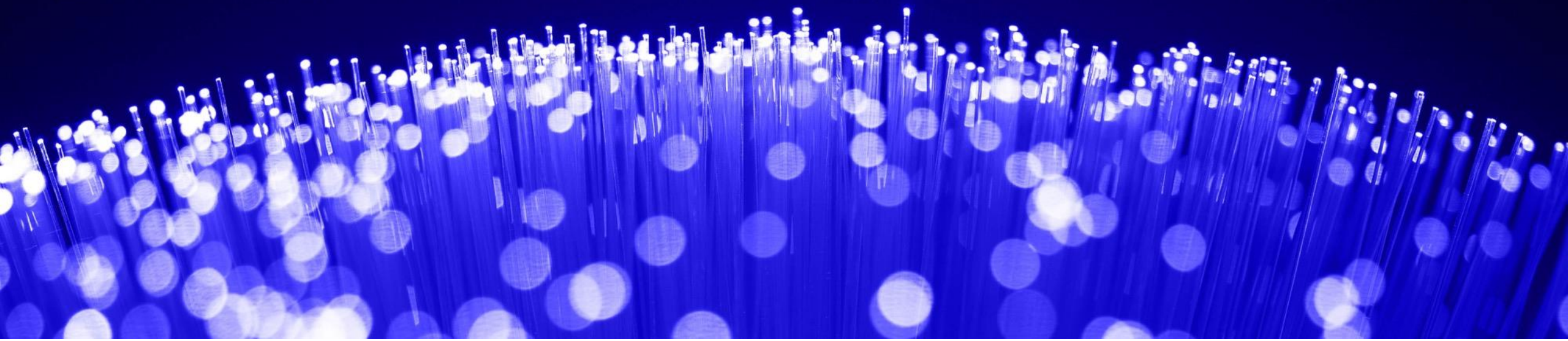
Classification: //Secureworks/Confidential - Limited External Distribution:

ご清聴有難うございました

ご質問、ご要望は下記にお願いいたします

SCWX_PreSales@secureworks.com

TEL 03-6893-2317



Classification: //Secureworks/Confidential - Limited External Distribution:

Classification: //Secureworks/Confidential - Limited External Distribution: