D3 SECURITY

SOAR
(Security Orchestration, Automation, and Response)
これからの進化する「IT/OT」セキュリティ運用の自動化に！

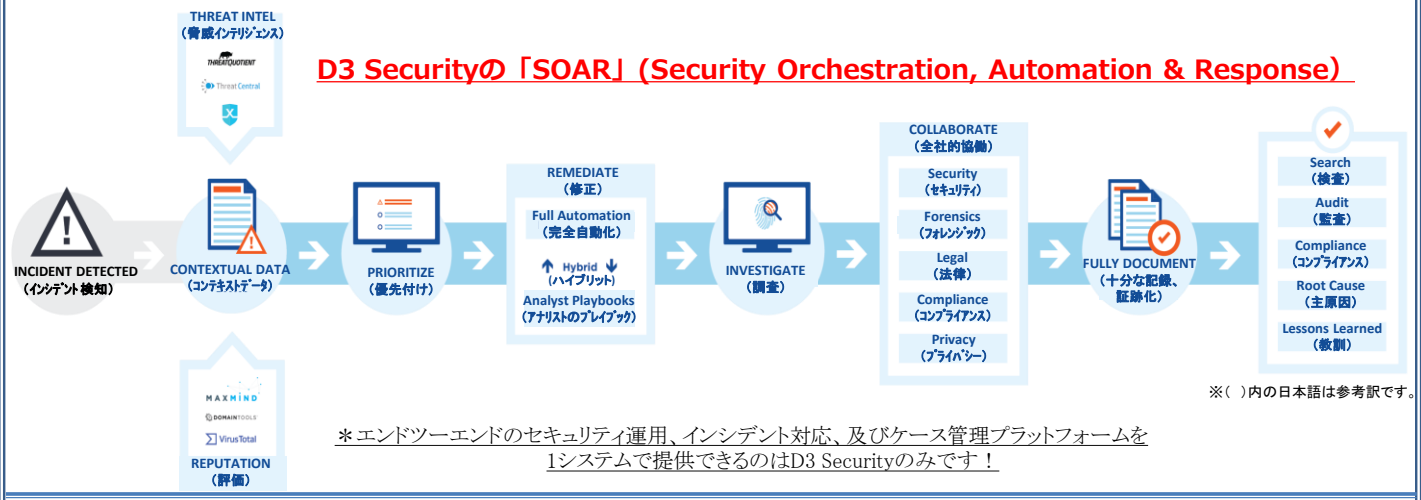
IT/ OT

既にFortune500社で100社以上の実績を誇る「D3 Security」は世界で最も先進的なセキュリティ運用の基盤です！
部門間のコラボレーションを円滑にし、管理、人的及び機械的プロセスの調整や、組織が業界の要件や
コンプライアンス報告基準を確実に満たすために取られた全ての行動を文書化します！

主な導入メリット

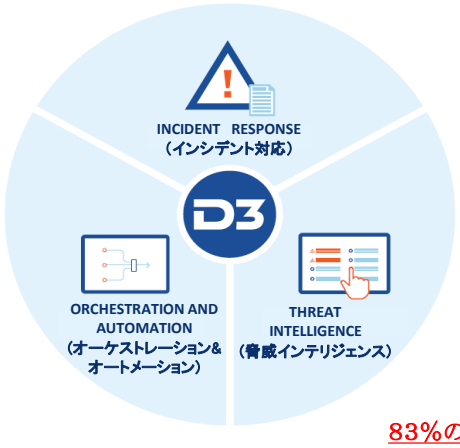
- そのまま使えるプレイブックはNIST（National Institute of Standards and Technology； アメリカ国立標準技術研究所）などの業界基準に従うユーザ独自のインシデントレスポンス/トリアージプロトコルを実装するための強力なテンプレートを提供！
- 人手やスキルに依らないセキュリティの自動化運用を可能に－ 圧倒的な人件費の削減！
- SIEMを含むあらゆるセキュリティ機器の世界レベル統合インシデント監視・管理システム。各セキュリティベンダーとの調整やインシデントレポーティングの効率化！

D3 Securityの「SOAR」(Security Orchestration, Automation & Response)



※( )内の日本語は参考訳です。

＊エンドツーエンドのセキュリティ運用、インシデント対応、及びケース管理プラットフォームを1システムで提供できるのはD3 Securityのみです！



既に100+ のオーケストレーション実績

- **インシデントレスポンス**：インタラクティブフォームがユーザーの入力をキャプチャし、IRプレイブックを通じてアナリストをガイド
- **オーケストレーション**：API /スクリプトを使用して様々なセキュリティソリューションに接続
- **自動化：**日常業務を自動化するためのアプレット(スクリプト)
- **ダッシュボードとレポーティング**：分析、レポーティング、レビューのために取り込まれたメトリクス

83%のセキュリティ対策コスト削減例

CYBERSECURITY BREAKTHROUGH AWARDS 2018

D3 Security が2018年にサイバーセキュリティ自動化ソリューションのトップベンダーに！

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。Rev A

サイバープラットフォーム（D3システムにおける技術的機能と特長）

●インシデント・レスポンス・モジュール

D3 Securityプラットフォームは、インシデント・レスポンス/ケース管理プランの構築及びオーケストレーションを行い、サードパーティのテクノロジーと連携し、インシデント、調査、及びリスクの企業規模のビジョンにわたってデータ主導型決定を適用するためのハブを提供します。

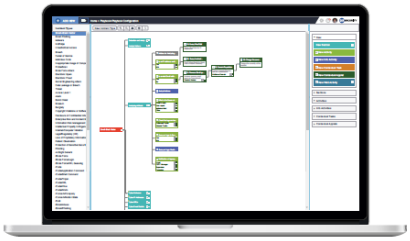
このテクノロジーは、全てのセキュリティツールによって最初から最後までフィルタリングされるイベントを管理するためのバックボーンとしての役割を果たし、プロセスエンジン、全ての脅威調査のためのSoR(system of record: システム・オブ・レコード(記録のためのシステム))として機能します。

SOCチームへのインシデント/脅威情報のスムーズな配信を促進する

インシデント報告 は、設定可能なフォーム、通知、許可、ワークフロープロセスの柔軟なフレームワークを利用して各部署のインシデント管理のニーズや優先順位に直接応える、世界レベルのインシデント・レスポンス管理プラットフォームです。

主な特長

・すぐに使えるNIST/SANS基準ベースのプレイブック
・あらゆる種類のインシデントに関する各社のポリシーや手順に対する完全な設定を実現するアクションの追加/削除を可能にするビジュアル・プレイブック・エディタ
・アナリストにインシデント・ライフサイクル全体を説明する、ガイダンスを利用した容易なDecision Tree(決定木)構造
・インシデントの容易なロギングや追跡を可能にする、フォーム、通知の設定可能なフレームワーク
・SOC通信を改善するための高度な通知設定
・ベストプラクティスについて助言し、現行のSOC運用を改善する、専任CISSP役
・きめ細かいアクセス制御や監査証跡
・システム内の全てのアクションの時刻/日付スタンプの追跡
・インシデント・レベル・セキュア・メッセージング機能を有するコラボレーション機能
・SaaS,又はオンプレミスの展開オプション
・機械学習をベースとした、インシデントのフォールスポジティブ分類



統合可能なセキュリティツールの一部

splunk> / Symantec. / cisco / McAfee by Intel / JUNIPER NETWORKS / IBM Radar / Office 365 / G Suite / paloalto / Exchange / CYLANCE / lastline / FireEye / Carbon Black. / IMPERVA INCAPSULA / CYPHORT / RSA / Cisco Umbrella / TANIUM / VECTRA / MICRO FOCUS / Jira Software / Active Directory / TREND MICRO / BLUE COAT / VirusTotal

●セキュリティ・オートメーション/オーケストレーション・モジュール

SOC効率を改善するセキュリティ・タスクの完全、又は部分的なオートメーションを利用する

オートメーション・モジュールにより、アナリストは、全てのインシデント・データを集中させ、相関させることができます。
SIEM、AV、ファイアウォール、脅威インテリジェンスなどと統合することにより、プロセスを改善し、非常に時間がかかる手動作業を排除するマシン・オートメーションを効率的に使用することができるので、アナリストは、リアクティブではないプロアクティブなセキュリティ・タスクに集中することができます。

主な特長

・セキュリティ・プロセスの部分的な要素、又は完全な要素の何れかに関する複数のプレイブックのオーケストレーション
・Pythonスクリプトでカスタムスクリプトを作成し、プロセスを自動化することが可能
・完全マシンベースのオートメーション、及び多数のアクション
 - プロセスの「強制終了」、「IPをブロック」、「修復、スキャンを実行」、「マシンを隔離」、「ユーザをブロック」する、等
・脅威インテリジェンス管理、及び自動データエンリッチメント
・AVソリューション及び/又はゲートウェイソリューションと統合する、自動化された修復機能
・一定の前提条件が満たされるまでの、自動化されたアクションの待ち状態(Wait State)遅延
・レスポンスを決定するための閾値して使用することができる、ワークフロー内のアクションのリスクスコアを決定するための高度な基準の重み付け
・低TCOを提供するシステム内での無制限のアクション

セキュリティツールの統合

・オートメーションを迅速に実現する、事前に書かれた300個のPythonスクリプトのライブラリ
・追加設定なしで、数百のセキュリティツールと統合
・SIEMに依存しない統合
・容易なカスタム統合を促進する、柔軟なAPIカスタマイズ

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。Rev A

●高度なアナリティクス

重要なSOCメトリックを追跡し、改善部分を特定し、サイバーリスクを明確に把握する。
D3 Securityを用いれば、システム内の事実上、如何なるフィールドについても報告することができるので、管理者は、効果的な意思決定を推進するサマリー報告や、メトリックベースの報告によって、セキュリティ運用を監督することができます。報告は、手動で作成、もしくは、閾値、スケジュール、期限に基づいてD3Securityのオートメーション機能によって管理することができます。

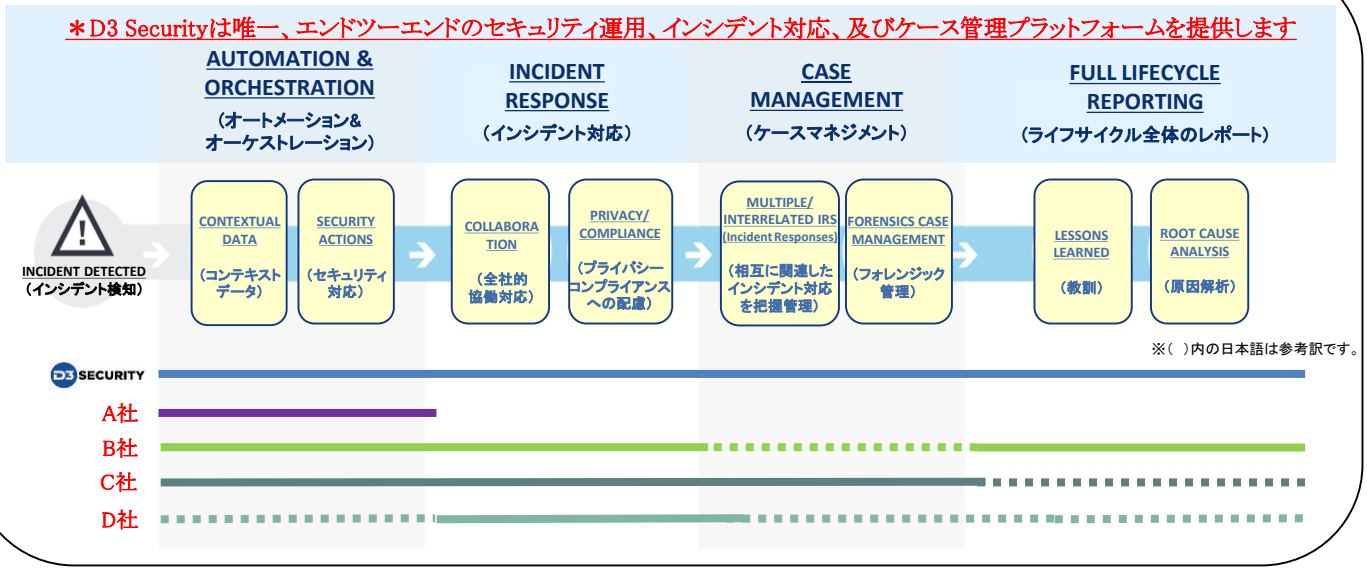
追跡できる報告のタイプ

・インシデントタイプ
・アナリストの有効性
・アナリストの作業負荷
・インシデント解決時間 - 対応するまでの時間/修復するまでの時間
・監査、eディスカバリ、コンプライアンスを目的とした報告

eアラート

従業員による容易なサイバー・セキュリティ・インシデントの報告。
このモジュールにより、企業の従業員、パートナー、又はサードパーティは、ウェブポータルを介して直接D3Securityシステムに情報を容易に送信することができます。この機能は、多くの書面フォームを排除し、インシデント・レスポンス・プラットフォームへのデータの取り込みを加速させることができます。
一般的なeアラートフォームは、下記についての容易な報告を可能にします
・紛失や盗まれたデバイス
・フィッシングメール
・詐欺

＊D3 Securityは唯一、エンドツーエンドのセキュリティ運用、インシデント対応、及びケース管理プラットフォームを提供します



Fortune 500
（実績の一部）

GOVERNMENT & PUBLIC
World Health Organization / NEW YORK CITY DOT / UKAD Protecting Sport / JFK / LGA

ENERGY & GAS
cenovus energy / ConocoPhillips / SCANA Power For Living / Sempra Energy / Anadarko Petroleum Corporation / HALLIBURTON / Exelon Enterprises / PPL / SNP

SOFTWARE & TECHNOLOGY
Seagate / Pinterest / amazon / SYNOPSYS / JUNIPER NETWORKS / Symantec. / AMD / UBER / Sprint / Tech Data

RETAIL & PROPERTY MANAGEMENT
TESCO / LOWE'S

MANUFACTURING
SPACEX / BOEING / Honeywell / FCA / Johnson Controls / HONDA / SAMSUNG / Continental / BAE SYSTEMS / GENERAL DYNAMICS / MONSANTO imagine

HEALTHCARE
UNIVERSITY OF MICHIGAN / Texas Children's Hospital / UPMC / SENTARA / MAYO CLINIC

MEDIA
News Corporation / VIACOM / NBC / FOX

BIOTECH & PHARAMACEUTICAL
Pfizer / gsk / MYLAN

EDUCATION
LAURIER Inspiring Lives / UNION COLLEGE / McMaster University / MEMORIAL UNIVERSITY / UNIVERSITY OF WATERLOO / TRINITY WESTERN UNIVERSITY / St. Lawrence College / UNIVERSITY OF THE FRASER VALLEY

TRANSPORT
ups / enterprise

FINANCE
Goldman Sachs / SallieMae / CoreLogic / mastercard / aetna / VISA / CapitalOne / Bank of America / Northwestern Mutual FINANCIAL NETWORK / THRIVENT FINANCIAL / WESTFIELD INSURANCE

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。Rev A

ケース管理モジュール

複雑なケースを調査し、協力し、コンプライアンスを維持する。
このモジュールは、相互に連結した複雑なものである可能性があるか、企業 に損害を与える組織的な取り組みの一部である、一連の関連インシデントの調査を可能にします。
これらのケースは、はるかに多くのリソースや手順を必要とする場合があり、全てに法律上/規制上の問題が伴います。ケースのタイプに基づいて、従業員は、解析を実施し、リマインダーを設定し、更なる証拠を追加し、助言を求め、システムの外部に直接ドキュメントを容易にエクスポートすることができます。

主な特長

・使い易いケース提出/ケース作成ポータル
・要件を満たすための設定可能な調査プロセス・テンプレート
・コンテキスト的な指示や段階ベースのワークフローを用いた、ガイド付き調査プロンプト
・エンティティを相関させて、パワフルな検索/フィルタリング/複製検出ツールセットにより調査プロセスを加速させるデータ・プロファイリング・エンジン
・物的証拠とデジタル証拠の両方のための証拠ロッカー
・明示的、且つ認証されたCOC(chain of custody:証拠の保全)追跡
・異なるデータ、ケース、人間の間の相関関係を評価する、自動化されたビジュアルリンク解析
・自動の法的報告/コンプライアンス報告
・サードパーティ、例えば、弁護士との間でのケース・コラボレーション・インポート/エクスポート機能
・自動のケース番号作成および書式設定

全社規模のセキュリティ運用の可視化

D3Securityは、施設、地域、ネットワークにまたがるインシデントを追跡して、繰り返し発生する脅威と攻撃者を識別できます。 詳細なトレンドレポートとパフォーマンスレポートは、重要な情報としてセキュリティチームや企業の役員に報告されます。

エネルギーと公益事業は、厳格なコンプライアンス要件と相まって、高額のセキュリティの脅威に直面しており、一貫性のある文書化されたプロセスが必要です。
D3 Securityはサイバー脅威、物理的脅威、リスクアセスメント、NERC CIPなどの規格への準拠状況にまたがる状況認識を可能にする一貫性のあるインシデント管理ソリューションで、エネルギー部門はD3 Securityに依存しています。

NISTベースのインシデントレスポンスプレイブック

公益事業などの重要なインフラストラクチャは、D3 Securityが地域の評議会や規制当局と共有するために、事前に構築されたプレイブックとメトリクス、及びレポートのライブラリでサポートするNISTフレームワークに従うことが必要です。

IT /OTや物理的な情報源を用いてセキュリティインシデントの修正

IT及びOTシステムをD3 Securityのインシデントレスポンスハブに接続して、サイバー及び物理的なセキュリティインシデントを集中管理します。

D3Security社（カナダ、バンクーバ、2004年設立）について

D3 Securityのオーケストレーション、自動化、対応、及びケース管理ソリューションは、**既にFortune 500の20%以上を含む、世界で最も先進的なセキュリティ運用の基盤になっています。**

D3 Securityは、セキュリティ運用センター内、及び部門間のコラボレーションを円滑にするだけでなく、管理、人的及び機械的プロセスの調整や組織が業界の要件やコンプライアンス報告基準を確実に満たすようにするために取られた全ての行動を文書化します。
詳細については、https://d3security.comをご覧ください。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。Rev A

SOAR
(Security Orchestration, Automation, and Response)

D3 SECURITY

進化するセキュリティ運用の自動化技術

SOAR-native SOC

● 1日目からSOARで始める理由

多くの人は、SOAR(セキュリティのオーケストレーション、オートメーション、レスポンス)プラットフォームはより成熟したSOC のためのものであると考えています。実際のところ、「SOAR-native SOC」を構築すること―1日目からSOARプラットフォームで新規のSOCを構築すること―は、ビジネスとロジスティックの両方の観点から見て道理にかなっています。

既に何らかの検出ツール(例えば、NIDS (Network-based Intrusion Detection System)、EDR Endpoint Detection and Response)、SIEM (Security Information and Event Management))、及びアドホックプロセスがあり、それらの要素を正式なSOCに変換している場合、今こそ、SOARプラットフォームの機能を活用して、限られたリソースや、ますます敵対的になる脅威環境を克服する方法を学ぶ最適な時期です。

● オーケストレーション

1. クイックスタート・プレイブック

アドホックプロセスがある場合、アドホックプロセスをSOARプラットフォーム内に構成して、一貫性を保つためにステップを標準化することができます。業界のベストプラクティスからのガイダンスを用いて既存のプロセスを自由に改善できる場合、そのまま使えるプレイブックは、NIST (National Institute of Standards and Technology; アメリカ国立標準技術研究所)などの業界基準に従うユーザ独自のインシデントレスポンス/トリアージプロトコルを実装するための強力なテンプレートを提供します。

● 自動化

2. 人間の専門知識を投入する&時間を最大限に生かす

新規のSOCでは、ユーザは既に複数の役割をこなしており、複数のツールやウィンドウの間でコピー＆ペーストするなどの操作で時間を失う余裕はありません。

十分に情報を得た上での意思決定を効率的に行うために、データ収集やデータ拡張を自動化し、適切な場合にのみ介入することによって、人間の経験と専門知識を必要とするタスクに時間を集中させます。

3. プロセスのドキュメンテーション&改善

ITセキュリティ運用における最大の課題の1つは、チームの知識を獲得し、保持し、取り出すことです。既存のプラクティスを、改善し続けるプレイブック、及びSOP(Standard Operating Procedure:標準作業手順書)に発展させるにつれて、SOARプラットフォームの自動履歴追跡は、手順やドキュメンテーションの品質、及び速度を改善することができます。

全ての試行、エラー、成功をログすることによって、各ステップを手作業で記録するために一時休止、又は後戻りする時間や手間、重要な詳細を忘れること、又は想定外のミスをすることを回避します。不要なステップを見直して除外することがより簡単なので、改善が体系的になります。

既に200を超えるセキュリティソリューションを統合

● レスポンス

4. 調査ケース管理

ITセキュリティ運用の中心的機能は、ログデータ、イベントアラート、インシデントなどを調査することです。
関連するイベント、インシデント、ケースは、複数の互換性のないシステムにわたって解析されるのではなく、一緒に解析されるべきです。
SOARプラットフォームに組み込まれる調査ケース管理システムは、常習者、疑わしい人物、脆弱性評価で見逃された標的にされた資産、その他の適用可能なエンティティの僅かな手掛かり、又は早期の指標を特定するのに役立つ有益な拡張であり、これらは全て、証拠価値のより強力なケースを作成するのに役立ちます。

5. セキュアで効率的なコラボレーション

SOCは、コラボレーションの必要に応じて閲覧されるか、又は隠される必要がある機密データを処理します。
きめの細かいロールベースのアクセス制御レベルを有するSOARプラットフォームは、全て同じシステム内で、チームが、職務権限にかかわらず、ケースに安全に協力し、適切なデータを適切な人と便利に共有するのに役立ちます。

6. 迅速なトレーニング&オンボーディング

SOCが大きくなり、新任のアナリストが参加した時、プロセスの完全性を損なったり、又はインシデントレスポンス時間の遅延なしに、新入社員を訓練する必要があります。
ガイド付きのプレイブックがあれば、SOARプラットフォームは、毎日24時間対応の指導者の役割を果たし、新任のアナリストにSOPをステップバイステップで説明することで、一貫性、学習、信頼を保証します。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.
文中の社名、商品名等は各社の商標または登録商標です。 Rev A

● ビジネス価値の実証

7. パフォーマンスを管理する&ROIを証明する

今日の大手企業のセキュリティ運用チームは、もはやコストセンターとは見なされていません。
セキュリティ運用チームは、組織のために節約された予算内でビジネス価値を実証することが期待されています。SOARプラットフォームは、SOCの「生きたビジネスケース」を維持するのに役立ちます。

・各アナリストはインシデントを特定、阻止、根絶するのにどの位の時間を費やしていますか?
・SOCが防止した損害のドル価値はいくらですか?
・オートメーションによってどのくらいの人時を節約しましたか?

SOARプラットフォームにおけるパフォーマンスメトリックを追跡/報告することは、ビジネス価値を明確にかつ視覚的に伝え、改善に重点を置くのに役立ちます。

8. プロのコンサルテーション

目標は、ユーザがテクノロジーの基本に取り組んで時間を費やすことではなく、ユーザのためにテクノロジーを機能させることです。

ますます複雑化する企業アプリケーション、ベンダ固有のコンフィギュアビリティ オプション、進化する脅威環境に伴い、SOARベンダの社内CISSP(Certified Information Systems Security Professional) 、ビジネスアナリスト、プロジェクトマネージャは、ユーザが既存のプロセスを複製可能なワークフローに進化させ、ビジネス問題をスケーラブルなビジネスソリューションに変えることを支援することによって、相当な時間と手間を節約することができます。

主な顧客

High Tech

Financial Services

Manufacturing

Energy & Utilities

＊公益事業などの重要なインフラストラクチャは、NISTフレームワークに従うことが必要ですが、D3セキュリティは地域の評議会や規制当局と共有するために、事前に構築されたプレイブックとメトリクス、及びレポートのライブラリでサポートします。

Media & Entertainment

Healthcare

Public Sector

- AUTOMATED RESPONSE
- PROVEN FRAMEWORKS
- A COMPLETE SECURITY OPERATIONS PLATFORM
- RECOGNIZED BY USERS AND EXPERTS

● D3 セキュリテイ

D3セキュリティは、組織がセキュリティ運用や調査にデータ主導型の意思決定を十分に活用できるように2002年にバンクーバー(カナダ)で設立されました。以来、我々の専門チームはイノベーションの最前線から、世界で最もターゲットを絞った組織の多くで最も困難な課題を解決するのを助けてきました。D3セキュリティは、組織の規模や業界に関係なく、脅威を迅速に修復し、その根本的な原因を排除するために必要なガイダンスと洞察を与えることができます。

コーネットソリューションズ株式会社
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.
文中の社名、商品名等は各社の商標または登録商標です。