

報道関係者各位

デジタルアーツコンサルティング株式会社

デジタルアーツコンサルティング、 Exabeam「Smarter SIEM」を活用し、 自社サービスと組み合わせた 『セキュリティ運用管理改善サービス』を提供開始

～ 2024年までに、セキュリティ運用コスト30%削減^{*1}のニューノーマル定着を支援 ～

高度なサイバーセキュリティ対策が求められるエンタープライズ環境において、CISOサービス(セキュリティコンサルティングサービス)を手がけるデジタルアーツコンサルティング株式会社(本社:東京都千代田区、代表取締役社長:松本 忠雄、以下デジタルアーツコンサルティング)は、Exabeam, Inc.(本社:米国カリフォルニア州、共同創設者兼CEO:ニール・ポラク、以下Exabeam)と販売代理店契約を締結し、「Exabeam Smarter SIEM」を活用した「セキュリティ運用管理改善サービス」を提供開始します。

テレワークの急速な普及により、インシデントの検知・復旧等を含むリスク管理の需要が高まる

昨年後半から世界中にパンデミックを引き起こしているCOVID-19等により、事業やワークスタイルのあるべき姿の再定義と適用が待たなすで求められており、国内ではテレワークへの急速な移行に伴って、リスク管理の需要がこれまで以上に高まっています。

その中で、他国と比較し日本企業が特に後れを取っているのは、内部不正や攻撃者侵入によるセキュリティインシデントが発生した際の検知・対応・復旧等へのサイバーセキュリティ対応です。多くの日本企業の情報セキュリティ対策は、外部攻撃や内部情報漏洩に対する防御策を講じることに終始しており、インシデントが発生した際の対応については明確な規程を設けておらず、セキュリティの国際規格であるISO27001にも、明確なガイドラインが定められていません。

このままセキュリティ運用の欠如を放置すると、インシデントに対して適切に対処できず対応が後れ、情報漏洩やサービス妨害等、セキュリティリスクの増大のみならず、事業継続性、収益悪化、ビジネス機会の損失等を引き起こす可能性があります。

こうしたセキュリティ運用については、SIEM(Security Incident and Event Monitor/ログの収集・管理、脅威の検知・分析)、SOAR(Security Orchestration, Automation and Response/インシデントレスポンスに必要な分析手順を自動化)といったテクノロジーにより、限られたリソースで運用管理することが可能となっています。しかしこれには、シナリオをベースに相関分析や検知ロジックの組み立て、運用方法によってはインシデント発生時のアラートの発動や受け取り方や対応・連携・管理等が属人的になってしまう等、一部の有識者への依存や大規模な体制構築が不可欠でした。

行動分析やタイムラインの生成により、 未知の脅威も含めたリスクの顕在化を実現するプラットフォーム

UEBA(User and Entity Behavior Analytics/機械学習を用いた行動分析)/SIEM分野におけるリーダー^{*2}であるExabeamは、こうしたSIEMやSOARへの対応はもとより、人・物の行動・特性を、学習・タイムライン管理し、異常で危険と思われる行動を容易に特定するUEBAの機能を踏襲した「Exabeamセキュリティマネジメントプラットフォーム(Exabeam SMP)」を提供しています。

これは、Collect(ログの収集)・Detect(攻撃の検知・解析)・Respond(インシデント対応)の運用要素をより効率的・効果的にするためのセキュリティプラットフォームで、従来の機械学習による行動の学習、ログデータ収集に加え、ユーザーの行動分析や膨大な複数のログソースからセッション、イベント化を行い人・物に紐づけたタイムラインを生成することで、これまで見えなかった人やシステムの行動を時系列で自動的に可視化し、正常な振る舞い以外の振る舞いを検知するなど、未知の脅威も含めたリスクを顕在化させる次世代のSIEMプラットフォームです。インシデント発生からその後の処理までをナレッジ化する、セキュリティ運用自動化を実現します。

デジタルアーツコンサルティング独自のサービスで 最適なセキュリティ運用を実現し、運用コストを削減

こうしたセキュリティ運用の刷新による運用コスト削減を多くの企業様・団体様にご導入いただくには、サイバーセキュリティに関する高い知見を有するコンサルティングとエンジニアリングが必要となります。

デジタルアーツコンサルティングでは、お客様にビジネスに対しての必要性があることをしっかりお伝えし、理解いただいたうえであるべき姿を見直し、業務改善を支援するコンサルティングの側面と、導入後の運用を考えた、運用設計・導入を支援するエンジニアリングの側面の両方から、ビジネスに即した最適なセキュリティ運用をお客様にご提案します。

SIEM等を導入したもののうまく使いこなせていなかったお客様、複数のセキュリティデバイスの存在により、運用工数増加にお悩みのお客様、インシデント発生後の対応等に不安を感じられるお客様など、セキュリティ運用に多くの時間や労力を費やしていた企業様・団体様に対し、内部不正や攻撃者侵入の効率的な検知・対応・復旧を可能とすることで、運用のROIを削減し、セキュリティ運用のニューノーマル(新常态)をご提案してまいります。

セキュリティ運用管理改善サービスの概要

(1) リスクアセスメントサービス

デジタルアーツコンサルティングのコンサルタントが、お客様のセキュリティガイドラインや情報セキュリティ基本方針等と、現行業務・IT資産・稼働システム等とのFit&Gapや、業務フローを整理します。その後、ソリューションアーキテクトが加わり、既存のレイアウトや構成情報、実稼働中の製品とExabeam Smarter SIEMの連携方法を調査・整理する事で、セキュリティ対策の妥当性が判らないお客様に対し、現状の可視化と、実ビジネスを考慮したお客様要件の整理や解決案をご提示(仮説案の構築)します。

(2) 特権ID管理プラットフォーム構築支援サービス

デジタルアーツコンサルティングのソリューションアーキテクトが、リスクアセスメントサービスで整理した仮説に対する検証(Proof of Value(POV))支援を行い、実ビジネスを考慮したお客様価値の可視化と、Smarter SIEMが提供する下記機能のうち、顧客ニーズに即したものを抽出しコンセプト的な設計をまとめます。その後、導入・サポートエンジニアにより、抽出した機能を活用した導入・運用設計、構築、保守・運用代行サービスを提供します。

提供機能

Exabeamのセキュリティマネージメントプラットフォーム(SMP)は、モジュール形式でコンポーネント化されており、用途に応じた必要なライセンスをご利用頂けます。

1) データ収集(ビッグデータアーキテクチャ)

【データレイク】ログ保管量に依存しないログ収集/管理機能

【クラウドコネクター】Office365やBox等、40以上のクラウドサービスログを収集する機能

2) 検知・調査(アナリティクス & マシンラーニング)

【アドバンスドアナリティクス】ユーザーのベースラインから導き出す振る舞いベースのログ解析機能(未知の脅威、内部不正対策含む)

【エンティティアナリティクス】機器(サーバー、端末、IoT等)のベースラインから導き出す振る舞いベースのログ解析機能(未知の脅威対策含む)

【スレットハンター】複雑なクエリ構文を不要とし、直感的なUIでスレットハンティングを効率的に行う事が可能な脅威検索機能

3) 対応(セキュリティオーケストレーション)

【インシデントレスポンス】オートメーション・オーケストレーションによる対処自動化機能

【ケースマネージャー】インシデントケース管理機能

DACサービスの特長(他サービスとの連携モデル)

1)クラウド態勢管理基盤構築サービス(Palo Alto Networks Prisma Cloud)

×
セキュリティ運用管理改善サービス(Exabeam SMP)

業界標準のセキュリティ/機器設定ガイドラインに準拠したマルチクラウド態勢管理、インシデント対応設計、運用管理改善をワンストップで提供

2)サイバー衛生管理基盤構築サービス(Tenable Tenable.io) × セキュリティ運用管理改善サービス(Exabeam SMP)

脆弱性 × 脅威両方の観点から、継続的なリスク最優先課題の抽出・管理、インシデント対応設計、運用管理改善をワンストップで提供

3)特権アクセス管理基盤構築サービス(CyberArk PAS) × セキュリティ運用管理改善サービス(Exabeam SMP)

特権IDの奪取・昇格による甚大なセキュリティ被害を防ぐ人・物の権限設計、脅威検知、インシデント対応設計、運用管理改善をワンストップで提供

デジタルアーツコンサルティングでは、今回サービス販売を開始するセキュリティ運用管理改善サービスとこれまでの提供サービスを組み合わせ、今後ますます重要性が増す企業システムにおけるセキュリティ強化と、ICT利活用による最適な経営環境の提案を目指してまいります。

| 取り扱い製品

Exabeam Smarter SIEM 「セキュリティマネジメントプラットフォーム(SMP)」

Exabeam SMPは、「Context Engine」、「Session Engine」、「Behavioral Engine」、「Risk Engine」の4つのエンジンを用いて、ユーザー・アセット情報の識別、ユーザー行動のタイムライン化、行動特性の学習と理解、振る舞いのプロファイリングを通じてリスクを人・物ごとに評価することで、アナリストが、異常で危険と思われる行動をしているユーザーを容易に特定し、迅速かつ適切な行動を取ることができる次世代型SIEMプラットフォームです。

| Exabeam, Inc.について

Exabeamは、これまでのSIEMで課題となっていた分散型攻撃や未知の脅威への調査・修復の自動化、人・物の振る舞いによる脅威の検知、過剰なログ保管料(ライセンス・環境)、基盤プラットフォームのSaaS化を実現する事で、リードタイムの短縮や、今までよりも51%^{※3}少ない時間でサイバー攻撃を検出、調査、対応できるようにしたSmarter SIEMのリーディングカンパニーです。

<https://www.exabeam.com/>

| デジタルアーツコンサルティングについて

デジタルアーツコンサルティング株式会社は、経営部門へのIT戦略コンサルティングを得意とするメンバーを集結し、2016年4月1日に設立いたしました。

昨今、企業や官公庁を対象とした外部からのサイバー攻撃や、内部からの機密情報の漏洩が日本国内だけでなく、世界的にも深刻な問題として認識されるようになり、セキュリティ製品の導入支援のニーズも高まっていることから、デジタルアーツが情報セキュリティ業界で培った顧客基盤やノウハウを活かしながら、市場のニーズに柔軟かつ早急に対応すべく、特に製造・金融・製薬業界の大手企業を対象としたサイバーセキュリティ対策の導入支援を主に行っております。

<https://con.daj.jp>

※1 Gartner, Inc.のレポート「the Gartner Predicts 2020: RPA Renaissance Driven by Morphing Offerings and Zeal for Operational Excellence report」(December 10, 2019)では、2024年までに、ハイパーオートメーション技術と再設計された運用プロセスを組み合わせることにより、組織は運用コストを30%削減すると予測しています。

<https://www.gartner.com/en/documents/3976135/predicts-2020-rpa-renaissance-driven-by-morphing-offer>

※2 Gartnerによる「Magic Quadrant for Security Information and Event Management」(2020年発行)で、ExabeamはLeader のうちの1社として位置づけられました。

<https://www.gartner.com/doc/reprints?id=1-5WG67KN&ct=181205&st=sb>

※3 Exabeam, Inc.のレポート「セキュリティチームは、レガシーツールで約25%の時間を誤検出の追跡に浪費 by 米調査会社ポネモン・インスティテュートとの共同調査」(August 1, 2019)では、企業がセキュリティタスクに費やす合計時間を51%削減することができたと報告しています。

<https://www.exabeam.com/pr/ponemon-institute-reveals-security-teams-spend-approximately-25-percent-of-their-time-chasing-false-positives-response-times-stymied-by-legacy-tools/>

デジタルアーツコンサルティング、DigitalArtsConsulting、当社・当社製品関連の各種ロゴ・アイコンはデジタルアーツコンサルティング株式会社の商標または登録商標です。 ※その他、上に記載された会社名および製品名は、各社の商標または登録商標です。

デジタルアーツコンサルティング株式会社 概要

<本サービスに関するお問い合わせ先>

デジタルアーツコンサルティング株式会社 坂田 TEL : 080-8819-9536 / FAX: 03-5220-1130 / E-mail : info@con.daj.co.jp

<本リリースに関するお問い合わせ先>

デジタルアーツ株式会社 マーケティング部 広報担当 山田 TEL : 090-1555-7254 / FAX: 03-5220-1130 / E-mail : press@daj.co.jp

<本リリースの素材につきまして>

下記URLよりダウンロードいただけます。

<http://download.daj.co.jp/temp2/?name=200618dac.zip>

DigitalArtsConsulting®