フィジカルセキュリティにおける サイバーセキュリティ

今日のサイバー攻撃から防御し、フィジカルセキュリティシステム内の
機密情報保護を実現するためのガイドブック

Genetec™

本書の内容

サイバー犯罪発生件数は過去最高に。対応は万全ですか？

サイバー犯罪の発生件数はこれまでになく急速に増加しています。 Cybersecurity Ventures によると、世界全体での犯罪被害は 2025 年までに年間 10.5 兆ドルに達すると指摘されています。これは年間 15% の伸び率で、史上最大の経済的富の移転が生じると指摘されています。

こうした状況に対し、企業は進化する脅威に迅速な対応を迫られています。セキュリティエコシステムに多重保護層を構築することはその第一歩となりますが、それだけでは充分ではない可能性があります。

今日、万全の対応力を備えるには、より積極的なサイバーセキュリティ戦略が求められます。加えて、脅威をより低減することが可能な自動化されたツールを持つ信頼できるパートナーを選択する必要があります。

この電子ブックでは、サイバーセキュリティゲームにおいて勝利し、ビジネスを保護するために必要なものすべてを見つけることができます。

セクション 1

サイバー脅威の全体像を理解

「サイバーセキュリティは、弊社を含めすべての人たちにとっての関心事です。弊社はコミュニティと社会に対してより広範な責務を負っており、プライバシーとサイバーセキュリティに関して率直に発信してきました。セキュリティとプライバシーは共存でき、分離するよりも大きな利便性をもたらすことができると強く信じています。また、そうした価値観を共有する組織との継続的な成功を促進する原動力になると考えています。今後も信頼を得るために懸命な努力を続けてまいります。」

–Pierre Racz
Genetec CEO

サイバー脅威はどこから来るのか

セキュリティシステムへのハッキングはさまざまな方法で行われます。
現在の代表的な攻撃手法は次のものです。

スパイウェア

被害者のコンピュータに悪意のあるソフトウェア（マルウェア）をインストールしたり、偽装したサイトに誘導してクレジットカード番号やパスワードを入力させて盗み出します。

ランサムウェア

マルウェアをインストールすることで重要なデータやシステムへのアクセスをブロックし、被害者が攻撃者に対価を支払わない限りアクセスを復元できなくします。

サービス拒否 (DDoS) 攻撃

攻撃目標にされたマシンやネットワーク上のトラフィックを溢れさせたり、システム停止を引き起こす情報を送信してユーザーのアクセスを妨害します。

ブルートフォース攻撃

パスワードを推測したり、簡単なアルゴリズムを使用してパスワードを解読してシステムやネットワークへのアクセス権を不正に獲得します。

中間者攻撃

パケット盗聴を用いてネットワーク上で通信されるユーザー名、パスワードやビデオコンテンツなどの情報を不正に取得します。

フィッシング攻撃

信頼できる送信元からの通信を偽装することで受信者を騙してマルウェアをインストールさせたり、機密情報を盗みだします。

こうした脅威から防御するには？
次のリソースをチェックしてください。

ハイライト
一般的なサイバーセキュリティアーキテクチャ

ブログ
サイバーレジリエンスを強化する 10 ステップ

ビデオ
サイバーセキュリティビデオシリーズ

サイバー攻撃によるビジネスへの経済的な影響

企業は情報漏洩に対応するための法的、規制当局との調整や技術的コスト負担に直面しています。

ソフトウェア、ネットワーク、Web サイトのダウンで通常のオペレーションが困難になると組織の生産性は低下します。

多くの場合、被害企業はダメージを受けたデバイスの復旧や交換作業、問題のある Web サイトのコードの修正作業の費用を負担しなければなりません。

顧客データの漏洩は信頼を失い、顧客の離反が増加します。

上場企業の株価パフォーマンスはサイバー攻撃により急落を招きます。

数字で見る情報漏洩の影響

漏洩の 19%

は、クレデンシャル情報が盗まれたり不正侵入が原因

引用元

142 万ドル

信頼喪失が原因の事業損失の平均コスト

引用元

30.8% の下落

サイバー攻撃による情報漏洩後の 3 年間の株価

引用元

435 万米ドル

データ漏洩による損失平均コストは 2022 年に過去最高に

引用元

CEO の 75%

は 2024 年までにサイバーセキュリティインシデントに対して個人責任を問われる

引用元

60% パーセント

の中小企業は、サイバー攻撃を受けた後、6 ヶ月以上ビジネスを維持できない

引用元

情報漏洩の 16%

フィッシング攻撃によるものだった

引用元

サイバーセキュリティ防御能力についての 5 つの質問

メーカー固有の古いセキュリティテクノロジーは、今日のサイバー脅威から保護できるように設計されていません。それはサイバーセキュリティとプライバシーの保護を根本的にサポートできないだけでなく、データの機密性、完全性、可用性も保証できません。

既存の古い設備がサイバーセキュリティ対応を妨げていないかを判断するために、次の質問に答えてみてください。

1. 何百台ものカメラの 1 台にセキュリティ上の問題があり、そのデバイスが顧客情報漏洩への経路となった場合の経済的および運用上の影響を知っていますか?
2. セキュリティチームが毎月各種ソフトウェアやファームウェアを更新したり、システムやサイバーセキュリティの運用を管理するのにどれだけの時間を費やしているか把握していますか?
3. 強度の高いパスワードポリシーを策定および維持し、データアクセスを効果的に制限する能力はありますか? 多階層の認証においてシングルサインオン機能を提供できていますか?
4. 既設システムでは、進化する脅威にいち早く対応するための最新の暗号化方式やサイバーセキュリティ機能を採用することができますか ?
5. もし顧客や警察当局から録画されたビデオ映像を開示する要求を受けたときに、映像フレーム内の他の個人情報を保護しながら、それらの録画を安全に共有できますか ?

アップグレードすべき時期とお考えですか? これらのリソースをご覧ください。

ソリューション
Security Center とは何かを見る

ビデオ
Security Center のサイバーセキュリティ機能の有効化

ブログ
サイバー脅威から保護するための 5 つのステップ

Lee Health

ヘルスケア サイト全体で機密情報を保護

Lee Health は、米国フロリダ州に 100 箇所以上の拠点を持つ最大の公共ヘルスシステムを運営しています。最近、本医療機関は 20 拠点で Genetec Security Center の導入により業務を標準化しました。チームは現在、一元化された直感的なソリューションを通じてさまざまなシステムを監視しています。

セキュリティチームが企業をフィジカルな脅威からの保護対応で忙しい間でも、Security Center はサイバーリスクを警告します。システムメンテナンス時には、正常動作監視機能がセキュリティチームにとって非常に役立つものとなります。

Lee Health のセキュリティテクノロジーおよび非急性期治療ディレクターである Sean Owens 氏は次のように説明します。「以前のシステムでは、システムの改善点や問題点について全体を把握することができませんでした。Security Center は、そうしたレベルの詳細情報を提供してくれるので、どのデバイスに問題があるかを即座に把握し、正常動作監視履歴レポートを実行して状況に対処することができます。」

今後、Lee Health はすべての拠点の管理を Genetec のプラットフォーム上で稼働させるために取り組んでいます。現在 700 台以上のカメラと 325 ヶ所のドアが Security Center に接続されており、その数は来年中に 2 倍になると予想されています。

「Security Center は、サイバーセキュリティの観点から安全が確保されている長期間の実績があり、それは特に情報システム部門にとって重要でした。旧来の既存設備に関してのクレームのひとつは、現在のサイバーセキュリティの必要基準を満たしていないということでした。Security Center の導入により、これらのギャップを埋め、IS パートナーの要件を満たすことができます。

–Sean Owens
Lee Health セキュリティテクノロジー& 非急性期治療ケアディレクター

セクション 2

データ保護対策の強化

「サイバーセキュリティは弊社の活動の中核です。設計段階からリリースまで、フィジカルセキュリティ製品の開発に IT セキュリティのベストプラクティスをもたらすよう努めています。」

–Mathieu Chevalier
Genetec リードセキュリティアーキテクト

実践の必要性がある 3 つの最も重要な サイバーセキュリティ対策

今日、フィジカルセキュリティの導入と合わせて攻撃からの耐性能力を高めるために行えることは少なくありません。より多階層の防御を実装すればするほど、ビジネスはより強く保護されます。以下の最も重要なサイバーセキュリティツールをチェックしてください。

第 1 階層 - 暗号化

暗号化は、ビデオカメラ、入退室管理リーダー、その他の IoT センサーといったセキュリティデバイスとサーバーやクライアントワークステーションとの間で送受信されるすべてのフィジカルセキュリティデータを保護することを可能とします。これは情報をエンコードしたり、読み取り可能なテキストをスクランブル化することで、不正なユーザーから判別できない状態にして保護します。

Tip! 特にビデオ監視映像の暗号化に関しては、転送中のデータと保存されているデータの両方を強力な暗号化で処理することが不可欠です。一般的に転送中のデータはより脆弱であるとされており、攻撃者は常に最も脆弱なエントリポイントをターゲットにします。

第 2 階層 - 認証

認証は、保護されたリソースへのアクセスを許可する前に、ユーザー、サーバー、クライアントアプリケーション等へ接続するための ID を検証するプロセスです。クライアント上の認証にはユーザー名とパスワードの組み合わせやセキュリティトークンが含まれます。サーバー上では、信頼できる第三者機関から発行されたデジタル証明書を通じた確認が行われます。

Tip! 複数の認証方式を導入することでより高度な安全性を追加できます。ユーザー名とパスワード以外に、電話認証アプリ、生体認証、または YubiKey やスマートカードなどのハードウェアセキュリティトークンを導入して、サイバー脅威からさらに防御することを検討する必要があります。

第 3 階層 - 権限付与

権限付与は特定のユーザーごとに権限を定義し、アプリケーションにアクセスできるユーザーと各アプリケーション内での閲覧制限や実行権限の制限を行うためのプロセスです。セキュリティシステム内での権限付与には、内部や外部と、いつ、どういった種類の情報を共有できるか、あるいはどれだけの期間データを保持するかも含まれます。

Tip! セキュリティシステムと Microsoft Active Directory を連動することで、これらの詳細な権限のプロビジョニングを自動化できます。これは認証設定の簡素化に役立つだけでなく、従業員が会社を退職するとシステム上の権限も確実に取り消されることになります。

弊社のサイバーセキュリティへのアプローチ

弊社はサイバー攻撃防御機能を内蔵した製品を提供しています。それにより機密情報を侵入者の目から保護することを確かなものとします。

情報に手が届かないように保護

高度な暗号化、権限管理、認証方法によって、データを保護し漏洩を防ぎます。ビデオ映像へ電子透かしとデジタル署名機能を追加してデータが改竄されていないことを保証します。

データを常時利用可能な状態に保つ

ディザスター―リカバリーを実行し、サイバーセキュリティの状況をリアルタイムで追跡し、レジリエンスを強化するための推奨ガイドに従ってください。これらすべては、データが常に利用可能な状態にありシステム内のすべてのコンポーネントが確実に正常動作することを支援します。

ソフトウェアとデバイスを維持

内蔵された正常状態監視機能とアップデートサービスにより、常にシステムを最高のパフォーマンスでの稼働状態を維持します。また、ソフトウェアとファームウェアのアップデートのスケジュール化、パスワードの自動ローテーションなどを集中管理して潜在的な脆弱性にすばやく対処することができます。

システムを監査しユーザーのアクティビティを追跡

内蔵の監査履歴とユーザーアクティビティレポートを使用して完全な保護対策を維持します。ID管理を合理化し、ユーザーとロールのアクセスレビューをスケジュール化することで、監査要件と企業ポリシーに適合します。

審査され適合したソリューションに基く

弊社の開発基準とソリューションの完全性をご信頼ください。弊社は国際的な機関と協力して最新のサイバーセキュリティのベストプラクティスに適合しています。弊社の製品に対しても侵入テストと監査が定期的に実施されています。

サイバーセキュリティへのアプローチの詳細を知るには？ ここからです。

ソリューション
サイバー犯罪者の攻撃から守る

ハイライト
弊社のサイバーセキュリティ認証

ビデオ
3分で知るサイバーセキュリティのベストプラクティス

統合化がデータを保護するための容易でより効果的な方法となる理由

ハッカーを阻止しビジネスを保護するために、多くの組織は単一で包括的なデータ保護とプライバシー戦略を導入しようとしています。Security Center は、すべてのフィジカルセキュリティシステムにおいてサイバーセキュリティ対策を標準化することでそのプロセスを簡素化します。以下の詳細をご覧ください。

データ保護の一元化

統合化プラットフォーム上で運用を行うと、サイバーセキュリティの安全性を確認したり、システムの稼働状態を把握するために異なる個別のソリューションをチェックする無駄な時間から解放され、統合化されたひとつのインターフェース上ですべてのシステムからのデータをコントロールできます。

多重防御システムを装備

統合化されたツールとサービスは、潜在的な脆弱性を警告し更新作業の合理化に役立ちます。その他の機能は、システムへのアクセスやユーザー権限を制限し、セキュリティスコアを提示して本格的なシステム防御体制の構築を支援します。

シングルログインでリスクを低減

プラットフォームが統合化されることで、ユーザーに必要なのは一組のログインとパスワードとなります。これにより別々に存在しているパスワードの盗難、ハッキングの危険性や漏洩の可能性を最小限に抑えられます。また、現地で求められる法的な要件を満たすために、グローバル拠点のデータ保存ポリシーを地域に応じてカスタマイズすることも可能です。

組み込みのサイバーセキュリティ機能に関心がありますか？こちらをご覧ください。

エクスペリエンス
Genetec アップデートサービス

ポッドキャスト
危険なビジネス - パート 1

ビデオ
デバイスを保護するための内蔵機能

テクノロジーベンダーのサイバーセキュリティ能力を評価するための 10 の質問

リスクを低減する最良の方法のひとつは、信頼できるベンダーを選択して協業することです。
最近では誰もがサイバーセキュリティ対応を宣伝していますが、以下の質問は、既存のサプライチェーンや新しいベンダーの信頼性を評価するときに役立ちます。

1. ベンダーは、新しい脅威の発生を積極的に監視し、そのオペレーション、データ、人員への潜在的な影響を考慮していますか?
2. セキュリティ上の問題点や脆弱性を解消するための包括的な戦略は存在しますか?
3. サイバーセキュリティに対してどういったポリシーが存在しますか?
4. そのソリューションは、高度な認証や暗号化技術など、何層のセキュリティレイヤーで開発されていますか?
5. どのように組織のデータと顧客のプライバシーを保護していますか?
6. その企業はセキュリティとデータ保護にプライオリティを置いているパートナーと協業していますか？ また、高度なレベルのサイバーセキュリティとコンプライアンスを実現するために慎重に審査した上でパートナーを選択していますか?
7. サイバーセキュリティの優れた対応手段に関して顧客への情報の提供やサポートのためにどのような取り組みを行っていますか?
8. 既知の脆弱性をいち早く把握し、迅速に対応するための戦略と修正技術を共有していますか?
9. ISO 27001 などの情報セキュリティ基準に準拠していますか? または他の規制当局や国際機関からの認証を得ていますか?
10. 第三者組織による監査を受け、セキュリティ上の問題点を特定して対処するための侵入テストを実施していますか?

信頼できるパートナーのネットワークに関心がありますか? 次をご覧ください。

ビデオ
サイバーセキュリティに関する強固なパートナーシップ

エクスペリエンス
弊社パートナーのグローバルネットワーク

ブログ
サイバーセキュリティ認証について

Cytiva

バイオテクノロジー企業でのサイバーセキュリティ対応の強化

40 カ国以上に 100 ヶ所以上の拠点を構える Cytiva は、治療薬の開発と製造を推進、加速するためのテクノロジーとサービスを提供しています。

今日、Cytiva のチームは重要な研究および製造拠点に Security Center SaaS エディションを導入して入退室管理とビデオ監視を行っています。

「以前は、脆弱性へのパッチ適用やソフトウェアアップデート、さらにそれらの環境を管理することは非常に難しいものでした。Genetec Security Center SaaS エディションを導入・運用することで、ソフトウェアのライフサイクル管理の負担を最小限にできます。ベンダー側のシステムで大部分が処理されるため、時間が短縮でき信頼性が向上します。」と Allen 氏は述べています。

Cytiva はすべてのグローバル拠点において、現地のさまざまな規制や法令を遵守しつつ、高度なセキュリティの維持を実現しています。その一部は、サイバーセキュリティの高度な対応を維持することも含まれています。

「以前は、各種アクセス要請に対応するために、より多くの人員にフィジカルセキュリティシステムへのアクセスを許可する必要がありました。現在では、プロビジョニングワークフローはすべて Genetec ClearID ™ 内で自動化されたため、アプリケーション本体へのアクセスは非常に限られたシステムユーザーグループに制限することができました。これにより、セキュリティオペレーションはさらに安全となり、レジリエンス力を備えています。」と Allen 氏は続けます。

「サイバーセキュリティにおける対応能力を充分に備えていない企業は少なくありません。また、備えていても我々のように準備に必要な情報を保有していないこともあります。Genetec は、弊社のアセスメントをサポートするために多くのドキュメントを提供し、非常に短時間でこうした状況を変化させました。これは、Genetec は単に導入準備作業のための情報を提供するだけでなく、あらゆるサイバーセキュリティの側面について知見を備えていることを示しています。」

–Larry Allen
Cytiva 施設、セキュリティ、危機管理テクノロジー製品担当

セクション 3

強固なサイバーセキュリティ戦略の堅持

「サイバーセキュリティのベストプラクティスで最も重要なものは常に高い意識です。何が良い行動で何が悪い行動なのか、やるべきこととすべきでないことを知り、適切な行動をしないときのリスクを理解する必要があります。企業には揺るぎのないインシデント対応計画も必要です。なぜなら、高い防御力を備えていたとしても、インシデントが発生する可能性はゼロではありません。損害を最小限とし、企業のデータと資産の速やかな保護を実現するための計画が求められます。

–Mathieu Chevalier
Genetec リードセキュリティアーキテクト

クラウドとハイブリッドクラウドによるサイバーセキュリティの強化

高度なサイバーセキュリティ能力を維持しながら物理的な拠点建物を保護するには、オンプレミスシステム上での多くの追加作業が必要となります。数百もの拠点が世界各国に存在する場合、その複雑性は計り知れません。クラウドサービスは、IT チームとセキュリティチームのシステム維持への負担を低減し、より容易にサイバーレジリエンス能力を得ることができます。以下の詳細をご覧ください。

最新のサイバーセキュリティ機能を利用可能

クラウドベースのフィジカルセキュリティソリューションを利用することで、通信中および停止中の暗号化、詳細なプライバシーコントロール、強固なユーザー認証、各種システム正常性監視ツールといった最新の組み込みサイバーセキュリティ機能を常に活用できます。

即座に修正プログラムとアップデートを適用

Genetec クラウドサービスでは最新バージョンが提供され、修正プログラムがリリースされれば即座に導入可能となります。これにより、フィジカルセキュリティシステムが常に最新であり、脆弱性から保護されていることを確実なものとできます。

データ冗長性の強化

ハイブリッドクラウドでの運用を選択すれば、クラウド上にビデオ映像をアーカイブしながら、オンプレミスでのセキュリティシステム運用を選択できます。これでビデオ映像の 3 つのコピーをクラウドに保存することができ、より高レベルの冗長性と可用性を確保できます。

クラウドへの拡大を検討中ですか？
これらの情報をご覧ください。

ソリューション
弊社の Stratocast Cloud VMS

ハイライト
パネルディスカッション：クラウドファースト

ホワイトペーパー
クラウド上のセキュリティ

サイバーセキュリティ戦略を効果的に維持するには

フィジカルセキュリティ上のサイバーセキュリティの維持は、攻撃から防御することを目的とするだけではありません。顧客やパートナーとの信頼を築き、将来に渡りビジネスの成功を担保することです。そのためにはデータ保護とプライバシー対策を継続的に査定し、再確認、アップデートする必要があります。以下がその方法となります。

脅威の状況を把握

サイバー脅威からの保護に関する情報源を他の IT 部門やセキュリティの専門家に依存するのを止めます。進化するリスクとそれに対応する戦略の更新に最善を尽くしてください。さらに、従業員にすべきこととすべきでないことを教育し意識を高めます。

リスク評価を実施し管理対象リストを作成

適切なサイバーセキュリティメカニズムを導入するために、自社の環境への「イン」と「アウト」を把握します。また、コンピュータ、IoT デバイス、ユーザー、データの種類などのリストを作成します。これは、より高度なサイバーセキュリティ対策を維持するときに役立ちます。

システムのアップデートとセキュリティパッチを常に適用

セキュリティパッチは特に脆弱性に対処するためのものので潜在的に高いリスクを低減します。フィジカルセキュリティシステムの強度を維持するためにも、自動的にソフトウェアやファームウェアのアップデートの存在を通知するツールの導入を検討ください。

多要素認証の導入

パスワードは簡単に盗まれたり共有される恐れがあるためパスワードに依存するのは避けるべきです。今日のサイバー脅威からの保護には、さまざまな認証方法の組み合わせが必要です。パスワードを使用する場合は定期的な変更を行います。

侵入、漏洩時の復旧計画の立案

すべての努力のゴールはサイバー脅威からの保護を100%達成することです。しかしそれでも、攻撃者から完全に防御するには十分でないこともあります。攻撃などを検出可能なフィジカルセキュリティシステムを保有することは不可欠ですが、サイバーセキュリティインシデント対応計画を備えておくことも重要です。

多くのサイバーセキュリティリソースが必要ですか？
次が参考になります。

ビデオ
Security Center の高度なセキュリティ設定

レポート
フィジカルセキュリティの状況

ハイライト
弊社のシステム可用性監視

サイバーセキュリティをレベルアップできる 3 つの強化ツール

フィジカルセキュリティシステムがすべて同じレベルのサイバーセキュリティ対策で構築されているわけではありません。確かに一部のベンダーは基本的な保護機能を提供するかもしれませんが、今日の脅威状況に対応するにはより多くが求められます。Genetec は既存の枠組みにとらわれず、対応復旧能力の獲得を支援する独自の強化ツールを提供いたします。以下の詳細をご覧ください。

自動コンプライアンス追跡

セキュリティシステムの正常稼働性の把握が必要ですか？　容易に行えます。弊社のセキュリティスコアウィジェットは、システムのセキュリティ状況をリアルタイムでチェックする動的な強化ツールです。ガイドラインを作成し、システムのさまざまな要素が適合しているかどうかを監視します。そして、ウィジェットはコンプライアンス状態を採点して改善のための推奨事項を示します。

更新スケジュール機能の強化

製品のアップデートは、多くの場合、新しい脆弱性に対する重要な修正を含んでいます。しかし、依然として重要なアップデートがサイバーセキュリティ能力の維持に不可欠なことが見落とされるケースが少なくありません。弊社の Firmware Vault は、IP カメラの新しいファームウェアがリリースされたことを通知するツールです。数回クリックするだけで、アップデートをダウンロードして展開し、最新の防御機能を確保することができます。

効率的なパスワード管理

デバイスの保護にはパスワード管理ポリシーが重要となります。Security Center 内では内蔵のパスワードマネージャーを使用して、サポートするデバイスメーカーのルールに準拠した強固でランダム化されたデバイスパスワードを自動的に生成できます。さらに、スケジュールまたはバッチ処理でカメラのパスワードを自動更新するようにシステムを設定することも可能です。

これら独自の機能に関心がありますか？資料をチェックください。

製品
Firmware Vault をチェック

ビデオ
サイバーセキュリティ機能の有効化

ブログ
そのカメラは安全ですか？

Sykes

直感的な自動化ツールの導入により サイバーセキュリティ対策を合理化

SYKES は、ビジネスプロセスアウトソーシングと IT サポートサービスのリーディングプロバイダーです。SYKES のチームはグローバルに Security Center および Genetec Streamvault™ によるインフラソリューションを導入し、拠点全体のビデオ監視と入退室を管理しています。

「弊社は Microsoft Azure クラウド環境内で全ての Genetec プラットフォームを運用しており、メンテナンスが必要な物理的なハードウェアは存在していません。そして、Streamvault アプライアンスに関しては、サイバーセキュリティへの優れた対応方式が事前に導入されていることを高く評価しています。オフィスに鎮座している従来の DVR には固有の脆弱性があります。Streamvault により弊社が脅威から保護されていることは共通の認識であり、それによりチームの心配事がひとつ減ることになります。」と Slone 氏は述べています。

今日、SYKES は厳格な監査プロセスやその他の重要な要件を満たし、さまざまなコンプライアンス基準を遵守できるよりよい位置にあります。内蔵の正常性監視ツールは、潜在的な脆弱性が検出されないという自信をチームに与えます。

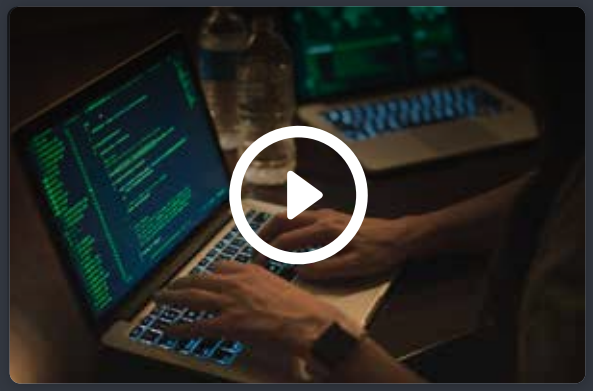
Slone 氏は次のように説明します。「Security Center のプラットフォームは、古いシステム上で以前は見ることができなかった情報を表示してくれます。例えば、ファームウェアのアップデートが必要なデバイス数やハードウェア障害の有無を簡単に確認できます。これにより、我々のチームは常にシステムを最新の状態に保ち、安全を確保することができます。」

「Genetec Security Center プラットフォームに移行して以降、グローバル全体でセキュリティを改善しただけでなく、ブランドパートナーにデータ保護とフィジカルセキュリティへのアプローチに積極的であることを示すことができています。」

–Christopher Slone
SYKES グローバルセキュリティ サイバーオペレーションディレクター

サイバーセキュリティへの知見を深める 5 分のビデオ

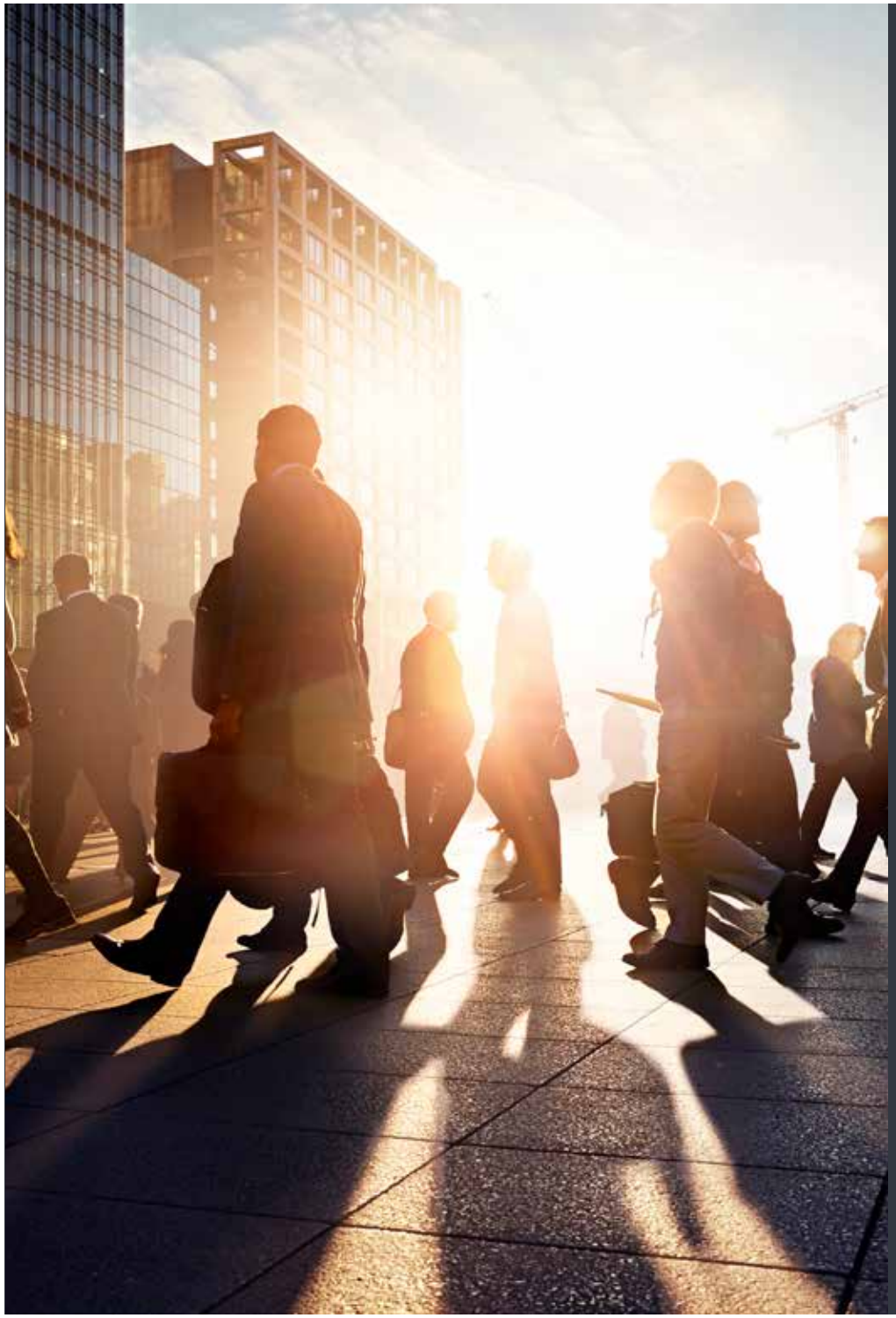
サイバーセキュリティに関しての最新トレンドや機能について、自身の知見を深めるための時間を持つことは大切です。ぜひ、Genetec の YouTube チャンネルをチェックして、データ保護のトレンド、推奨ツールや戦略に関する最新情報をご覧ください。



サイバーリスクの評価と低減の重要性

セキュリティハードウェアをサイバー攻撃から保護

フィジカルセキュリティシステムの正常稼働性と可用性を維持する方法



Genetec とデータ保護戦略を立案

年々、サイバー犯罪者による攻撃はより巧妙化しています。これは、既存のサイバーセキュリティ対策や既存の基準や認証で対応できるか精査するよう組織に圧力をかけています。さらにこうした課題はフィジカルセキュリティシステムを超えて、サプライチェーンエコシステム全体におよびます。なぜなら、昨年有効であったことは、将来のサイバー脅威を防御するには充分ではないかもしれないからです。

Genetec は最も機密性の高い情報を柔軟に保護することを支援し、サイバーレジリエントなソリューションを構築しています。ただそれだけに止まりません。弊社は新たなサイバー脅威の動向を敏感に感知し、パートナーやお客様と協力してサイバーセキュリティ対策を進めていきます。これにより、常にサイバーセキュリティ対策を強固に保つことが可能となります。

データとプライバシー保護に対する弊社のアプローチについては、Genetec トラストセンターをご覧ください。

サイバーセキュリティ対策を標準化する準備はできましたか?

統合化されたセキュリティアプローチの詳細をご覧ください。

弊社および製品の詳細については、ウェブサイト genetec.com をご参照ください。

Genetec Inc.
Genetec.com
info@genetec.com
@genetec

UDPT: 20-09-2022