2020/09/24

“EcoStruxure マシンアドバイザー”のサイバーセキュリティについて

Our position on Cybersecurity

Schneider Electric's products and solutions are being used in critical infrastructure as well as manufacturing plants. In these areas, the demands of cloud computing, the Internet of Things (IoT), and increasing threats against critical infrastructure have elevated cybersecurity as top priority. For Schneider Electric, Cybersecurity and data privacy encompasses the measures, actions, and practices employed to protect Digital offerings and solutions from cyber threats.
A corporate White Paper (i) covers in depth how Schneider Electric mitigates Cyber risks to ensure we can thrive securely in today’s digital economy.

サイバーセキュリティに対する私たちの立場

シュナイダーエレクトリックの製品とソリューションは、製造工場だけでなく重要なインフラストラクチャでも使用されています。 これらの分野では、クラウドコンピューティング、モノのインターネット（IoT）、および重要なインフラストラクチャに対する脅威の増大により、サイバーセキュリティが最優先事項として高まっています。 シュナイダーエレクトリックの場合、サイバーセキュリティとデータプライバシーには、デジタル製品およびソリューションをサイバー脅威から保護するために採用されている対策、アクション、およびプラクティスが含まれます。

企業の白書（i）では、シュナイダーエレクトリックがどのようにサイバーリスクを軽減し、今日のデジタル経済において安全に成功できるかを詳しく説明しています。

EcoStruxure

EcoStruxure is our open, interoperable, IoT-enabled system architecture and platform. EcoStruxure delivers enhanced value around safety, reliability, efficiency, sustainability, and connectivity. EcoStruxure leverages advancements in IoT, mobility, sensing, cloud, analytics and cybersecurity to deliver Innovation at Every Level. This includes Connected Products, Edge Control, and Apps, Analytics & Services.
EcoStruxure Machine Advisor is part of the top layer "Apps, Analytics & Services" while our Cybersecure measures are integrated to protect end-to-end, from products to solutions and services.

EcoStruxure

EcoStruxureは、オープンで相互運用可能なIoT対応のシステムアーキテクチャおよびプラットフォームです。 EcoStruxureは、安全性、信頼性、効率性、持続可能性、および接続性に関する価値を高めます。 EcoStruxureは、IoT、モビリティ、センシング、クラウド、分析、およびサイバーセキュリティの進歩を活用してあらゆるレベルのイノベーションを実現します。 これには、コネクテッドデバイス、エッジコントロール、およびアプリケーション、アナリティクス&サービスが含まれます。

EcoStruxure マシンアドバイザーは最上位層の "アプリケーション、アナリティクス&サービス"の一部ですが、サイバーセキュリティの対策は製品からソリューションやサービスまで、エンドツーエンドを保護するために統合されています。

Secured on all dimensions

Our security position focuses on key aspects:

- Protecting strategic IT systems and assets and securing internal activities.

- Leading the digital transformation of energy management and automation.

Designing and developing new solutions and products within a Cybersecure framework.

あらゆる方向に対して安全

私たちのセキュリティのポジションは重要な側面に焦点を当てています。

- 戦略的なITシステムと資産を保護し、内部活動を保護する。
- エネルギー管理と自動化のデジタル変革を先導。

サイバーセキュリティの枠組みの中で新しいソリューションや製品を設計し開発する。

Secured infrastructure

The service implementation relies on Microsoft Azure and therefore uses state of the art technologies and security practices. See (ii).

安全なインフラストラクチャ

サービスの実装はMicrosoft Azureに依存しているため、最先端のテクノロジとセキュリティプラクティスを使用しています。 （ii）を参照ください。

Secure by design

Considering the design of the solution, Schneider Electric EcoStruxure Machine Advisor is developed with cyber security concern in mind:

- Designed with Customer security constraints as main input and In-Depth Security architecture principles.
- Follow a strict Secure Development Lifecycle detailed just after.
- Conduct regular Cybersecurity assessments, with periodic penetration tests and code scans, managed by a global Schneider Electric Cybersecurity instance, and based on ISO 27001 and IEC 62443.

The service uses global Schneider Electric's EcoStruxure Technology Platform (ETP) for Machine to Machine data exchange and Time Series Storage. This platform is implemented on top of Microsoft Azure too.
Users access is protected and authorized by global Schneider Electric's Identity & Access Management system (IDMS), with a multifactor authentication for increased security providing a Single Sign On with other Schneider Electric services.

設計による安全

ソリューションの設計を考慮して、シュナイダーエレクトリック EcoStruxure マシンアドバイザーは、サイバーセキュリティへの配慮を念頭に置いて開発されています。

- お客様のセキュリティ上の制約を主な要件と詳細セキュリティアーキテクチャの原則として設計されています。
- その直後に詳述されている厳格なセキュア開発ライフサイクルに従います。
- 定期的な侵入テストとコードスキャンを使用して、グローバルなシュナイダーエレクトリックのサイバーセキュリティインスタンスによって管理され、ISO 27001およびIEC 62443に基づいて、定期的なサイバーセキュリティ評価を実施します。このサービスでは、マシン to マシンデータ交換と時系列ストレージに、グローバルなシュナイダーエレクトリックのEcoStruxure Technology Platform（ETP）を使用しています。 このプラットフォームは、Microsoft Azure上にも実装されています。

ユーザーのアクセスは、グローバルなシュナイダーエレクトリックのアイデンティティ＆アクセス管理システム（IDMS）によって保護および承認されています。セキュリティ強化のための多要素認証により、他のシュナイダーエレクトリックサービスとのシングルサインオンが可能になります。

Secured operation

A well-designed service wouldn't be considered as secure if not properly monitored. On that aspect, EcoStruxure Machine Advisor follows the global Schneider Electric's policy by implementing an Incidents Response Plan.

We also take care of Segregation of duties and Principle of Least Privilege: only a limited set of authorized Schneider-Electric personnel have access to service management.
Traceability is part of the service: all accesses and activities into EcoStruxure Machine Advisor application are securely logged to allow full traceability.

安全な運用

適切に監視されていないと、適切に設計されたサービスは安全であるとは見なされません。 その点で、EcoStruxure マシンアドバイザーは、インシデント対応計画を実施することによって、世界的なシュナイダーエレクトリックの方針に従います。

また、職務分掌および最低特権の原則にも気を配っています。サービス管理を利用できるのは、限られた権限を与えられたシュナイダーエレクトリック担当者だけです。
トレーサビリティはサービスの一部です：EcoStruxure マシンアドバイザーアプリケーションへのすべてのアクセスとアクティビティは、完全なトレーサビリティを可能にするために安全に記録されます。

Secure Development Lifecycle

Schneider Electric has adopted a best in class ISO:2700X based process that defines a Secure Development Lifecycle (SDLC) that is followed by all the offers to guarantee security best practices at each stage of application development.
Dedicated organization named "Product Security Office" (PSO) is responsible to create a Trustworthy & Compliant Control Environment (TCCE) within Schneider. The TCCE is comprised of our secure products that are tested and validated and combined with our services to solve customer cyber security objectives. The PSO aims to build products based on the Secure Development Lifecycle methodology and OWASP recommendations to ensure the creation of secure and reliable Schneider products and services that our customers can rely on.
Before any major customer release, Schneider Electric tests and validates EcoStruxure Machine Advisor offerings thanks to a dedicated world class cyber security testing in the form of penetration tests. As a final step, a complete final security review is performed by Schneider Electric PSO to confirm GO for deployment.
In case of Cyber security incident, Schneider Electric has a CERT team to manage vulnerabilities.

安全な開発ライフサイクル

シュナイダーエレクトリックは、セキュア開発ライフサイクル（SDLC）を定義するクラス最高のISO：2700Xベースのプロセスを採用しており、その後にアプリケーション開発の各段階でセキュリティのベストプラクティスを保証します。

"Product Security Office"（PSO）という専用組織が、Sシュナイダー内に信頼とコンプライアンスの管理環境（TCCE）を構築する責任を負っています。 TCCEは、お客様のサイバーセキュリティ目標を解決するためにテストおよび検証され、当社のサービスと組み合わされた当社の安全な製品で構成されています。 PSOは、セキュアな開発ライフサイクル方法論とOWASPの推奨事項に基づいて製品を構築し、お客様が信頼できる安全で信頼性の高いシュナイダー製品およびサービスを確実に作成することを目指しています。

主要な顧客リリースの前に、シュナイダーエレクトリックは、侵入テストの形での専用のワールドクラスのサイバーセキュリティテストのおかげで、EcoStruxure マシンアドバイザー製品のテストと検証を行っています。最後のステップとして、完全な最終セキュリティレビューがシュナイダーエレクトリック PSOによって実行され、導入のためにGOが確認されます。

サイバーセキュリティインシデントの場合、シュナイダーエレクトリックには脆弱性を管理するためのCERTチームがあります。

Secured data collection

EcoStruxure Machine Advisor does everything to keep customers' data secure and restrict the ability of cyber attackers to intercept or tamper data exchanges.

Options for the collection of machine data are described below:

- Zero connectivity: No connection at all between the machine and the cloud. User is manually uploading a csv file containing the machine's historical data into the machine's page in EcoStruxure Machine Advisor.
- Schneider Electric or third-party gateway used to send live data from a machine to EcoStruxure Machine Advisor (how to documents explaining how to connect your gateway are available directly in Machine Advisor). Common factors over gateway connections are:
    - Transmission flow between onsite gateways and Schneider Electric's services is encrypted using TLS 1.2 (HTTPS or MQTTS).
    - Connectivity doesn't require inbound connection into the Customer Network Infrastructure.
    - The flows are only meant and designed to send Assets measurement data to cloud.
    - Each gateway is provided a time limited security token that can be revoked anytime

Schneider Electric focuses on securing data flows, and on aligning to the latest data integrity and privacy regulatory requirements such as the European General Data Protection Regulation, GDPR. We run dedicated compliance controls to align to these regulations.

安全なデータ収集

EcoStruxure マシンアドバイザーは、顧客のデータを安全に保ち、データ交換を傍受または改ざんするサイバー攻撃者の能力を制限するためにあらゆることを行います。

マシンデータを収集するためのオプションは以下のとおりです。

- 接続性ゼロ：マシンとクラウドの間にまったく接続がありません。ユーザーは手動でマシンの履歴データを含むcsvファイルをEcoStruxure マシンアドバイザーのマシンのページにアップロードしています。
- マシンからEcoStruxure マシンアドバイザーにライブデータを送信するために使用されるシュナイダーエレクトリックまたはサードパーティのゲートウェイ（ゲートウェイの接続方法を説明する文書への追加方法は、マシンアドバイザーで直接利用できます）。ゲートウェイ接続を介した一般的な要因は次のとおりです。
    - オンサイトゲートウェイとシュナイダーエレクトリックのサービス間の伝送フローは、TLS 1.2（HTTPSまたはMQTTS）を使用して暗号化されています。
    - 接続性は、顧客ネットワークインフラストラクチャへのインバウンド接続を必要としません。
    - フローは、資産測定データをクラウドに送信することのみを意図して設計されています。
    - 各ゲートウェイには、いつでも無効にできる期限付きのセキュリティトークンが提供されます。

シュナイダーエレクトリックは、データフローの保護、およびヨーロッパの一般データ保護規制（GDPR）などの最新のデータ整合性およびプライバシー規制要件への対応に重点を置いています。これらの規制に合わせるために、専用のコンプライアンス管理を行っています。

References

(i) Cybersecurity at Schneider Electric Whitepaper https://www.schneider-electric.com/en/download/document/998-20244304/

See also:
https://www.schneider-electric.com/en/work/support/cybersecurity/overview.jsp

(ii) Microsoft Azure Cybersecurity https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security

See also:
https://docs.microsoft.com/en-us/azure/security/ https://docs.microsoft.com/en-us/azure/security/azure-security

参考文献

（i）シュナイダーエレクトリックホワイトペーパーのサイバーセキュリティ白書（英語版）
https://www.schneider-electric.com/en/download/document/998-20244304/

こちらも参照：サイバーセキュリティサポートポータルサイト（英語版）
https://www.schneider-electric.com/en/work/support/cybersecurity/overview.jsp

（ii） Microsoft Azureのサイバーセキュリティ（日本語）
https://www.microsoft.com/ja-jp/trustcenter/Security/azure-security

こちらも参照：（日本語）
https://docs.microsoft.com/ja-jp/azure/security/