Datasheet

サイバー空間における監視および対応システム

(Security Operation Center - S.O.C)

viettel security

セキュリティオペレーションセンター

セキュリティオペレーションセンター（S.O.C）は、団体の安全情報について故障を検出、分析、対応、防止、調査して、安全情報を確保するために、安全情報の問題を監視して修理する機能を備えたシステムです。

S.O.Cは**過程、人、技術**の３つの要素で構成されています。

S.O.Cの必要性

全世界が賢い国という時代に向けている背景で、第4次産業革命が世界中で推進されています。当然のことながら、インターネット上でのやり取りは増加しており、次のような理由によって、安全情報で保護されないリスクが高まっています。

・発展している情報技術によって、ハッカーはより精巧で予測不能な方法を用い、より大規模な攻撃を行うための理想的な環境を作り出しました。

・安全情報についてユーザーの認識が寡聞です。

・安全情報分野で組織の投資が不十分でパッチワークです。

・安全情報政策を厳守する事での困難さ。

ベトテルのS.O.Cシステム

ベトテル・サイバーセキュリティ・カンパニー(Viettel Cyber Security)の安全情報の故障監視・対応サービスは24時/7日/365日で顧客の包括的な監視を支援し、安全情報の故障を早く検出してインシデント対応を行います。サービスは、ベトテル・サイバーセキュリティ・カンパニー(Viettel Cyber Security)の専門家チームに提供され、世界中で認められ、合理的で競争力のあるコスト、明確なサービス水準合意（SLA）を保証し、顧客がサービスの優れた機能を完全に体験する事を保証します。

供給サービスは次のことを含みます

ワークステーションとサーバーを監視するシステム（エンドポイント - Endpoint)

ワークステーションとサーバーシステムが24時/7日/365日に監視されます。 監視範囲は：

・悪意のあるコードの制御サーバーへの接続の合図とかシステムに悪意のあるコードが広まっている合図などのようなサイバー攻撃についての合図を監視し、検出します。

・顧客のシステムのエンドポイント（ワークステーションとサーバー）で異常な合図を検出し、監視します。

・エンドポイントで侵入合図を検出します。

サイバー攻撃の監視と検出

潜在的なサイバー攻撃脅威と異常な合図を自動的で検出して分析するために、ネットワーク　トラフィックと製品種類はセンサーで収集され、分析され、自動的で悪意のあるコード分析技術（サンドボックス）と組み合わされます。ネットワーク監視モジュールーは、チームがサイバー攻撃の跡を追跡し、深く分析するための支援ツールも提供します。

セキュリティ幹事と自動反応のプラットフォーム

ベトテル(Viettel)のS.O.Cシステムはセキュリティ幹事と自動反応のプラットフォームに基づいて運用されています。このプラットフォームが、故障に対する監視、分析、修理のより緊密に結びついた安全情報T製品エコシステムを設定するためにセキュリティ技術や手順をシステム運用に自動的に統合するのに役立ちます。

統合ログ管理・分析

統合ログ分析・収集・監視のシステムは、S.O.Cシステムで事で全体的な監視プラットフォームで、中心的な役割を果たす事です。このシステムは、組織の情報技術システムで発生される全ての安全情報イベント、ログを収集、標準化、保存、相関分析し、リアルタイムで運用データを監視・分析する能力を提供します。組織がシステムで安全情報の脅威・故障を早く検出する事を最大限にサポートするために、このソリューションを使用すると、さまざまなデバイスによって生成されるすべてのデータソースを検索、監視、分析、視覚化できます。

24時/7日で故障対応とリアクション

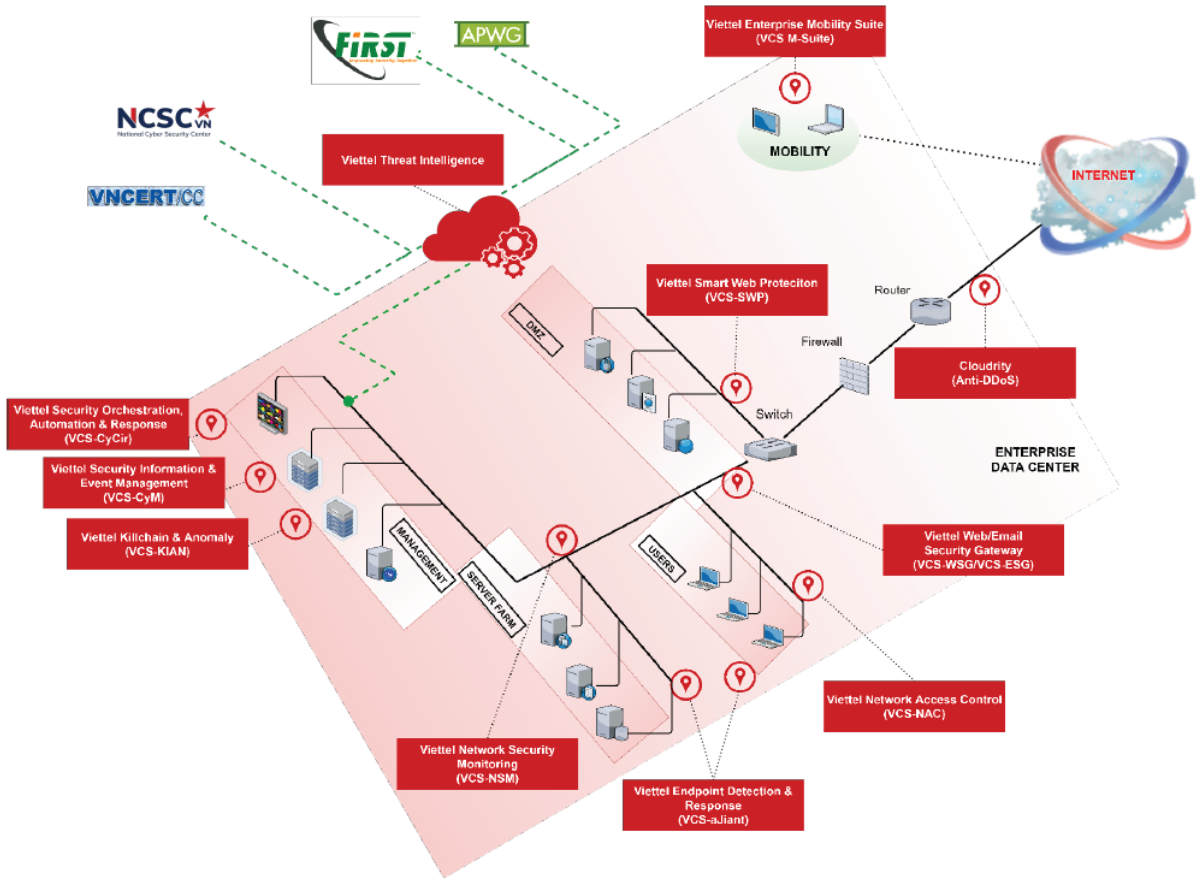
顧客のシステムは24時/7日でベトテル・サイバーセキュリティ・カンパニー(Viettel Cyber Security)の専門家チームによって監視されます。侵入攻撃が検出されると、サイバーセキュリティ専門家が調査を行い、攻撃が発生した範囲を特定し、顧客のシステムから攻撃範囲を隔離し、その後、感染範囲の拡大を防止して対応して処理するためにネットワーク全体での業務対応、監査、反応を実行します。

故障対応が完了された後、顧客は攻撃過程に悪用された脆弱性、感染時間、侵入方法を含む報告を受け取ります。

知識提供と安全情報の広告

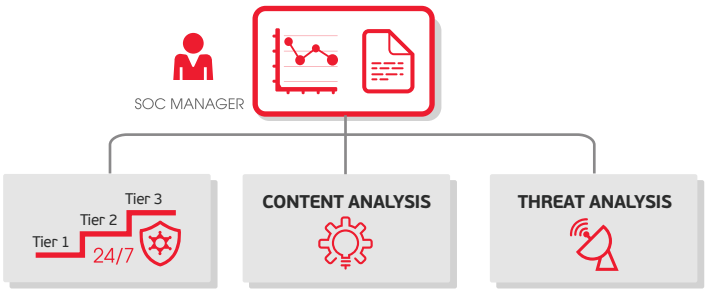
顧客がシステムの安全情報状況の情報と世界で攻撃傾向について把握して更新できるように、サービス利用中に定期的な報告が提供されます。

S.O.Cシステムで内の部分のインタラクティブおよび展開モデル



システム運営組織

ベトテル(Viettel)は、顧客にS.O.C　システム運営人材部分の国際標準を達成したモデルを作成します。6グループに分かれます。



- **ティア 1（ベトテル - Viettel):** 24時/7日で監視し、指示に従って故障を処理する責任を負います。
- **ティア 2（顧客）：**ティア1から故障を受け取り、通常な故障を修理し、処理に失敗した故障に対してティア3に移動します。
- **ティア 3（ベトテル - Viettel)：**ティア2からエスカレーションされた故障を受け取り、もっと深いレベルで処理し、同時に同様の故障に対する処理手順を書き直し、ティア2の指導とトレーニングを行います。
- **内容分析-Content Analysis（ベトテル - Viettel)：**システムの修理能力を改善し、向上し、最適化します。
- **脅威分析-Threat Analysis（ベトテル - Viettel)：**システムへの新しい脅威の知識を更新し、分析し、レビューします。
- **・S.O.Cマネージャー（ベトテル - Viettel）：**システムの仕事でパフォーマンスを検査して評価し、システム運営を管理します。

品質へのこだわり

ベトテル(Viettel)は、国内と近隣諸国で一流のインターネットサービスプロバイダである強みとして、ネットワーク全体にわたる異常な問題、安全情報の危険性を早く検知する能力を持っています。
ベトテル(Viettel)は、S.O.Cシステムと最先端の安全情報政策エコシステムを提供し、すべてのレイヤーで安全情報を確保して完全に技術を所有しています。

- Gateway (ゲートウェイ): VCS-WSG, VCS-ESG
- Network (ネットワーク): VCS-NSM, VCS-NAC, VCS-Anti DDoS
- Endpoint (エンドポイント): VCS-aJiant, VCS M-Suite
- Application (アプリケーション): VCS-SWP, Cloudrity
- Management (管理): VCS-CyM, VCS-CyCir, VCS-KIAN, VCS-スレットインテリジェンス(Threat Intelligence)

また、ベトテル(Viettel)は、世界中で認められ専門家チームとともに、顧客に最も信頼性で最も効果的なS.O.Cサービスを提供することを約束します。
ベトテルによって提供されているS.O.Cサービスに対するサービス水準合意（SLA）を約束する事は次の事を含みます:

- 安全情報のイベントに対するSLA
- 安全情報古書にたいするSLA
- 安全情報に反し、脆弱性を修理する事に対するSLA
- 最適化アラートに対するSLA
- 安全情報の脅威を管理する事に対するSLA