パートナー様ご紹介

株式会社クエスト

セキュリティ監視センター（SOC）業務をフルアウトソースし、サイバー攻撃を迎え撃つ

当社（クエスト）は、お客様とともにITの価値向上を実現し、お客様の信頼を得ることを追求していきます。そのために、コンサルティングからシステムの構築、運用・保守までの「システムライフサイクル」全体を捉えたワンストップサービスの提供を展開しています。今回はセキュリティ製品の導入から運用・監視までをワンストップで実現するサービス「Q-MSS」をご紹介します。

増加するサイバー攻撃

標的型攻撃や不正アクセスなどのサイバー攻撃による内部情報の漏洩事故は、年々増加の一途を辿っています。更にマイナンバーをはじめとする個人情報に関する制度改正や施行に伴い、サイバーセキュリティ対策は業種や業態・事業規模を問わず、全ての事業者において重要視される経営課題の１つとなっています。

経済産業省と独立行政法人情報処理推進機構(IPA)は2015年12月に「サイバーセキュリティ経営ガイドラインVer.1.0」を策定、その中の重要な対策の大項目として、以下の4点を挙げています。

①リーダーシップの表明と対策の構築
②サイバーセキュリティリスク管理の枠組みの決定
③リスクを踏まえた攻撃を防ぐための事前対策
④サイバー攻撃を受けた場合に備えた準備

特に④は「情報収集の重要性」について注意喚起した内容となっており、「事故対応を適切に実施するために常に情報収集を行い、これを関係者と共有する事で事故による極小化を目指す」ことを謳っています。

セキュリティに関するノウハウの結晶「Q-MSS」

当社は、これまでのプライベートSOC（セキュリティ監視センター）の構築や運用で培ってきたノウハウを基に、高品質でありながら低価格なマネージドセキュリティサービス「Q-MSS」を立ち上げました。

「Q-MSS」は、独自のセキュリティ監視センター「Q-SOC」を準備、専門のセキュリティアナリストによるセキュリティログの監視分析のサービスを提供します。

また、パロアルトネットワーク社製品をはじめとするセキュリティ機器についてコンサルティング、導入、運用、セキュリティログを活用した監視分析をワンストップで提供します。

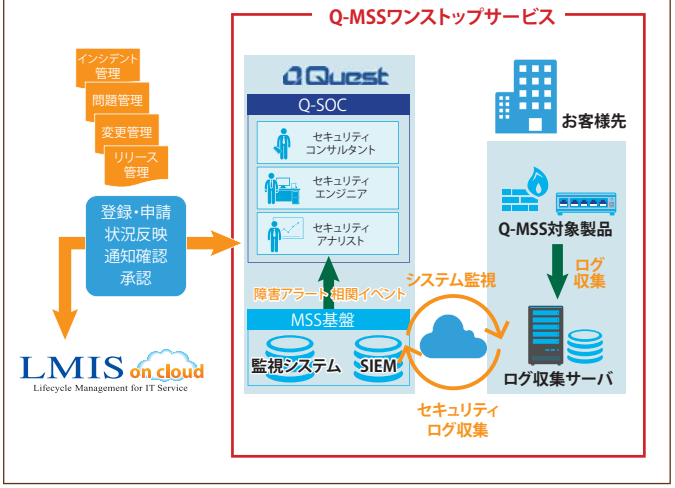
「Q-MSS」では、監視基盤にSIEM（Security Information and Event Management）を活用する事で、従来のSOCでは困難なサイバー攻撃の予兆を検知する事や、万が一にも攻撃者の侵入を許してしまった時の影響範囲の特定を可能とする様な監視分析を行い、実害の発生を未然に防ぐための施策をお客様に提案します。

「Q-SOC」とユニリタの「LMIS on cloud」による統合的なSOC運用の実現

「Q-SOC」では、セキュリティ機器より得られる（セキュリティ）ログやSIEMによる監視分析により判定したインシデントを「LMIS on cloud」に登録・管理する事で、正確かつスピーディに「Q-SOC」内部の情報共有を行うとともに、SOC運用に不可欠なITILの重要な構成要素である問題管理、変更管理、リリース管理についても、「LMIS on cloud」をフル活用することで、統合的に管理したSOC運用を実現しています。

当社は、今後も「Q-SOC」の管理面における業務効率化を図る上で「LMIS on cloud」を更に活用すると共に、ノウハウを蓄積、テンプレート化を図る事で、プライベートSOC構築等のインテグレーション案件にも展開していきます。

システム概要図



株式会社ユニリタ　www.unirita.co.jp

本　　社	〒108-6029	東京都港区港南2-15-1 品川インターシティA棟	TEL 03-5463-6383
大阪事業所	〒541-0059	大阪市中央区博労町3-6-1 御堂筋エスジービル	TEL 06-6245-4595
名古屋事業所	〒451-0045	名古屋市西区名駅3-9-37 合人社名駅3ビル(旧48KTビル)	TEL 052-561-6808
福岡事業所	〒812-0013	福岡市博多区博多駅東2-2-2 博多東ハニービル	TEL 092-437-3200

ユニリタグループ　株式会社アスペックス ／ 株式会社ビーティス ／ 株式会社データ総研
備実必(上海)軟件科技有限公司 ／ 株式会社ビーエスピーソリューションズ
株式会社ユニ・トランド