



サイバーセキュリティ監視体制 (SOC)の構築・運用

リスクシナリオを軸とした体系的アプローチ

セキュリティ監視体制の必要性

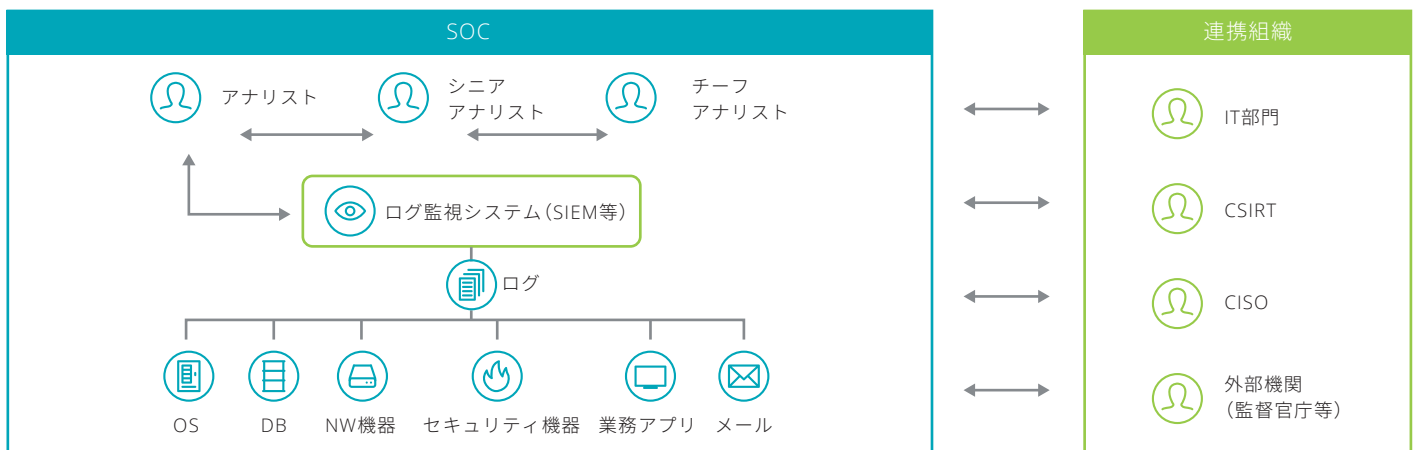
近年、企業を狙ったサイバー攻撃(標的型攻撃等)の被害が急増しています。これらの攻撃は、価値の高い情報資産(技術/生産/個人情報等)の搾取等を目的として行われ、その対策は企業にとって重要な課題となっています。従来型の予防対策のみでこれらの攻撃に対処することは、未知のマルウェアの使用等を想定しても困難な状況にあり、攻撃を迅速に検知・対処するための新たな仕組み、セキュリティ監視体制(Security Operation Center)の構築が必要となっています。

デロイトのアプローチ

デロイト トーマツ グループは、グローバルレベルでの長年の経験に基づく独自の метод論を活用し、企業のSOC構築を支援します。デロイトの方法論は、ビジネス視点とリスクアプローチに重点を置き、優先度の高いリスクを考慮した上で、監視対象やSOC機能を特定し、企業にとって最適なセキュリティ監視体制を早期に実現します。そのコアエンジンとして、SIEM(Security Information and Event Management)ソリューションを最大限に活用し、企業を取り巻く様々なリスクに対処するために、最適な監視体制を実現します。




セキュリティ監視体制のイメージ

SIEMをコアエンジンとして、様々な機器から収集したログを継続的に監視します。危険度の高いインシデントを抽出し、必要に応じて社内外の組織と連携し迅速に対応を行います。



導入後の効果

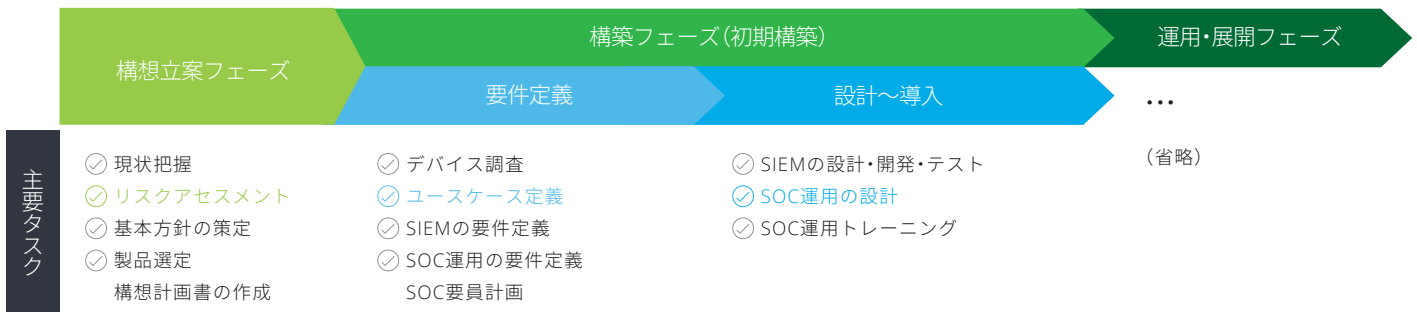
セキュリティ監視体制(Security Operation Center)の仕組みを導入することで、情報漏洩等による被害の低減が期待されます。

- 
ケース1 アンチウイルスで検知できないマルウェアについて、Proxy・Firewall・IPS/IDS等のログを相関的に分析することにより感染PCを特定し、その後の感染拡大および情報漏洩を防止
- 
ケース2 IDS/IPS・アンチウイルス等の複数デバイスのログを相関的に分析することにより、トリアージ(インシデントの優先度付け)に要していた工数を50%低減
- 
ケース3 内部者による営業秘密の不正送信を発見し、競合企業への情報流出を未然に防止

本サービスの流れ

構想立案フェーズで組織のビジネス要件やリスク対応の優先度等を特定し、それらを踏まえた基本方針を策定します。その後、構築フェーズにて段階的に運用プロセスや監視インフラの導入を行い、様々なセキュリティ脅威への監視および対処を実施します。

SOC構築・展開のアプローチ



各フェーズのアウトプット例



デロイト トーマツ リスクサービス株式会社

本社 〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル Tel:03-6213-1300
名古屋 〒450-6337 愛知県名古屋市中村区名駅1-1-1 JPタワー名古屋 Tel:052-565-5950

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームおよびそのグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ 税理士法人およびDTI弁護士法人を含む)の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約8,700名の専門家(公認会計士、税理士、弁護士、コンサルタントなど)を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト(www.deloitte.com/jp)をご覧ください。

Deloitte(デロイト)は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを Fortune Global 500® の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約225,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド(“DTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数指します。DTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細はwww.deloitte.com/jp/aboutをご覧ください。

Member of
Deloitte Touche Tohmatsu Limited