CRESCO

AI × SOC により、すべての企業に 24 時間 365 日の安心を

CRESCO Managed Security Services

SOC 監視を中核に、脅威の検知・通知から初動対応、調査、セキュリティ運用体制の
整備までをワンストップでご支援し、お客様が安心して業務に集中できる環境をご提供します。



特徴

SIEMとAI分析の活用による高度なセキュリティ監視

- Microsoft Sentinel と AI 分析を活用
- 大量のセキュリティイベントから脅威をリアルタイムに検知
- 自動トリアージにより重要なインシデントを効率的に抽出

業界特有の脅威に対応するセキュリティ運用

- 金融業界をはじめとする業界特有の脅威への対応実績あり
- 各業界のリスクや攻撃傾向に応じた検知ルールを継続的に見直し・改善
- セキュリティ運用をトータルでサポート

24時間365日のSOC運用体制

- グローバル SOC 体制により、24時間365日の有人監視を実現
- 夜間・休日を含めた継続的な監視
- 脅威の早期発見から初動対応までを迅速に支援

導入しやすいサービス設計

- 既存環境を活用したスムーズな導入
- 最短1か月で監視体制を構築
- 運用状況や予算に合わせたスモールスタートが可能

ご提供サービス

基本サービス	SOC（24時間365日監視）
オプション	EDR（端末監視） デジタルフォレンジック ※2027年度リリース予定 インシデント初動対応 プライベートSOC
その他	セキュリティコンサルティング

セキュリティ監視の仕組み

お客様環境（各種システム・サービス）

- ファイアウォール（FW）
- EDR/ 端末
- サーバ・オンプレ機器
- クラウドサービス
- ネットワーク機器
- 業務システム・アプリ

ログ
アラート

CRESCO Managed Security Services（SOC）

データ基盤
- Microsoft Sentinel
- AI分析

監視・分析
- セキュリティアナリストが24時間365日体制で監視・分析

1 収集・正規化 → 2 AI分析 → 3 脅威検知 → 4 トリアージ（重要度判定） → 5 アラート通知

お客様への提供

- アラート通知
- 対応状況の共有
- ポータル
- 月次レポート
- 定例ミーティング

お問い合わせ
株式会社クレスコ
〒108-6026
東京都港区港南 2-15-1 品川インターシティ A 棟 26 階
URL https://www.cresco.co.jp/

https://wakuwaku.cresco.co.jp/solution/managed-security-service