MBSD Managed Security Service

MBSD-SOC

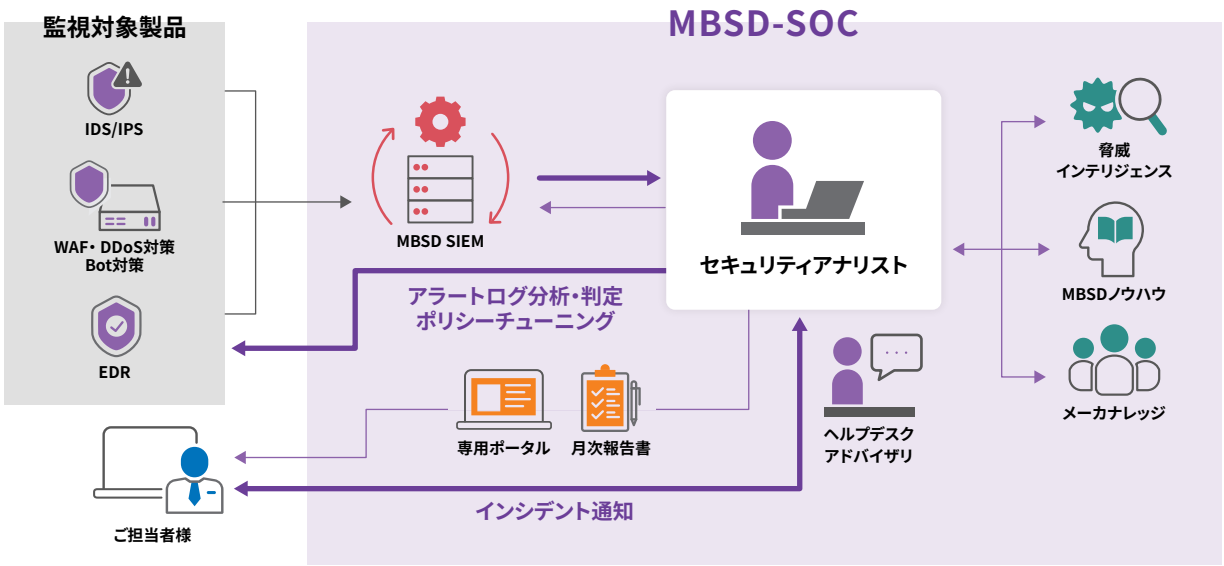
24時間365日脅威を逃さない
今求められるサイバー防御

大量のアラート処理に追われていませんか？

20年を超える豊富な経験・実績・知識・脅威情報を活用し、MBSD-SOCのセキュリティアナリストが、お客様のオンプレミス・クラウド上に設置されているセキュリティ製品を、24時間365日体制で、日々進化するサイバー攻撃からお客様の環境を守り続けます。
セキュリティ監視（アラートログの分析・判定・通知・お問い合わせ）からセキュリティ運用（ポリシーチューニング）までセキュリティアナリストが一貫して対応いたします。

サービス紹介

MBSD-SOCでは、お客様環境に設置されているセキュリティ機器のアラート・ログを弊社のSIEM基盤で収集し、セキュリティアナリストが詳細な分析、必要に応じてお客様への通知および緊急対処を行います。



詳しくは裏面へ ⟶

サービスの特長/メリット

セキュリティアナリストが24時間365日のセキュリティ監視・運用を提供します。

01

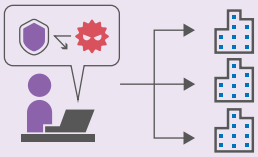
- セキュリティアナリストが24時間365日お客様のネットワークを監視

02

- 多角的な分析（パケットペイロード分析・レスポンス分析・ホスト情報照合・攻撃コードの動作確認）を実施

03

- MBSDではカスタムシグネチャの作成および提供の実績が多数



04

- 複数の脅威インテリジェンスを活用し、より高い精度で分析

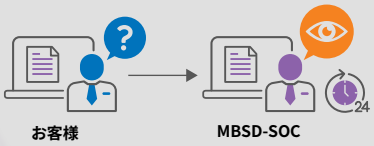
セキュリティ監視・運用にてお困りの課題をセキュリティ専門家が解決いたします。

現状調査→状況確認→解決案確認の過程ごとに専門知識が必要

すぐに相談できる安心感

セキュリティ専門家による適切なアドバイス

24時間365日サービス提供しており
常に状況を把握していることから
お客様の問題解決をサポート

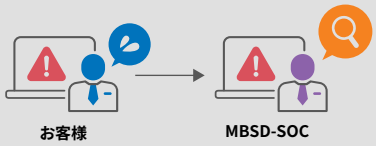


大量のアラートが発生し、自社にどのような影響があるか確認が必要

分析・判断の代行

お客様のセキュリティ運用の負担を最小限化

危険性が高いインシデントのみ緊急通知
攻撃の早期発見により速やかに対応着手

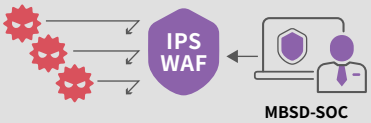


多くのシグネチャから自社に合うチューニングの検証・実施が必要

セキュリティ運用の最適化

セキュリティ製品の検知／防御力を最大化

最新の脆弱性情報や新しい攻撃手法等に
対応したタイムリーなチューニング
攻撃の遮断設定で被害拡大の最小化



監視対象製品

MBSD-SOCでは、以下セキュリティデバイスの監視を提供しております。

UTM（IPS）	Gateway WAF	IPS/IDS	Server Security	SIEM	EDR	ZTNA
PaloAlto PAシリーズ	F5 Big-IP AWAF XC WAAP	Trellix Network Security IPS	F5 NGINX App Protect	Azure Sentinel	Defender for Endpoint	PaloAlto Prisma Access
Fortigate	Cloudflare WAF/DDoS	F5 Big-IP IPS	TREND MICRO Deep security	splunk	Crowd strike	Cloudflare Zero Trust
	AWS WAF					
主要なメーカを対象にした境界・サーバ監視				エンドポイント・他へ拡大		

その他、情報漏えい調査・セキュリティ監視・セキュリティ対策・セキュリティ診断など、様々な場に応じたセキュリティに関するサービスを扱っております。お気軽にお問い合わせください。

開発元

三井物産セキュアディレクション株式会社
〒103-0013
東京都中央区日本橋人形町1-14-8
JP水天宮前ビル 6階
TEL: 03-5649-1961
Mail: sales-info@mbsd.jp

製品に関する最新情報はこちらから ⟶ **www.mbsd.jp**

お問い合わせ

MS11-1001-2510