X-SOC for Cybereason

EDR製品導入の際、多発するアラートへの対応が課題となります。
発生したアラートの多くは誤検知・過検知に分類されますが、
専門知識が無いとアラートの分類は困難です。
X-SOC for Cybereasonでは専門のアナリストがお客様に代わり
アラートの分析からその後の対応までを行うサービスです。

検知 (Detection)

SOCアナリスト

- アラート (Malop) 受信
- エンドポイントログ分析
- 推奨対応の提示
- セキュリティインシデント通知連絡
- 発生したインシデントに関する問合せ対応
- 月次レポート (通知履歴)

SOCアナリストがお客様のセキュリティリスクを監視
セキュリティの専門家が、お客様社内で発生したセキュリティリスクを分析し、対処を判断

and

対応 (Response)

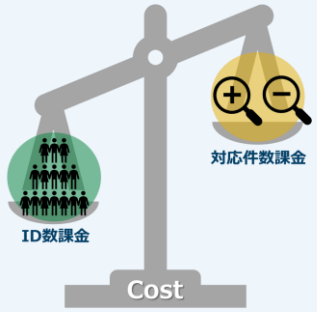
SOCオペレーター

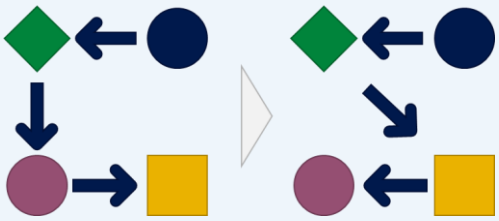
- プロアクティブレスポンス
- 実施したレスポンスに関する問合せ対応
- ポリシー設定変更の受付
- ホワイトリスト/ブラックリスト登録
- チケット管理
- 月次レポート (対応履歴)

SOCオペレーターによるインシデントハンドリング代行
お客様に代わって遠隔からインシデントの対処を実施
本サービスの窓口機能として、ご質問やご依頼に対応

X-SOCの特徴①
対応件数課金による安価な価格設定

- X-SOCは、『ID数課金ではなく』、『**対応件数課金**』です。
  - ✓ アラート件数が少ないお客様に有利
  - ✓ 多層防御を導入されているお客様に有利
- PoCまたは1ヶ月程度の監視運用で、過検知を限りなく減らしてから本番運用に入ります。





X-SOCの特徴②
プロセスのカスタマイズが可能

- お客様の要望に合わせて、インシデント対応プロセスや判断基準をカスタマイズできる部分があります。
  - ✓ 例：初動対応プロセスのカスタマイズ
  - ✓ 例：対処前の判断基準のカスタマイズ

X-SOCの特徴③
柔軟な組合せが可能

- Cybereasonが提供するMDRと組み合わせてのご提供も可能です。お客様のご予算やご要望に応じ最適な組み合わせでご提案致します。
  - ✓ 例：初動対応プロセスのカスタマイズ
  - ✓ 例：対処前の判断基準のカスタマイズ

ライセンス	インシデント検知・分析	インシデントレスポンス
Cybereason EDR/EGAV	Cybereason MDR Complete	
Cybereason EDR/EGAV	Cybereason MDR Essentials	X-SOC for Cybereason (Response)
Cybereason EDR/EGAV	X-SOC for Cybereason (Detection)	X-SOC for Cybereason (Response)

サービス詳細

Cybereason解析サーバーで、セキュリティの脅威を検知

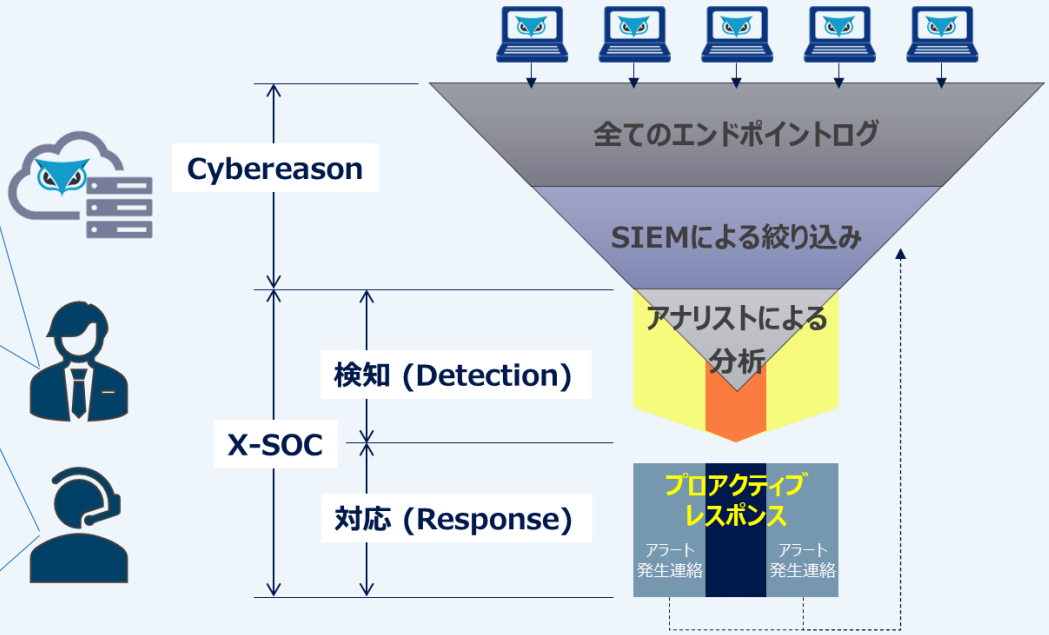
セキュリティ脅威を調査・分析し、対処の要否、Severityを判断

SOCオペレーターに対処を指示

SOCアナリストの指示に基づき、対処を実施

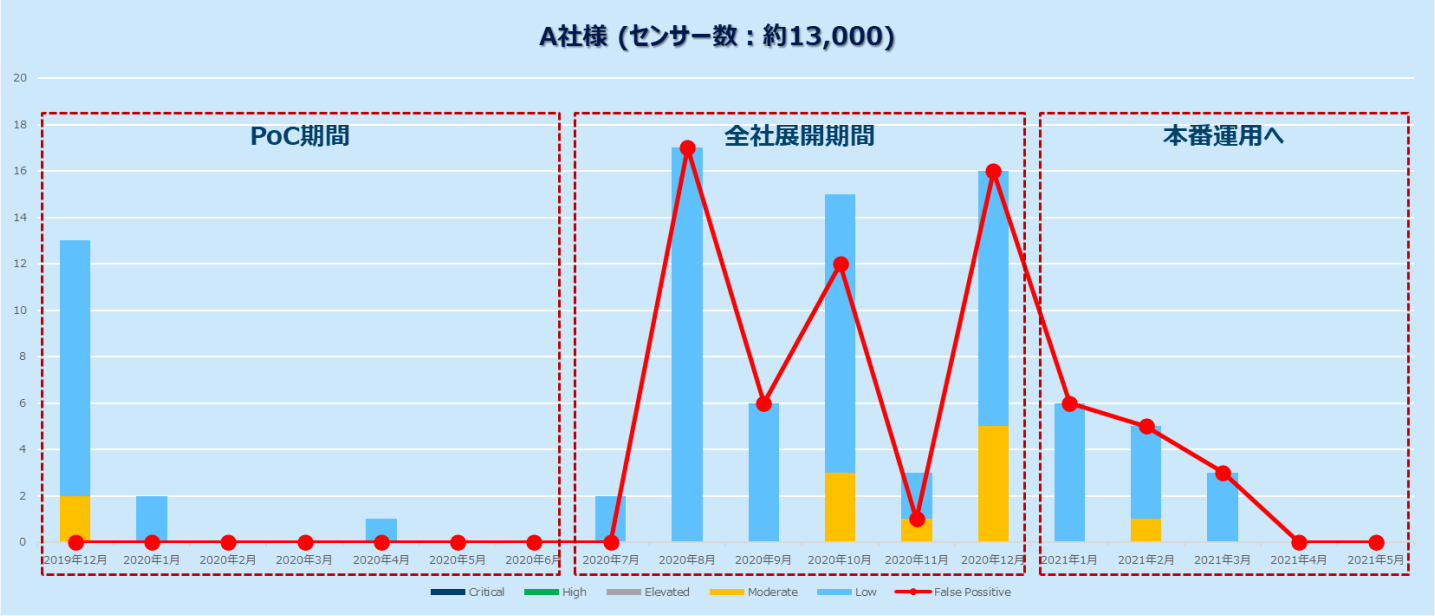
セキュリティインシデントの発生、対処した内容のご連絡

セキュリティインシデントの内容、対応状況をポータルから確認



X-SOCサービスは以下3つのメニューで構成されています。
初　期　作　業：監視モードで運用し、誤検知のホワイトリスト登録を行います。
検知サービス：アナリストが脅威分析し、本当に緊急度の高いものだけを抽出、対応を指示します。
対応サービス：オペレーターがアナリストの指示に応じ、アラート対応や設定変更作業を行います。

アラート発生事例



過検知のチューニング後に本番運用に入ることで、Malop発報が減少するため、対応件数を押さえることができます。
X-SOCサービスではお客様の運用に則したサービスをご提供致します。

サービス価格表

項目	サービス提供価格
サービス初期費用	400,000円
インシデント検知サービス	150,000円/月～

項目	サービス提供価格
インシデント対応基本サービス	100,000円/月
インシデント対応チケット	60,000円/チケット
ポリシー設定変更チケット	40,000円/チケット