Microsoft Copilot for Security

導入・活用支援サービス

インシデント対応、迅速な把握・調査・報告を目指すために。

計画

現在の業務にどのように Copilot for Security を活用するのがよいのか、目標やスコープをお客様と一緒に定義します。

導入

インシデントレスポンスの実践、各種機能の使いこなし方、プロンプトの活用方法、運用自動化の提案など、お客様のニーズに応じた幅広いサポートを提供します。

運用

Copilot for Security の機能追加にあわせた最新情報のご報告や、質問対応などで、お客様のセキュリティ運用を継続的にサポートします。

POINT!

実務ベースで『活用ノウハウ』があります！

ラックは、マイクロソフト社の早期アクセスプログラム（Early Access Program：以下、EAP）に参加し、プロンプトの生成のコツや運用方法など、正式リリース前の段階から活用ノウハウを蓄積してきました。
これらの知見により、経験豊富なエンジニアがお客様の運用・課題にあった活用を支援します。

＼実践レポート！／
Microsoft Copilot for Securityで、インシデント調査をしてみた

※ラックのwebサイトに移動します。

Microsoft Copilot for Security とは

Microsoft Defender XDR などの Microsoft サービスに組み込んで使える、生成 AI を活用したセキュリティソリューションです。インシデントなどの専門的な状況の解説や対処方法の提案、世界的な脅威情報との照合など、セキュリティ担当者の業務を強力にサポートします。

サービス概要

	検証・導入支援	運用支援
概要	試験導入をしたいお客様向けに、導入～初期段階の活用をサポート	年に複数回ある機能追加・変更への対応や運用にあたり生じた 疑問・トラブル対応への支援など、継続的なセキュリティ運用をサポート
支援内容	● PoC の目標 / スコープの定義 ● 各機能の使いこなし方 ● 運用を楽にするプロンプト活用方法 ● Azure Logic Apps などの機能と組み合わせた運用の自動化の提案	● 最新の製品情報についての定期報告 ● テクニカル QA 対応 - QA 対応例その1 - QA 対応例その2 など
想定期間	2か月程度 ※ご要望に合わせ短期での対応も可能です。	1か月～
提供形態	個別契約	月額契約

詳細は、ラックのWebサイトで！

※バナーをクリックすると、ラックのwebサイトに移動します。

株式会社ラック
https://www.lac.co.jp
【問合せ先】
〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー

サポート例

計画 導入

1 何から始めていいか分からない…。

Copilot for Security はライセンス上はすぐに始められますが、しっかりと活用するためにはログの集約などの前準備が大切です。

担当者：Copilot for Securityをはじめたいけれど、どこから手をつければいいかわかりません…。

ラック：どのように活用するのか、目標やスコープを決めていきましょう！
例えば、専門的な知見の補助を目的とした活用ですと、Defender XDRの画面でCopilotによる補助を受けるところから始めることが多いです。さらに、専用ポータルを活用することで、知見の補助の元で詳細な調査がしやすくなります。

担当者：そうなんですね！もっと詳細を聞きたいです。一度打ち合わせをしませんか？

ラック：もちろんです！
課題の明確化から目標・スコープまで、しっかりとサポートいたします！

担当者：しっかりと準備をしてからはじめることで、無駄な期間を削減できました！

導入 運用

2 インシデントの調査が難しい…。

インシデントを調査するためには、まずある程度の専門的な知識をもとにして、本当の事象か誤検知かを判断する必要があります。

担当者：検出されたインシデントの判断が難しく、対応の初動が遅くなってしまっています・・・。

ラック：今回は、不審なログインに関するインシデントですね。こちらで内容を要約してみましたのでご確認ください。

2024/5/31 10:00 に以下のインシデントが発生しました。
インシデント名 Atypical travel
概要
移動不可能な距離からのログイン施行を検知しました。
以下の KQL を実行し、アカウント侵害されていないことを確認してください。

```
SigninLogs
| where …
```

ラック：このようなインシデントに対する調査方法と、今後のために推奨する対策についても、あわせてご提案しますね！

担当者：判断が正確になり、初動までの対応時間もグッと短くできました！

運用

3 次々と新しい情報が追加されて把握が大変！

Copilot for Security は適用範囲は日々広がってきており、連携できるサービスの数も増えています。

担当者：Copilot for Seuciryの新機能が多すぎるし、関連サービスまで把握しきれない…。

ラック：最新の情報をまとめてご報告いたします！

2024 年 5 月 Copilot for Securty 更新情報

- Azure Firewall の統合（プレビュー）
- Azure Web Application Firewall(WAF) の統合（プレビュー）
- Azure Firewall の連携（プレビュー）
- Azure Web Application Firewall(WAF) の連携（プレビュー）
- Microsoft Defender for Cloud との連携（プレビュー）
- セキュリティ管理者の権限拡大
- ……

担当者：面白そうな機能ですね！弊社でもこの機能を活用してみたいので相談できますか？

ラック：承知しました。
御社の運用方法にあわせ、どのように活用するのがベストか、一緒に考えましょう！

一部のサポートから全体的なサポートまで、ご要望に合わせ費用対効果の高い対応策をご提案します。