ヴィジル
セキュリティログ可視化ツール

ヴィジル
セキュリティログ可視化ツールのご提案

PAGEONE DOCUMENT

ご提案

株式会社ページワン
PAGEONE co., ltd.

ヴィジル

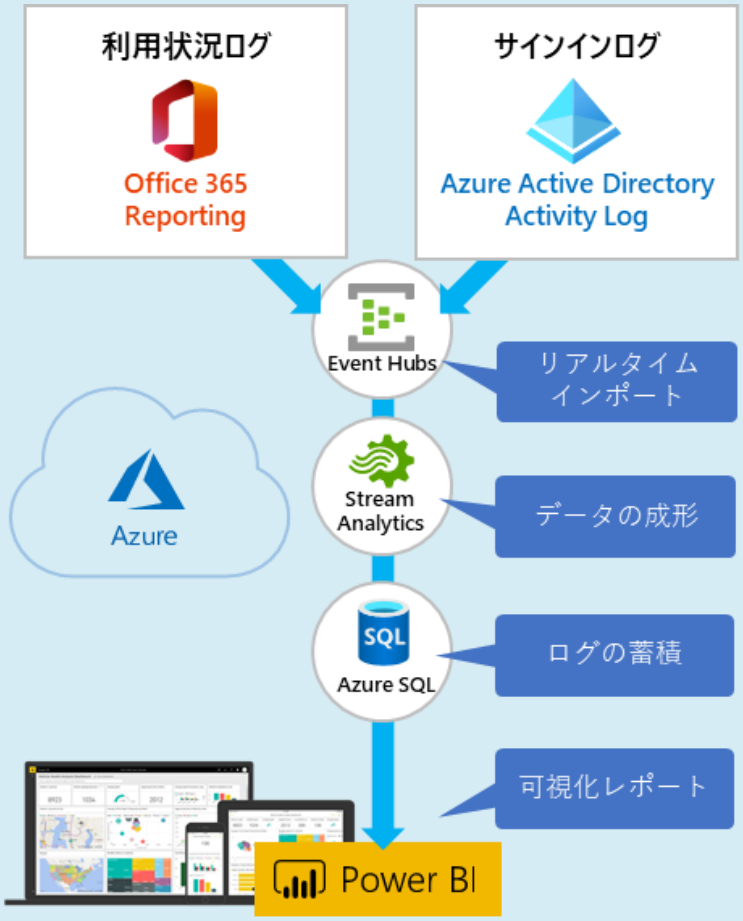
セキュリティログ可視化ツール

スムーズなセキュリティ監視やリスク管理の導入を支援する価値のある可視化レポートをご提供します

Office 365 Reporting や Azure Active Directory Activity Log からは様々なログデータを取得することができますが、出力されたままのログデータを詳細に把握し、リアルタイム性を持って活用するためには専門知識が必要になってしまいます。そこで、株式会社ページワンの可視化ソリューションでは、あらかじめ関連性の高い情報や重要度の高い情報を集約し、可視化されたレポートとして出力できるテンプレートをご用意しております。

Azure ＋ Power BI

ViSLでは Azure のクラウドサービスを利用し、Office 365 アプリケーションの監査ログや、Azure Active Directory のサインインログなどを収集・可視化しています。



Azure
クラウド活用 データ蓄積 → 安全なデータ保守 長期運用

Power BI
効果的な 視覚化ツール → ログの有効活用 社内共有・活用

利用状況 レポート出力 → 運用の改善 ライセンス最適化

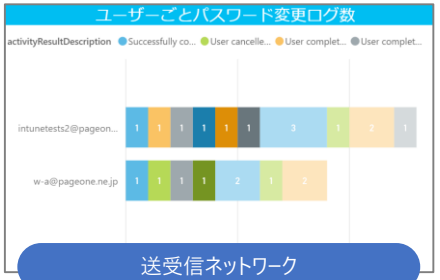
不正利用の監視 形跡確認 → 被害の未然防止 被害拡大阻止

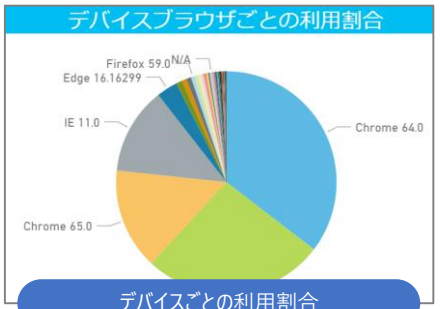
【Azure Active Directory】サインインログ

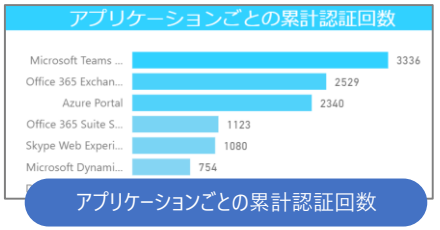
Azure Active Directory

Azure Active Directory アカウントへのサインインや操作のログを収集し、セキュアな運用を支援します。
管理者は、サインインに成功したユーザーはもちろん、失敗やエラーになった操作のログを把握することができ、サインインしたユーザーに紐づけられたIPや端末情報からの不正な形跡はないか、パスワードの総当たり攻撃を受けていないかなど、サービスのセキュアな運用を行う上で最も重要な要素である入り口の監視をサポートします。

日付	UPN	ユーザー表示名	アプリ名	IPアドレス	デバイスOS	デバイスブラウザ	国	都道府県	都市	サインイン成否
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	Application Registration Portal	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Success
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	Azure Portal	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Success
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	Microsoft Office 365 Portal	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Success
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	Office 365 Suite Shell	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Success
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	PowerBIApp	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Failure
2018年4月9日	AAADConnectUser@pageone.ne.jp	AAAD ConnectUser	PowerBIApp	220.109.213.26	Windows 10	Firefox 59.0	Japan	Tokyo	Tokyo	Success
2018年4月9日	crmsrvuser@pageone.ne.jp	CRM Web Service User	Microsoft Dynamics CRM	138.91.17.24	N/A	N/A	Japan	Osaka	Osaka-Wan	Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Azure Portal	220.109.213.26	Windows 10	Edge 16.1629	Japan	Tokyo	Tokyo	Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Dynamics 365 Portal	220.109.213.26	Windows 10	Edge 16.1629	Japan	Tokyo	Tokyo	Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Dynamics CRM Online	220.109.213.26	Windows 10	Edge 16.1629	Japan	Tokyo	Tokyo	Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Microsoft App Access Panel	106.156.15.113	Android 5	Chrome Mobile 65.0	Japan	Aomori		Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Microsoft Dynamics CRM Learning Path	220.109.213.26	Windows 10	Edge 16.1629	Japan	Tokyo	Tokyo	Success
2018年4月9日	c-t@pageone.ne.jp	c-t	Microsoft Invitation Acceptance Portal	106.156.15.113	Android 5	Chrome Mobile 65.0	Japan	Aomori		Success





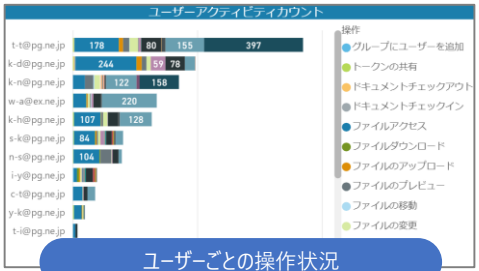


【SharePoint / OneDrive】ファイルアクセス・操作ログ

Office 365

組織内のファイルの共有等に利用されるSharePoint・OneDrive内に保管されたフォルダやファイルへのアクセスと操作を可視化します。管理者は、アクセス頻度や、閲覧・編集・削除、設定の変更といった操作などのログを、ユーザー毎やファイル毎など多角的な視点から追うことができ、不正利用や過剰アクセスなど、SharePoint・OneDrive運用におけるさまざまな潜在リスクの監視をサポートします。

ファイル名の検索



ユーザーごとの操作状況

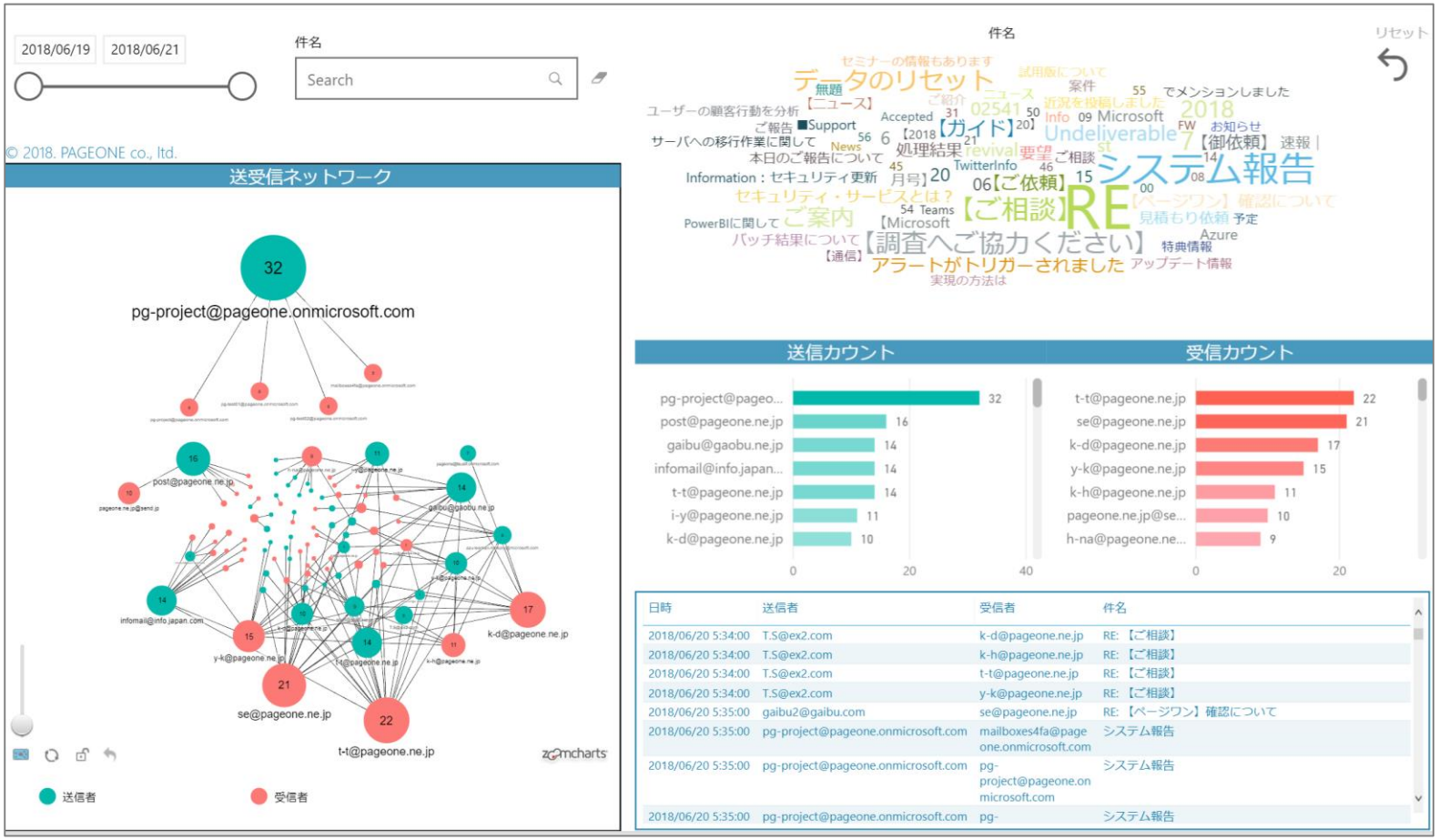
日付	操作	ユーザーID
2018年6月23日	検索クエリの実行	k-d@pg.ne.jp
2018年6月24日	トークンの共有	k-h@pg.ne.jp
2018年6月24日	トークンの共有	s-k@pg.ne.jp
2018年6月24日	ドキュメントチェックイン	k-d@pg.ne.jp
2018年6月24日	ファイルアクセス	k-d@pg.ne.jp
2018年6月24日	ファイルアクセス	k-h@pg.ne.jp
2018年6月24日	ファイルアクセス	s-k@pg.ne.jp

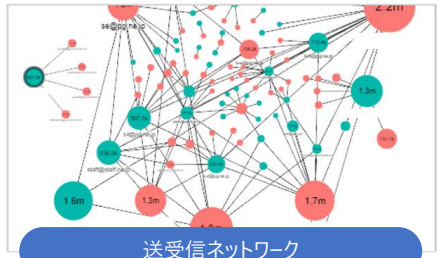
操作履歴

【Exchange Online】メール送受信ログ

Office 365

組織の内外と情報の送受信を行うメールサービスにおける通信履歴のログを分析します。
管理者はユーザーが送受信したメールから送信元、送信先、件数、バイト数、件名傾向などを可視化することができるため、メール送信先に不正なアドレスは含まれていないか、不自然な件数の送受信や、容量の大きすぎる添付ファイルの送受信が無いかなど、組織内外のメール運用におけるさまざまな潜在リスクの監視をサポートします。

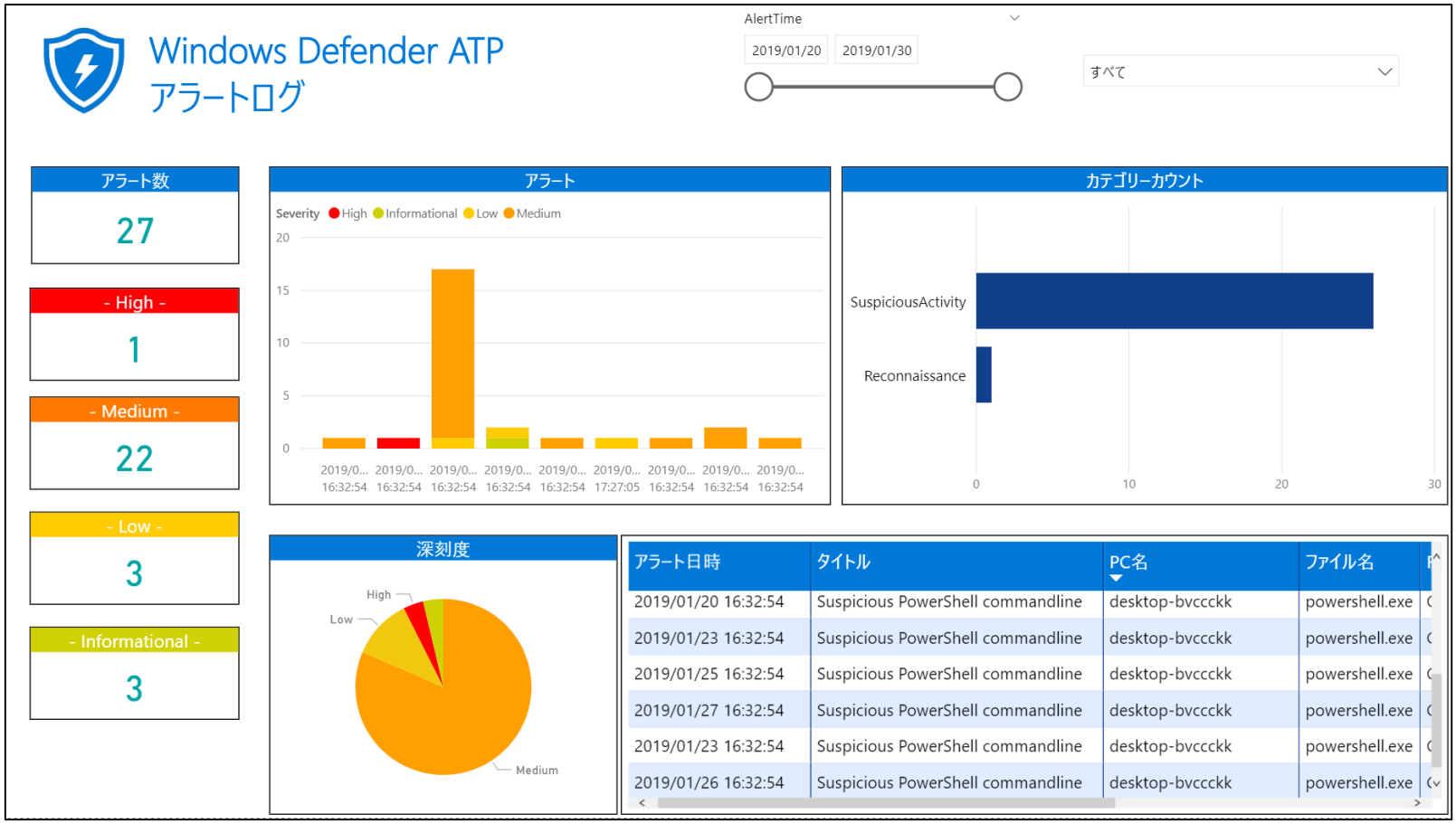


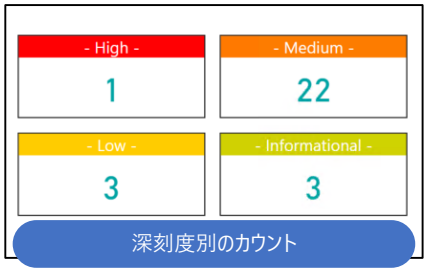


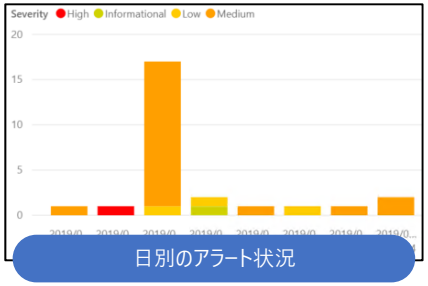
【Windows Defender ATP】アラートログ

Windows Defender ATP

Windows Defender ATPから送信されるアラートを一つのレポートで可視化します。アラートが送信された日時やアラートタイトル、操作したPC名、ユーザー名などの詳細なログを深刻度ごとにフィルタリングすることが可能です。
悪意のある攻撃や疑わしいコマンドの実行、ハッキングやマルウェアの検知などのアラートを可視化することで、組織のセキュリティ監視をサポートします。







※Windows Defender ATP　アラートログレポートはオプション機能となります。

必要ライセンス・サービス

ヴィジルをご利用いただく場合は、以下のライセンスとサービスが必要となります。

■ **Azure Active Directory Premium P1 または P2**
Office365とAzure Active Directoryのサインインやセキュリティのログを収集します。

■ **Power BI Pro**※
収集したログを可視化したレポートの作成を行います。
※文教向けはPower BI Pro for Faculty

■ **Azure Cloud Services**
(Stream Analytics / Event Hub / Log Analytics / Azure Automation / SQL Database)
ログの収集・長期保存を行います。

オプション機能【Windows Defender ATPアラートログ】をご利用の場合は以下のサービスが必要となります。

■ **Windows 10 Enterprise E5 or Education A5または Microsoft 365 E5 or A5**
Windows Defender ATPアラートを収集します。

※各ライセンスとサービスのコンサンプションは期間やログデータの量によって異なります。

株式会社ページワン

PAGEONE co., ltd.

info@pageone.ne.jp　www.pageone.ne.jp

青森本社

〒030-0845 青森県青森市緑 1-5-1

TEL : 017-732-4433　FAX : 017-732-4435

東京支社

〒101-0054 東京都千代田区神田錦町3丁目7番2号
東京堂錦町ビル706

TEL : 03-6403-7989

Google Partner

Microsoft Partner　Gold Cloud Platform

Microsoft

SoftBank PARTNER

ISMS 認証取得
登録事業所：本社

ISO / IEC 27001

ISMS-AC ISMS ISR022