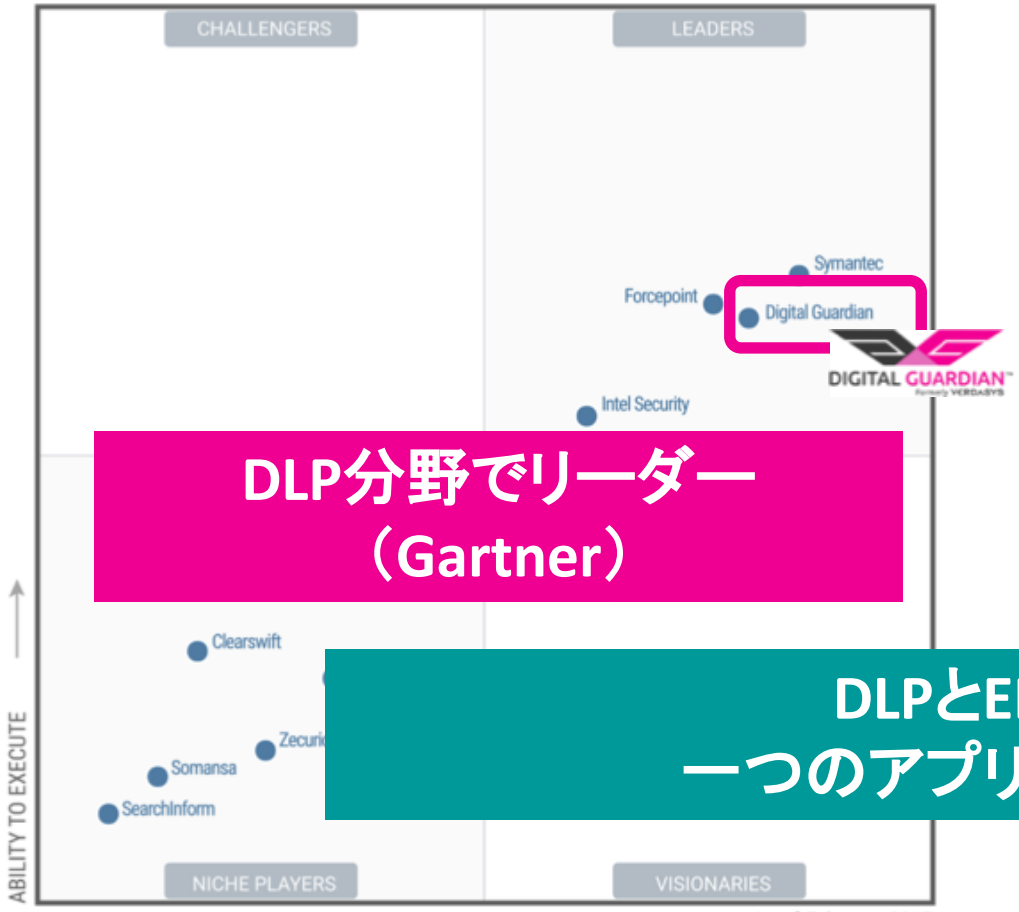
DIGITAL GUARDIAN™
Formerly VERDASYS

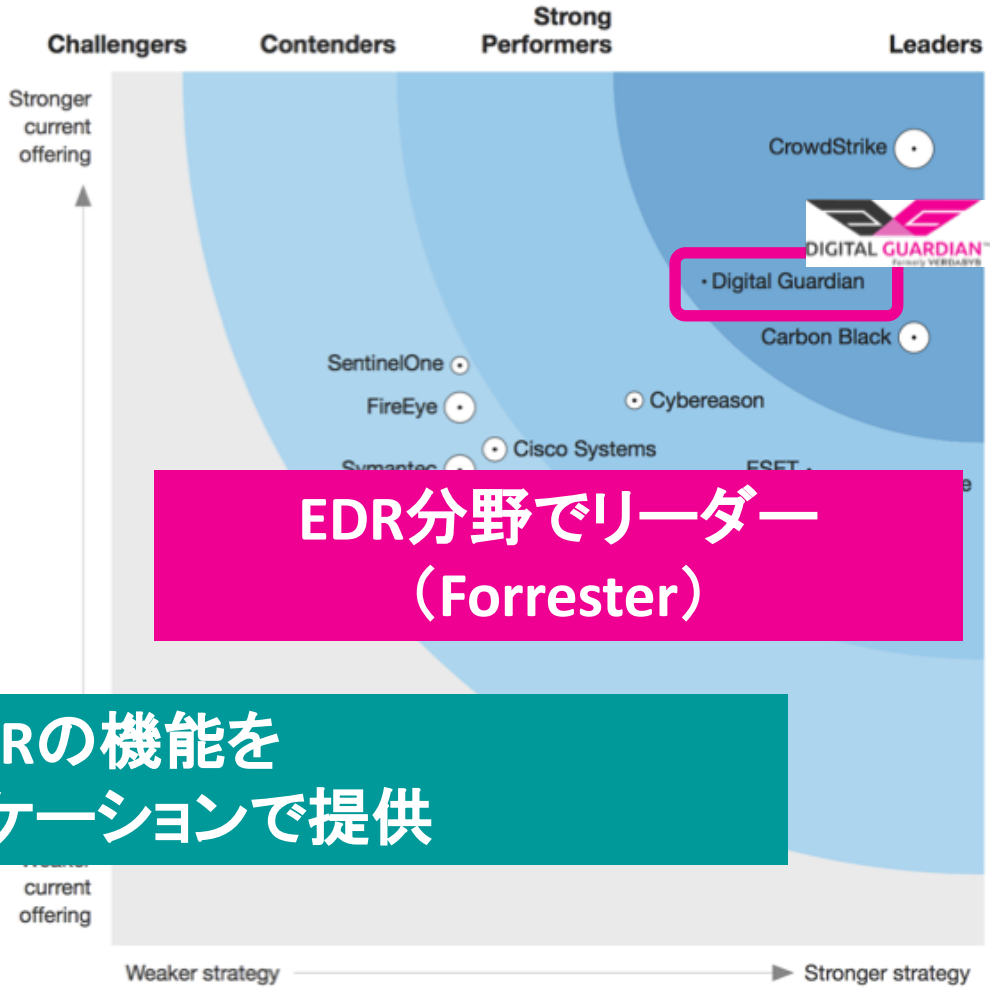
Digital Guardianについて

デジタルガーディアン株式会社
2018年09月04日

DLPとEDRの両方の分野でリーダーに選定された唯一のソリューション



DLP分野でリーダー（Gartner）



EDR分野でリーダー（Forrester）

DLPとEDRの機能を一つのアプリケーションで提供

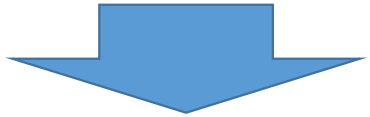
EDR分野にて、DGが評価されたポイント

1. 独自性
   - DLPのテクノロジーをベースにしたEDRソリューション
   - ファイル分析機能により、攻撃者がアクセスしたデータの重要度の判別
2. 先進性
   - AI
     - ユーザーとエンティティの行動分析機能（UEBA）
3. 操作性
   - ビッグデータを前提とした高速で柔軟な分析基盤
     - 柔軟にクエリの作成が可能
     - 高い検知能力
     - 豊富なインシデントレスポンス機能

本日のテーマ

これまでの異常検知における課題

- ✓企業にとっての正常値（ベースライン）が設定できないため、ログから異常値を見つけることができない。
- ✓ルールのチューニングを怠ると、ノイズや過検知が多くなる。
- ✓常に最新の攻撃や不正に対応するには、多くのリソースが必要となる。
  - 攻撃や不正の兆候や漏えい経路の抽出するために、ログの精査
  - 攻撃の兆候を早期に検知するためのルールの作成



コンピューターによる自動学習により、普段と異なるユーザーの行動を検知することで解決します。
（ユーザーとエンティティの行動分析：UEBA）

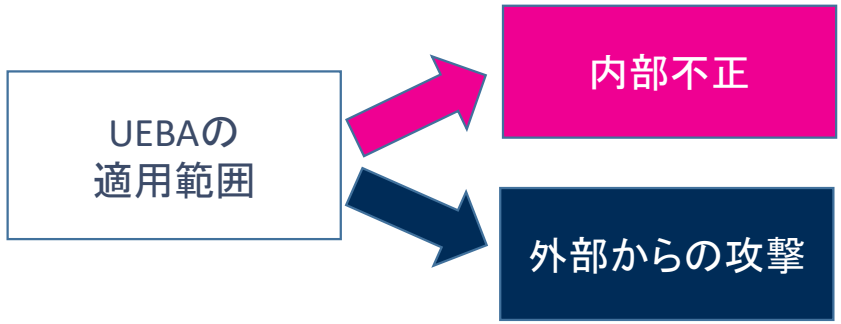
UEBAのメリット

- エンドポイント上のイベントを機械学習し、普段と異なるユーザーの行動を検知します。

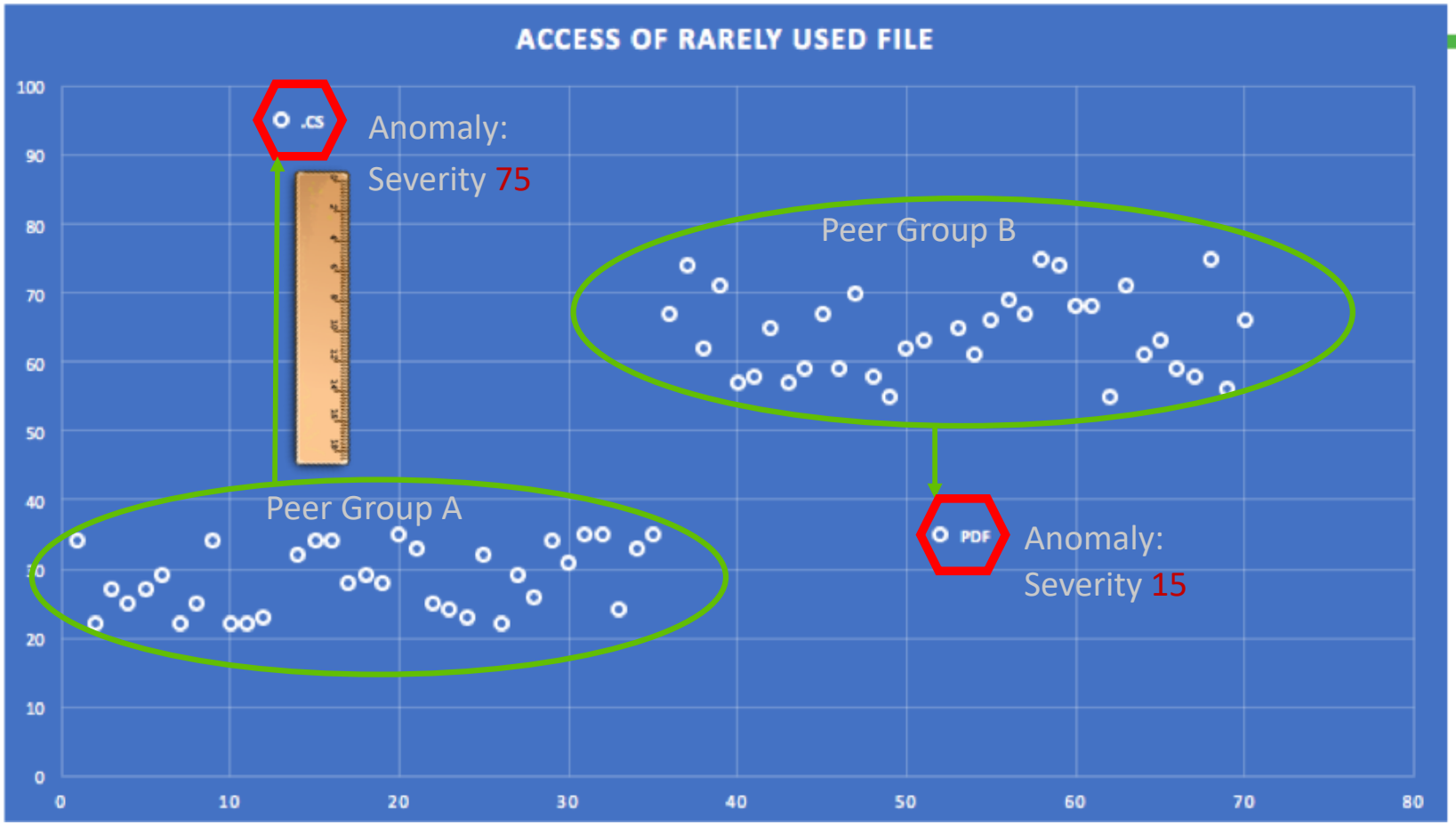
普段と異なるユーザーの行動とは？

- これまでしなかったこと
- 滅多にしないこと
- 普段よりも回数が大幅に多い
- 普段よりも量（サイズ）が大幅に大きい

- UEBAの適用範囲



UEBAのイメージ


ACCESS OF RARELY USED FILE
.cs
Anomaly:
Severity 75
Peer Group B
Peer Group A
PDF
Anomaly:
Severity 15
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80

UEBAで対応可能な内部不正が疑われる行動パターン

1. 未許可のシステムや業務に関係のないシステムへのアクセス
2. 管理者や別のユーザーでログインといった権限の昇格
3. 個人用のアカウントへのメール送信（アップロード含む）
4. 危険な振る舞い
   - 突然、休日出勤する　等
5. 難読化（分かりにくくする）
   - Torブラウザ、普段使わない暗号化ソフトやVPN等
6. セキュリティコントロールの回避
   - 機密データを他のファイルへ貼り付け
   - パスワードのクラッキングアプリケーションの利用
   - セキュリティツールの無効化　等

出典：https://www.darkreading.com/vulnerabilities---threats/insider-threats

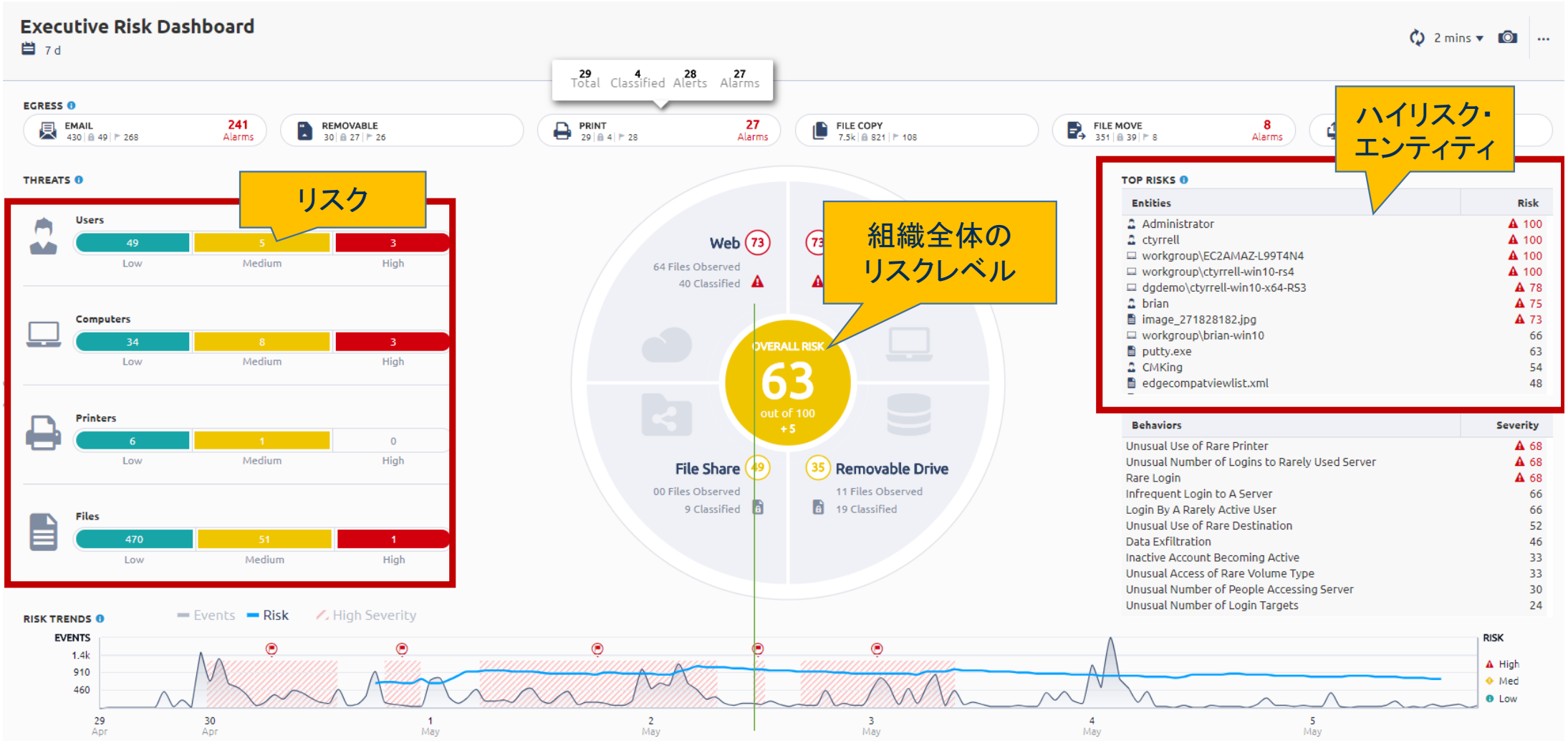
UEBAで対応可能な外部攻撃が疑われる行動パターン例

1. 普段、利用していないアカウントの利用
2. ログイン失敗の回数が通常より多い
3. 普段とは異なるサーバへのアクセスした時間
4. 普段、使わないファイルの種類
5. 普段、アクセスしないサーバ
6. これまで実行されたことのないプロセスの実行
7. 普段、アクセスしないIPアドレス　等

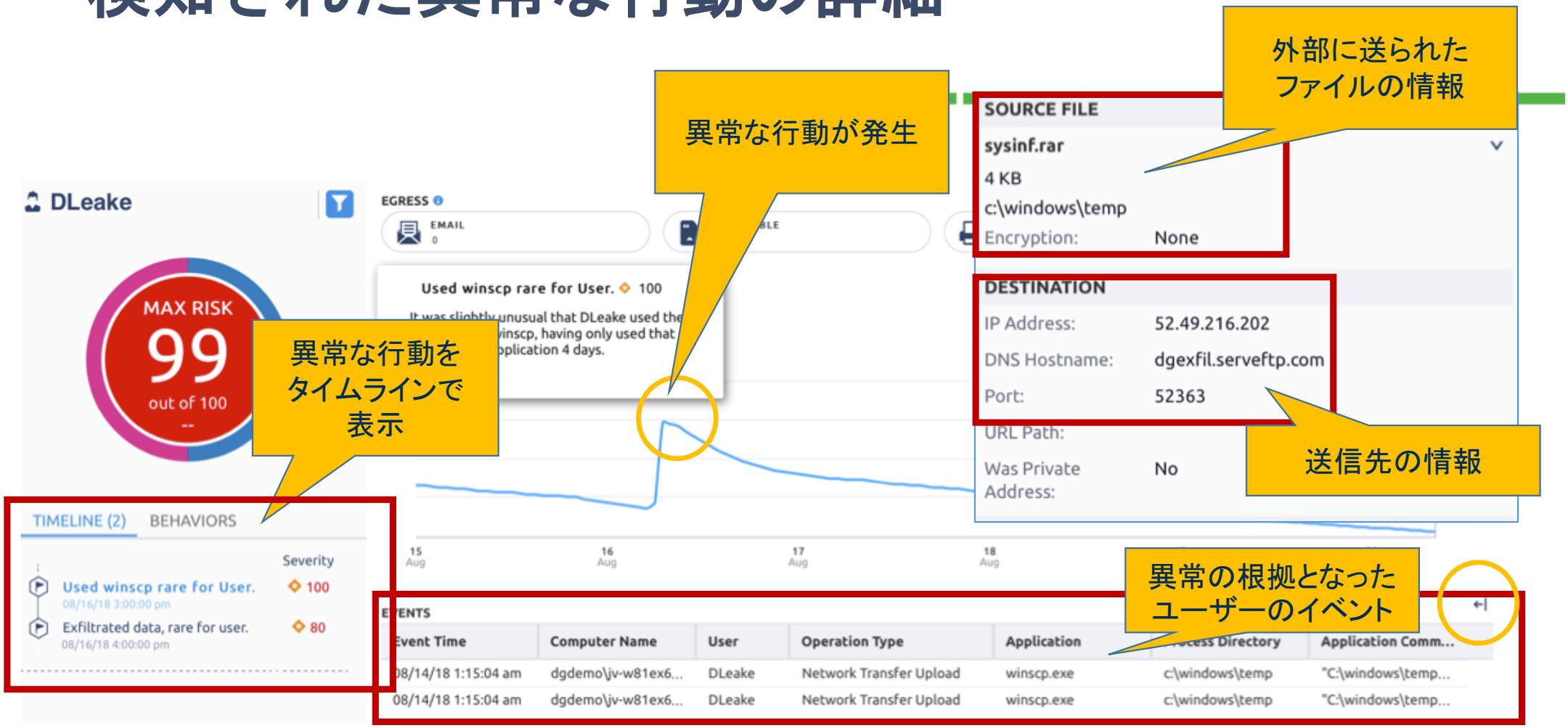
ユーザーの行動分析用ダッシュボード

エンドポイントから来る
すべてのイベントをAIが分析し、
普段と異なる行動から、
リスクの高いユーザー等を特定し、
リアルタイムで表示します。

ユーザーの行動分析用ダッシュボード

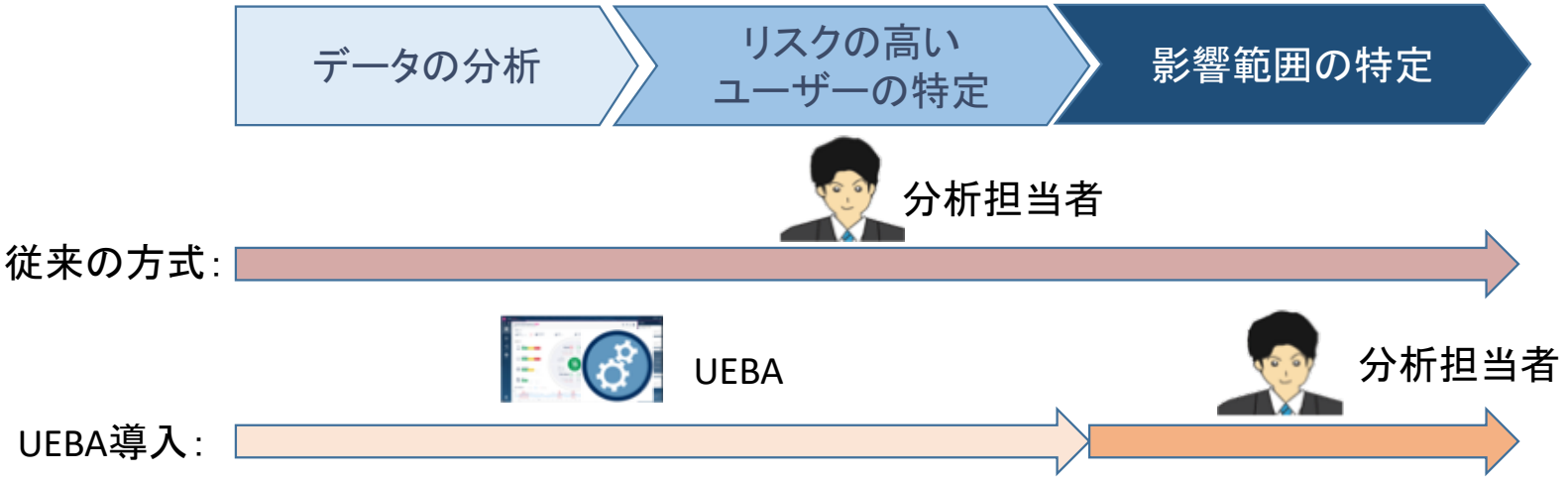


検知された異常な行動の詳細



UEBAの位置付け

- UEBAは、データマイニングの作業の一工程です。
- UEBAにおいて、リスクの高いユーザーやエンティティを特定するということは、「不正の可能性の高さ」を示すだけであり、「不正の行為を断定」するわけではあります。
- 不正の有無の判定は、当該ユーザーやエンティティについて、ログの調査やインタビューを通して行います。



UEBAのメリット

- ✓ データの分析において、サンプリング（もしくは長年の勘）ではなく、全データが対象となる
- ✓ 分析担当者の負担が減る

操作性

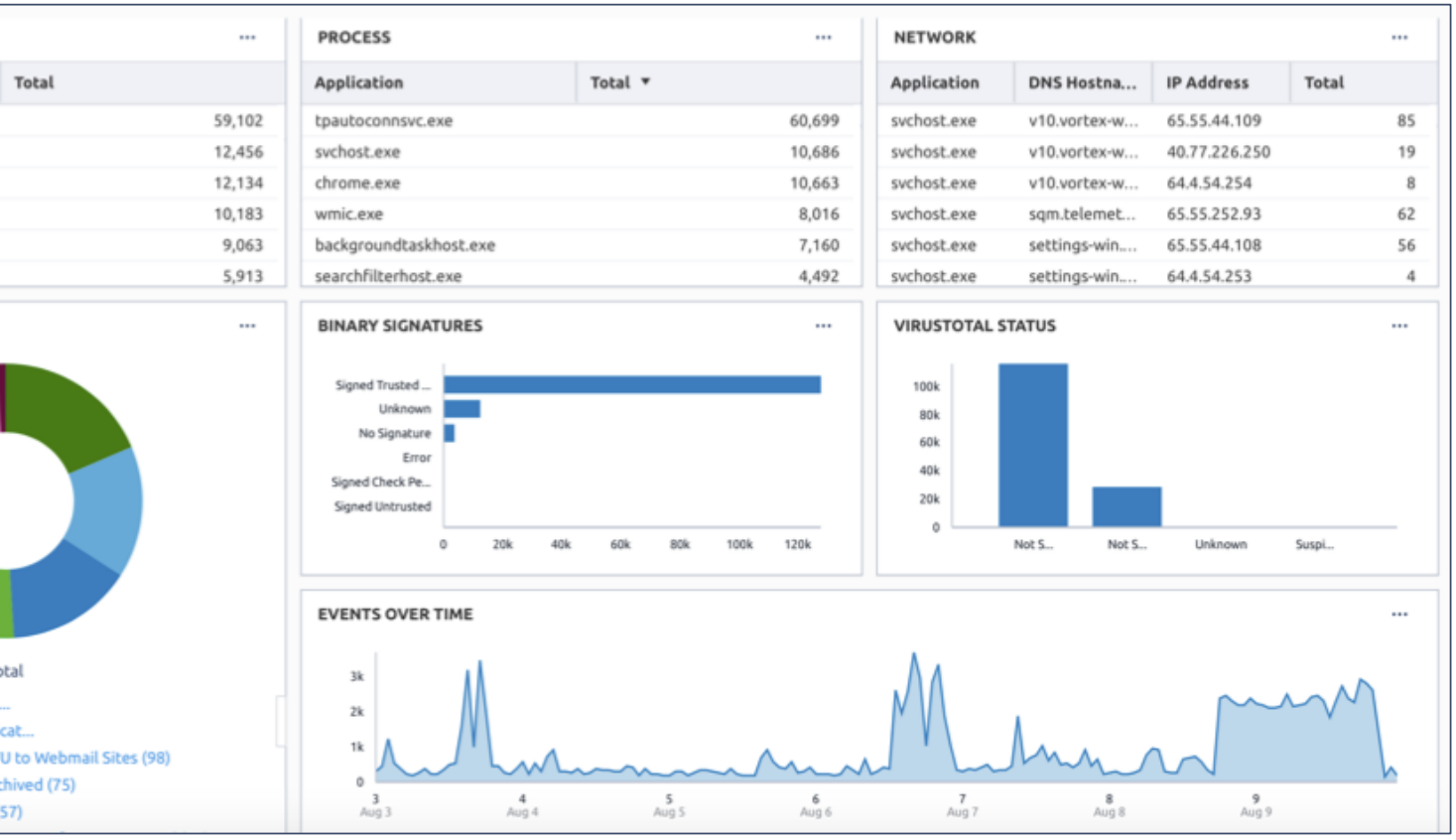
エンドポイントを隔離

- データの分析用サーバから右クリックにより、エンドポイントの操作が可能です。
  - メモリダンプ等のエビデンスの取得
  - エンドポイントのネットワークからの切り離し　等

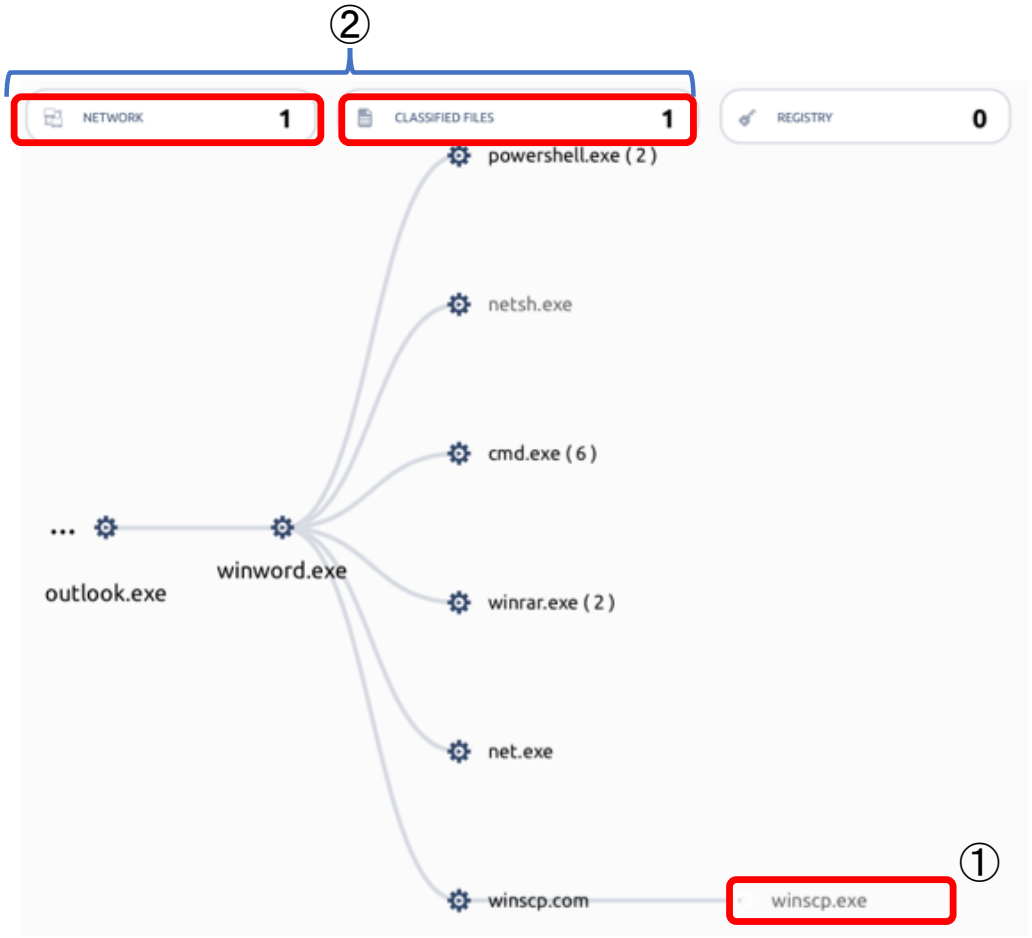
影響範囲の特定

- エンドポイントから取得したイベント情報を素早く解析できる分析用のエンジン（DG ARC）
- 世界的な大企業での実績を積んだ、侵害の有無を正確にかつ素早く分析できるダッシュボード
- サイバーセキュリティの専門家がデザインしたダッシュボードを標準で提供します。
- 別々のイベントから関連性を見出すことが可能
- 攻撃の全体像の把握が可能

影響範囲の特定
～ エンドポイント分析用ダッシュボード ～



プロセスツリー

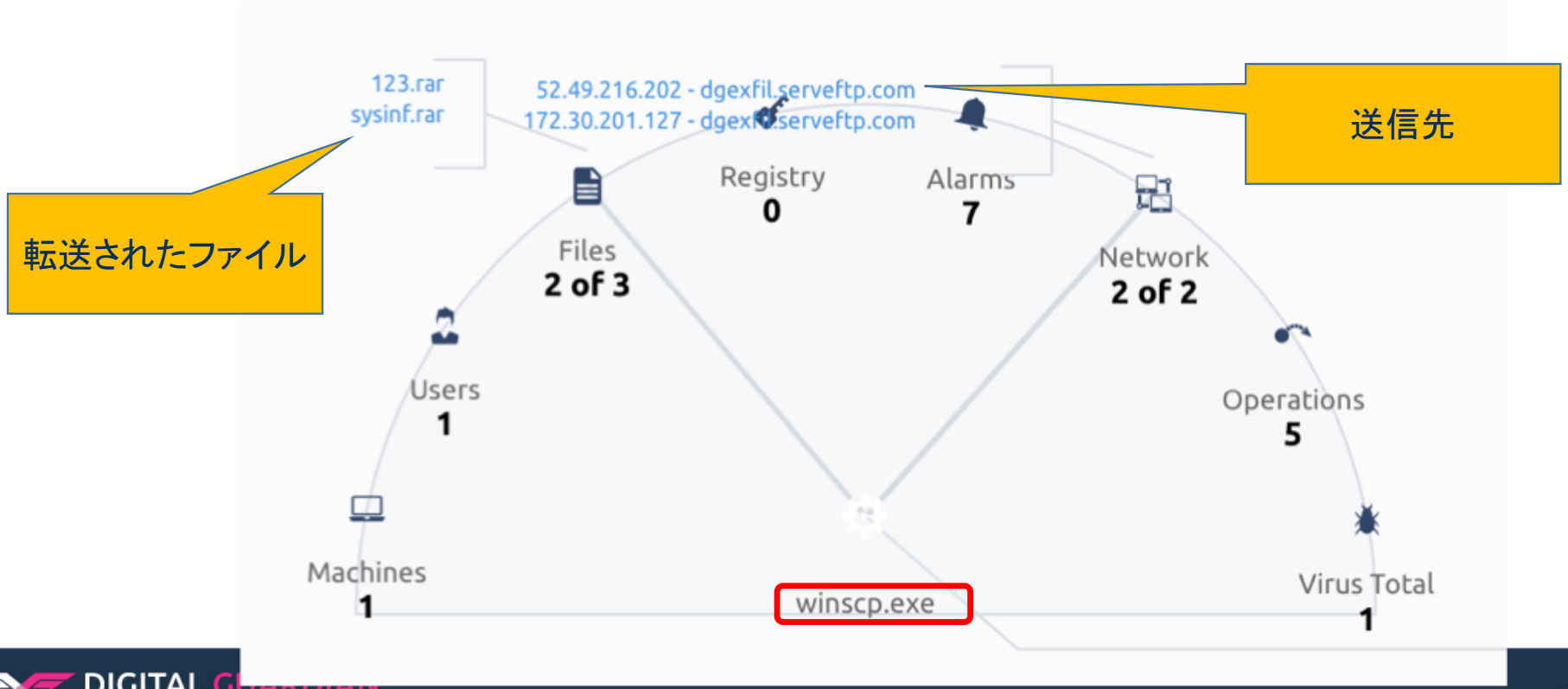


- 左図のプロセスツリーから、winscp.exeは、Outlookに添付されたWordファイルから起動されたことが分かります。
- 本インシデントは外部からの侵入によって発生したと判断できます。

- winscp.exeにフォーカスすると（左図①）、winscp.exeから重要ファイルとネットワークへのアクセスがあったことが分かります（左図②）。
- 次ページでは、winscp.exeを中心に見ていき、winscp.exeがアクセスしたネットワークと重要ファイル等の全体像を捉えます。

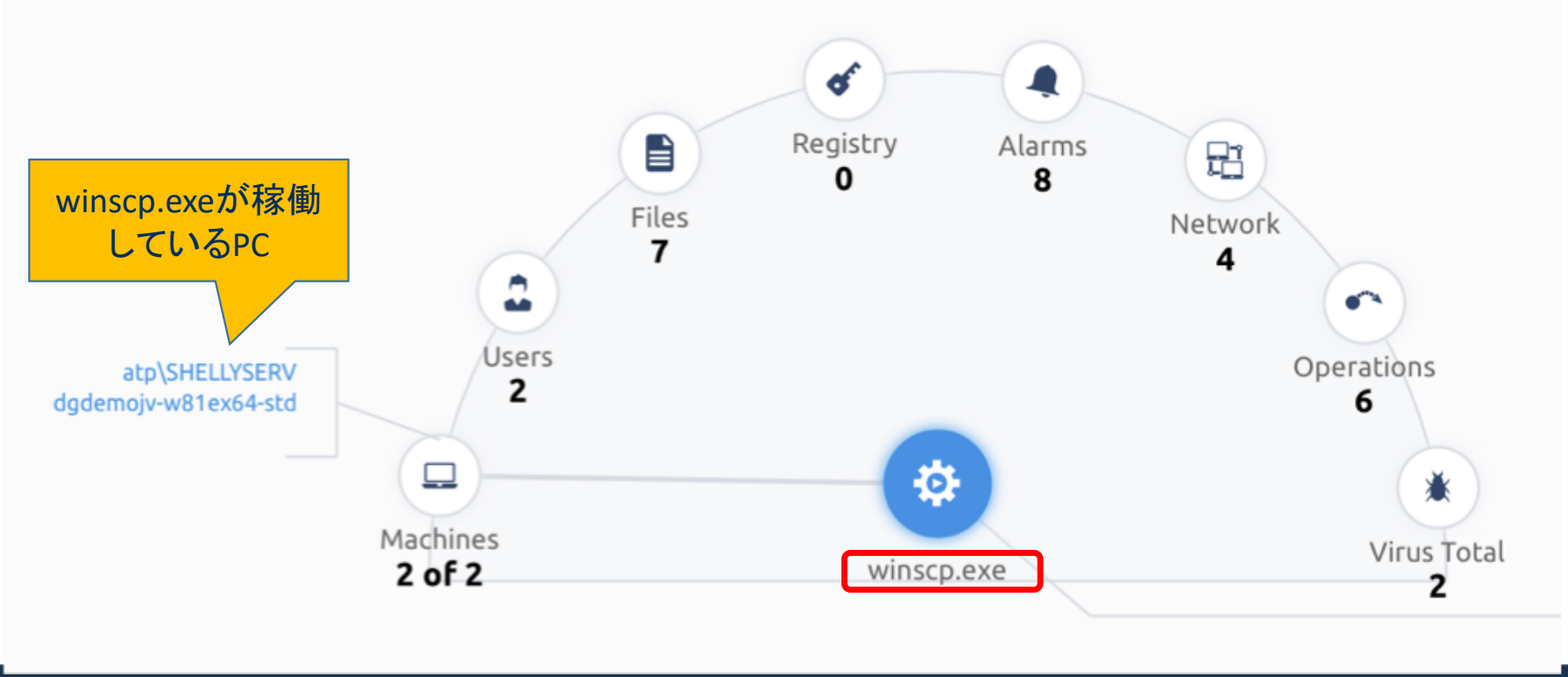
ユーザーと関連情報の多次元分析用ダッシュボード

- ユーザーと特定プロセス（winscp.exe）に絞り込んだ結果です。
- これにより、winscp.exeがアクセスしたファイルや転送先を簡単に取得できます。



ユーザーと関連情報の多次元分析用ダッシュボード

- 特定プロセス（winscp.exe）が稼働しているエンドポイント情報を抽出した結果です。
- winscp.exeが2台のPCで稼働していることが分かります。



Next Generation Data Protection Platform