GREYCORTEX

NTAソリューションの概要

セキュリティギャップ

防止策と境界の防御対策の失敗

＋

（既存製品の）不十分な
ネットワーク可視化機能

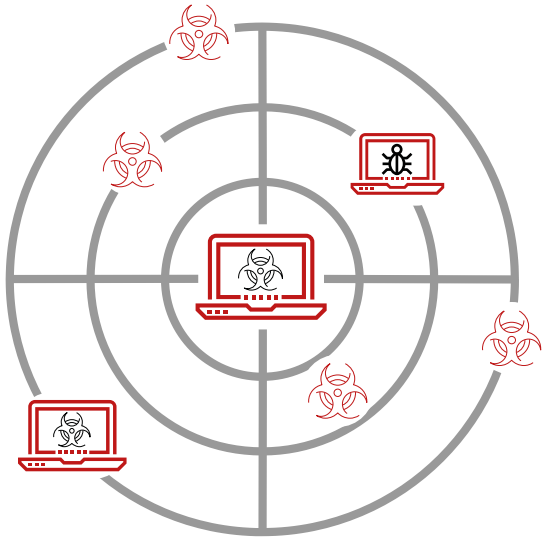
＋

複雑なネットワーク、IoT、BYOD

＋

より高度な脅威がさらに頻繁に発生

→ 攻撃検出の遅れ ＝

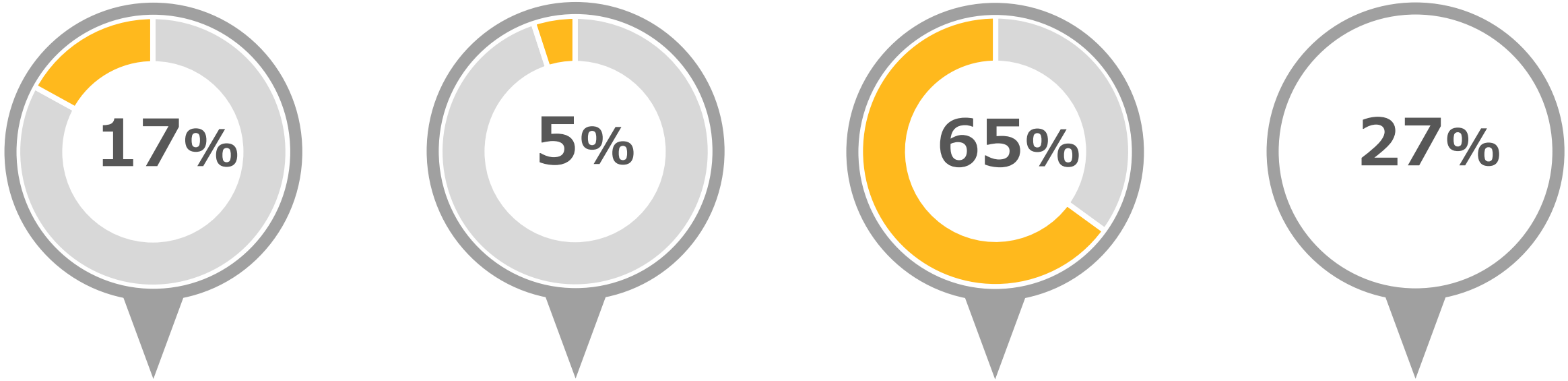


ネットワークへの
侵害

GREYCORTEX

深刻な被害

攻撃による被害は深刻で長期に及び、情報漏えい自体の金銭的被害だけに留まりません。顧客データの損失からの回復に約12カ月かかる場合もあります。*



ブランド価値の喪失　株価の下落　顧客の信頼低下　顧客離れ

被害からの回復には平均 9.3 カ月必要

*Ponemon Institute の調査（2011-2017 年）による

GREYCORTEX

既存ツールでは対応できないケース

IPS（「次世代」を含む） → …未知の脅威や潜在的な脅威

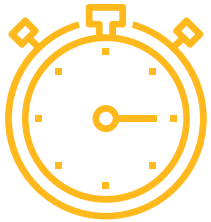
サンドボックス → …遅効性の脅威、その他の攻撃ベクトル

SIEM → …設定の不備、検出不能の場合

NetFlow 収集と分析 → …セキュリティが考慮されていないデータ

エンドポイントセキュリティ → …エンドポイント保護が適用されていないIoT/BYOD

パッチ → …未知の脅威全般（脆弱性が公開されてはじめて適用可能）



49 日

既存ツールのみで検出する場合の平均所要時間*

*2017 Trustwave Global Security Report –修復に必要な時間を除く

GREYCORTEX

GartnerのNTAに関する解釈

= 統計分析、**機械学習**、**人工知能**、メタデータ、およびコンテンツ検査によるネットワーク上の疑わしい活動の検出

≠ NetFlow分析、フルパケットキャプチャ

検出されないマルウェア

内部人員による脅威

フォレンジック

ネットワークの可視化

迅速な検出と対応

セキュリティオペレーションセンター

脅威の特定を可能にするトラフィックを検知し、
検出能力やセキュリティ対策の品質を
効果的に改善

GREYCORTEX

GREYCORTEX MENDEL

隠れた脅威の検出

全面的なネットワーク可視性

AI、機械学習、ビッグデータ + シグネチャベースの検出 + DB

的確な行動　リスクの低減　損害の軽減

コスト削減

GREYCORTEX

短期間でメリットを実感

検出の能力の向上

1分～6時間
検出の平均所要時間

導入が容易

30～60分
MENDEL導入の平均所要時間

パフォーマンス監視
ネットワークの可視化

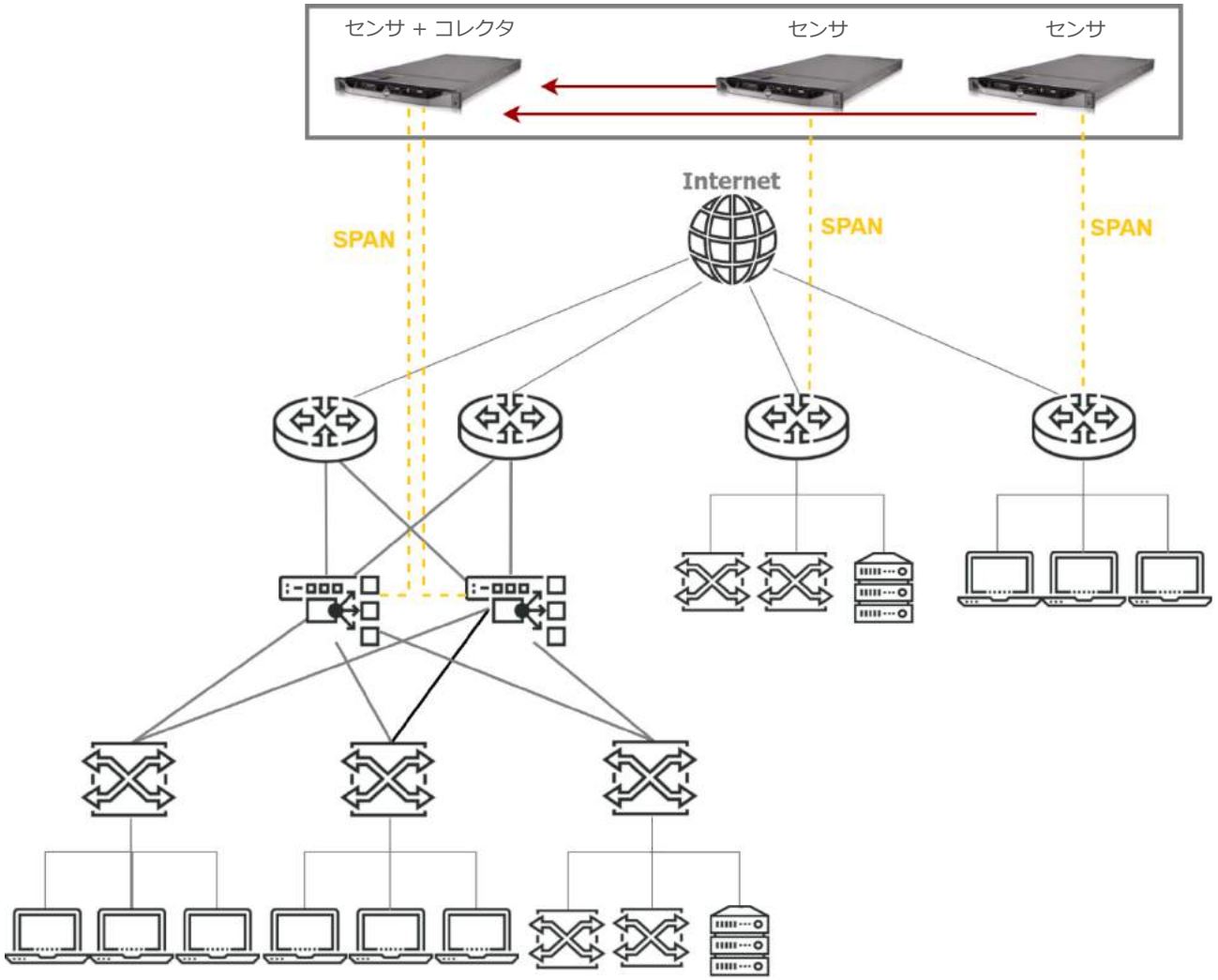
ネットワークの依存性
過剰な通信
新しいデバイス
脆弱なアプリケーション

直感的なインターフェース

イベントのフィルタリング機能
表示を詳細にカスタマイズ可能
検出が容易

GREYCORTEX

導入



センサ

ASNM 出力 (トラフィックの 0.5%～1%に相当)

100Mbps ～ 10Gbps
(40Gbps は 2018年第2四半期に提供予定)

コレクタ

ASNM 入力

1 コレクタ = 最大 50 センサ

40Gbps以上の集約された入力

イベントコレクタは10以上のコレクタを
クラスタ化したもの

アプライアンス

パッシブ

オンプレミス

HW または仮想配備

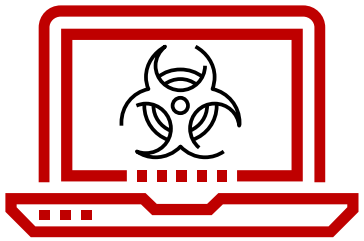
GREYCORTEX

ユースケースの紹介

1. 感染したデバイスおよびユーザ
2. 従業員による不注意
3. 機密情報資産の保護
4. フォレンジックおよび根本原因分析

GREYCORTEX

ユースケース① 感染したデバイスやユーザ



ネットワーク全体であらゆる攻撃段階の未知の脅威を検出。タイムリーに検出できなければ、以下のような被害が生じる可能性があります。

- 機密情報 (顧客データ、ノウハウ) の漏えい
- 組織への攻撃

検出例

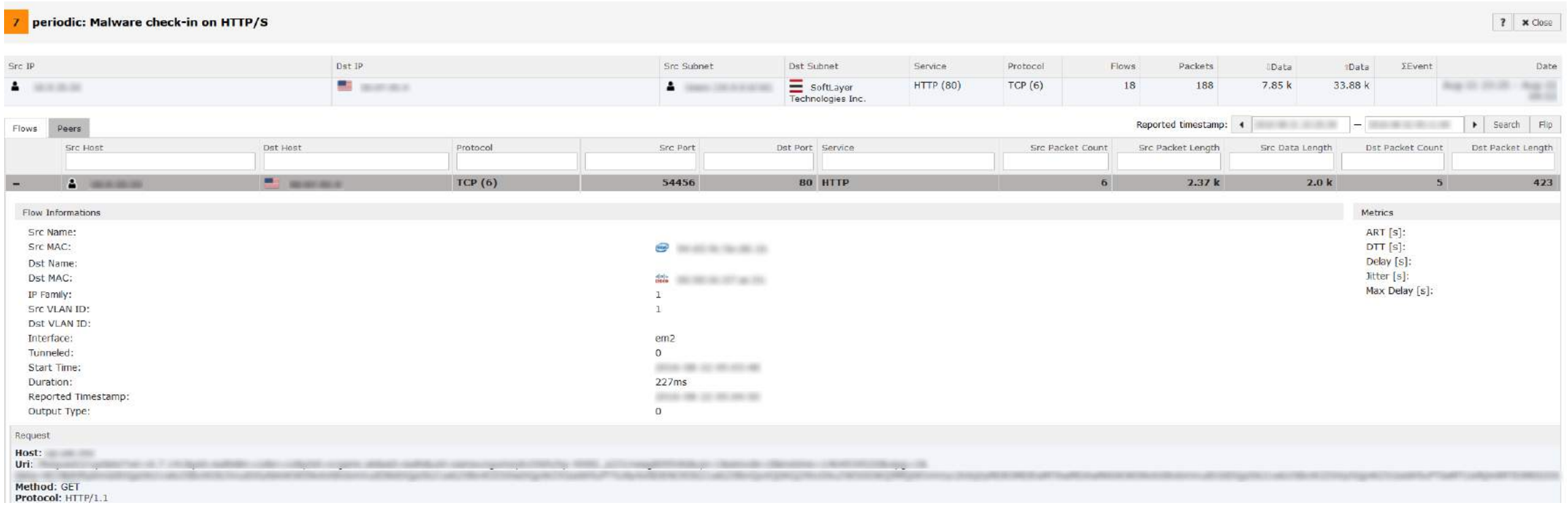
- ネットワークの偵察
- ボットネット通信
- 情報漏えい
- 通信の異常
- ファイアウォール、IPS、エンドポイント保護などで検出されなかった脅威

その他、標的型攻撃や標的型脅威、
リモートアクセス型トロイの木馬、
アクティブなボットネット、
BYODまたはIoTデバイス上のマルウェア
などの兆候

GREYCORTEX

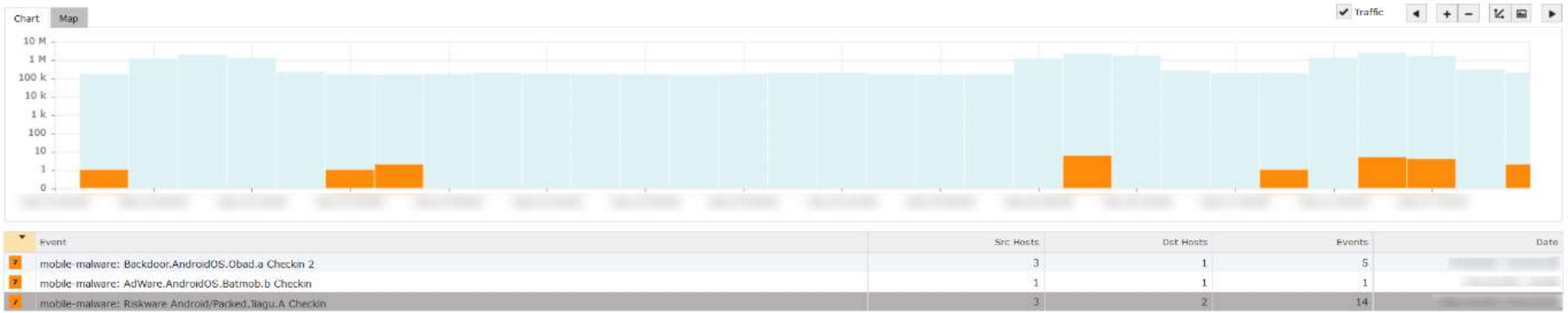
定期的な通信の検知

正規なはずのIPアドレスとの定期的な通信があり、ネットワークメタデータが異常だと判断されました。このケースでは、ユーザが未知のマルウェアが含まれるソフトウェアをインストールしていました。



モバイルデバイス上のマルウェア

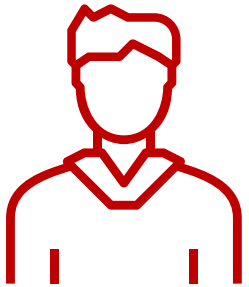
トロイの木馬やバックドアなどのマルウェアがモバイルデバイスに存在したケースです。



Event	Src Hosts	Dst Hosts	Events	Date
mobile-malware: Backdoor.AndroidOS.Obad.a Checkin 2	3	1	5	
mobile-malware: AdWare.AndroidOS.Batmob.b Checkin	1	1	1	
mobile-malware: Riskware Android/Packed.Jiagu.A Checkin	3	2	14	

GREYCORTEX

ユースケース② 従業員の不注意



従業員の過失（故意のケースもある）により、ポリシー違反が発生する場合があります。その結果、攻撃のリスクが高まると同時に、最悪、以下のような事態をもたらす可能性があります。

- 機密情報 (顧客データ、ノウハウ) の漏えい
- 別の組織への攻撃
- コンプライアンスに関わる問題

検出例

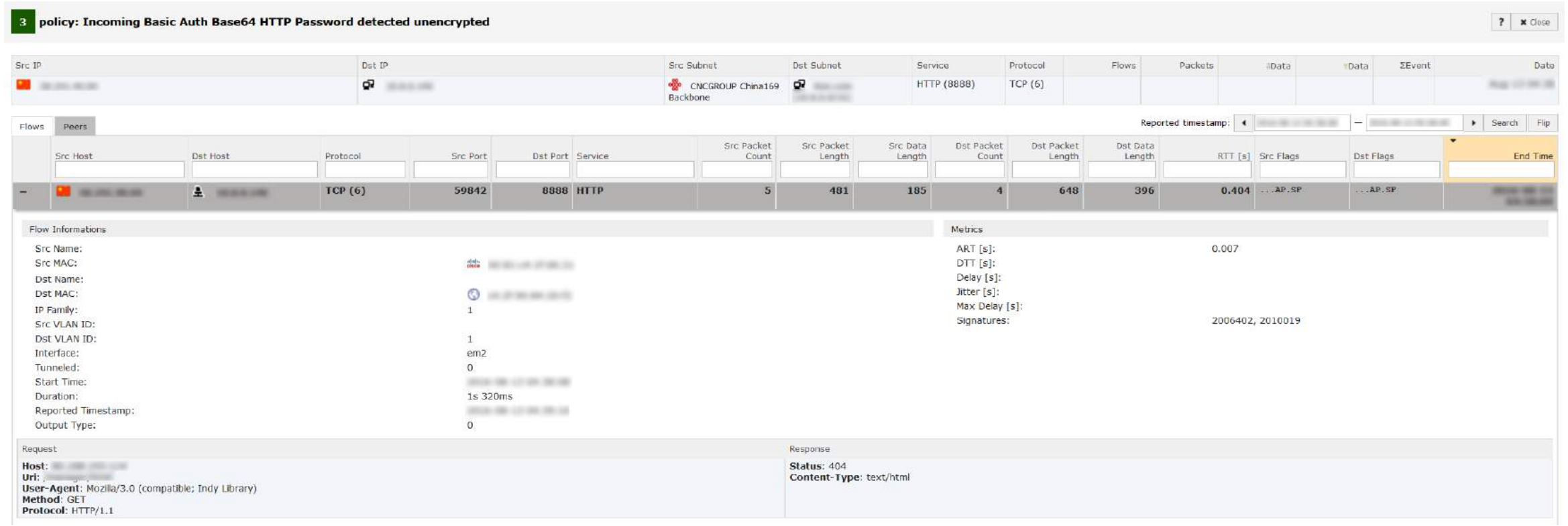
- 平文パスワードの使用
- デバイスやサービスの設定の誤り
- 感染したBYOD
- TorやP2Pなどの通信
- 脆弱性のあるSWバージョンの使用
- 外部パブリックストレージの使用
- 内部ポリシー違反
- 不正な通信

その他のさまざまなネットワーク設定エラーやポリシー違反

GREYCORTEX

ポリシー違反

暗号化されていないHTTPサービスを使った無防備なネットワークデバイス管理を行っていた組織が、中国からの不正アクセスの標的になりました。



3 policy: Incoming Basic Auth Base64 HTTP Password detected unencrypted

? ✖ Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	↑Data	↓Data	ΣEvent	Date
[redacted]	[redacted]	CNCGROUP China169 Backbone	[redacted]	HTTP (8888)	TCP (6)						[redacted]

Flows | Peers

Reported timestamp: [redacted] — [redacted] Search Flip

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	RTT [s]	Src Flags	Dst Flags	End Time
–	[redacted]	[redacted]	TCP (6)	59842	8888	HTTP	5	481	185	4	648	396	0.404	...AP.SP	...AP.SP	[redacted]

Flow Informations

Src Name:	
Src MAC:	[redacted]
Dst Name:	
Dst MAC:	[redacted]
IP Family:	1
Src VLAN ID:	
Dst VLAN ID:	1
Interface:	em2
Tunneled:	0
Start Time:	[redacted]
Duration:	1s 320ms
Reported Timestamp:	[redacted]
Output Type:	0

Metrics

ART [s]:	0.007
DTT [s]:	
Delay [s]:	
Jitter [s]:	
Max Delay [s]:	
Signatures:	2006402, 2010019

Request

Host: [redacted]
Uri: [redacted]
User-Agent: Mozilla/3.0 (compatible; Indy Library)
Method: GET
Protocol: HTTP/1.1

Response

Status: 404
Content-Type: text/html

GREYCORTEX

ユースケース③ 機密資産の保護

MENDELは、ビジネス上重要な資産や機密度の高い資産を優先的に保護します。また、そのための特別なポリシーを設定することも可能です。

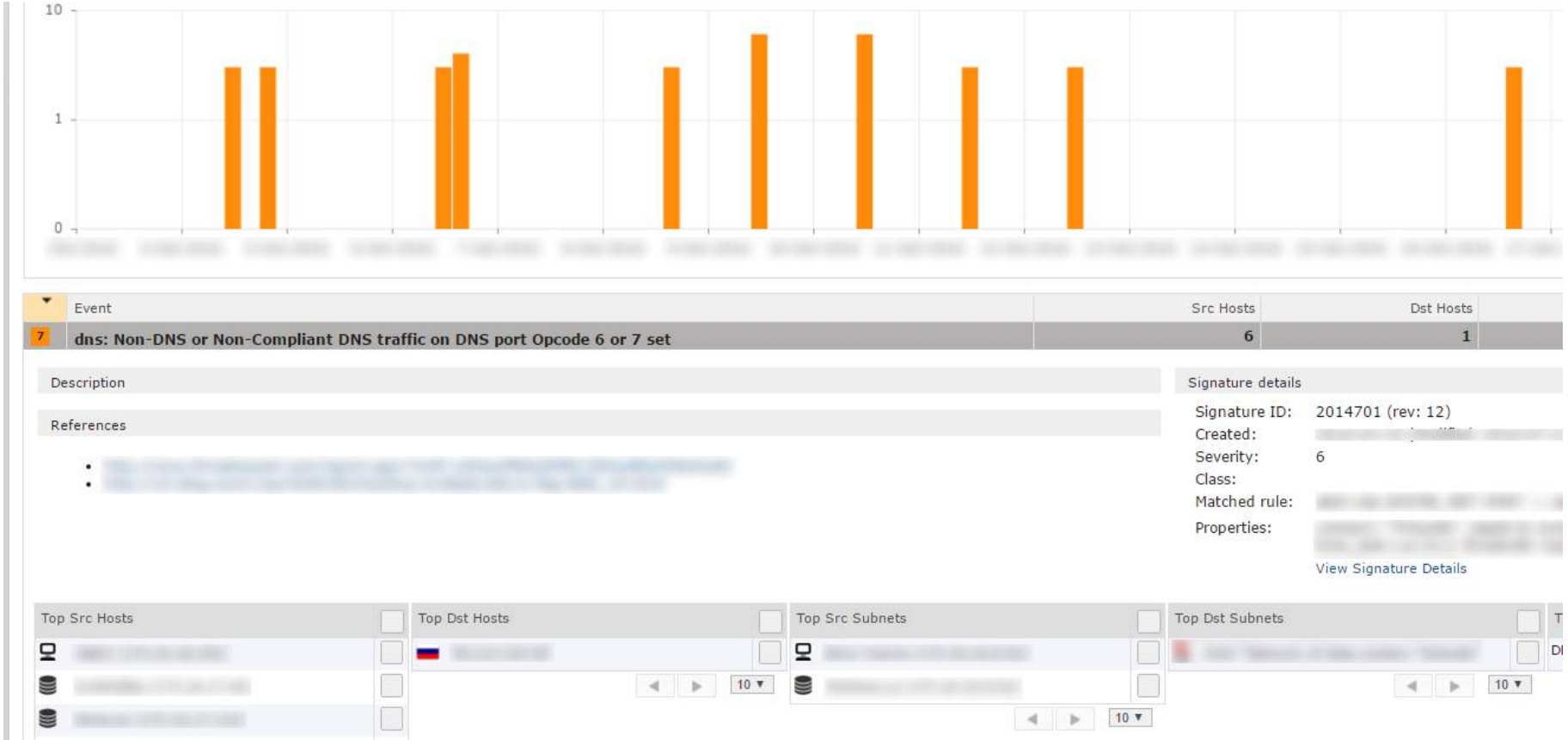
検出例

- ポリシー違反
- 通信の監査
- 情報漏えい
- 通信の異常

GREYCORTEX

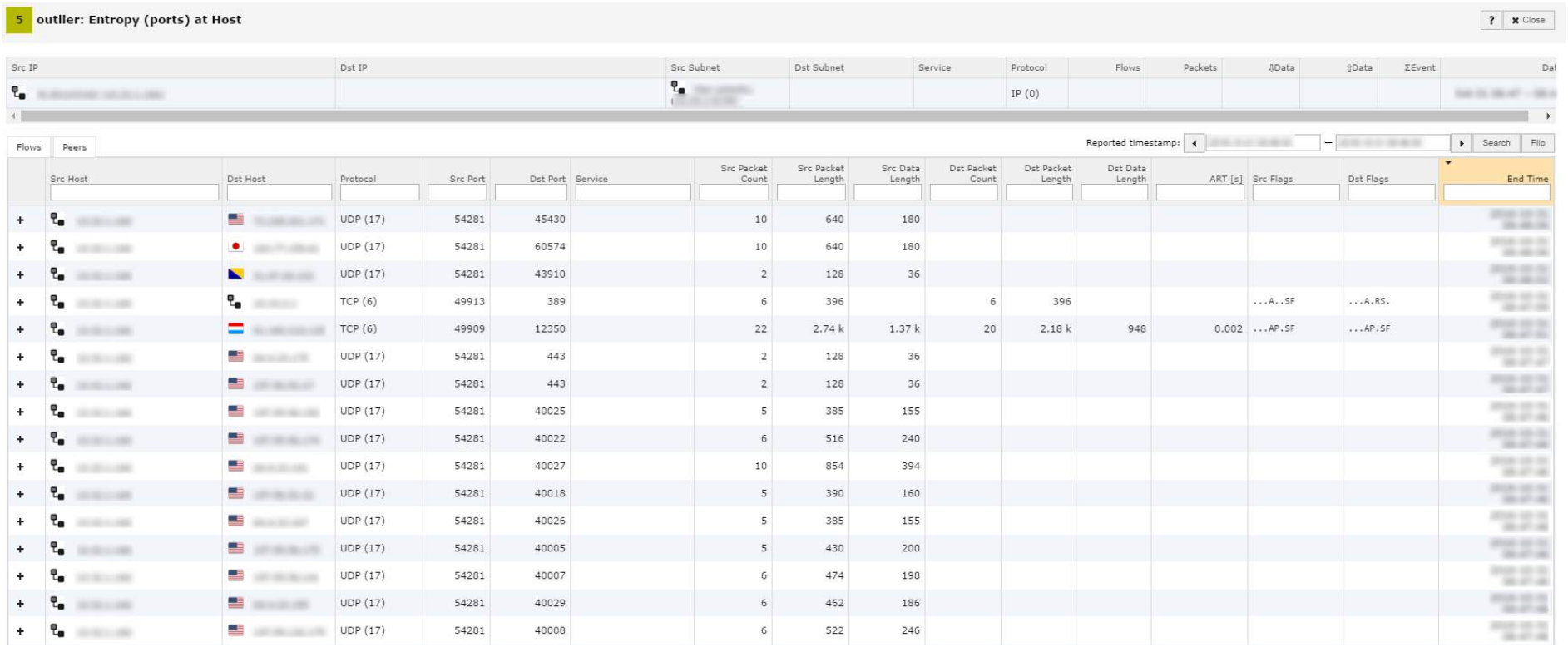
DNSトンネル

地理的に見て異常なIP アドレス (ロシア) へのDNSトンネルが存在し、当該デバイスから、DNSプロトコルに対応しないデータが異常に大量に漏えいしていました。



過剰な通信

通常、1~8個のネットワークサービス経由で通信しているデバイスが、39ものサービス経由で、日本を含む世界中の120ものデバイス（ブラジル、セルビア、ボスニア・ヘルツェゴビナ、米国、シンガポールなど）との通信を試みています。



5 outlier: Entropy (ports) at Host

? ✖ Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	⇩Data	⇧Data	ΣEvent	Dat
[redacted]		[redacted]			IP (0)						[redacted]

Flows | Peers

Reported timestamp: [redacted] – [redacted] Search Flip

	Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	ART [s]	Src Flags	Dst Flags	End Time
+	[redacted]	[redacted]	UDP (17)	54281	45430		10	640	180							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	60574		10	640	180							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	43910		2	128	36							[redacted]
+	[redacted]	[redacted]	TCP (6)	49913	389		6	396		6	396			...A..SF	...A.RS.	[redacted]
+	[redacted]	[redacted]	TCP (6)	49909	12350		22	2.74 k	1.37 k	20	2.18 k	948	0.002	...AP.SF	...AP.SF	[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	443		2	128	36							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	443		2	128	36							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40025		5	385	155							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40022		6	516	240							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40027		10	854	394							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40018		5	390	160							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40026		5	385	155							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40005		5	430	200							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40007		6	474	198							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40029		6	462	186							[redacted]
+	[redacted]	[redacted]	UDP (17)	54281	40008		6	522	246							[redacted]

GREYCORTEX

ユースケース④ フォレンジック／根本原因分析

MENDELは数カ月分のネットワークトラフィックメタデータを記録・保存し、さまざまな問題の根本原因分析のために、詳細な情報を瞬時に提供します。

この情報を利用することで、事前に対策を講じ、ネットワークやその他の重要サービスにおける問題や中断の長期化を回避し、ダウンタイムを最小化できます。

可視化の例

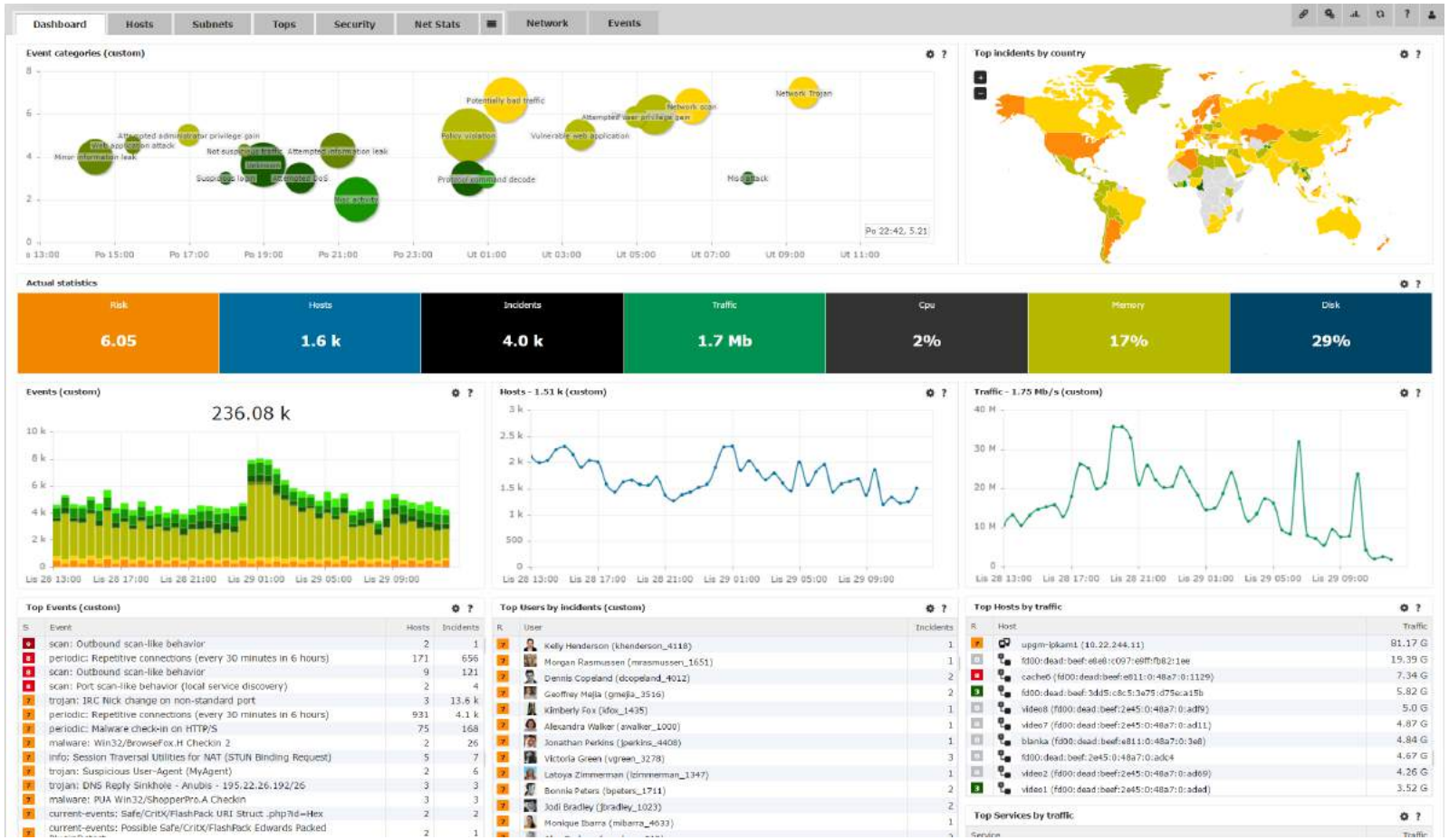
- デバイスの通信
- 通信パートナー
- デバイスやサービスへの接続問題
- パフォーマンス異常
- 通信のメタデータ

その他の情報もクリック数回で可視化が可能

GREYCORTEX

ネットワーク可視化するMENDEL

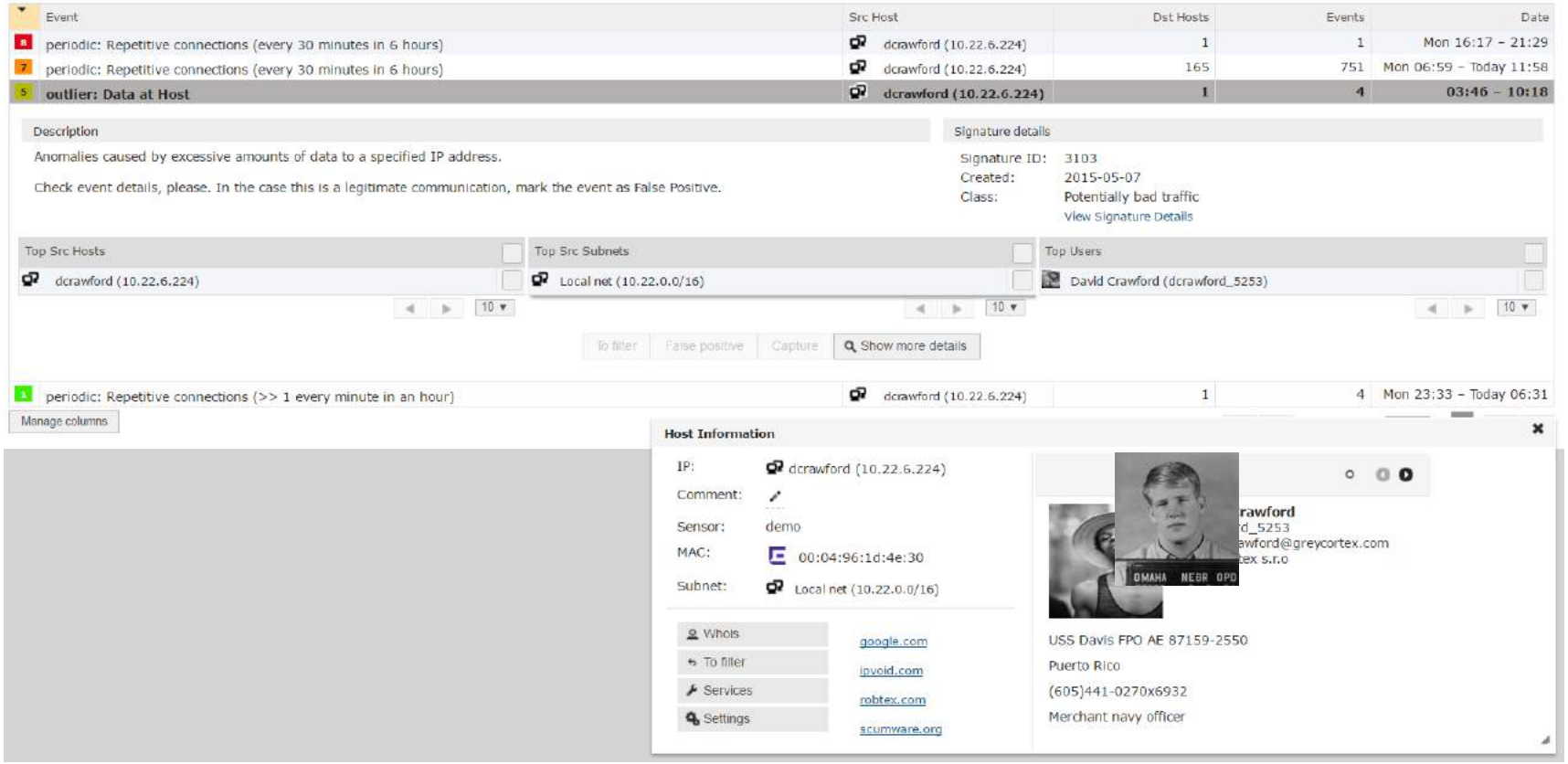
ユーザが設定したダッシュボード上で、ネットワークや主なセキュリティ上・運用上問題となる情報に迅速にアクセスできます。（情報はカスタム可能）



GREYCORTEX

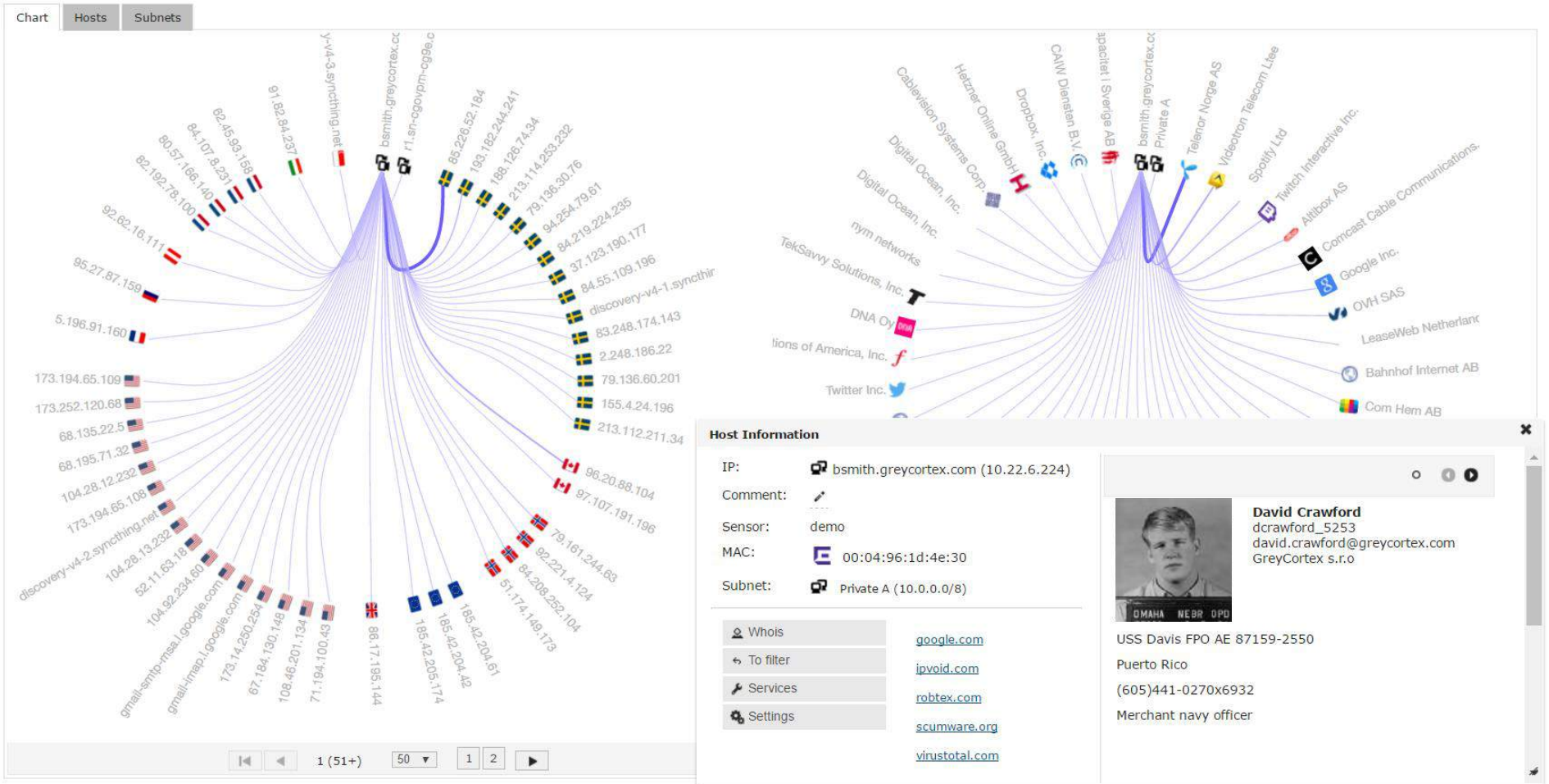
ユーザの行動

ユーザの行動に起因する異常なイベントを簡単にフィルタできます。ここでは、異常な定期的な通信に続き、異常なデータ転送が行われています。これはリスクの高い情報漏えいの兆候を示しています。



ユーザの通信

ユーザの通信を、通信パートナーおよびサブネットワーク別に表示します。



ユーザがアクセスしたサービス

当該ユーザがアクセスしたサービスを、転送されたデータによってフィルタし、
アプリケーションとネットワークのパフォーマンス指標とともに表示します。

Service	Port	Service Type	Protocol	Flows	Packets	Data [B]	Data ⇩ [B]	Data ⇧ [B]	Peers	øRTT [s]	øART [s]	øDTT [s]	øDelay [s]	øJitter [s]
	40197	REMOTE	UDP (17)	264	87.38 k	88.16 M	2.04 M	86.12 M	264					
HTTP	80	REMOTE	TCP (6)	1.54 k	168.57 k	25.93 M	14.06 M	11.87 M	978	0.015	0.128	0.020	0.020	870.98 n
HTTPS	443	REMOTE	TCP (6)	2.77 k	48.65 k	12.14 M	8.48 M	3.66 M	2.52 k	0.072	0.453	127.48 µ	252.33 µ	30.45 µ
	60415	REMOTE	UDP (17)	51	4.25 k	5.55 M		5.55 M	51					
IMAPS	993	REMOTE	TCP (6)	246	14.8 k	3.67 M	3.07 M	602.54 k	225	0.011	0.014	140.4 µ	396.71 µ	298.97 n
	60180	REMOTE	UDP (17)	1	26.5 k	1.84 M		1.84 M	1					
Panagolin-ident	9021	REMOTE	TCP (6)	9	18.32 k	1.34 M	51.86 k	1.29 M	9	0.018				
	11530	REMOTE	UDP (17)	1	19.02 k	1.33 M		1.33 M	1					
	52072	REMOTE	UDP (17)	631	8.56 k	1.27 M		1.27 M	616					
	51413	REMOTE	UDP (17)	1.24 k	8.89 k	1.26 M	107.71 k	1.15 M	1.23 k					
	35001	REMOTE	UDP (17)	615	8.23 k	1.2 M		1.2 M	601					
	53410	REMOTE	UDP (17)	349	6.92 k	1.12 M	530.23 k	593.31 k	347					
Savant	3391	REMOTE	UDP (17)	320	6.71 k	1.1 M	529.28 k	572.45 k	320					
	49180	REMOTE	UDP (17)	545	6.95 k	1.02 M		1.02 M	528					
	11382	REMOTE	UDP (17)	538	6.98 k	1.0 M		1.0 M	520					
	24513	REMOTE	UDP (17)	502	6.37 k	927.41 k		927.41 k	479					
	30880	REMOTE	UDP (17)	476	5.81 k	854.32 k		854.32 k	467					
	53298	REMOTE	UDP (17)	224	4.22 k	691.27 k	332.3 k	358.98 k	224					
	30343	REMOTE	UDP (17)	392	4.67 k	681.92 k		681.92 k	380					
	51413	REMOTE	TCP (6)	1.1 k	5.68 k	674.66 k	301.25 k	373.41 k	1.08 k	0.034	0.025	55.98 µ		55.98 µ
	45093	REMOTE	UDP (17)	336	4.15 k	622.25 k		622.25 k	333					
	23877	REMOTE	TCP (6)	920	4.55 k	619.37 k	307.38 k	311.99 k	871	0.007	0.010	32.67 µ		32.67 µ
Matahari	49000	REMOTE	UDP (17)	153	3.12 k	542.07 k	306.99 k	235.09 k	153					
	52463	REMOTE	UDP (17)	249	3.68 k	534.97 k	202.88 k	332.09 k	249					

GREYCORTEX

MENDELを選ぶべき理由

迅速な検出と対応

コンプライアンスの強化と実証

ネットワークの
トラブルシューティング

コスト削減

評判低下とデータ損失のリスクを低減
ネットワーク管理の効率化

GREYCORTEX

MENDELを選ぶべき理由

強力なネットワーク検出機能

他のツールでは検出できない脅威やリスクの検出

- きわめて先進的な行動検出機能
- 独自の検出アルゴリズム
- DPI (45,000以上のIDSシグネチャ) による強力なシグネチャベース検出機能
- 競合製品 (Darktrace、Fidelis、LanScope、LightCyber/Palo Alto、Flowmon) に対する優位性を幾度も実証済み

独自のネットワーク検索と可視化

サブネット、デバイス、通信、サービスとメタデータを個別にフィルタ

- 効果的な連携 (セキュリティ分析を効率化)
- 単一の GUIにすべて表示 - 検出されたイベントからネットワークフローまで、数クリックで表示が可能
- すべて (すべてのレベルのデータ表示と詳細) をフィルタ、並べ替え可能
- 誤検知の排除 など

GREYCORTEX

他のNTAソリューションにない機能

ネットワークとアプリケーションのパフォーマンス監視
(ネットワークパフォーマンス監視と診断)

Solarwinds、Riverbed ほか

Netflow 収集と分析

nfsen ベースのソリューション: ntop、Flowmon、Paessler ほか

SIEM / ログ管理

Splunk、QRadar、Arcsight ほか

IPS / IDS

Fortinet、Checkpoint、Cisco ほか

GREYCORTEX

SIEMの利用価値向上

検出したイベントをSIEMに報告

ネットワークの可視性を向上させ、検出した脅威についてコンテキストを提供

NetFlowのエクスポート

フローエクスポート機能を備えた SIEM モジュールは高価

GREYCORTEX