

まだEDR？

パロアルトネットワークスの
推奨するXDRとは？

CORTEX XDR™

 paloalto
NETWORKS®

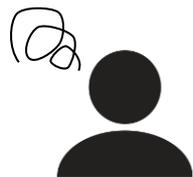
高度なサイバー攻撃にはディテクション(検知)とレスポンスが必要



99%以上のサイバー攻撃は正しいツールを使うことで阻止可能

1%未満のサイバー攻撃

課題：サイロ化された各セキュリティ機能。。。。



大量のアラート生成

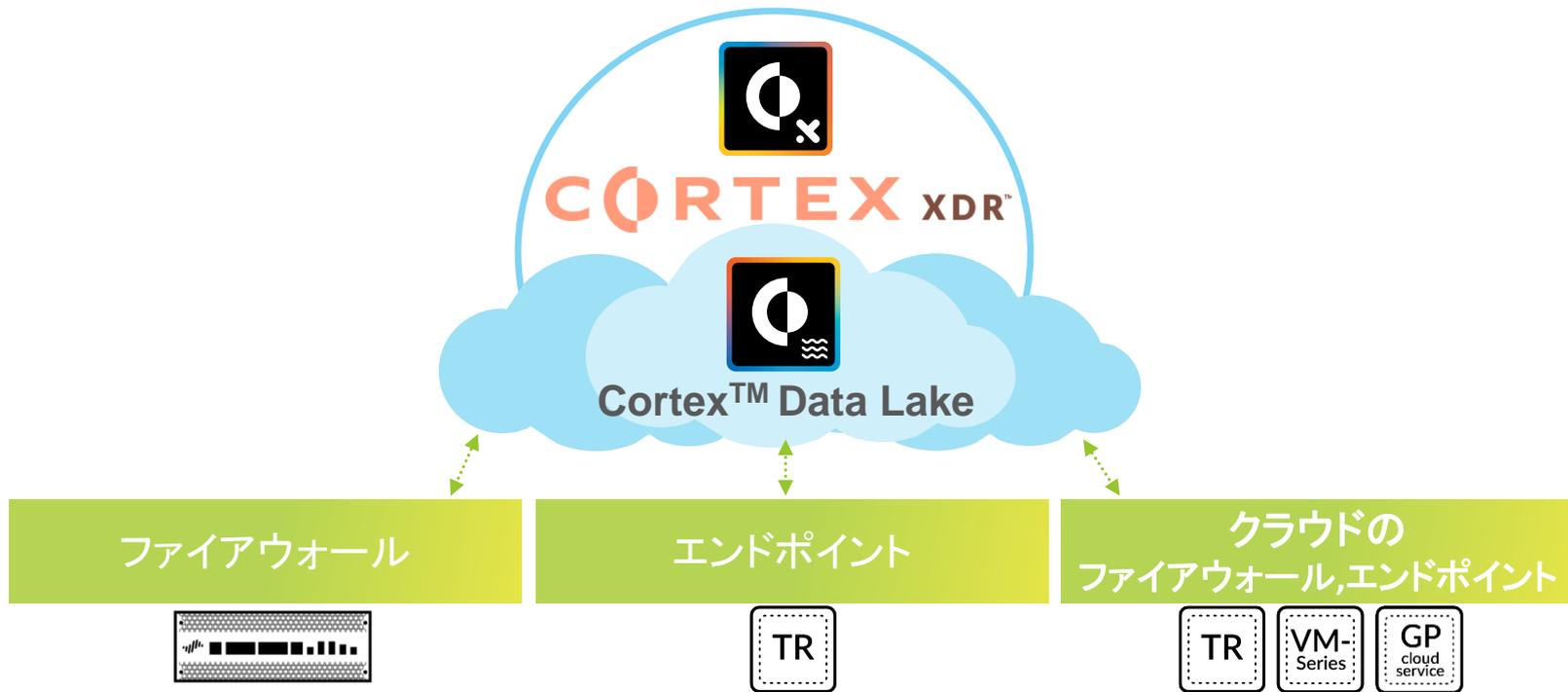


アラートに関連すると思わ
れるデータを手動収集



人海戦術での
相関分析が難しい

解決策: Cortex XDR 単一ベンダーによる包括的なディテクション&レスポンス

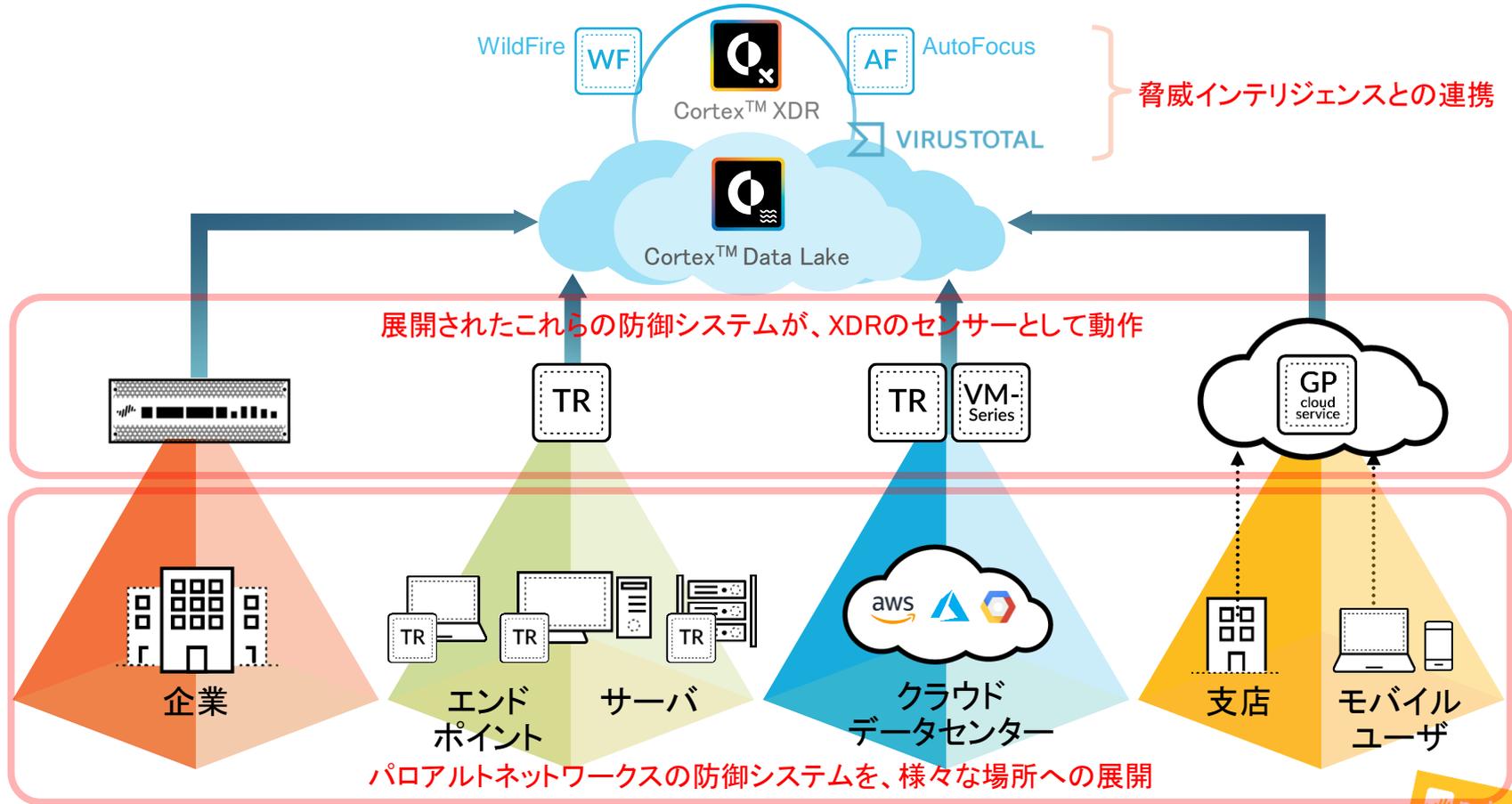


調査に必要なデータを
自動で収集

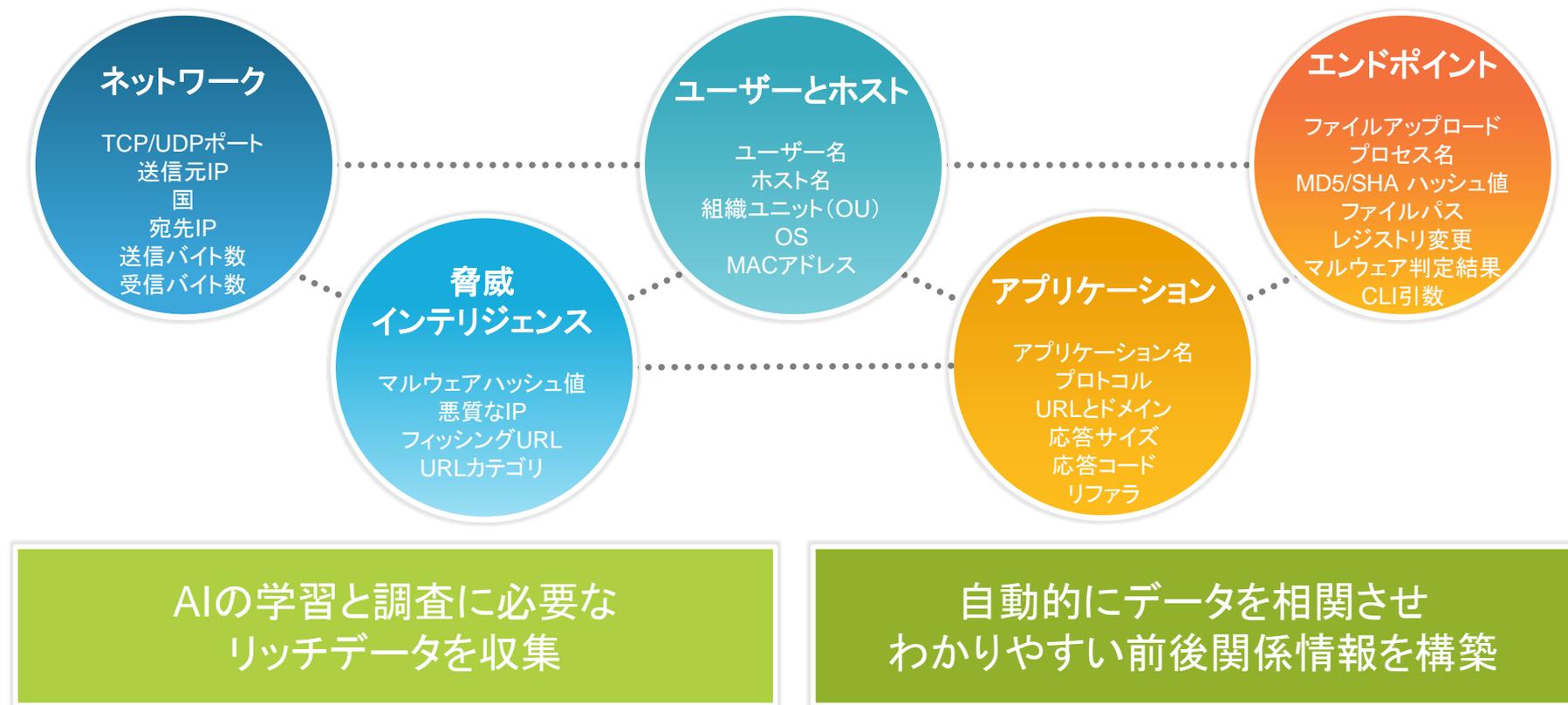
データをAIが分析
自動的に攻撃を検出

再発防止策を迅速に
防御システムに適用

ネットワーク、エンドポイント、クラウド全ての脅威を可視化



リッチデータとビッグデータでデータドリブン



Cortex XDR で組織のセキュリティを総合的かつ効率的に高める

1 防御・阻止
次世代ファイアウォール
Trapsのカバー範囲



2 自動化された検知

- 機械学習をつかった挙動分析
- カスタマイズ可能な検知ルール
- 自動化された脅威ハンティング

4 **Cortex XDRのカバー範囲**

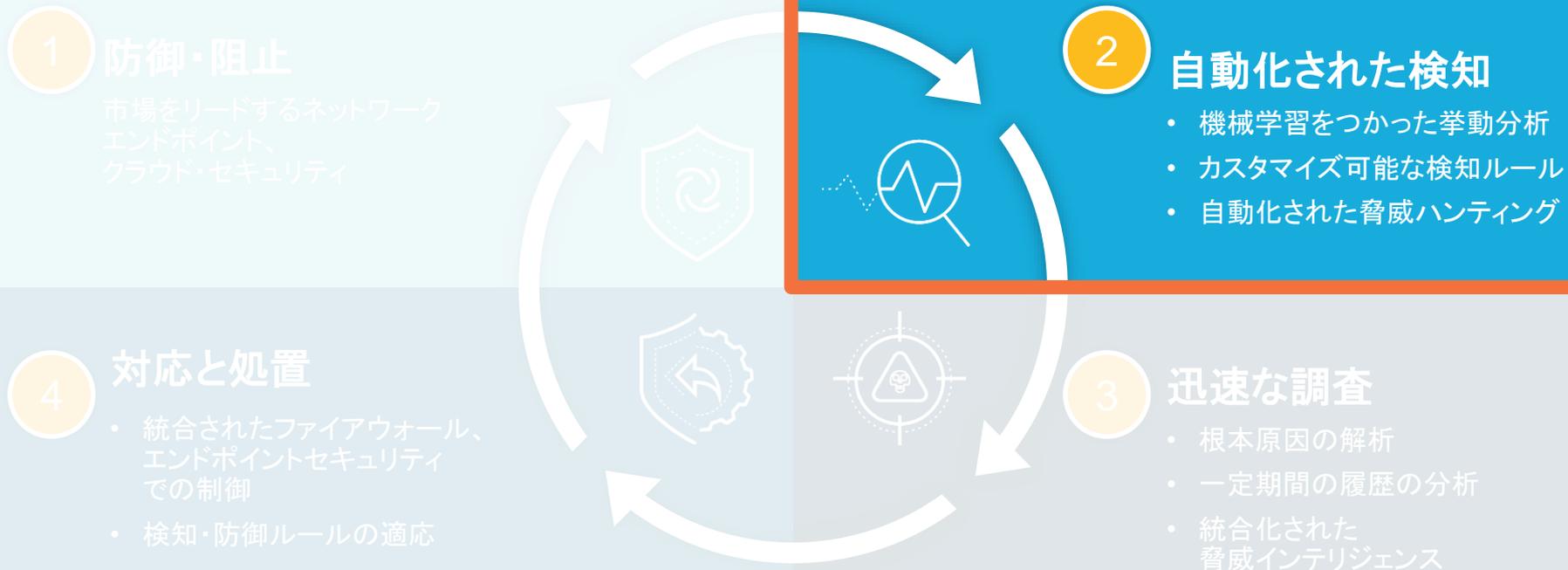
検知と処置
エンドポイントセキュリティ
での制御

- 検知・防御ルールの適応

迅速な対応

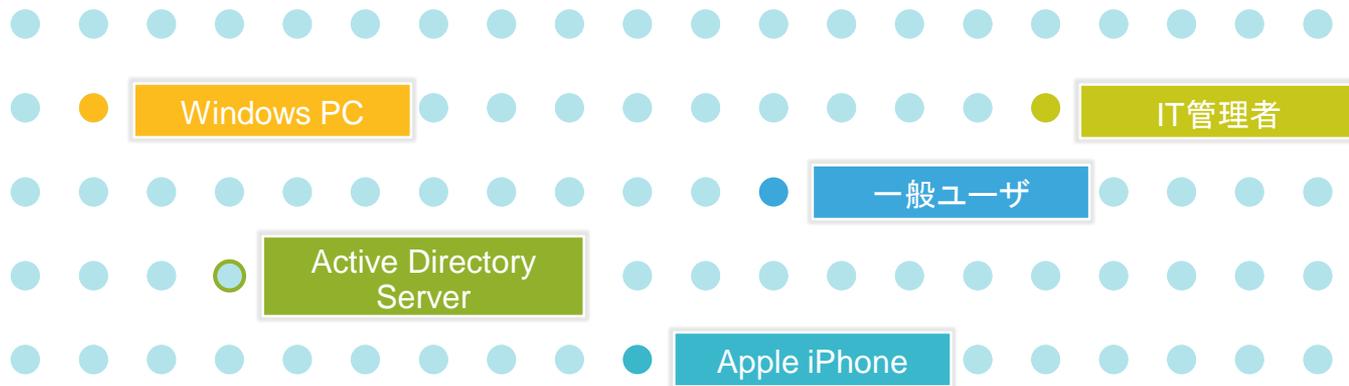
- 根本原因の特定
- 一定期間の履歴の分析
- 統合化された脅威インテリジェンス

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める



AIによる分析で攻撃を自動検知

企業ネットワーク

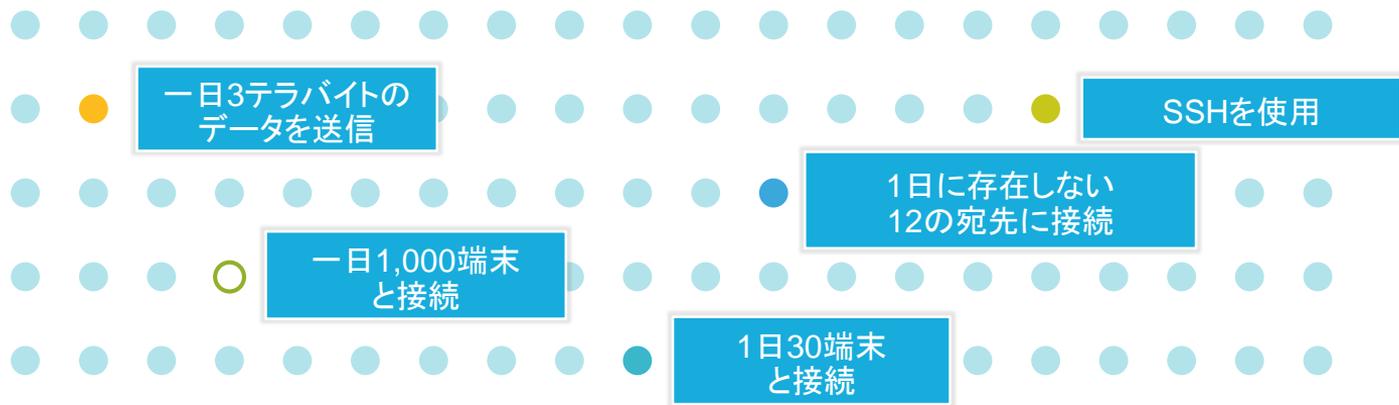


1

ユーザとデバイスの
アクティビティを分析

AIによる分析で攻撃を自動検知

企業ネットワーク



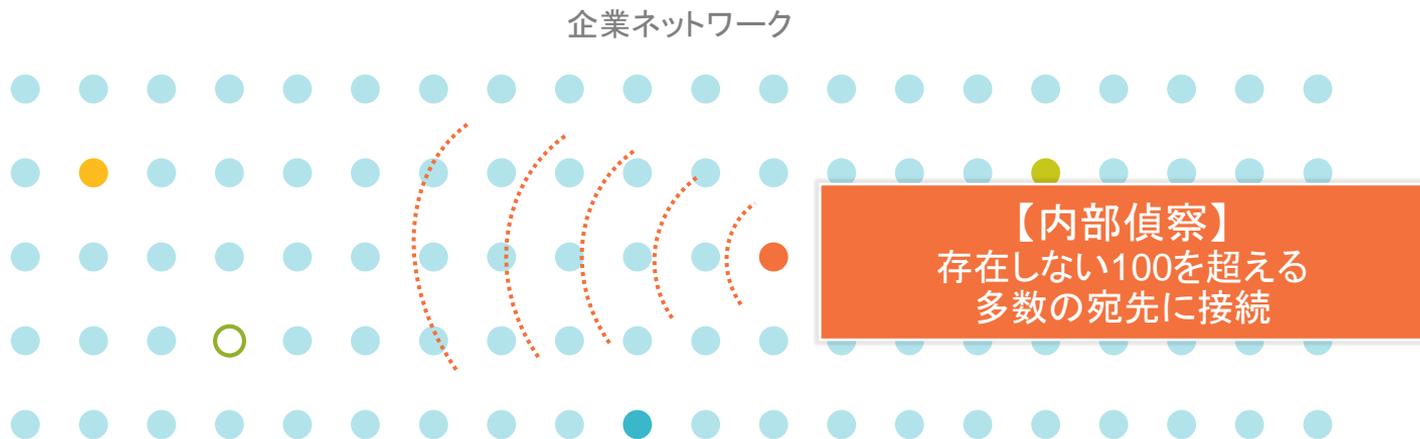
1

ユーザとデバイスの
アクティビティを分析

2

ユーザやデバイスの
ふるまいをプロファイル化

AIによる分析で攻撃を自動検知



1

ユーザとデバイスの
アクティビティを分析

2

ユーザやデバイスの
ふるまいをプロファイル化

3

攻撃の可能性を示唆する
不審な行動を見つけ出す

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める



迅速な調査: 調査作業を簡素化、迅速化

ENV21¥Sauron



Traps alert



1

様々なアラートを
ワンクリックで調査

2

自動的にアラートの
根本原因を明確化

3

脅威インテリジェンスや
前後関係でインシデント特定
と重要度を判定

Your Cortex Apps

Palo Alto Networks SE Japan-For hands-on



Directory Sync



Cortex Data Lake



Explore



Analytics



Investigation & Response



Traps

More Available Palo Alto Networks Apps



Log Forwarding

Allows customers to share data collected by Cortex Data Lake with third-party tools.

[Learn More](#)



Security Lifecycle Review

Discover which applications and threats are exposing vulnerabilities in your security posture.

[Activate](#) [Learn More](#)



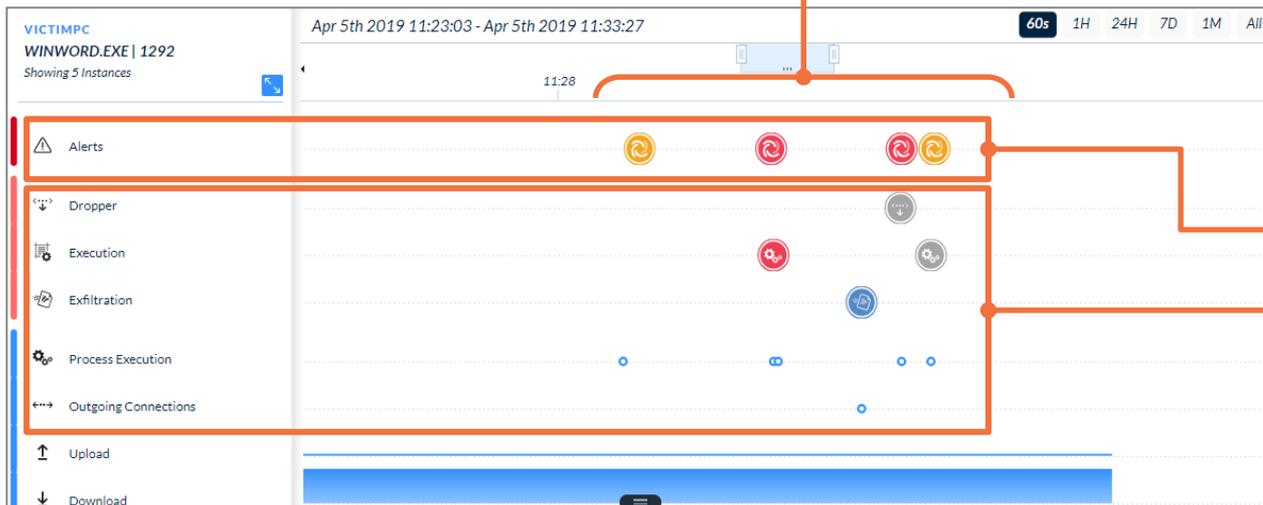
Demisto

Demisto's SOAR platform enables users to standardize security flows and accelerate response through playbook...

[Activate](#) [Learn More](#)



タイムライン調査



タイムライン

検知したアラート

マルウェアの
活動を攻撃フェーズ毎に
応じて自動分類

Apr 5th 2019 11:23:03 - Apr 5th 2019 11:33:27 Found 15 Results

	TIM...	USER NAME	INITIATED...	ACTION TY...	PR...	TH...	DESCRIPTION
<input type="checkbox"/>	Apr 5th ...	EXAMPLE\victimuser	powershell.exe	Dropper	3112	4068	File [action type = all AND name = *.exe, *.scr, *.dll, *.sys, *
<input type="checkbox"/>	Apr 5th ...	EXAMPLE\victimuser	powershell.exe	Network Outgoing	3112	4068	Type : Network Outgoing Source : 192.168.157.12:55501 t
<input type="checkbox"/>	Apr 5th ...	EXAMPLE\victimuser	powershell.exe	Exfiltration	3112	4068	Suspicious macro detected
<input type="checkbox"/>	Apr 5th ...	EXAMPLE\victimuser	cmd.exe	Process Execution	1444	3568	Process : C:\Windows\System32\WindowsPowerShell\v1.0\
<input type="checkbox"/>	Apr 5th ...	EXAMPLE\victimuser	WINWORD.EXE	Process Execution	1292	2544	Process : C:\Windows\System32\cmd.exe Started with CMD

各プロセス動作
の分析

内部監視／内部不正対策

The screenshot displays the Cortex XDR Analytics interface. On the left, a sidebar lists alerts for device 172.16.20.253, including 'Failed Connections (None)' and 'New Administrative Behavior'. The main panel shows the details for the 'Failed Connections (None)' alert, which occurred on Dec 23, 2017, between 4:00 AM and 5:10 PM. The alert description states that the device failed to connect to 201 nonexistent destinations, with a common App-ID of 'incomplete'. It also provides baseline information: a peer group baseline of 7 destinations and a total of 2,653 failed sessions. Below the description, a network diagram visualizes the failed connections. The central node is 172.16.20.253. It shows connections to three other nodes: 172.16.0.0-172.31.25... (Private network) with 148 failed incomplete connections, 192.168.0.0-192.168... (Private network) with 2 failed incomplete connections, and 100.0.0-10.255.255.2... (Private network) with 51 failed incomplete connections. A 'Baseline' node shows 7 failed incomplete destinations.

不審な行動を検知した
アラートを確認

検出理由

通信先の情報など
詳細内容の確認

動作の可視化

Cortex XDR で組織のセキュリティを総合的かつ効率的に高める

1 防御・阻止

市場をリードするネットワーク
エンドポイント、
クラウド・セキュリティ

2 自動化された検知

- 機械学習をつかった挙動分析
- カスタマイズ可能な検知ルール
- 自動化された脅威ハンティング

3 迅速な調査

- 根本原因の解析
- 一定期間の履歴の分析
- 統合化された
脅威インテリジェンス

4 対応と処置

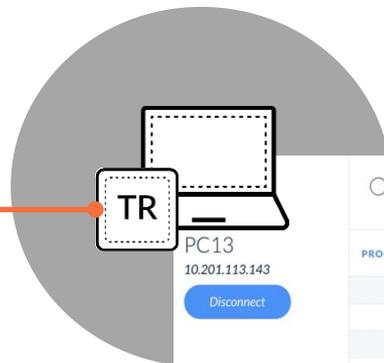
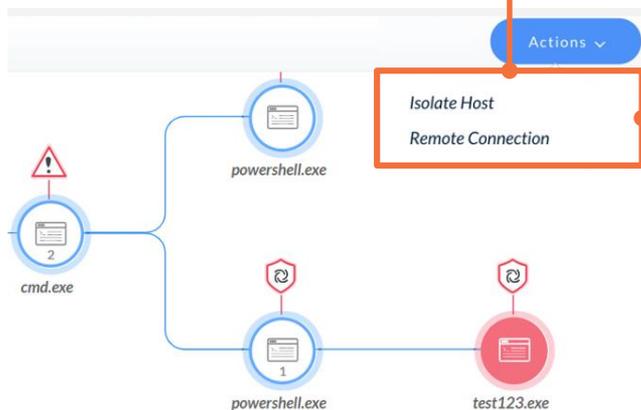
- 統合されたファイアウォール、
エンドポイントセキュリティ
での制御
- 検知・防御ルールの適応

簡単なレスポンス

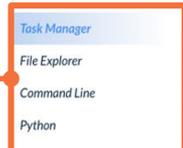
ネットワークから
エンドポイント隔離



管理者



エンドポイント
リモート操作



Filter results

PROCESS HIERARCHY	PROCESS ID	PARENT ID	USER NAME
SearchIndexer.exe	1116	528	NT AUTHORITY\SYSTEM
spoolsv.exe	1204	528	NT AUTHORITY\SYSTEM
svchost.exe	1244	528	NT AUTHORITY\LOCAL SERV
cyserver.exe	1440	528	NT AUTHORITY\SYSTEM
CyveraService.exe	1496	528	NT AUTHORITY\SYSTEM
taskhost.L	1556	528	ENV21\Sauron
tlaservice.L	1612	528	NT AUTHORITY\SYSTEM
tlawo	1840	1612	NT AUTHORITY\SYSTEM
tlawo	1848	1612	NT AUTHORITY\SYSTEM
VGAuthSe	1704	528	NT AUTHORITY\SYSTEM
vmtoolsd.L	1752	528	NT AUTHORITY\SYSTEM
svchost.exe	2164	528	NT AUTHORITY\LOCAL SERV
svchost.exe	2232	528	NT AUTHORITY\NETWORKS
svchost.exe	2700	528	NT AUTHORITY\SYSTEM
msdt.exe	2980	528	NT AUTHORITY\NETWORKS
...

- ・プロセスの停止、調査
- ・ファイル操作
- ・コマンドライン操作

簡単なレスポンス

ネットワーク上で
通信を遮断

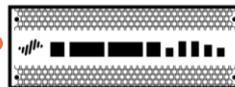


Investigate in xDR ▾ Actions ▾

- ✓ Resolve
- ⊗ Dismiss
- 📁 Add to Whitelist
- 🔴 High
- 🟡 Medium
- ✓ 🟢 Low
- 🚫 Add to Block List

● Executable: winscp.exe

- WildFire verdict: Benign
- Seen on [this host](#) only
- Signed by: Martin Prikrn (Verified)
- MD5: 29604f4e3a63aa568afd160d2863fc7c
- SHA256:
bdc366e6df98612ba46da9f8e16e1bd168036c8444c



次世代ファイアウォール



CORTEX XDR により

エンドポイント、ネットワーク、クラウドを可視化し、
AIにより、効率的な運用性を持つ
ディテクション&レスポンスを実現



