サイバー脅威に向けた最新CyberRecoveryソリューション（CyberSense）の徹底技術解説

デル･テクノロジーズ株式会社
ＤＰＳ事業本部

DELL Technologies

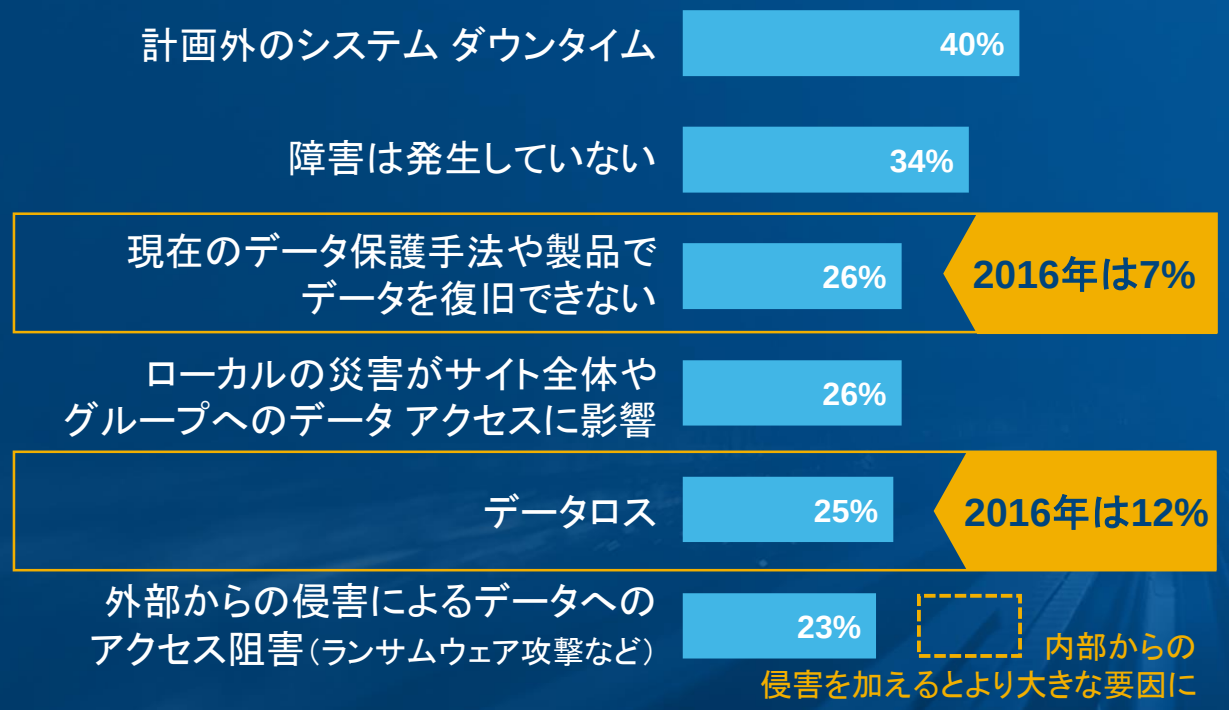
アジェンダ

- Cyber攻撃への備え
- Cyber Recovery Solutionのおさらい
- CyberSenseとは？
- サイバー分析：兆候の検出
- ダイレクト・インデックス
- 技術仕様
- フルコンテンツ分析とメタデータ分析
- CyberSenseによるリカバリ
- サイバーレジリエンス（復元力）
- Cyber Recoveryの管理GUIとの統合
- まとめ

Cyber攻撃への備え - 障害インシデントの代償

障害のタイプ

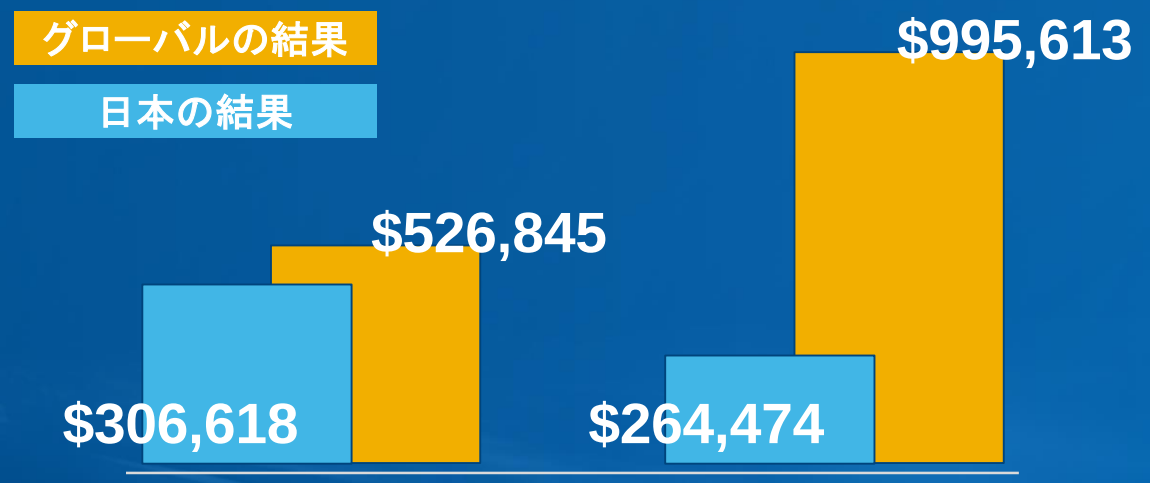
66% の日本企業・組織が過去12カ月の間に何らかのタイプの障害を経験



引用元：Dell EMC Data Protection Index 2018 より

障害の代償

日本では、過去12カ月におけるデータロスのコストより、ダウンタイムのコストの方が大きい



ダウンタイムによる平均損失額（$756,159：ドイツが最も多い）

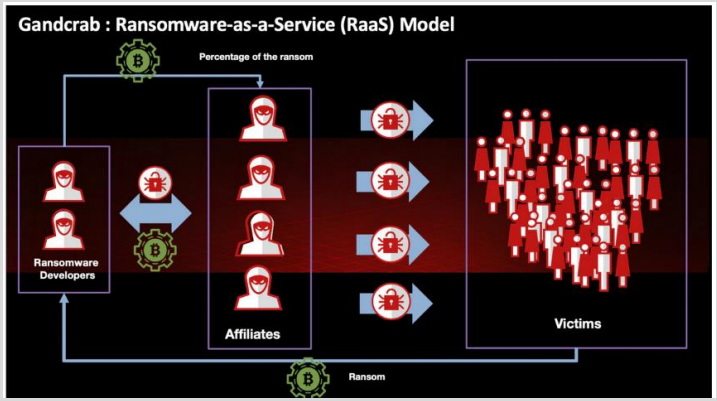
データロスによる平均損失額（$1,950,000：英国が最も多い）

平均 **17時間の計画外システム ダウンタイム**

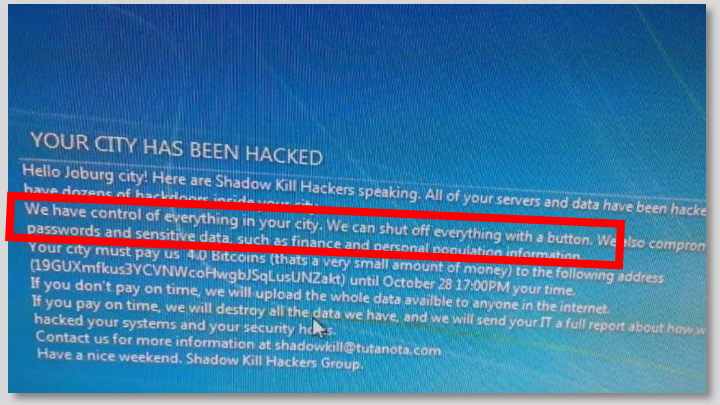
平均 **1.70TB のデータ損失**

DELL Technologies

ランサムウェアに関する最近の記事

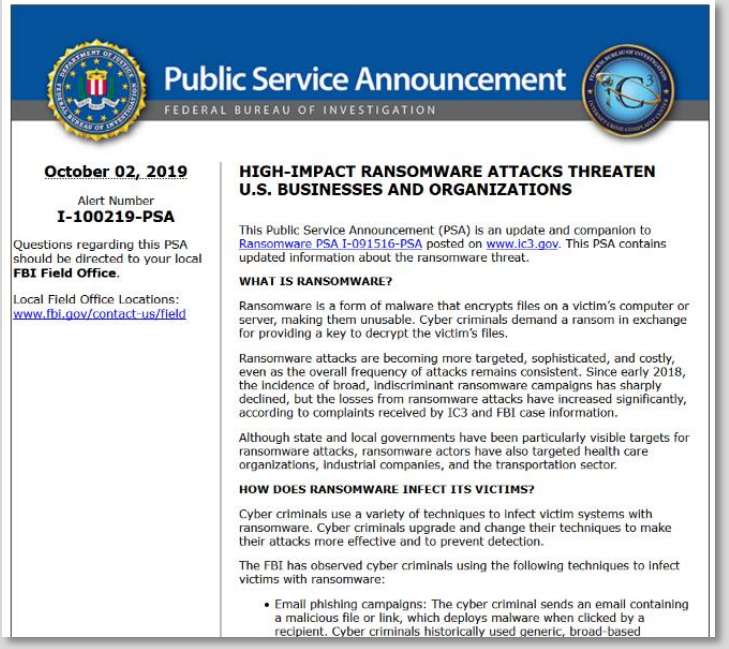


Ransomware as a Service



ランサムウェアが個人情報漏洩
にも発展している

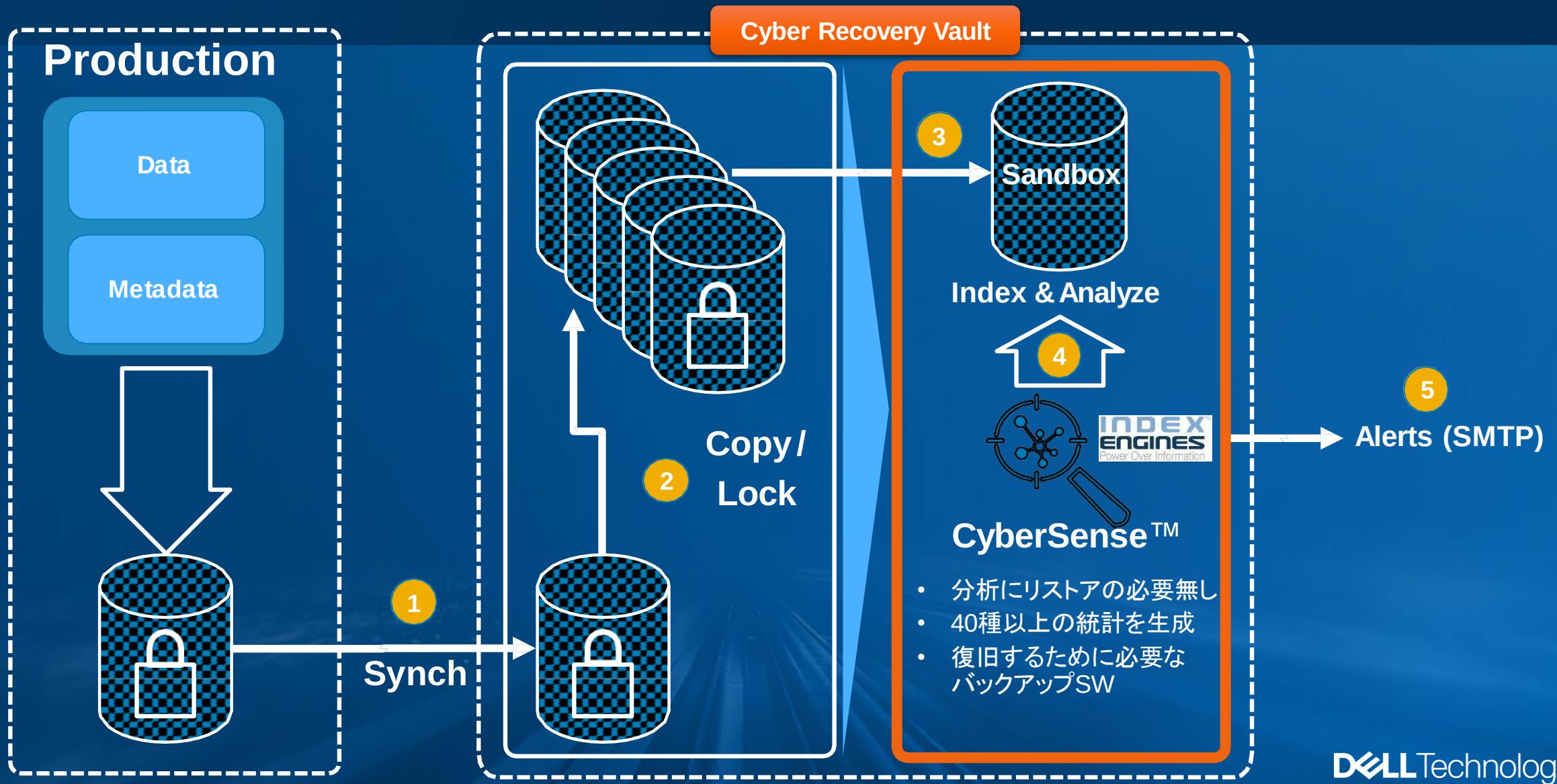
貴重なデータが永久に失われる



定期的にデータをバックアップ
することで、安全性を検証する

DELL Technologies

CRS(Cyber Recovery Solution) のおさらい



DELL Technologies

CyberSenseとは？

機械学習による解析やフォレンジック（証跡調査）を行うツール

サイバー攻撃を迅速に検知し、リカバリを行う

- 機械学習を利用した独自のフル・コンテンツレベルの分析
- 不審な動きを検出する為に100以上の経験則に基づいた解析機能
- Cyber Recoveryソリューションと密に連携された自動化及びアラートの通知
- アタック後のフォレンジック結果やアタックベクター（侵入方法、経路）を基に影響を受けたデータを特定
- 感染する直前のクリーンなデータセットを特定
- アタック後の迅速なデータ復旧により、高度なレジリエンス（復元力）を提供

サイバー分析：兆候の検出

スキャン

CyberSense は、非構造化ファイルやデータベースなど、重要なデータソースをスキャンしてインデックスを作成。
データは、*NFS*またはバックアップ・イメージに配置

アナリティクス

インデクスから生成される**40**種以上の統計。。 統計情報には、ファイルエントロピーの変更、破損、大量削除/創作などの分析が含まれる

分析

機械学習アルゴリズムを統計情報の分析に使用。
データに対する攻撃が発生したかどうかを分析。

繰り返し

プロセスが繰り返され、バックアップデータをスキャンすることによって新しいインデックスが作成される。
データの変化を確認するために、以前のインデックスと比較される。

調査

フォレンジックレポートおよび分析ツールは、攻撃の後、破損したファイルを検出し、ランサムウェアの種類の診断に利用。

DELL Technologies

CyberSenseの機能：ダイレクト・インデックス

バックアップデータからインデックスを作成

- 標準的なバックアップSWによるバックアップデータのコンテンツを直接、インデックス化
- フル・コンテンツのインデックス化
- バックアップデータのリストアは不要

DELL EMC
- ✓ Networker
- ✓ Avamar
- ✓ PowerProtect Data Manager

VERITAS
- ✓ NetBackup

IBM
- ✓ TSM
- ✓ Spectrum Protect

COMMVAULT
- ✓ Commvault

技術仕様

非構造化ファイル：
文書、契約書、契約書、知的財産等

データベース：
Oracle,DB2,SQL,SharePoint等

コアインフラ:
DNS, LDAP, Active Directory等

分析可能なデータ

NBU, TSM/Spectrum, NetWorker, Avamar, 等のバックアップデータから直接、インデックス作成

オリジナルのバックアップSWは不要

データの復元はバックアップSWが行う

バックアップ SW

リソースは処理されるデータの容量に依存する

仮想サーバ上に構築（ESXi）
20 ~ 30 コア、128 ~ 256 GB RAM

CyberSense サーバ

CyberSenseによるリカバリ

01

検出: いつ発生したのか？

- バックアップデータを直接分析

02

調査: 何が起こったのか？

- 破損したファイルの一覧
- 使用されたユーザー アカウントとランサムウェアは何か？
- いつ起こったのか？
- クリーンで正常なデータが含まれているバックアップ セット

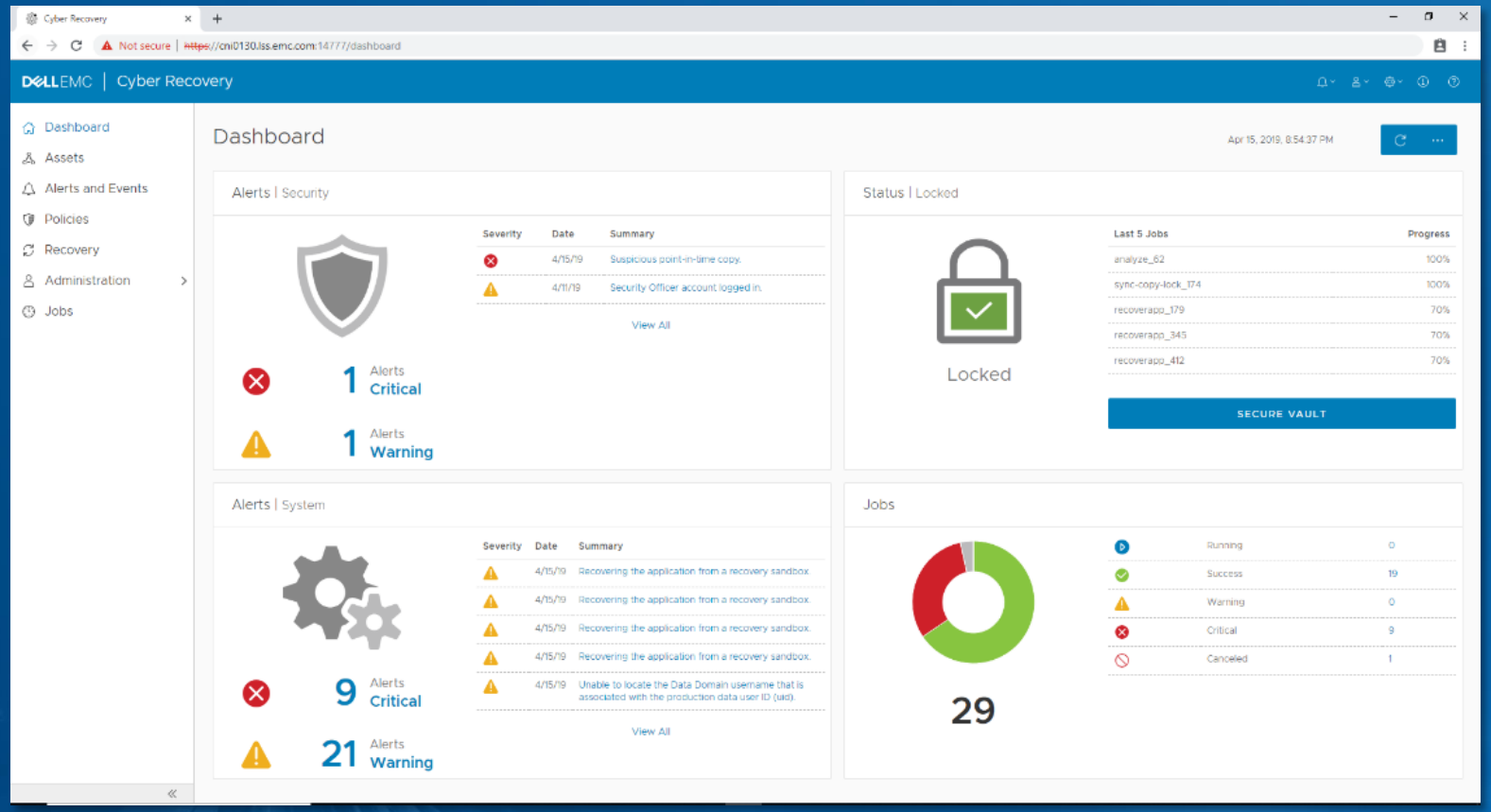
03

リカバリ: ダウンタイムを最小限に抑える

- 破損したファイルの一覧

Cyber Recoveryの管理GUIとの統合

- Cyber Recoveryのワークフローの中で、CyberSenseによる分析が行われる
- 疑わしいアクティビティが特定された際、アラートを送信
- 特定されたアタックベクターと影響を受けるデータをemailで通知



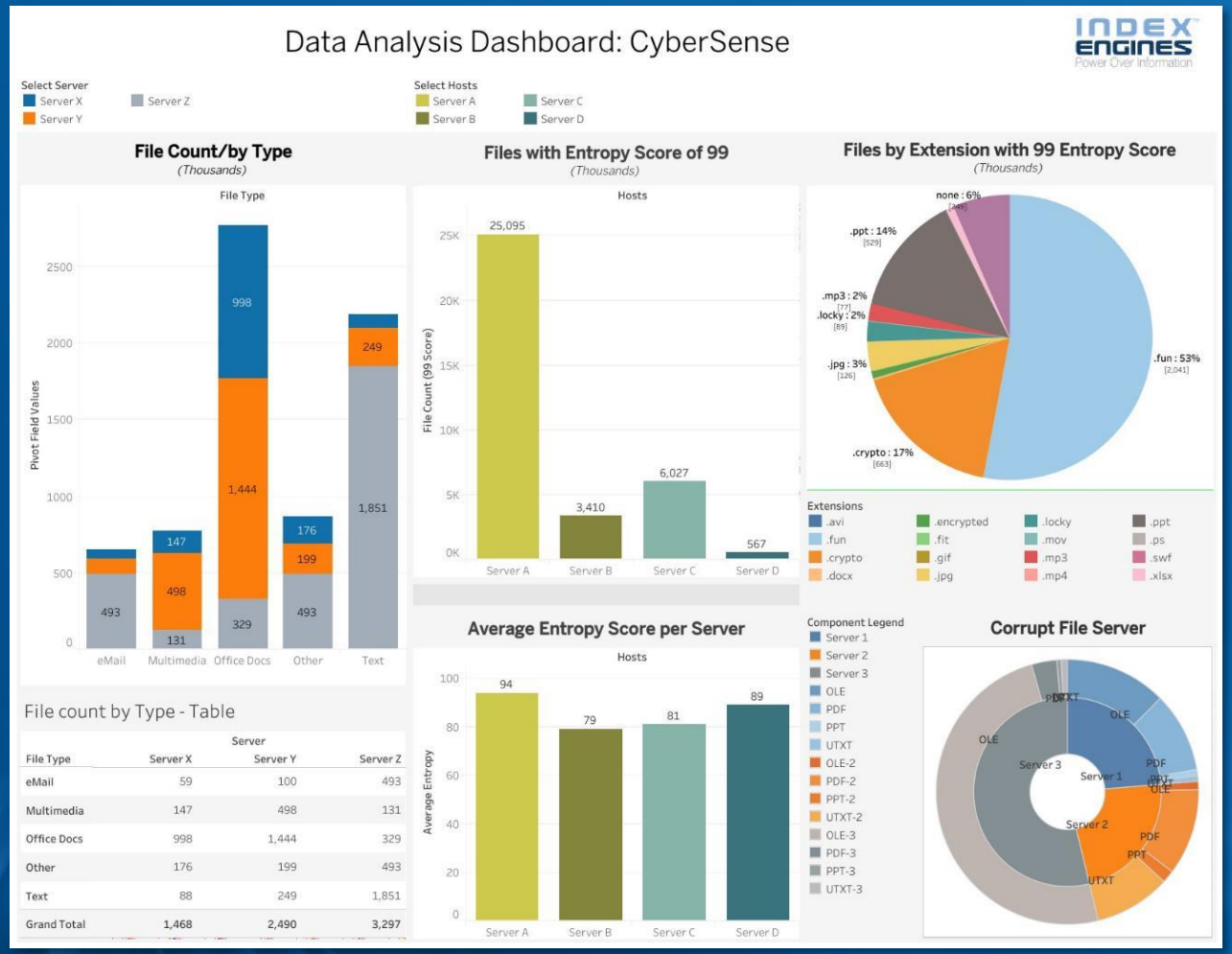
Cyber Recovery GUI：Dashboard

DELL Technologies

CyberSense レポート例：Dashboard

ベースライン・スキャン

- データの整合性をチェック
- 既知のランサムウェアの拡張子をチェック
- 破損したファイルをチェック
- ファイルが暗号化されたかどうかのチェック



CyberSenseのレポート例
（ダッシュボード）

DELL Technologies

CyberSense詳細レポート

- 機械学習アルゴリズムを用いた100以上の統計の分析
- データの変化の分析
  - エントロピーの変更
  - 類似性
  - 削除
  - 作成
  - ファイルの破損
  - ファイルの種類の不一致
  - ランサムウェアのファイル拡張子等など･･･
- 定義済みアタックベクターによる感染の特定

1	Backup Server	tilt.test.indexengines.com
2	Backupset ID	tilt.test.indexengines.com_1527689828-0
3	Backupset Root Path	D:/
4	Backup Client Type	1
5	Backup Time	1527689828
6	Volume Label	192.168.17.245-12.10.2019 at 11:45 AM-493
7	Compare ID	3
8	Stats ID	9
9	This File Count	2947
10	This Unique File Count	2947
11	This Mean File Size	570814
12	This Mean Entropy	89.679703
13	This Entropy Threshold	2054
14	This File Type Mismatch Count	101
15	This Corrupt File Count	3
16	This Ransomware Extension Count	0
17	This Archive Count	0
18	This Archive Bytes	0
19	This File Cat Office Count	737
20	This File Cat Images Count	0
21	This File Cat AudioVideo Count	0
22	This File Cat Mail Count	1
23	This File Cat Exec Count	0
24	This File Cat Office Extension Count	700
25	This File Cat Images Extension Count	0
26	This File Cat AudioVideo Extension Count	0
27	This File Cat Mail Extension Count	0
28	This File Cat Exec Extension Count	0
29	This File Cat Office Extension Suspect Count	0
30	This File Cat Images Extension Suspect Count	0
31	This File Cat AudioVideo Extension Suspect Count	0
32	This File Cat Mail Extension Suspect Count	0
33	This File Cat Exec Extension Suspect Count	0
34	This DEF File Count	2193
35	This DEF Unique File Count	2193
36	This DEF Mean Entropy	73.415001
37	This DEF Entropy Threshold	2041
38	This Backup Type	0

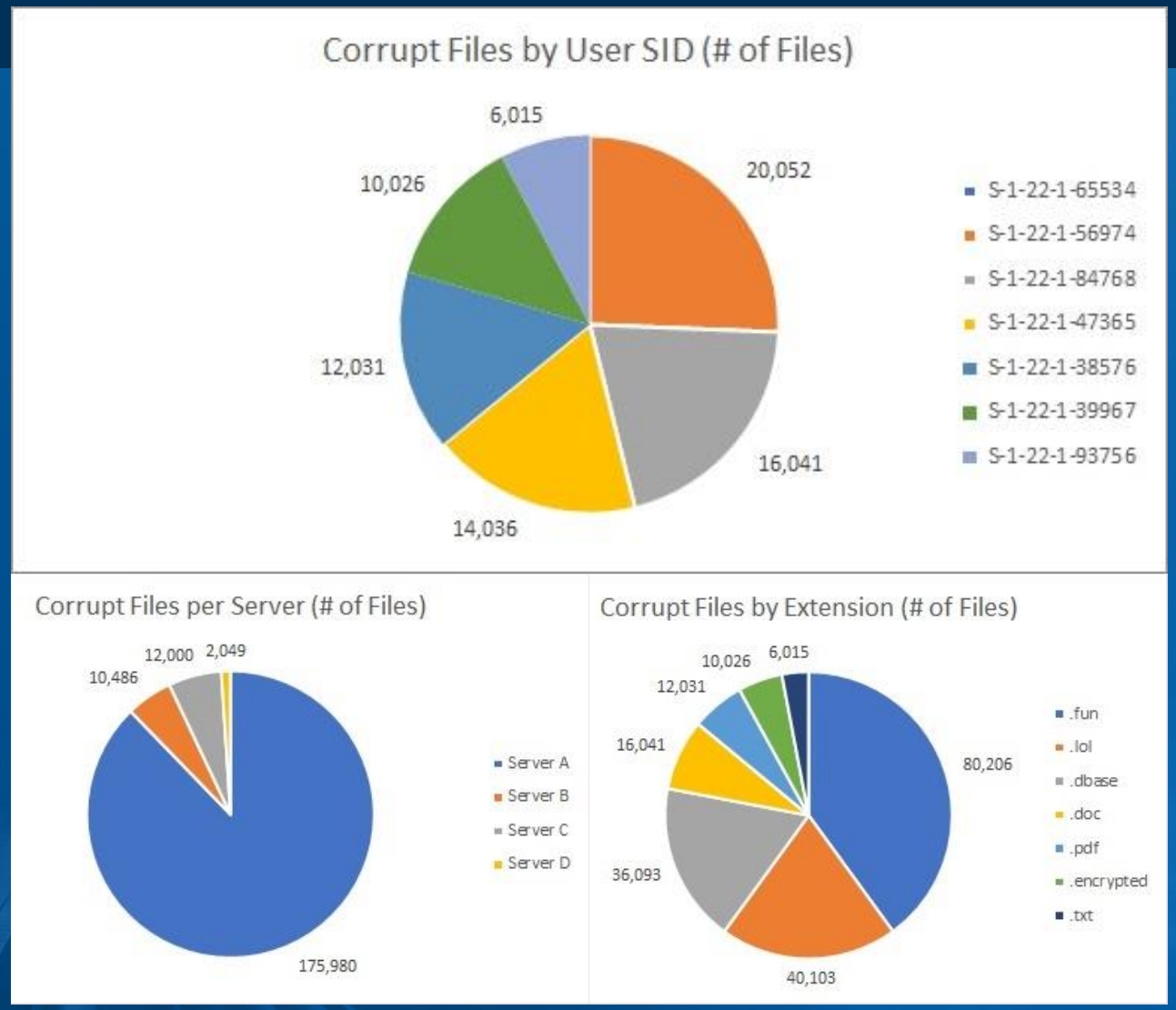
CyberSense Output Report with

82	Created Ransomware Extension Count	0
83	Created Ransomware Entropy	
84	Created Ransomware Entropy Threshold	0
85	Created Ransomware Unique Count	0
86	Created Ransomware Unique Backupset Count	0
87	Changed File Count	0
88	Changed Prior Unique Count	0
89	Changed This Unique Count	0
90	Changed Prior Mean Size	
91	Changed This Mean Size	
92	Changed Prior Mean Entropy	
93	Changed This Mean Entropy	
94	Changed Prior Entropy Threshold	0
95	Changed This Entropy Threshold	0
96	Changed Mean Similarity	
97	Changed File Type Count	0
98	Changed Ransomware Filter Count	0
99	Changed Prior-Deleted Mean Entropy	
100	Changed This-Created Mean Entropy	
101	Deleted Archive Count	0
102	Deleted Archive Bytes	0
103	Deleted File Cat Office Count	2627
104	Deleted File Cat Images Count	272
105	Deleted File Cat AudioVideo Count	4
106	Deleted File Cat Mail Count	11
107	Deleted File Cat Exec Count	0
108	Deleted File Type Mismatch Count	0
109	Created Archive Count	0
110	Created Archive Bytes	0
111	Created File Cat Office Count	737
112	Created File Cat Images Count	0
113	Created File Cat AudioVideo Count	0
114	Created File Cat Mail Count	1
115	Created File Cat Exec Count	0
116	Created File Type Mismatch Count	263
117	Infected	6
118	Data Issues	
119	Model Version	5

CyberSense Output Report with A

フォレンジックレポート

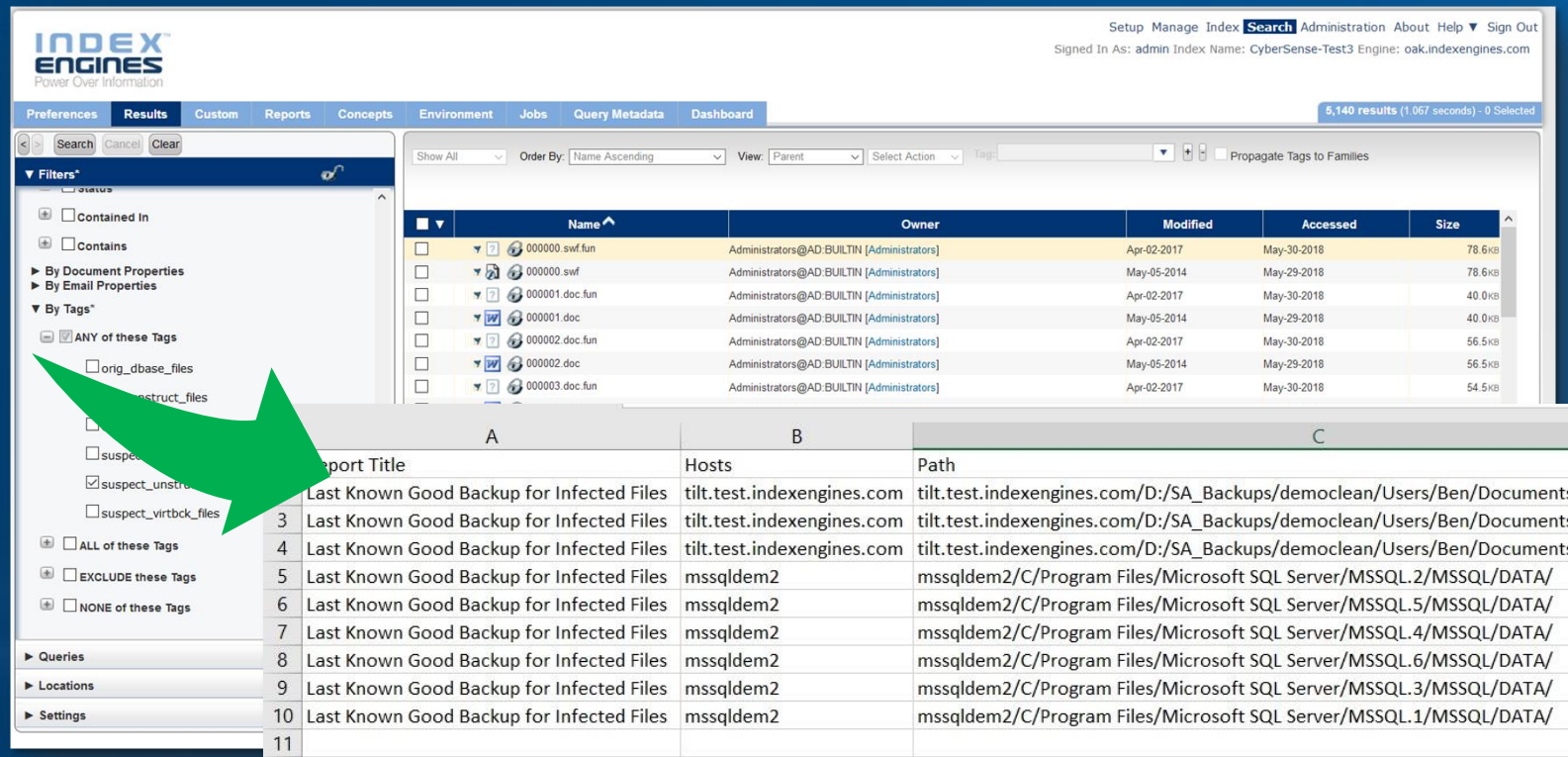
- データ破損を診断するための詳細レポートを生成する
- 攻撃が行われた証跡
  - 誰のデータ
  - 何のデータ
  - どこにあるデータ
  - いつのデータ



DELL Technologies

サイバーレジリエンス

バックアップデータの中から最新の感染されていないクリーンなバックアップセットをレポートする



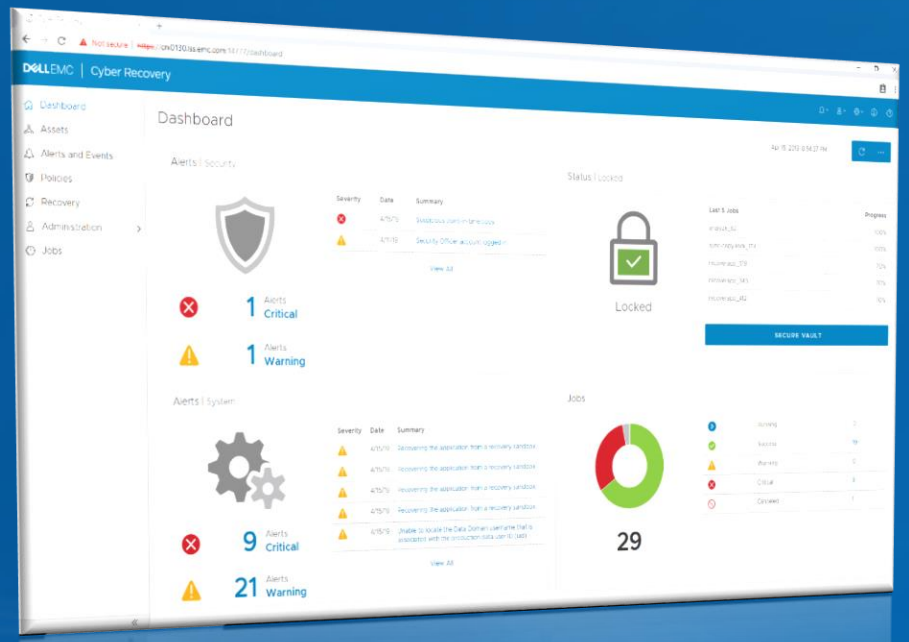
最新のクリーンなバックアップデータがあるバックアップセット

	A	B	C	D	E	F
	port Title	Hosts	Path	Backup Time	Backupset ID	# of Files
3	Last Known Good Backup for Infected Files	tilt.test.indexengines.com	tilt.test.indexengines.com/D:/SA_Backups/democlean/Users/Ben/Documents/govdocs/002/	Tue May 29 15:57:41 2018	tilt.test.indexengines.com_1527623861	983
4	Last Known Good Backup for Infected Files	tilt.test.indexengines.com	tilt.test.indexengines.com/D:/SA_Backups/democlean/Users/Ben/Documents/govdocs/001/	Tue May 29 15:57:41 2018	tilt.test.indexengines.com_1527623861	971
5	Last Known Good Backup for Infected Files	tilt.test.indexengines.com	tilt.test.indexengines.com/D:/SA_Backups/democlean/Users/Ben/Documents/govdocs/000/	Tue May 29 15:57:41 2018	tilt.test.indexengines.com_1527623861	973
6	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.2/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	2
7	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.5/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	1
8	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.4/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	2
9	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.6/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	1
10	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.3/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	2
11	Last Known Good Backup for Infected Files	mssqldem2	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.1/MSSQL/DATA/	Tue Apr 2 12:01:01 2019	mssqldem2_1554220861	2
12						

DELL Technologies

まとめ

- CyberSenseは、侵害や攻撃を受けたことを検出し、その結果のレポートを提供する
- ランサムウェア、暗号化、改ざん、一部の改ざん等の攻撃を検出
- バックアップデータをリストアすることなく、ランサムウェアに侵されたデータのインデックス作成が可能
- バックアップイメージの最初のスキャンにより、最大95%の精度で攻撃を検出でき、その後のパスでは、検出能力が最大99%向上する
- フォレンジック分析ツールは、サイバー攻撃からの復旧とアタックベクター（侵入方法、経路）の診断に利用



DELL Technologies

DELL Technologies