PCIDSSセキュリティフォーラム2013

PCI DSSを担う
最前線の見える化と制御

2013年7月10日

バーダシス株式会社

Verdasys のご紹介

Verdasys Inc.　情報漏えい対策のリーダー

- 2003年設立
- 本社：米国マサチューセッツ州 ボストン
- 名前の由来：Verdad（真実）+ System
- ガートナーのマジッククワドラントのリーダー
- 250 社以上の顧客
- 40 か国以上でグローバルサポート

バーダシス株式会社

- 2006年7月 日本にオフィスを設立

Growing Data Security Ecosystem

IBM 1Labs　hp ArcSight　splunk>　CITRIX　vmware　ManTech HBGary

TITUS　Autonomy an HP company　GENERAL DYNAMICS FIDELIS　Bit9　ATTIVO　Microsoft

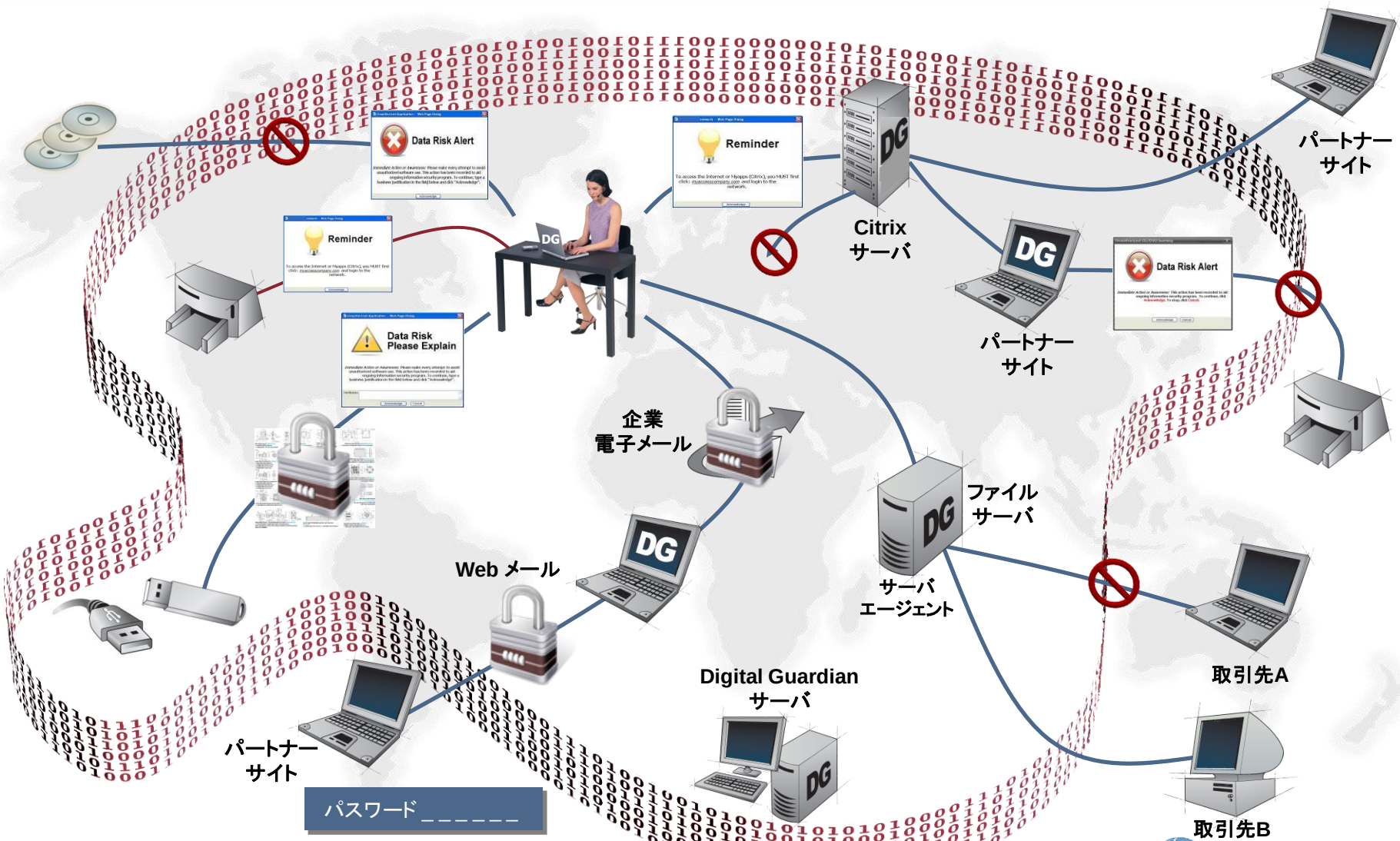
VERDASYS

アジェンダ

- 情報漏えいを防ぐ最前線

標的型攻撃から情報を守る

情報を守る仮想の防御ラインを構築



VERDASYS

PCI DSS での事例：金融サービス

ビジネスの要件

- PCI DSS 対応
- 6,000 台の Windows PC 環境 + Citrix デスクトップ

データ種別

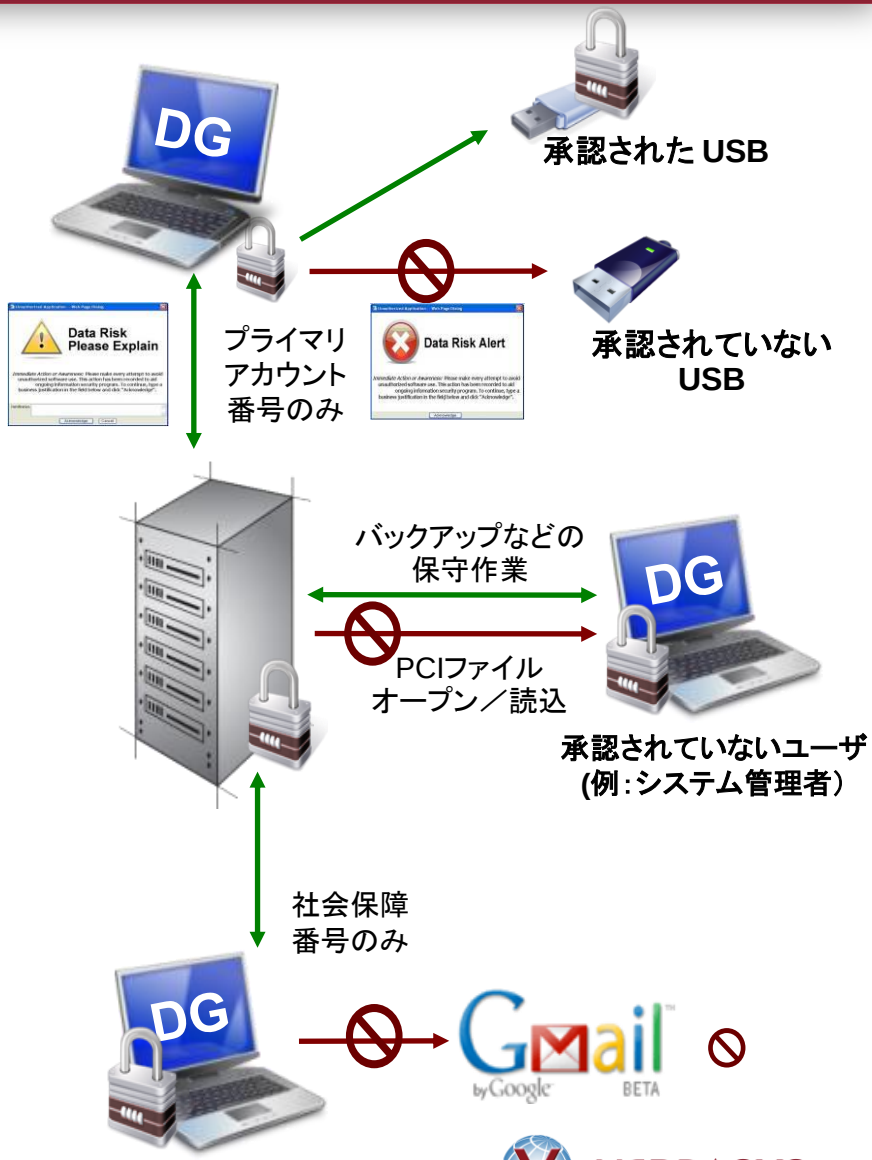
- 個人名、住所
- プライマリアカウント番号 (PAN)
- 国籍、国民保険番号、社会保障番号 (SSN)

ユーザ種別

- 全従業員
- PCI データへのアクセスが承認されているユーザ
- システム管理者、ネットワーク管理者

実現している制御

- ユーザへのプロンプト表示とログの保存
- データの自動暗号化／復号化とログの保存
- 承認されていない行為の禁止とログの保存



VERDASYS

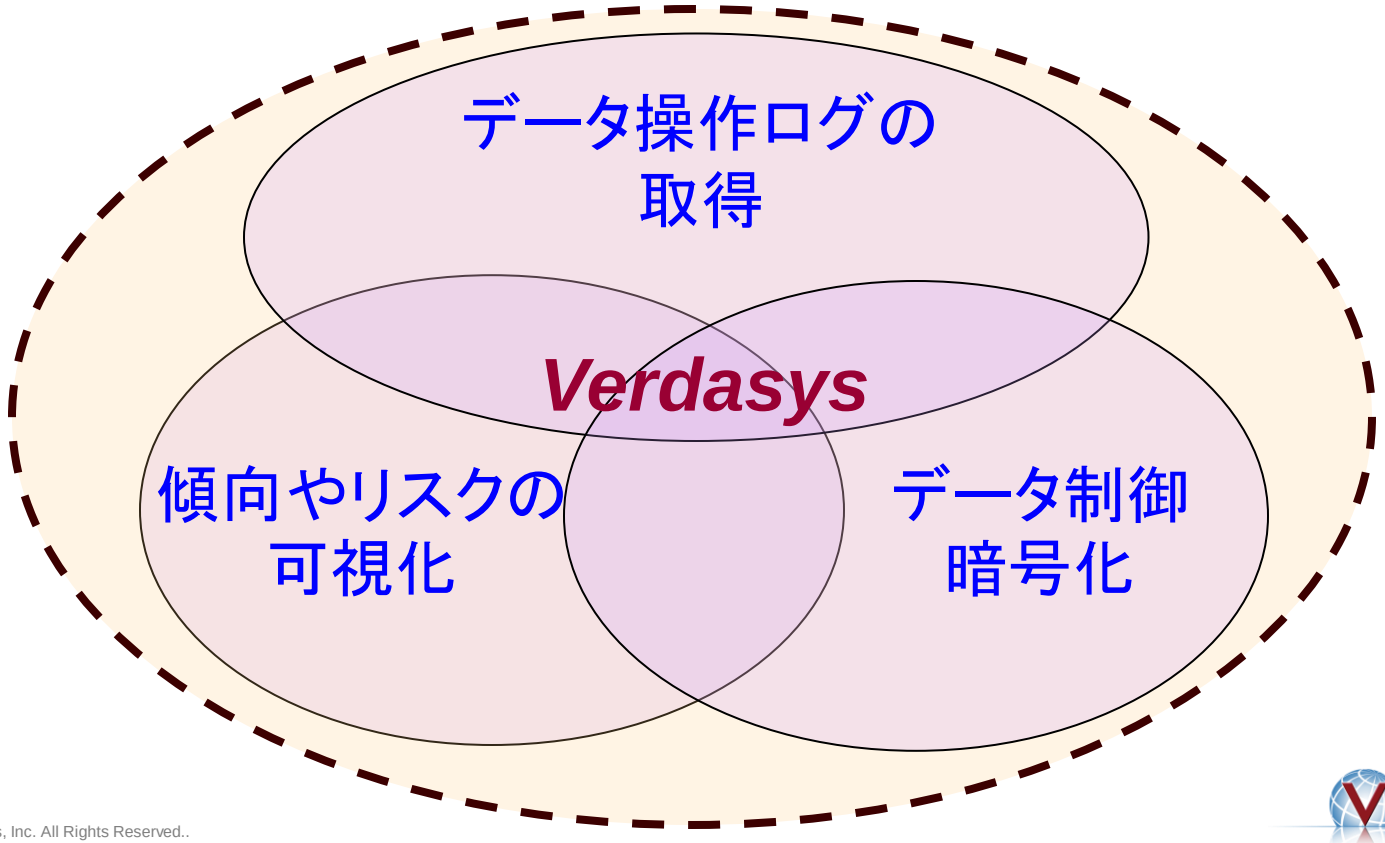
PCI DSS 2.0 の中での Verdasys

- アクセス制御
  - 要件7　　カード会員データへのアクセス
  - 要件8.5.4　契約終了したユーザのアクセスは直ちに取り消す
- プライマリアカウント番号の暗号化
  - 要件3.4
- ログの取得
  - 要件10.6 など
  - 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム(IDS)や認証、認可、アカウンティングプロトコル(AAA)、サーバ(RADIUSなど)のようなセキュリティ機能を実行するサーバを含める必要がある。
- 変更の保護
  - 要件10.5.2　監査証跡ファイルを不正な変更から保護する
- 要件実施の有無確認
  - 要件6.1　　パッチ適応など

特長1：検知と防御の統合

- 3つの機能がひとつになっています！
  - データ操作のモニタリング
  - データ操作の傾向やリスクの可視化
  - データ操作の制御と暗号化

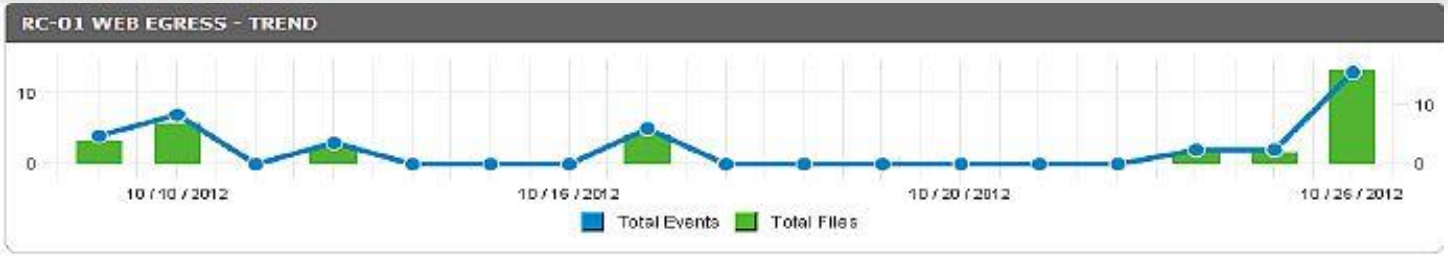
取得した操作ログを
フォレンジック調査用途
のみでなく、迅速な検知と
防御にまで活用する。
ここに、Verdasys の価値があり
ます



特長2：異常な動きを捕まえる

- 活動のベースラインを設ける
  - 外部にデータを送信する経路ごとに
  - ユーザごとに
  - マシンごとに
- ベースラインからの逸脱
  - 異常なユーザの活動のレポートを生成
- 「通常」との差を明らかにする
  - 通常より、どのくらいの差があるのか？
  - アップロードファイルの異常な数（バイト数）
  - 発生したアラートの数

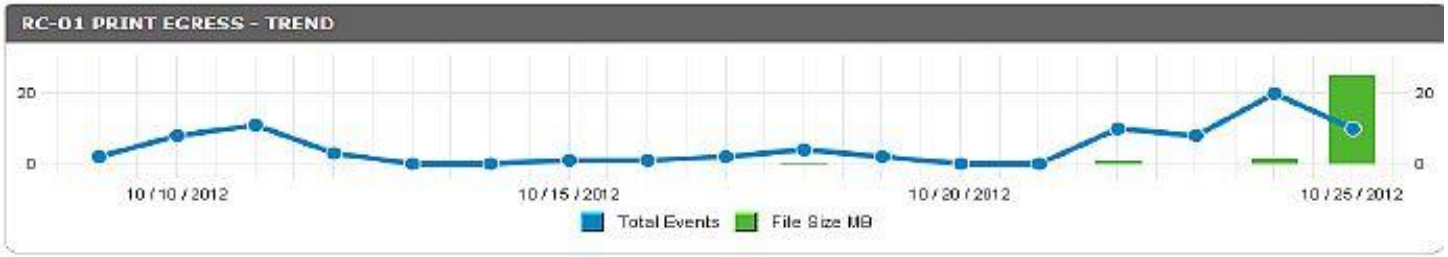
複数のデータを関連付けて異常を見つける



インターネットへのアップロード

メール送信

USBへの書き出し



印刷

VERDASYS

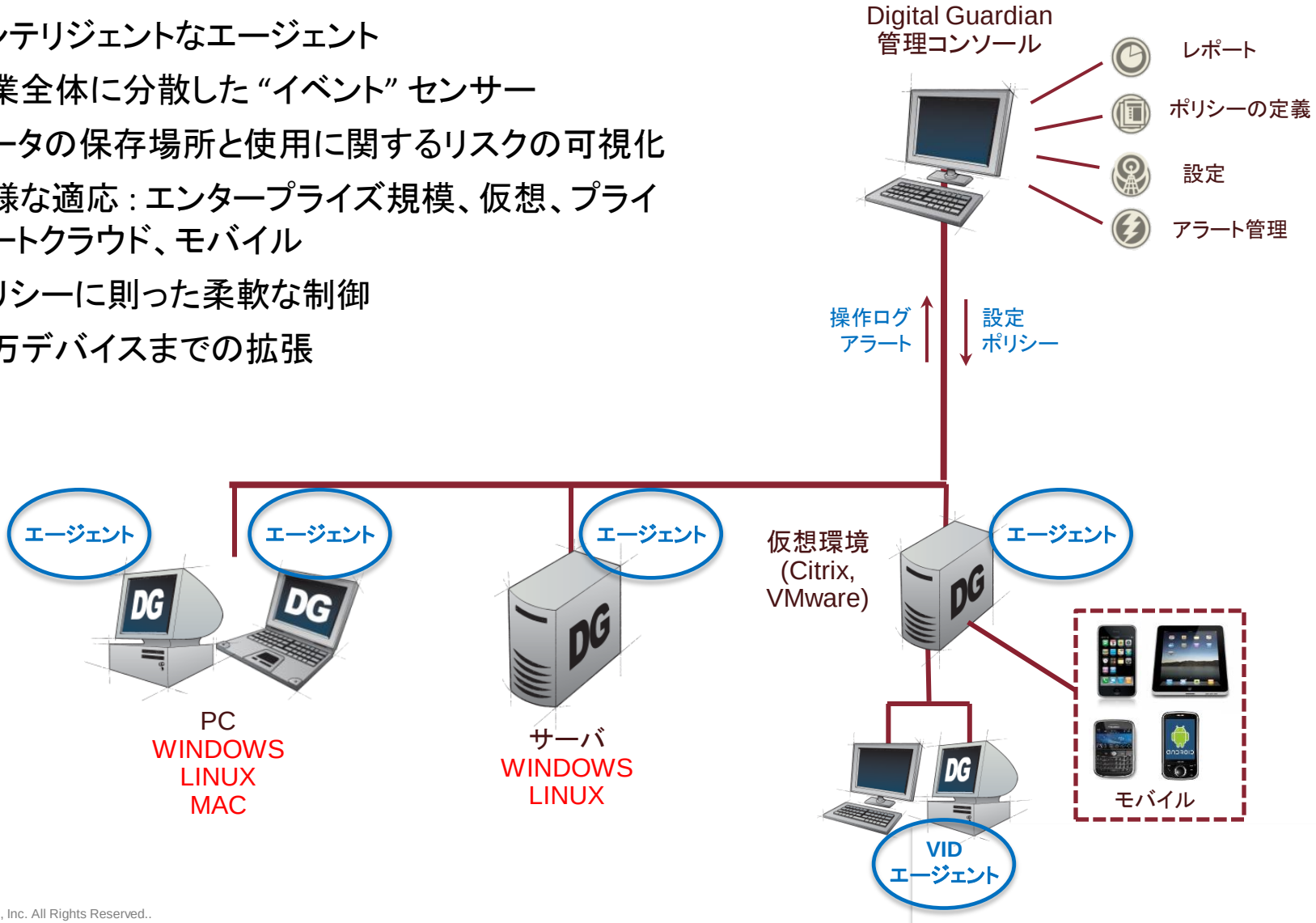
何が見えてくるのか？ （リスクアセスメント）

事例：直近 2 週間だけで・・・

- ビジネス上での申請なしに、80,000 以上のソースコードファイルが、共有ディスクから PC へコピーされた
- 5,739 のプロジェクトに関するファイルが、従業員所有のディスクへコピーされた
- 441 のプロジェクトに関するファイルが、暗号化されずに USB へコピーされた
- 41 のCADファイルが、カスタマネットワーク上の登録されていない、インターナルの IP アドレスへ直接 FTP転送された
- 仕事の情報を含んだ 43 の電子メールが、ひとりの従業員によって、個人の Gmail アカウントへ送られた
- 2 つの CADファイルが、Yahoo メールの知らないアドレスへメールで送られた
- 社内の重要情報が、6つの異なったクラウド共有サービス (Google Drive Sync, Dropbox, Box.com, Windows Live Mesh, Sugar Drive Sync, iCloud) に送られた

Digital Guardian のアーキテクチャ

- インテリジェントなエージェント
- 企業全体に分散した “イベント” センサー
- データの保存場所と使用に関するリスクの可視化
- 多様な適応：エンタープライズ規模、仮想、プライベートクラウド、モバイル
- ポリシーに則った柔軟な制御
- 25万デバイスまでの拡張



特長3：セキュリティに必要な要件を満たす

- Digital Guardian エージェントの「停止不可仕様」
  - **Admin権限を持ったユーザーでも、エージェントを停止できないセキュアなアーキテクチャ**
  - **監視や防御施策そのものを停止できる情報漏洩対策では意味がありません。**
    - ファイルシステム、レジストリ、「プログラムの追加・削除」、「タスクマネージャ」からも見えない「ステルスモード」
    - OS のセーフモード起動時にもエージェントのプロセスを停止できない 「停止不可仕様」
    - アンインストールできないので、物理的な不正改ざんも許さない
- カーネルレベルでのエージェントの稼働
  - **システム上での本来の操作や処理に、負荷はかけません**
  - **きめ細かい制御が可能**
- 管理サーバと接続していなくても、エージェントは単独で稼働

特長4：Verdasys のクラウドサービス
MSIP (情報保護のためのマネージドサービス)

MSIP

Verdasys の
安全なクラウド

Verdasysの
エキスパート

クラウドには
実際のデータは
保存しません

ソリューションエキスパート
がリスクを分析し、データポ
リシーを管理します

操作ログ
（ログのみ）

FIPS140-2

企業側

企業ネットワークに参加
している／していないに
関わらず、エージェント
が操作ログを取得し、ポ
リシーを適応します

ビジネスの観点から、
リスクと対策を確認
します

従業員

管理部門

VERDASYS

アジェンダ

- 情報漏えいを防ぐ最前線
- 標的型攻撃から情報を守る

MSCD
サイバー脅威保護のためのマネージドサービス

- Managed Service for Cyber Defense　の略
- 2013年5月21日　発表

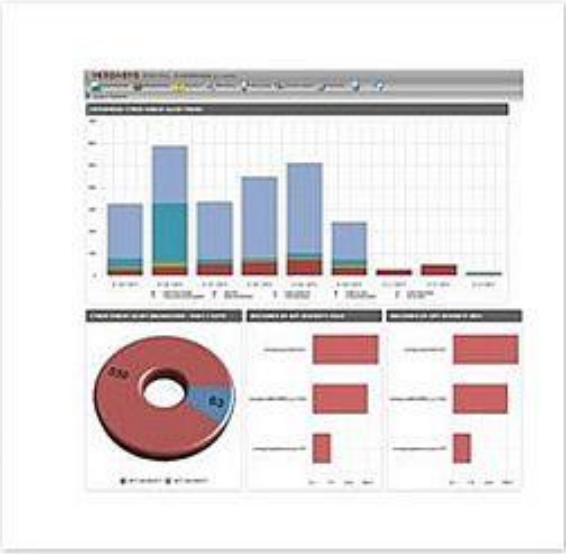
Verdasys Introduces New Managed Service for Cyber Threat Defense

Detects and Prevents Cyber Attacks on Endpoint Devices On or Off the Enterprise Network

Waltham, Mass. (PRWEB) May 21, 2013

Tweet Like +1 Share EMAIL

Verdasys today announced availability of its cloud-based Managed Service for Cyber Defense (MSCD), a fully managed, outsourced service for companies and government agencies that need to prevent increasingly sophisticated malware and persistent cyber attacks from stealing sensitive data.



MCSD leverages Verdasys' Digital Guardian data protection platform by making it available via a hosted service, extending its unique visibility into all data transactions and systems events as well as data exfiltration blocking with new capabilities for multi-layered prevention, detection, containment and investigation of targeted cyber attacks. The new managed solution provides organizations with service-based visibility and control over human and application exploit based cyber attacks, as well as visibility and containment control over the expansion, data access, manipulation and exfiltration stages of a data targeted attack. MSCD is uniquely capable of detecting and preventing cyber attacks on endpoint devices on or off the enterprise network infrastructure.

VERDASYS

Verdasys のクラウドサービス
MSCD (サイバー脅威保護のためのマネージドサービス)

MSCD

Verdasys の
安全なクラウド

Verdasysの
エキスパート

クラウドには
実際のデータは
保存しません

操作ログ
（ログのみ）

FIPS140-2

ソリューションエキスパート
がリスクを分析し、データポ
リシーを管理します

企業側

企業ネットワークに参加
している／していないに
関わらず、エージェント
が操作ログを取得し、ポ
リシーを適応します

従業員

ビジネスの観点から、
リスクと対策を確認
します

管理部門

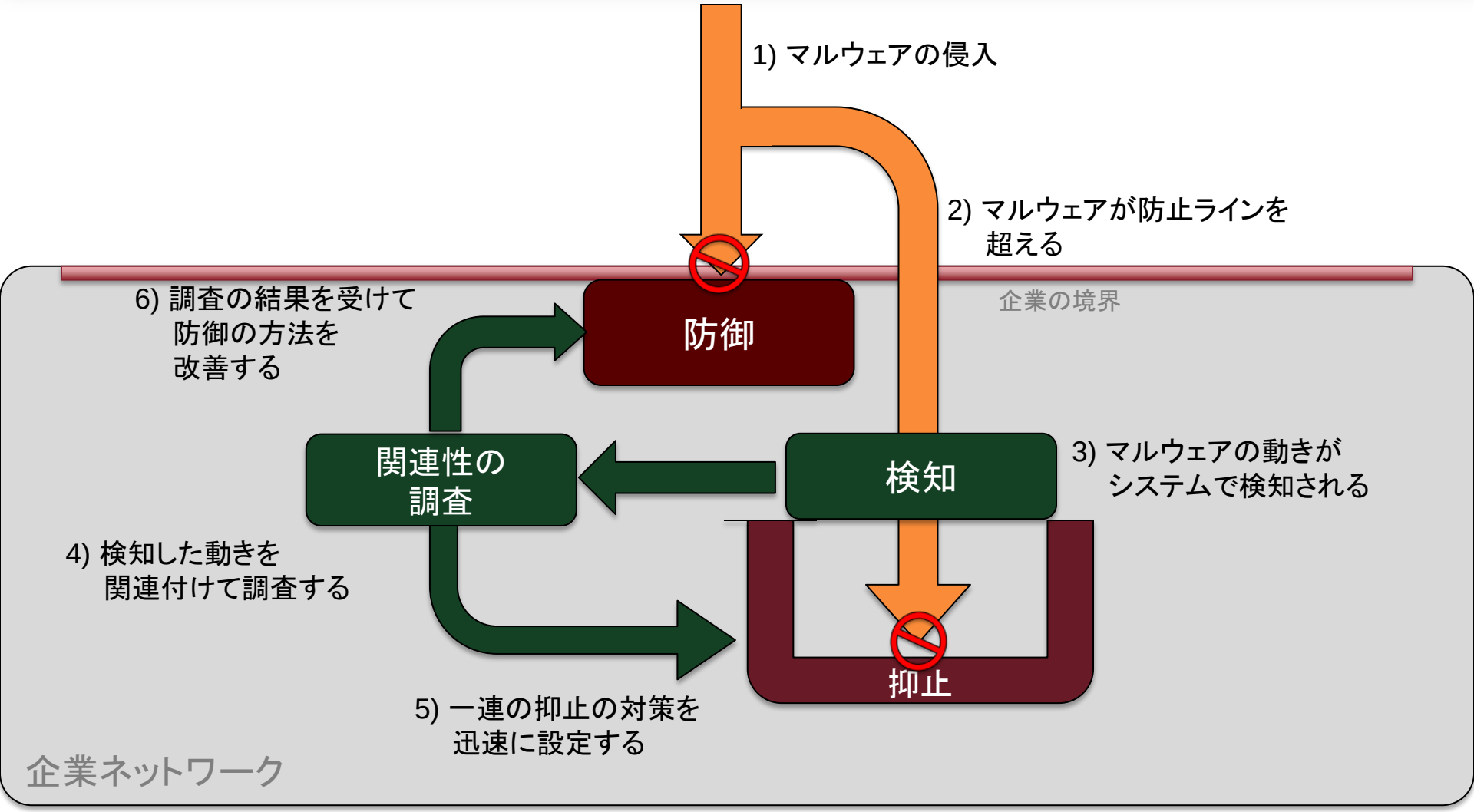
VERDASYS

標的型攻撃の流れを断ち切る

- 標的型攻撃の流れを断ち切る
  - 攻撃はすべてのステップを経なければならない
  - どこかで断ち切れば良い
- 多層的な検知とそれぞれのレイヤに合致した防御
  - 防御は時には失敗するかもしれない。そのため、多層的な検知が重要。
  - 迅速な検知こそが、迅速な対策へと通ずる
- 継続した改善を行う反復のプロセス
  - すべてのレイヤで、脅威に関する知識が蓄積されていく
  - 検知と防御の対策も、変わっていかざるを得ない

VERDASYS

反復するマルウェア検知のプロセス
検知 | 防御 | 調査 | 抑止



VERDASYS

マルウェアを撃退するためのポリシー ：35種類

- Adobe Acrobat or Reader Spawning Child Process
- Adobe reader creating executables
- Adobe Reader Writing EXE or DLL
- Alert on archive file creation from unknown archiver
- Alert on archive file creation from unknown archiver with sensitive data
- Alert on autorun.ini write at root directory
- Alert on multipart rar creation
- Alert on multipart rar creation from unknown archiver
- Alert on multipart rar from unknown archiver with sensitive data
- Alert on possible JAVA exploit
- Capture binaries deleted by user
- Capture JAVA cache
- Detect executables in Java cache
- Detect Java Launch From Browser (Part1)
- Detect Java Launch From Browser (Part2)
- Detect Outbound Threats
- Detect possible CMD.exe shell
- Hosts File Modified
- Inbound connection by system binary
- Incremental_Portscan_Outbound_Part1
- Incremental_Portscan_Outbound_Part2
- Incremental_Portscan_Outbound_Part3
- MS Office Processes Creating Executables
- Outbound connection by rundll32
- Outbound connection by system binary and filtered bad list
- Process bypassing DNS and filtered known bad
- Process launch from a directory root
- Suspicious executable in temp directory
- Suspicious Outbound UDP call (part1)
- Suspicious Outbound UDP calls ALERT (part2)
- Svchost child process NOT from Services.exe
- Using Dynamic DNS sites
- Win7x64 System Binary Not Launching from System32 or sysWoW64
- Win7x64 System Binary Not Launching from Windows directory
- Windows system binaries performing an NTD/NTU [with sensitive data]

VERDASYS

標的型攻撃のステージ ： マルウェア侵入

- ② マルウェア侵入
  - 個人情報を用いた攻撃
    - なりすましメールに添付されたマルウェア
    - なりすましメールのマルウェア感染サイトへのリンク
  - 脆弱性をついた攻撃
    - ネットワーク
    - オペレーティング・システム
    - アプリケーション

- 検知と対策
  - OSやアプリの最新パッチの適用
  - 最新ウィルス定義ファイルでの定期的なスキャン
  - 不正なアドレスからの添付ファイル付きメールの検知
  - 不正なサイトからの実行ファイルダウンロードの検知と防御
  - 不正なプロセス稼働の検知
  - 不正なプロセス実行の防御（ホワイトリスト、ブラックリスト）
  - 特定のプロセスによる子プロセスや実行ファイルの作成を検知
  - そこから作られたものの起動を防御

VERDASYS

標的型攻撃のステージ ： コマンド実行

- ③ コマンド実行
  - 外部との通信
    - マルウェアから外部への通信を試みる
    - 情報を送る（ユーザ、ネットワーク、マシン情報）
  - コマンドを受け取る
    - 次のターゲットの特定方法
    - データの外部送信の方法
  - マルウェアの分業化
    - 最初のマルウェアは容量が小さく、次のマルウェアを呼ぶ込むのが役割
    - ネットワークを流れる暗号化されていないログイン情報の収集マルウェア
    - 脆弱性をチェックするマルウェア、特定の脆弱性を攻撃するマルウェア

- 検知と対策
  - 脆弱性診断等による脆弱性の発見と対策 ＋ 最新パッチの適応
  - 外部との不正通信の検知
  - 不正なサイトからの実行ファイルダウンロードの検知と防御
  - システムファイルの改ざん検知
  - 不正なプロセス稼働の検知
  - 不正なプロセス実行の防御（ホワイトリスト、ブラックリスト）

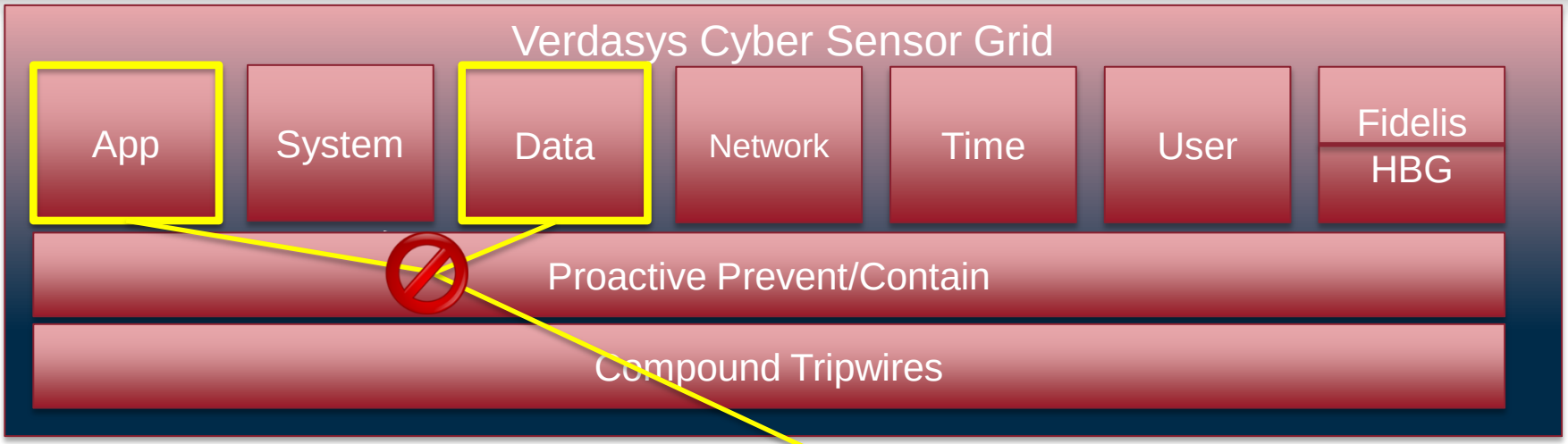
標的型攻撃のステージ ： 情報の持ち出し

- ⑥ 情報の持ち出し
  - 2つの流れ
    - 外部送信ポイントまで標的の情報を移動する、RAR, ZIP, CAB などで暗号化と圧縮を行い、難読化を図る。
    - 外部へデータを送信するための方法を特定する。脆弱性を持ったシステム、リモートアクセス可能なアプリケーション、対FTPサイト、メール送信
  - 時間を掛けて行う
    - 一度に大量のデータを送信する事件もあるが
    - 気づかれないように少しずつ外部送信を行うケースが多い

- 検知と対策
  - 脆弱性診断等による脆弱性の発見と対策 ＋ 最新パッチの適応
  - 出口対策
  - 不正なサイトへのデータ送信を検知 + 防御
  - ユーザがログインしていない時のデータ送信を検知 + 防御
  - プロセスによるアーカイブファイル作成を検知
  - 社外秘情報を定義して外部転送を防ぐ

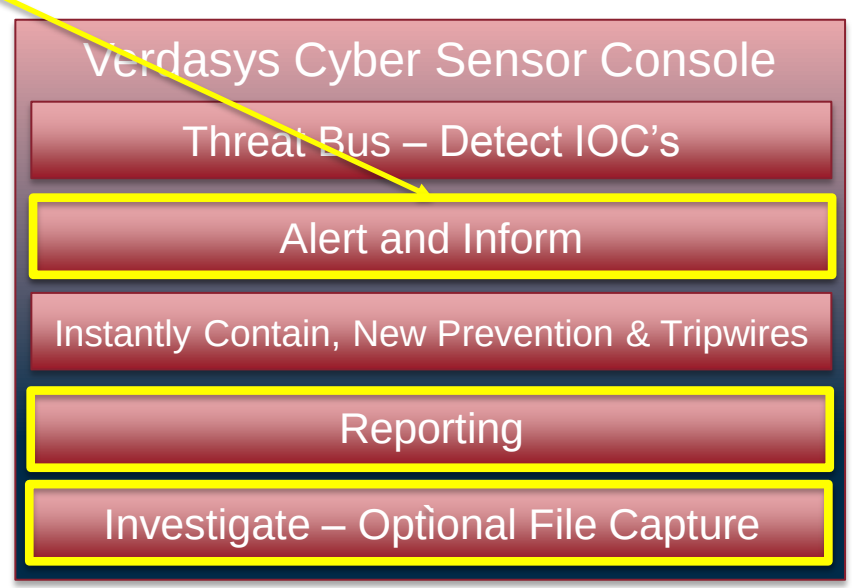
VERDASYS

サイバーフレームワーク
プロアクティブな防御



防御のためのルール例:
- ユーザが怪しいPDFファイルを開く
- Acrod32.exe がExe あるいは DLL ファイルの保存を試みる
- サイバールールがファイルの生成をブロックする
- 感染を防ぐ
- 怪しいPDFファイルを回収する

サイバーコンソールへ送られるアラート:
- 脅威のレベルを引き上げる
- SIEM へリアルタイムで、脅威の情報を送信する
- なりすまし発生のプロンプトをユーザに表示する
- 必要ならば、インシデント対応チームが脅威を調査する



アプリケーション実行　ダッシュボード

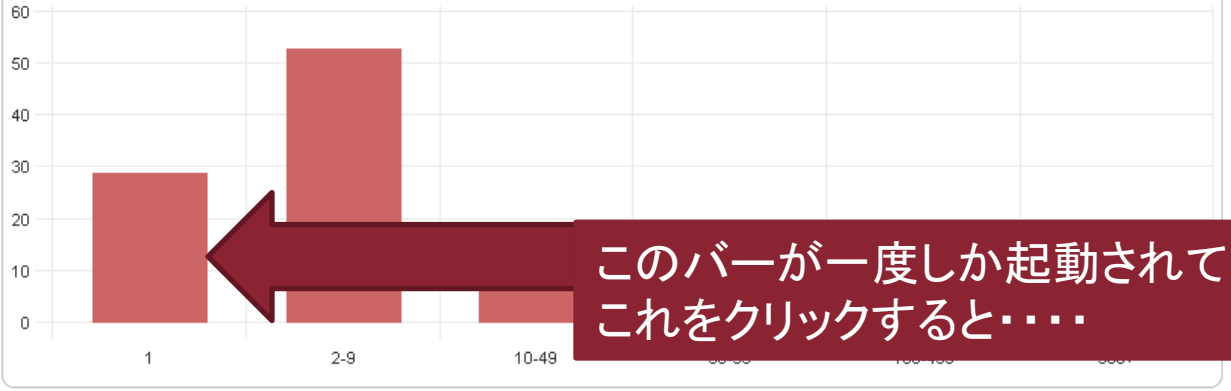
- 一度だけしか起動されていないアプリケーションは？

APT PROCESS RISK

4 records　Export to Excel

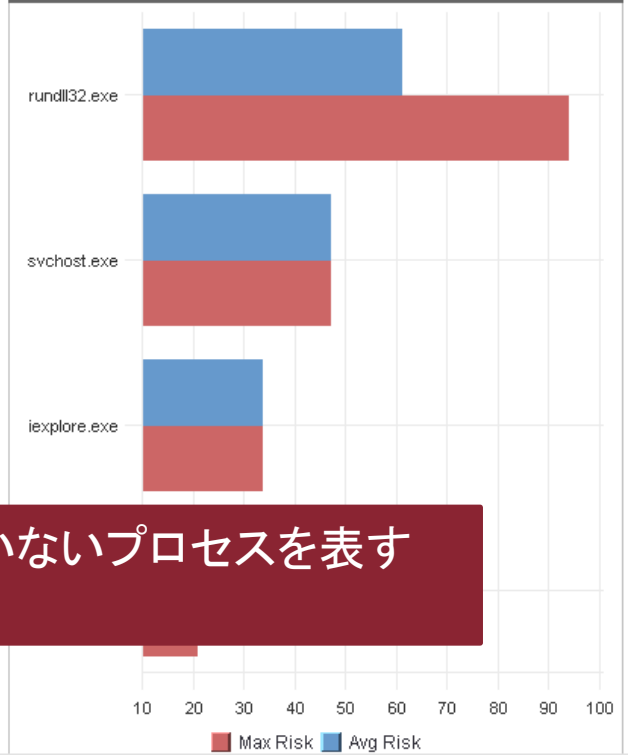
Process Name	Max Risk	Avg Risk
rundll32.exe	93.93	61.175000
svchost.exe	47.03	47.030000
iexplore.exe	33.53	33.530000
dgprompt.exe	20.71	20.710000

PROCESS LAUNCH HISTOGRAM - ABSOLUTE VALUE



このバーが一度しか起動されていないプロセスを表す
これをクリックすると・・・・

APT PROCESS RISK (CHART)



VERDASYS

アプリケーション実行の詳細(ドリルダウン)

- 疑わしいバイナリの詳細を見ることができる

HISTOGRAM PROCESS LAUNCH BY APP

70 records | Export to Excel | 1 2 3 | Records per page: 25

Application	Company Name	Product Name	Product Version	MD5 Hash	Total Launches
arjmjrng.exe				ce7d6a19-7b0a-e2c7-380a-e2de1403bc1f	1
awsylzbu.exe				de606865-7bee-d808-1256-825e777c13fb	1
bvkivhpn.exe				[illegible]	1
dqhimzxb.exe				b7b764bd-7a01-16b8-8216-282f6a0ad8c6	1
edwpvzzf.exe				[illegible]	1
eqnbioke.exe				a0423c3c-c77d-5144-d344-f6a16ee52f49	1
fioxlrcm.exe				d5097cc3-3b19-cd28-42b6-c4b0614a8c0e	1
fiplwjnl.exe				ddb06684-33c3-ffeb-aaa4-e67e89fc42e7	1
fpupycvx.exe				fc6d703d-623f-ec60-f491-bf347994e574	1
gmxdlffn.exe				d60ee4aa-9cde-3c50-ec01-ffce07e70add	1
gnkddmxw.exe				3de87bf8-a20d-e2a0-56dd-d726332f3470	1
gtbcheck.exe				46ce0111-bf61-a795-c057-504f8f920c86	1
hzzerqlx.exe				985fff60-2ebb-6c12-d1ca-0a5dd911c675	1
ichucmpg.exe				e9e8a403-c42b-9052-cadf-1a1fc8fe9b84	1
iqltuuma.exe				58b5b8c7-3a4c-cd8d-9877-b8168c483b4f	1
jlhxtlsi.exe				670baba3-fc62-f541-5ff5-a9b521b36281	1
leonskzt.exe				0f37e7e6-0367-363e-1a1a-878244d8c486	1

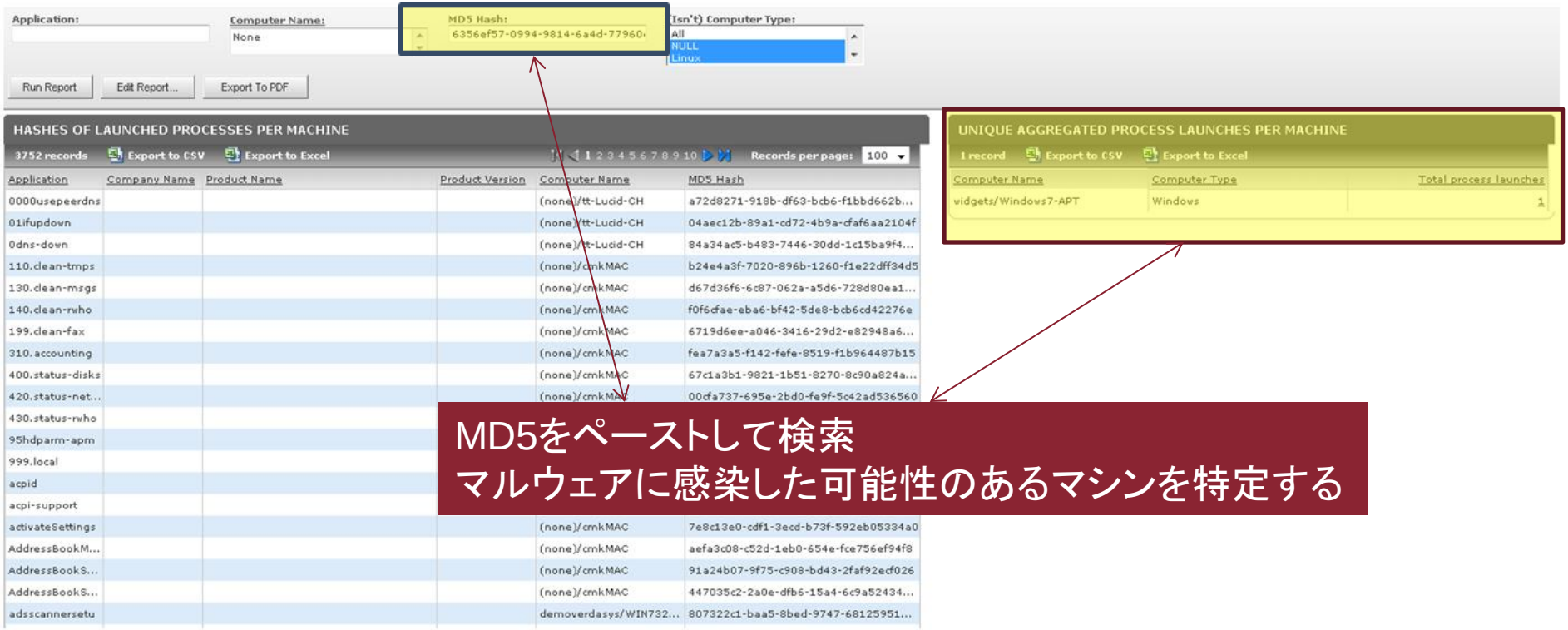
この詳細では:
- でたらめなアプリ名前
- 作成した会社名が入っていない
- プロダクト名もなし
- プロダクトバージョンもなし

ブロックするために、MD5のハッシュをコピーする

VERDASYS

アプリケーション実行／マシンの特定

- 怪しいアプリが稼働したマシンを特定する



VERDASYS

外部への怪しいデータ送信を見つける

1/18/2013 12:05:20 PM		File Delete	micros-pos-ffff\pos1	micros-pos-ffff	cmd.exe

2 records

		Source File	Source Drive Type
⚠		tmp42395410.bat	Fixed
⚠		zeus_binary_cdf3bb9c75000fc49c7c148b76c20b45[1].exe	Fixed

1/18/2013 12:05:20 PM	⚠	File Write	micros-pos-ffff\pos1	micros-pos-ffff	zeus_binary_cdf

1 record

	Source File	Source Drive Type	Destination File	Destination Drive Type	File Size
⚠	tmp42395410.bat	Fixed		Unknown	0 KB

1/18/2013 12:05:19 PM	⚠	Network Operation	micros-pos-ffff\pos1	micros-pos-ffff	explorer.exe

1 record

	Host name	Remote Por	Local Port	Protocol	Direction	Bytes Read	Bytes Written
⚠	www.awlknpetersen.com	80	1123	HTTP	Outbound	0	0

78.142.63.38
http://www.awlknpetersen.com/images/awlk.bin

1/18/2013 12:05:18 PM			fff\pos1	micros-pos-ffff	explorer.exe
1/18/2013 12:05:18 PM		File Rename	fff\pos1	micros-pos-ffff	explorer.exe

1 record

Source File	Source Drive Type	Destination File	Destination Drive Type
adky.uxa	Fixed	adky.tmp	Fixed

1/18/2013 12:05:17 PM	⚠	File Write	micros-pos-ffff\pos1	micros-pos-ffff	zeus_binary_cdf

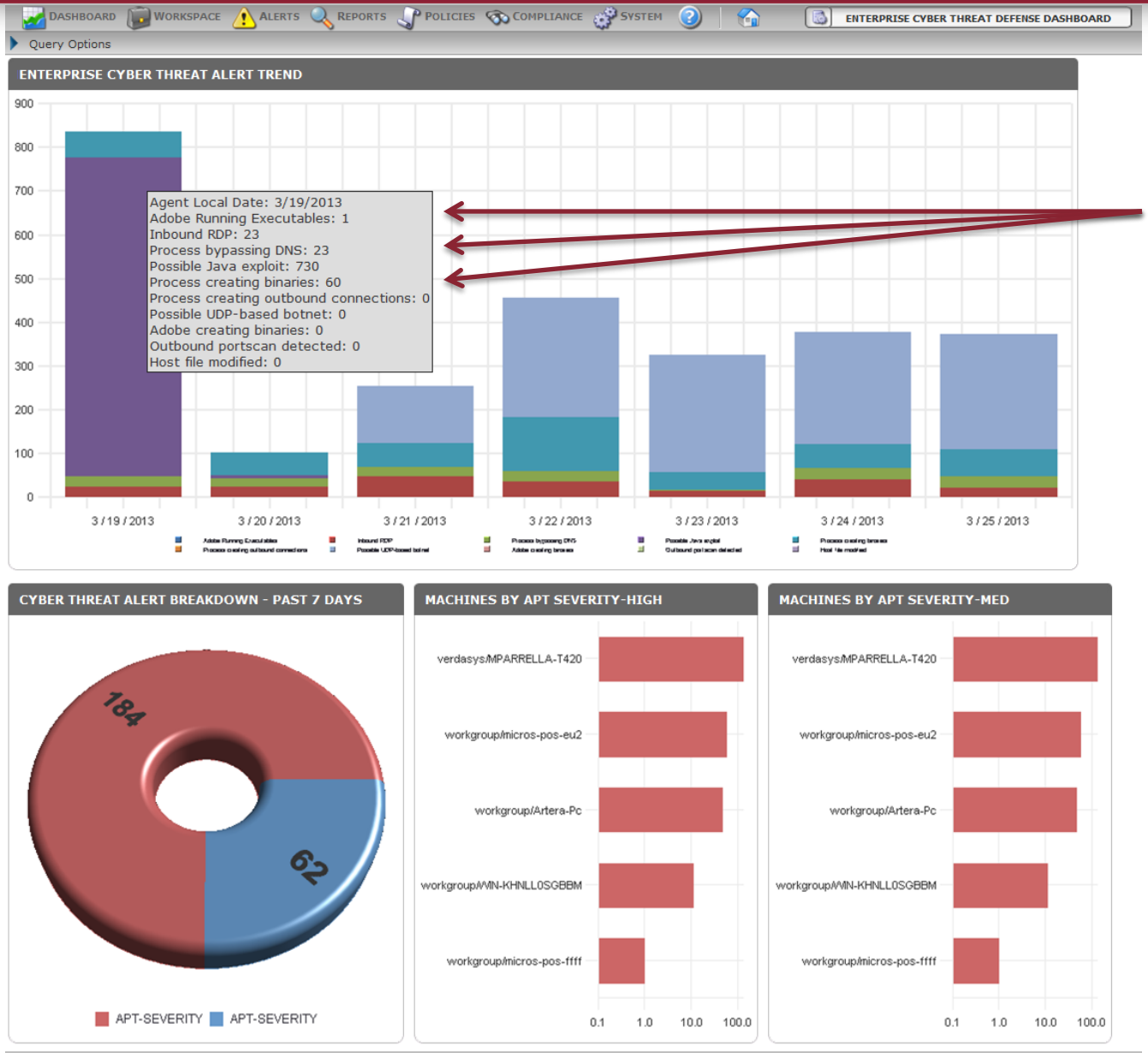
VERDASYS

1分以内で5回以上のボットネット接続

2/19/2013 2:59:28 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Alert on Outbound botn...	iexplore.exe
2/19/2013 2:59:28 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Alert on Outbound botn...	iexplore.exe
2/19/2013 2:59:28 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Outbound botnet call	iexplore.exe
2/19/2013 2:59:28 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Outbound botnet call	iexplore.exe
2/19/2013 2:59:28 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Outbound botnet call	iexplore.exe
2/19/2013 2:59:27 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Outbound botnet call	iexplore.exe
2/19/2013 2:59:27 PM	micros-pos-ffff\pos1	micros-pos-ffff	APT-TW:Outbound botnet call	iexplore.exe

VERDASYS

サイバー脅威から守るための企業ダッシュボード

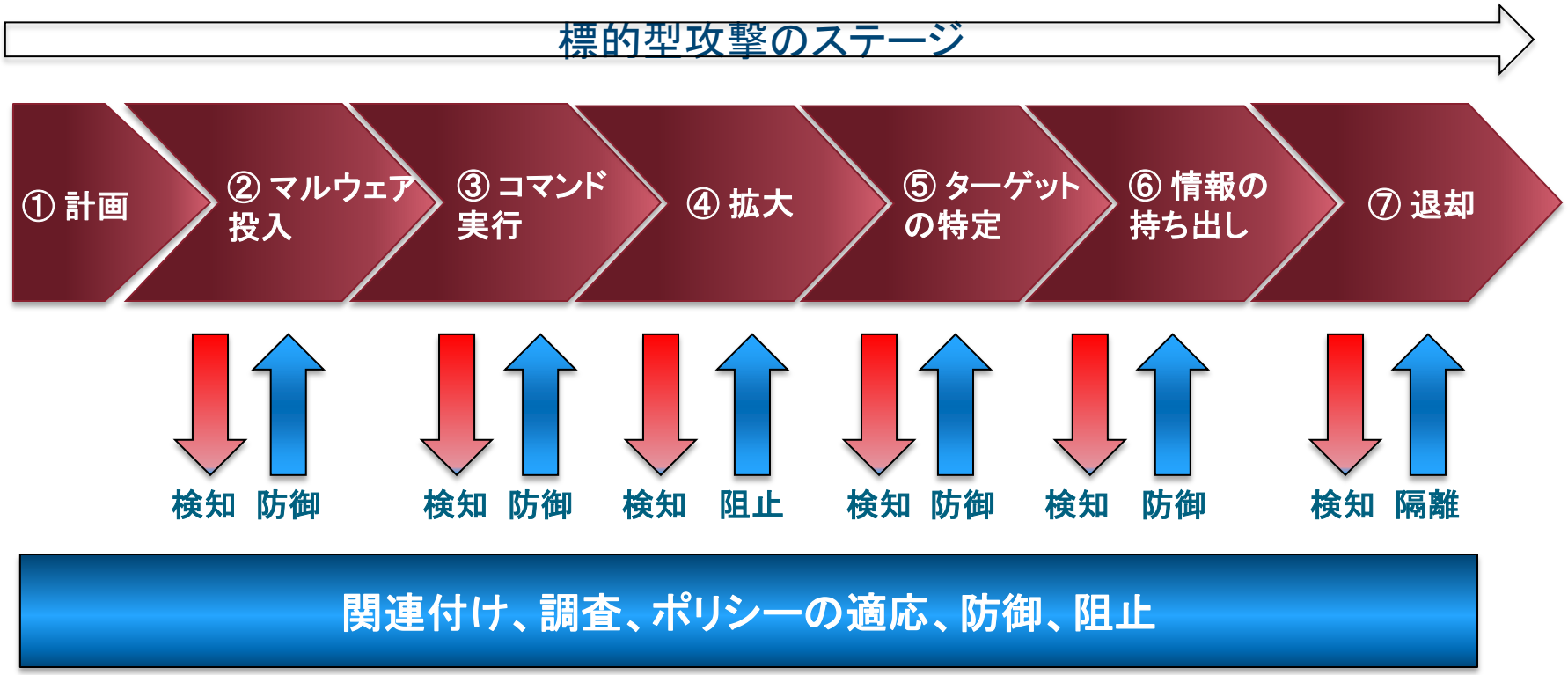


- 企業全体のアラートの傾向を特定する
- マシンごと、重大度ごとに発生したアラートを迅速に特定する

VERDASYS

標的型攻撃の流れを断ち切ります

- **最先端の検知と防御を提供します**



VERDASYS

まとめ

- 情報に特化してがっちりと守る
- 情報の操作ログをリアルタイムで活用する
- リスクを明らかにして、セキュリティレベルを上げていく
- 標的型攻撃への先進的なアプローチ

ご清聴まことに
ありがとうございました

Companies Serious About Protecting Their Information Chose Verdasys

バーダシス株式会社
東京都港区赤坂 2 - 10 - 12
フォーシーズ溜池山王ビル 5F
電話：03 - 3568 - 3157