



Harmony Endpoint ハンズオン勉強会

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

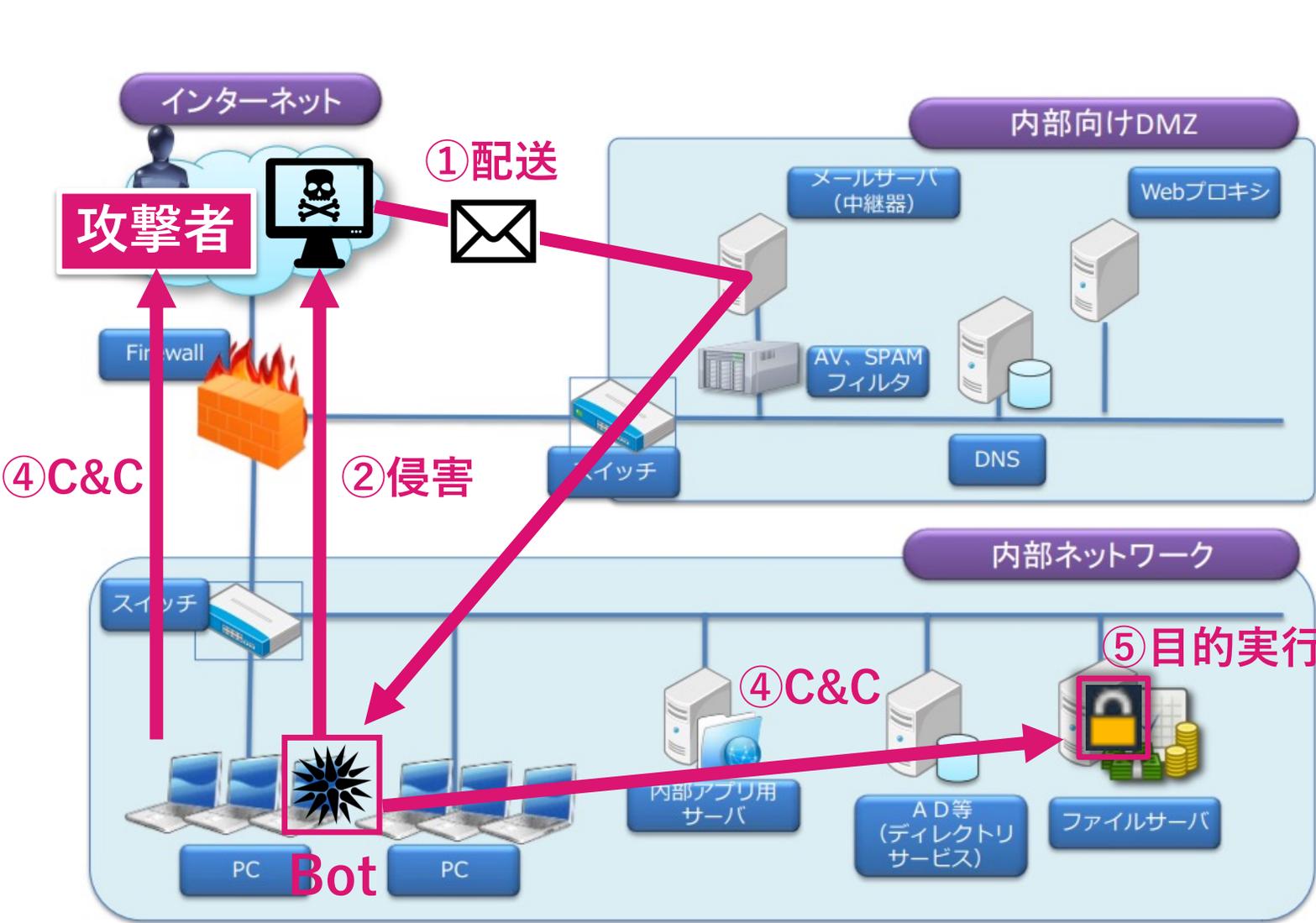
Agenda

- 攻撃者の行動と対策のポイント
- Harmony Endpoint の概要
- Harmony Endpoint 導入の流れ
- インシデントハンドリングでの活用
- Harmony Endpoint の構成概要
- 設定画面の概要
- クライアントのインストール
- クライアントソフトウェアの概要
- クライアントのアップグレード
- バーチャルグループによる管理
- ポリシーバージョンの確認
- Threat Prevention 設定
- 除外設定
- コンピュータの隔離、解放
- ログの表示
- フォレンジックレポート
- Threat Hunting
- アラート通知設定
- アンインストールパスワードの設定
- クライアントのアンインストール

攻撃者の行動と対策のポイント

YOU DESERVE THE BEST SECURITY

サイバー攻撃のイメージと防御機能



③侵入 組織内ネットワーク構成のモデル

偵察	<ul style="list-style-type: none"> • Zero-Phishing
武器化	<ul style="list-style-type: none"> • —
配送	<ul style="list-style-type: none"> • Anti-Malware
侵害	<ul style="list-style-type: none"> • Anti-Malware • URLフィルタ • Threat Emulation, Threat Extraction • Anti-Exploit
侵入	<ul style="list-style-type: none"> • Anti-Malware
C&C	<ul style="list-style-type: none"> • Anti-Bot • Behavioral Guard
実行	<ul style="list-style-type: none"> • Anti-Ransomware

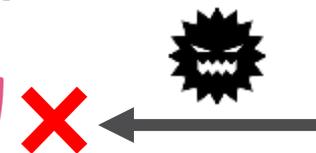
サイバーセキュリティ対策のポイント

1

検知 & 防止

まずはマルウェアに感染しないようにする！

Block!



2

封じ込め

万が一感染した場合、マルウェアによる影響を最小限に抑える！



3

可視化と分析

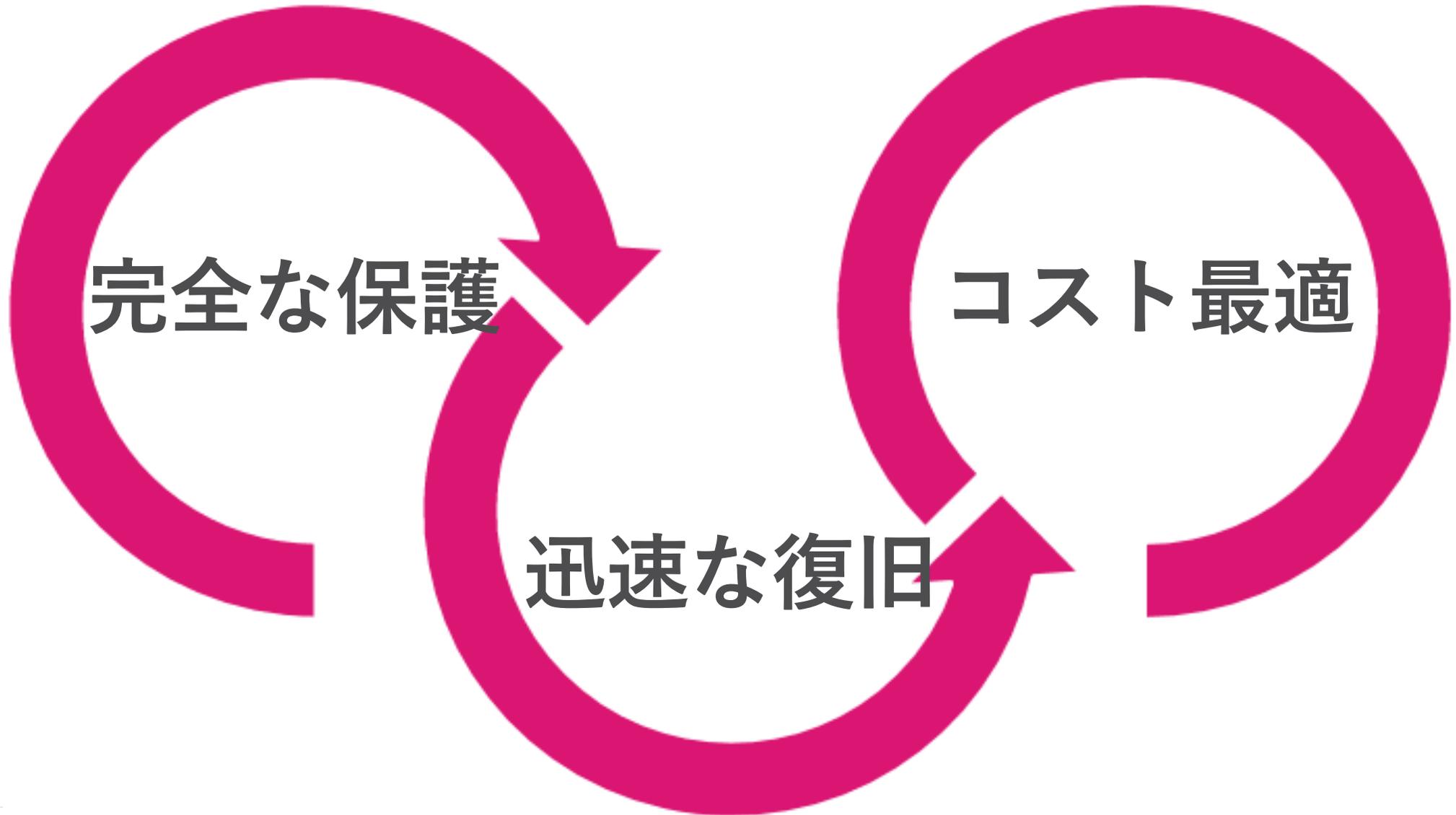
マルウェアを駆除したあと、事後対応や再発防止のために、なにがあったのかを把握する！



HARMONY ENDPOINT の概要

YOU DESERVE THE BEST SECURITY

Harmony Endpoint の特徴



エンドポイントに必要なすべての保護を提供

攻撃からの防御

EPP & NGAV

攻撃の検知と対応

EDR

検知 & 防止



アンチ・マルウェア



サンドボックス



ファイル無害化



ゼロ・フィッシング

封じ込め



アンチ・ランサムウェア



アンチ・ボット



アンチ・エクスプロイト

可視化と分析



フォレンジックレポート



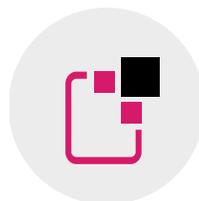
Threat Hunting

Harmony Endpoint の先進の防御技術



サンドボックス

OSレベルとCPUレベルの統合型サンドボックスで攻撃を遮断



ファイル無害化

ファイルの無害化による安全性と生産性の両立



ゼロフィッシング

フィッシングサイトからユーザの認証情報を保護



アンチ・ランサムウェア

ランサムウェアの攻撃を停止し、ファイルを自動復旧



アンチ・ボット

攻撃者との通信を遮断し、攻撃の拡大を阻止



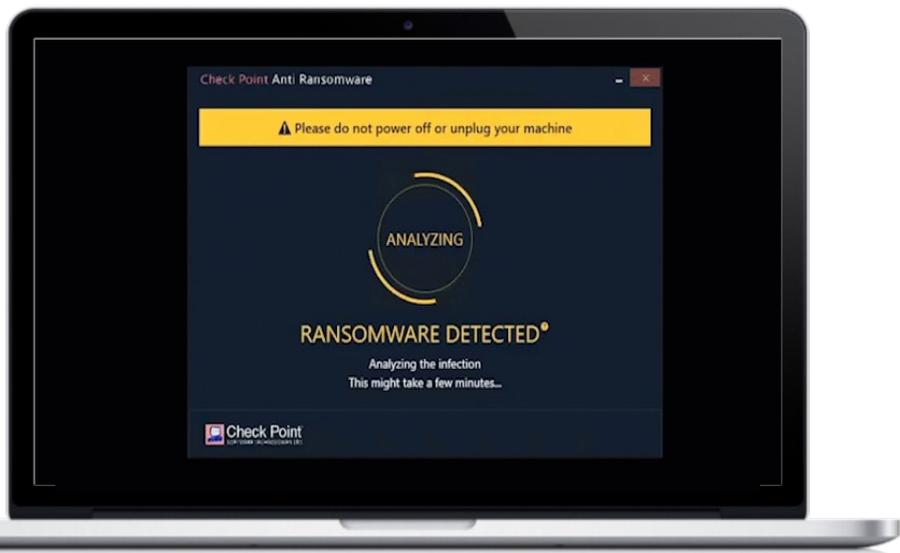
フォレンジックレポート

独自の解析技術による正確性の高い攻撃解析

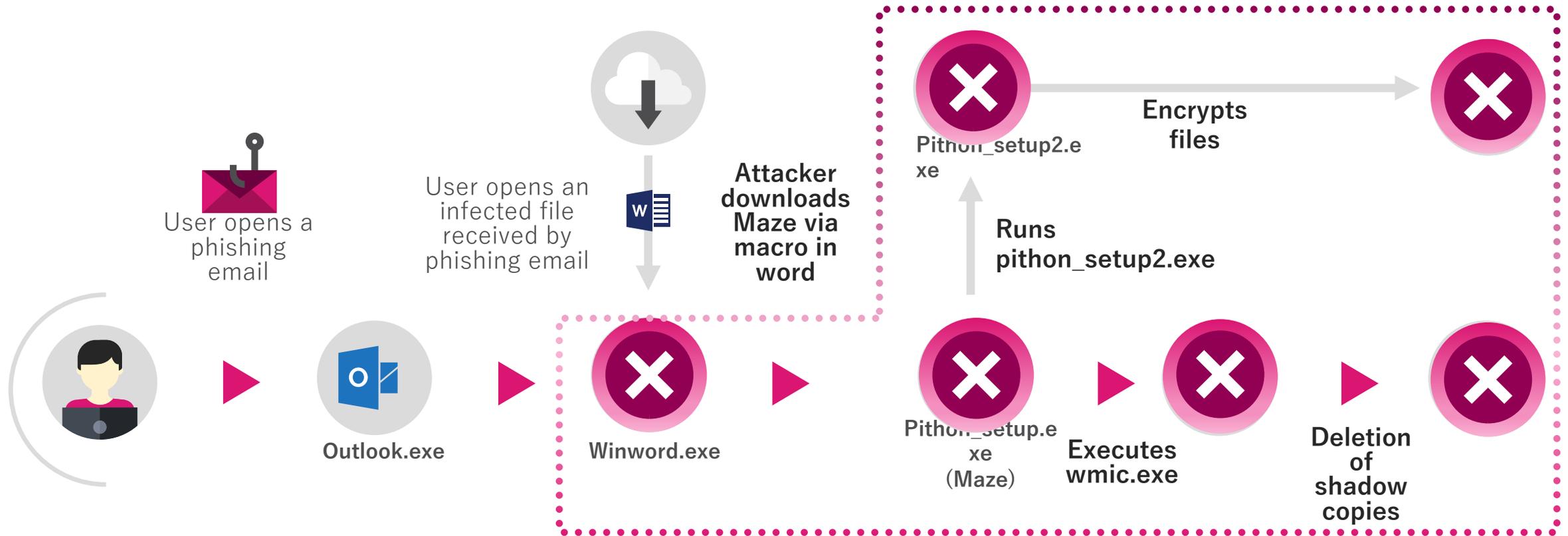
検知、調査、修復作業の 90% を自動化

自動化

- あらゆるイベントを監視、収集
- 攻撃を検知
- 悪意のある活動を隔離
- サイバーキルチェーン全体をクリーンナップ
- 暗号化されたファイルを復元
- フォレンジックレポートを提供



サイバーキルチェーン全体を自動的かつ完全に修復し、ビジネスの継続性を確保



HARMONY ENDPOINT 導入の流れ

YOU DESERVE THE BEST SECURITY

Harmony Endpoint 導入の流れ

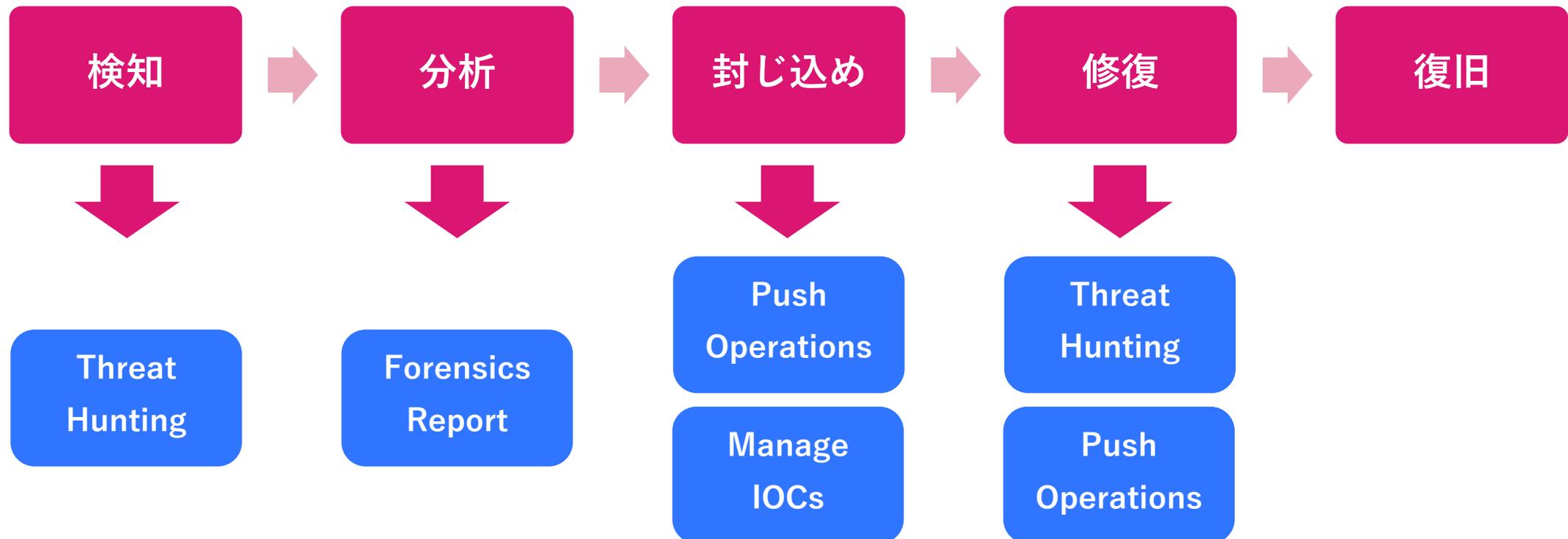


インシデントハンドリングでの活用

YOU DESERVE THE BEST SECURITY

インシデントハンドリングでの活用

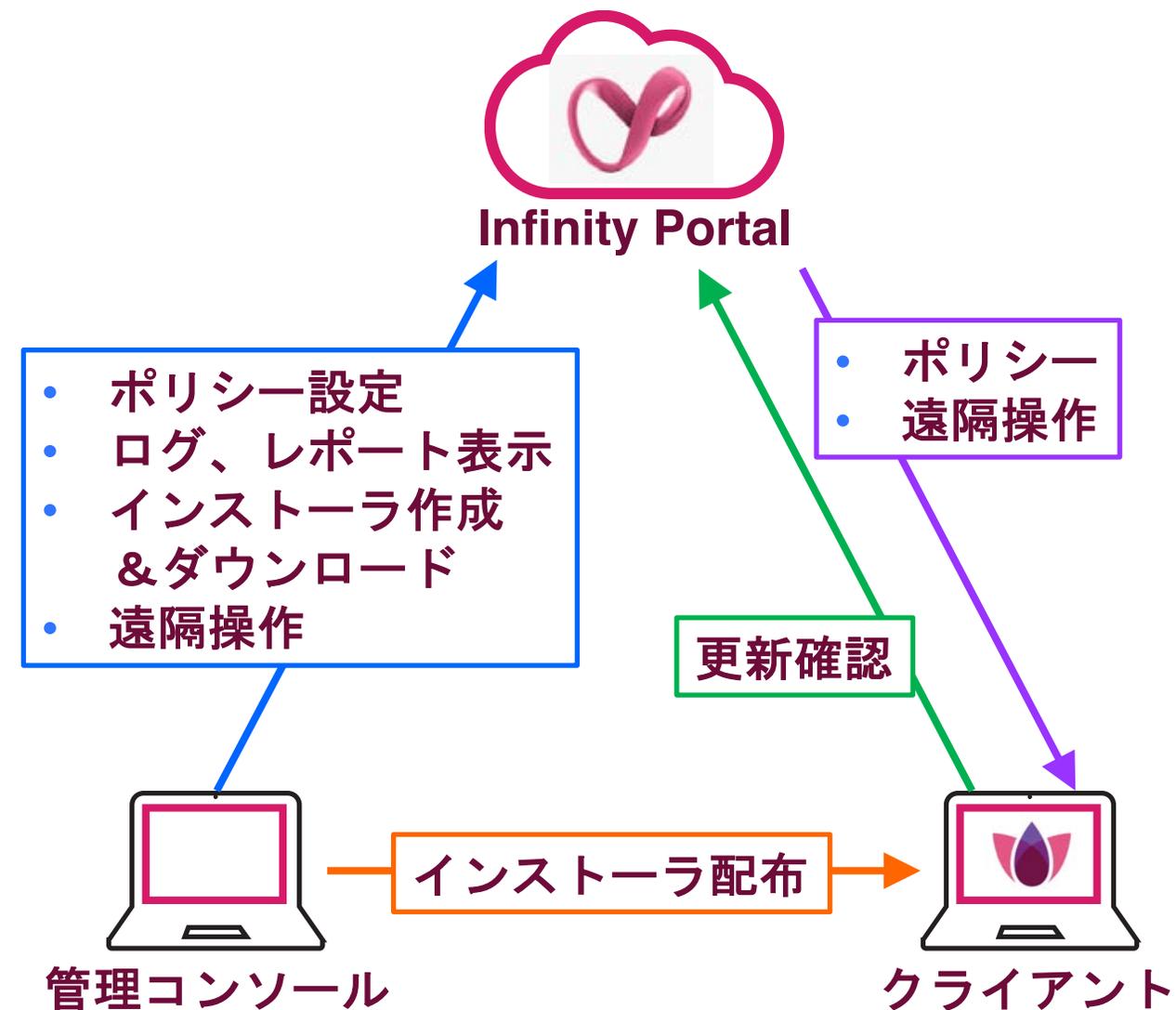
- 検知 : Threat Hunting により、イベントを検知し、管理者にメール通知をする
- 分析 : Forensics Report により、攻撃全体を把握し、侵入経路、影響、修復状況を確認する
- 封じ込め : Push Operations により、感染端末をネットワークから隔離する
- 封じ込め : Manage IOCs により、Forensics Report で確認した IOC に基づくポリシーを適用する
- 根絶 : Threat Hunting、Push Operations により、攻撃の痕跡を探索し、削除する



HARMONY ENDPOINT の構成概要

YOU DESERVE THE BEST SECURITY

Harmony Endpoint の構成概要



1. Infinity Portal

- クラウド上の管理サーバ
- セキュリティポリシーの設定や、ログ、レポートの確認などを実施

2. 管理コンソール

- Infinity Portal にアクセスして管理を行うパソコン
- ブラウザで管理を実施

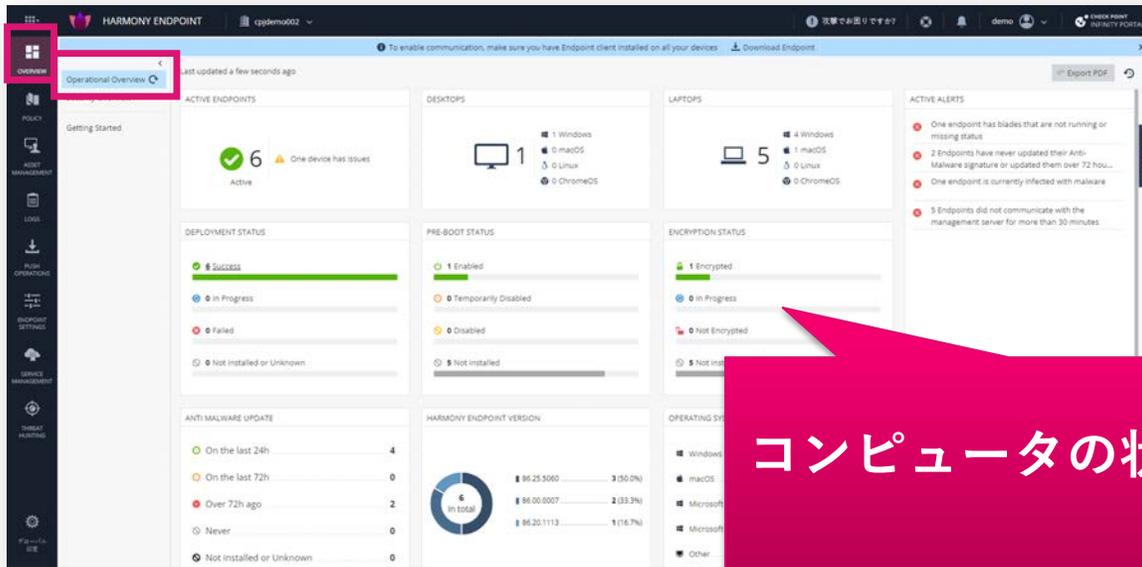
3. クライアント

- Harmony Endpoint がインストールされたパソコン
- 1分毎に Infinity Portal にポリシー等の更新を確認

設定画面の概要

YOU DESERVE THE BEST SECURITY

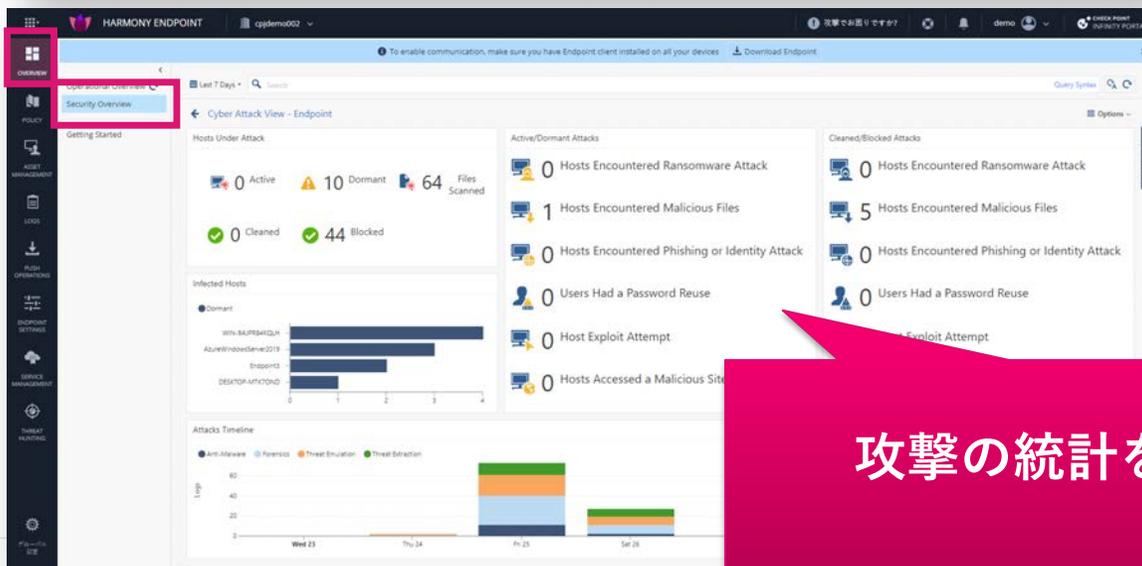
Overview ページ



コンピュータの状態を表示

Operational Overview

- 組織内のエンドポイントクライアントの展開ステータス、それらのヘルスステータス、クライアントバージョン、およびクライアント上のオペレーティングシステムを表示します



攻撃の統計を表示

Security Overview

- エンドポイントクライアントへの攻撃統計を表示します

Policy ページ

#	Rule Name	Applied To	Web & Files	Behavioral	Analysis
0	macOS	macOS			
1	Windows Server	Windows Se...			
2	demo	demo			
3	demo3	demo3			
4	Default settings for the entire organization	Entire Organ...			

設定項目を選択

グループごとに
ポリシーを構成

ポリシーの詳細
を構成

ポリシーを設定

- セキュリティポリシーを構成します
 - 脅威の防止
 - データ保護
 - アクセスとコンプライアンス
- クライアントの設定を構成します
 - ユーザーインターフェース
 - ログ
 - インストールとアップグレード
 - アンインストールパスワード
- クライアントの展開ポリシーを構成します
 - バージョン
 - ブレード (セキュリティ機能)
- インストールパッケージを構成します

Asset Management ページ

リモートからコンピュータを操作

一覧表示

一覧表示の条件選択

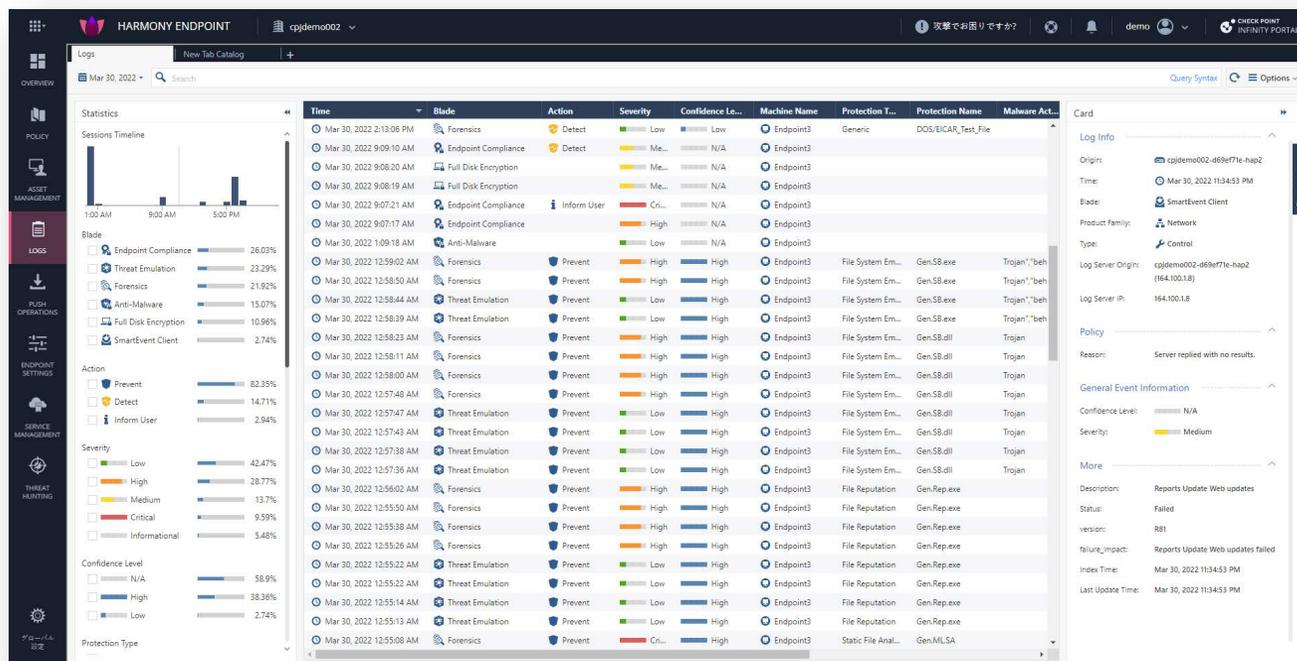
詳細表示

Status	Computer Name	Endpoint Version	OS Build	Device Type	Deployment Status	Deploy Time	Capabilities
Completed	AzureWindowsServ...	86.25.5060	10.0-17763-SP0.0-S...	Desktop	Completed	25 Mar 2022 07:11 pm	
Completed	DESKTOP-TGj6R26	86.00.0007	10.0-19043-SP0.0-S...	Laptop	Completed	22 Mar 2022 12:42 pm	
Completed	Endpoint2	86.00.0007	10.0-19043-SP0.0-S...	Laptop	Completed	18 Mar 2022 06:42 pm	
Completed	Endpoint3	86.25.5060	10.0-19043-SP0.0-S...	Laptop	Completed	25 Mar 2022 01:42 pm	
Completed	WIN-9AJPRB4KQLH	86.25.5060	10.0-17763-SP0.0-S...	Laptop	Completed	25 Mar 2022 01:38 pm	
Completed	adminnomacbook...	86.20.1113	11.6.4 (20G417)	Laptop	Completed	28 Mar 2022 07:37 pm	

コンピュータやグループを管理

- 展開ステータス、コンピューター上のアクティブなコンポーネント、コンピューターにインストールされているクライアントバージョンなど、各コンピューターに関する情報が表示されます
- 事前構成されたビューを選択して表示します
 - 展開
 - コンプライアンス
 - ヘルス
 - フルディスク暗号化
 - マルウェア対策
 - ホストの隔離
 - カスタム（必要な列を選択）

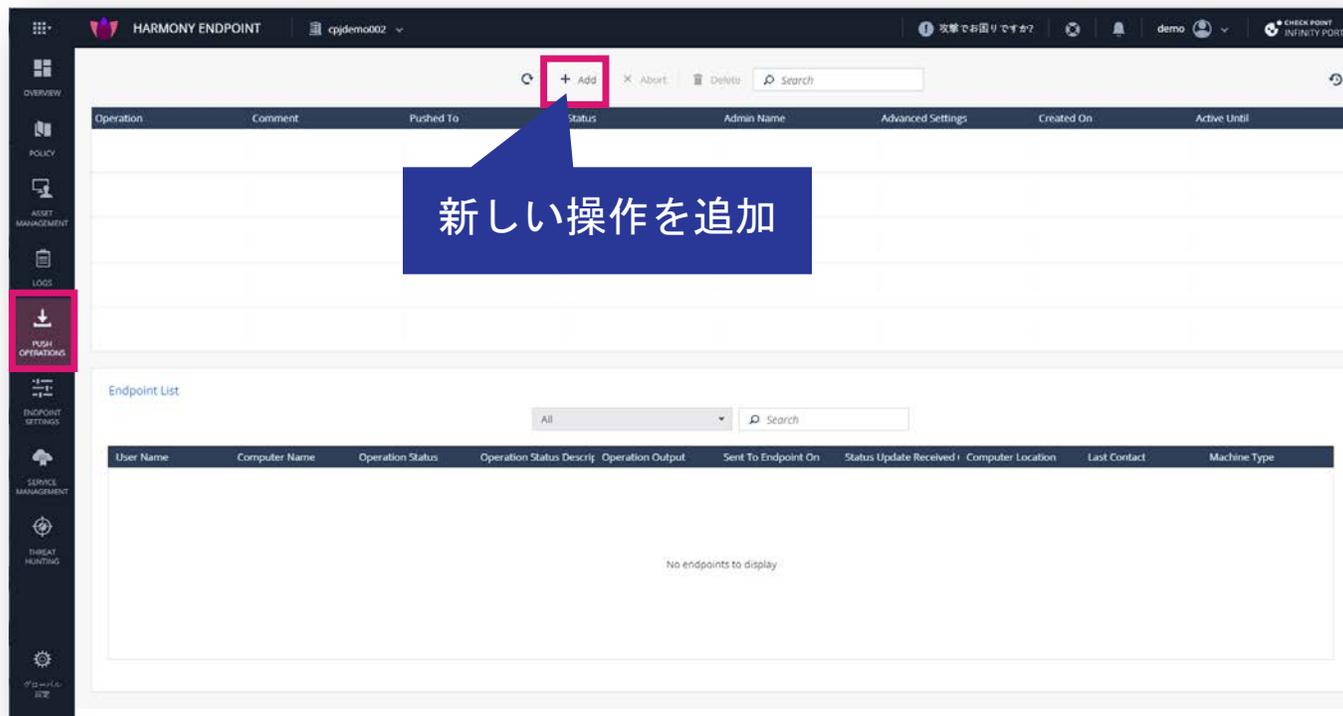
Logs ページ



- アクティビティのログを表示します
- フォレンジックレポートを表示します
- 事前定義された各種ビューやレポートを表示します

ログなどを表示

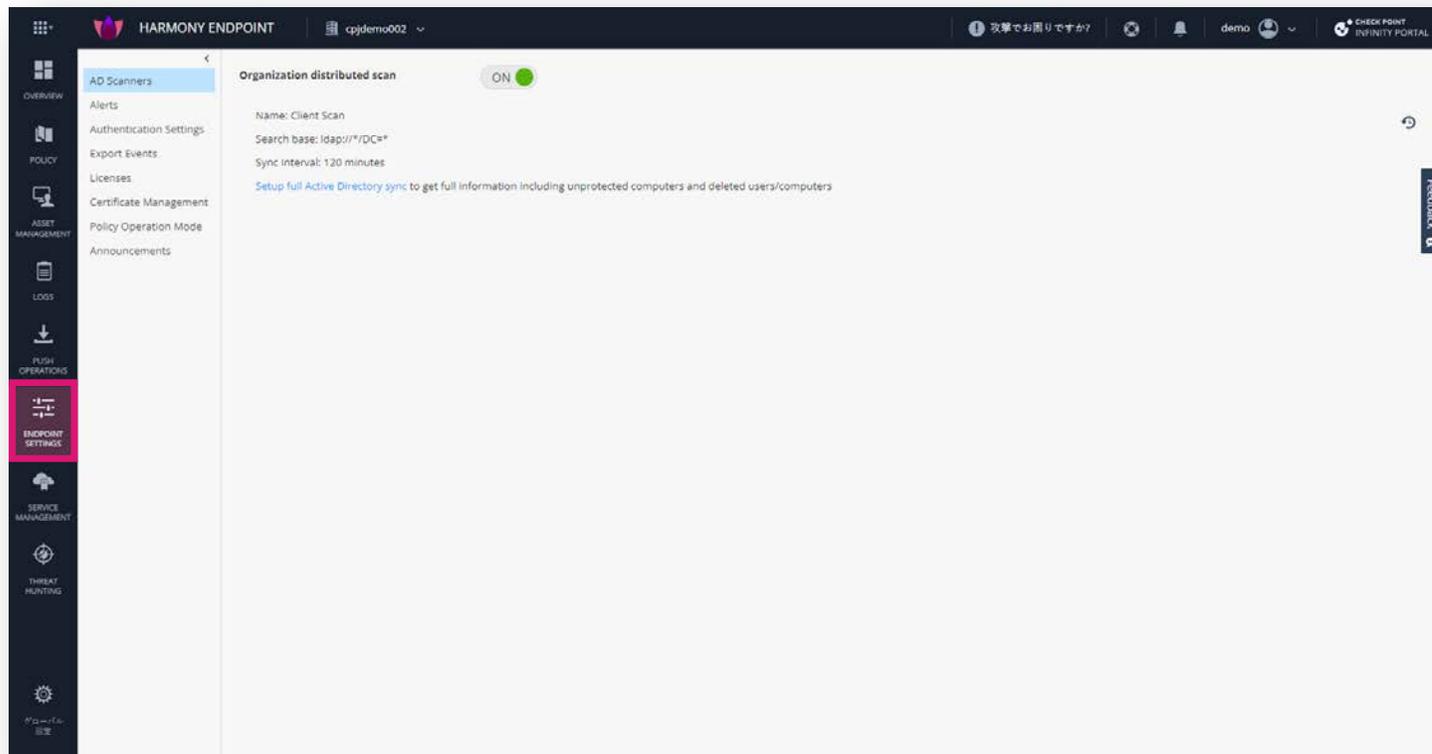
Push Operations ページ



遠隔操作を実施

- リモートからコンピュータを操作します
 - マルウェア対策
 - スキャンの実行
 - シグネチャの更新
 - ファイルを隔離から復元
 - フォレンジックと修復
 - IoC による分析
 - ファイル修復
 - コンピュータの隔離
 - コンピュータの解放
 - エージェント設定
 - クライアントログの収集
 - クライアントソフトの修復
 - シャットダウン
 - 再起動
 - アプリケーションスキャン
 - プロセスの停止
 - リモートコマンド

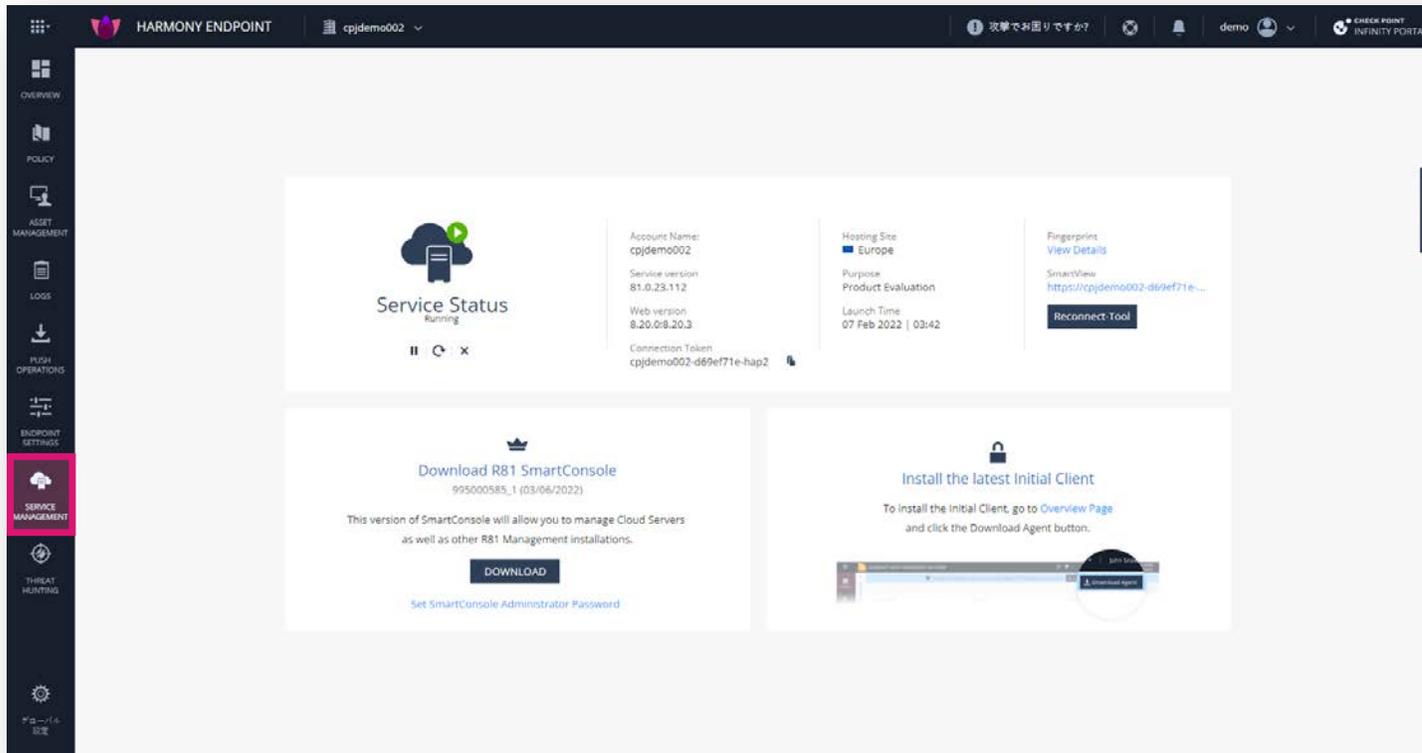
Endpoint Settings ページ



- AD 連携、ライセンス管理、ログのエクスポート (Syslog 連携) など、全体的な設定を行います

全体的な設定

Service Management ページ



サービス(管理機能)の管理を行います

- 一時停止
- 再起動
- 停止

管理サービスの管理

Threat Hunting ページ

- Threat Hunting は、コンピュータでの攻撃情報を収集する調査ツールです
- コンピュータで発生したすべての良性と悪性のイベントを収集し、可視化と調査を可能にします



脅威を探索

クライアントのインストール

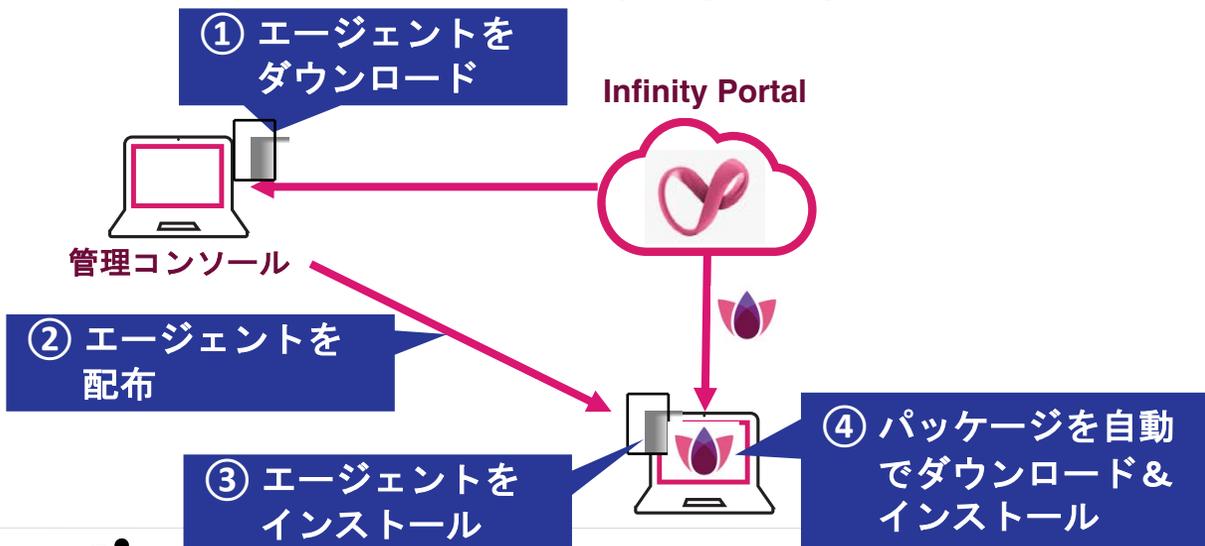
- クライアントの展開方法
- インストールパッケージの概要（オフラインインストール）
- クライアントのインストール

YOU DESERVE THE BEST SECURITY

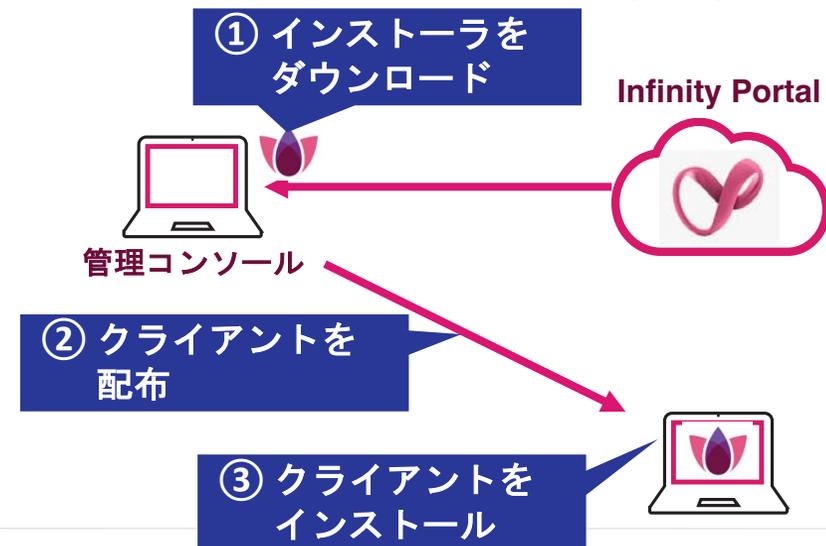
クライアントの展開方法

- オンラインインストールと、オフラインインストールの2種類の方法を選択できます
- **オンラインインストール**
 - 軽量のインストーラを用いてエージェントのインストールを行います
 - エージェントのインストール後にパッケージを自動でダウンロードしてインストールします
 - ホームワークやテレワークのコンピューターへのインストールにおすすめです
- **オフラインインストール**
 - 必要なセキュリティ機能を含むインストーラを用いてクライアントのインストールを行います
 - 社内ネットワークに接続されたコンピューターへのインストールにおすすめです
- ファイルサーバやメールでインストーラを共有する以外にも、Active Directory や 3rd Party のツールを使用してインストールすることも可能です

オンラインインストール



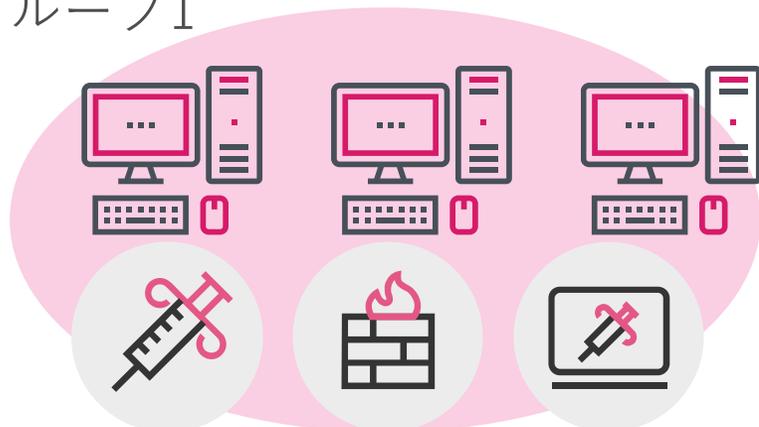
オフラインインストール



インストールパッケージの概要（オフラインインストール）

- インストールパッケージを作成する際は、クライアントのバージョン、インストールする機能、バーチャルグループ、VPNサイト（VPN利用時のみ）を構成します
 - バーチャルグループを指定することで、自動的にコンピュータをバーチャルグループに所属させることができます（Web UI でも変更可能です）
 - **Policy > Deployment Policy > Software Deployment** の設定は、インストールパッケージ作成時のクライアントバージョン、インストールする機能の構成と同じ設定にしてください。異なる場合、**Software Deployment** で設定したバージョン、機能にクライアントソフトウェアが更新されます
- インストールパッケージは、事前定義されたパッケージを使用することも可能です
 - Linux は、事前定義されたパッケージのみを使用可能です

グループ1



グループ2



インストールパッケージの作成 (1 / 5)

Policy > Export Packages > Endpoint Client

The screenshot displays the Harmony Endpoint management console. The left sidebar shows the navigation menu with 'POLICY' and 'Export Package' highlighted. The main content area shows a list of export packages, including 'Linux All Capabilities', 'macOS All Capabilities', and 'Windows All Capabilities'. A 'CREATE EXPORT PACKAGE' dialog box is open, showing the 'OPERATING SYSTEM' step. The dialog has three steps: 1. OPERATING SYSTEM, 2. CAPABILITIES, and 3. VIRTUAL GROUPS. In the 'OPERATING SYSTEM' step, the 'Package name' field is empty with a placeholder 'Type name...'. The 'Operating System' section shows two options: 'Windows' (selected with a blue checkmark) and 'macOS'. The 'Package version' dropdown is set to 'Any CPU'. Below the dropdown, there are two radio buttons: 'Windows 64bit' (unselected) and 'Windows 32bit' (selected). A 'NEXT' button is visible at the bottom right of the dialog.

インストールパッケージの作成 (2 / 5)

Policy > Export Packages > Endpoint Client

Windows

macOS

The screenshot shows the 'CREATE EXPORT PACKAGE' interface for Windows and macOS. The interface is divided into two main sections: Windows (left) and macOS (right). The Windows section has a sidebar with three steps: 1 OPERATING SYSTEM, 2 CAPABILITIES, and 3 VIRTUAL GROUPS. The macOS section has a sidebar with two steps: 1 OPERATING SYSTEM and 2 CAPABILITIES. The main content area for both sections includes a 'Package name' field, an 'Operating System' selection area, and a 'Package version' dropdown menu. The Windows section also includes a radio button selection for 'Windows 64bit' and 'Windows 32bit'. The macOS section includes a 'NEXT' button at the bottom right.

パッケージ一覧で表示されるパッケージ名を指定

OS を指定

Harmony Endpoint のクライアントのバージョンを指定

Windows OS が 64bit版 か 32bit版かを指定

インストールパッケージの作成 (3 / 5)

Policy > Export Packages > Endpoint Client

Windows

CREATE EXPORT PACKAGE

OPERATING SYSTEM

2 CAPABILITIES

3 VIRTUAL GROUPS

4 DYNAMIC PACKAGE

Capabilities

- Threat Prevention
 - Anti Malware
 - Anti Bot & URL Filtering
 - Anti Ransomware, Behavioral Guard and Forensics
 - Threat Emulation & Anti Exploit
- Data Protection
 - Full Disk Encryption
 - Media Encryption & Port Protection
- Remote Access VPN
- Access & Compliance
 - Compliance
- Firewall & Application Control

BACK NEXT

macOS

CREATE EXPORT PACKAGE

2 CAPABILITIES

3 VIRTUAL GROUPS

Capabilities

- Threat Prevention
 - Anti Malware
 - Anti Ransomware, Behavioral Guard and Forensics
 - Threat Emulation & Anti Exploit
- Data Protection
 - Full Disk Encryption
 - Media Encryption
- Remote Access VPN
- Access & Compliance
 - Firewall
 - Compliance

BACK NEXT

※ PushOperations で端末の隔離を実施する場合は、Firewall Bladeが必要

インストールパッケージの作成 (4 / 5)

Policy > Export Packages > Endpoint Client

Windows & macOS 共通

CREATE EXPORT PACKAGE

OPERATING SYSTEM

CAPABILITIES

3 VIRTUAL GROUPS

4 DYNAMIC PACKAGE

Virtual group

VPN site

BACK NEXT

パッケージをインストールしたコンピュータが所属するバーチャルグループを指定

リモートアクセスVPN機能を含める場合に、接続するVPNサイトを設定

インストールパッケージの作成 (5 / 5)

Policy > Export Packages > Endpoint Client

Windows のみ

CREATE EXPORT PACKAGE

To get an MSI file, run EndpointSetup.exe /CreateMSI

Minimize package size (takes longer)

General settings

Disable the Endpoint Security Client's user interface

Dependencies settings

Harmony Endpoint Client requires the following components to be installed.

- .NET Framework 4.6.1 Installer (60MB)
- 32-bit support (40MB)
- Visual Studio Tools for Office Runtime 10.0.50903 (40MB)

Total size of included dependencies: 40MB

Anti-Malware settings

Select the signature profile you wish to include in the package.

Included signatures:

Download package when saved

BACK FINISH

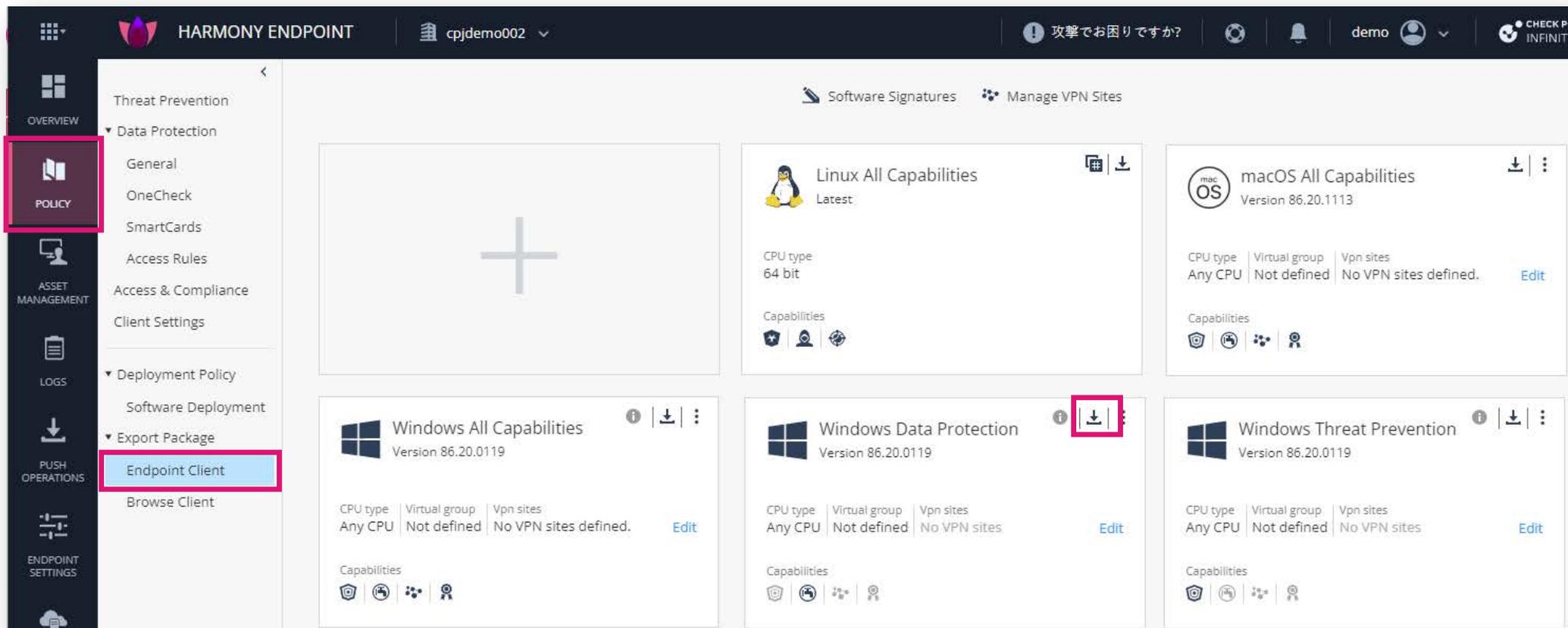
不要な機能を削減して、パッケージサイズを最小化することが可能

パッケージに含める Anti-Malware のシグネチャを選択

インストールパッケージのダウンロード

Policy > Export Packages > Endpoint Client

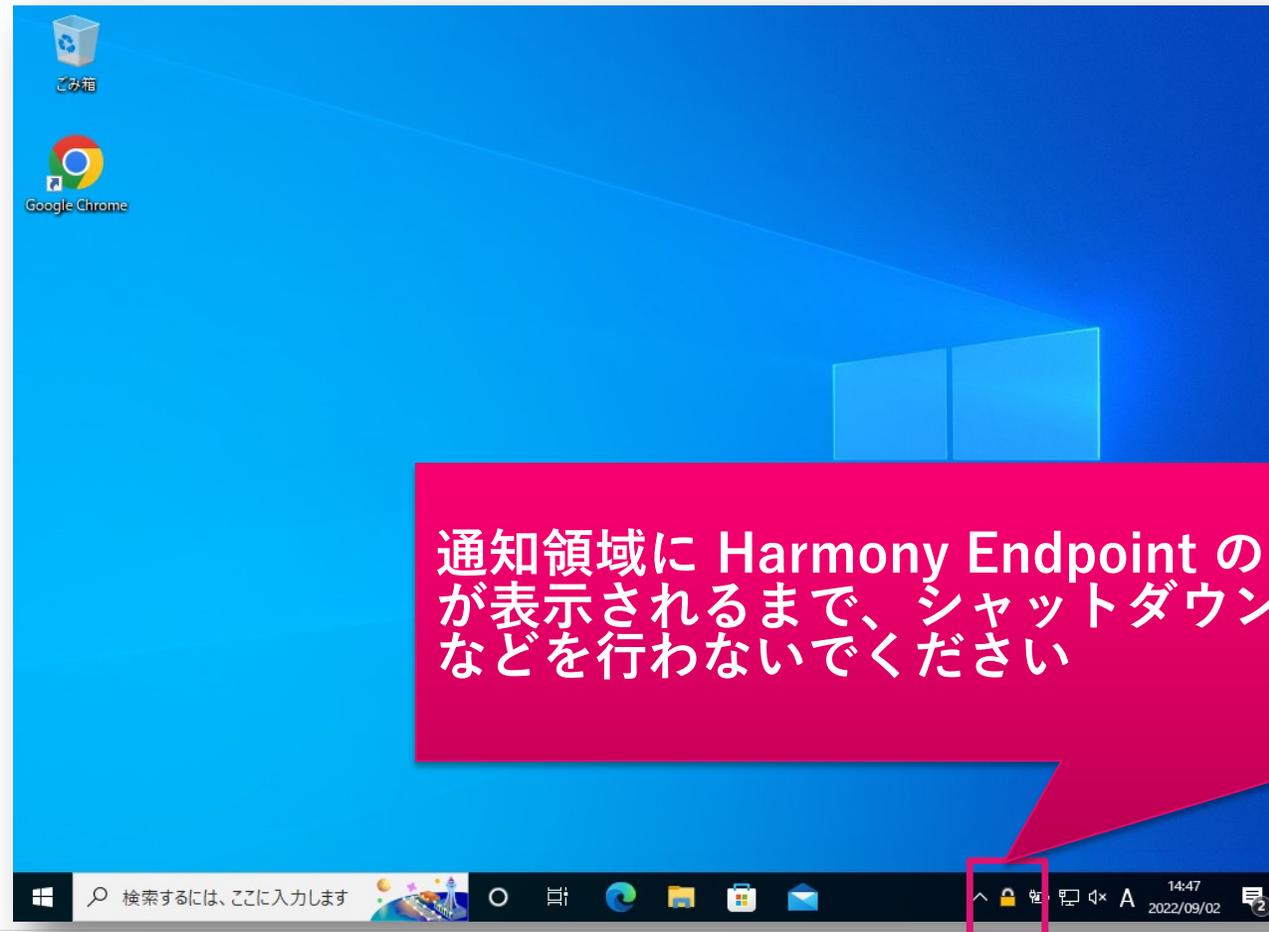
- ダウンロードするパッケージの  をクリックしてパッケージをダウンロードします



The screenshot displays the Harmony Endpoint management console. The left-hand navigation menu is visible, with the 'POLICY' section highlighted in a red box. Within the 'POLICY' section, the 'Export Package' sub-menu is expanded, and the 'Endpoint Client' option is highlighted in a blue box. The main content area shows a grid of software packages. The 'Endpoint Client' package is highlighted in a red box, and its download icon (a downward arrow) is also highlighted in a red box. Other packages shown include 'Linux All Capabilities', 'macOS All Capabilities', 'Windows All Capabilities', 'Windows Data Protection', and 'Windows Threat Prevention'. Each package card displays its name, version, CPU type, virtual group, and VPN sites, along with an 'Edit' button and a download icon.

クライアントのインストール

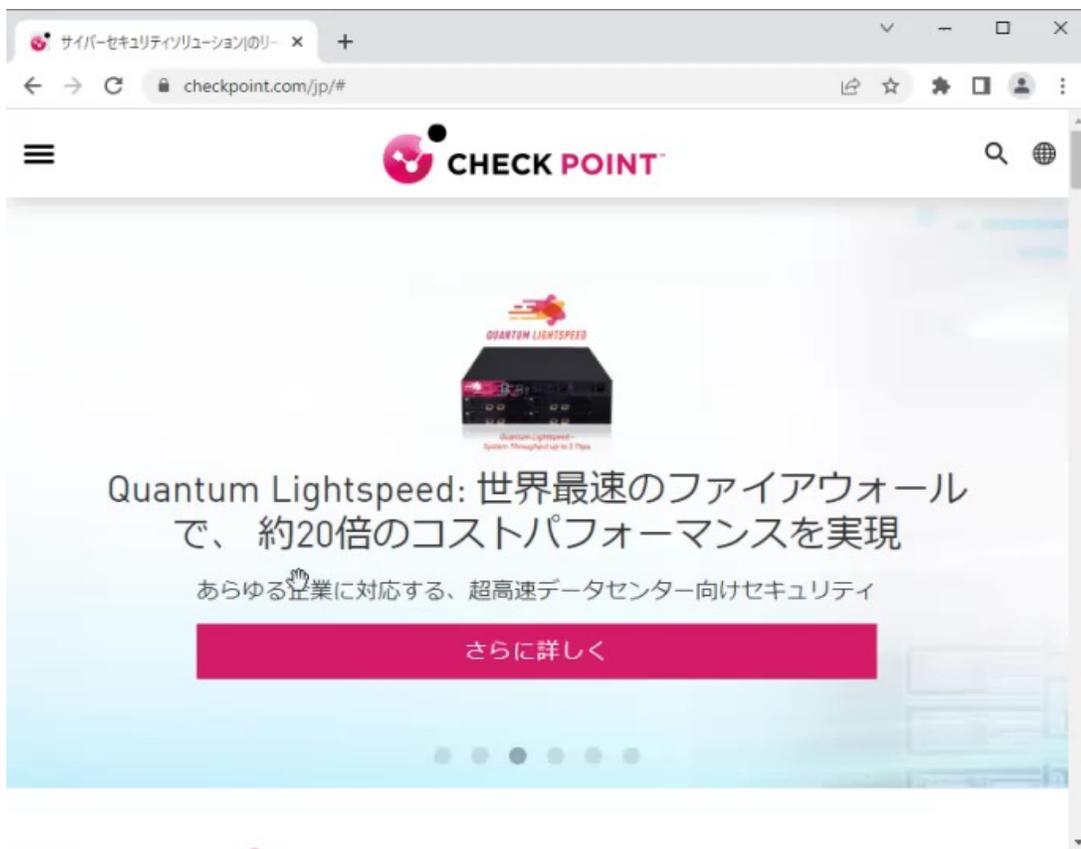
- インストールパッケージをダブルクリックします
- 通知領域に Harmony Endpoint のアイコン  が表示されるまで、シャットダウンや再起動などを行わないでください



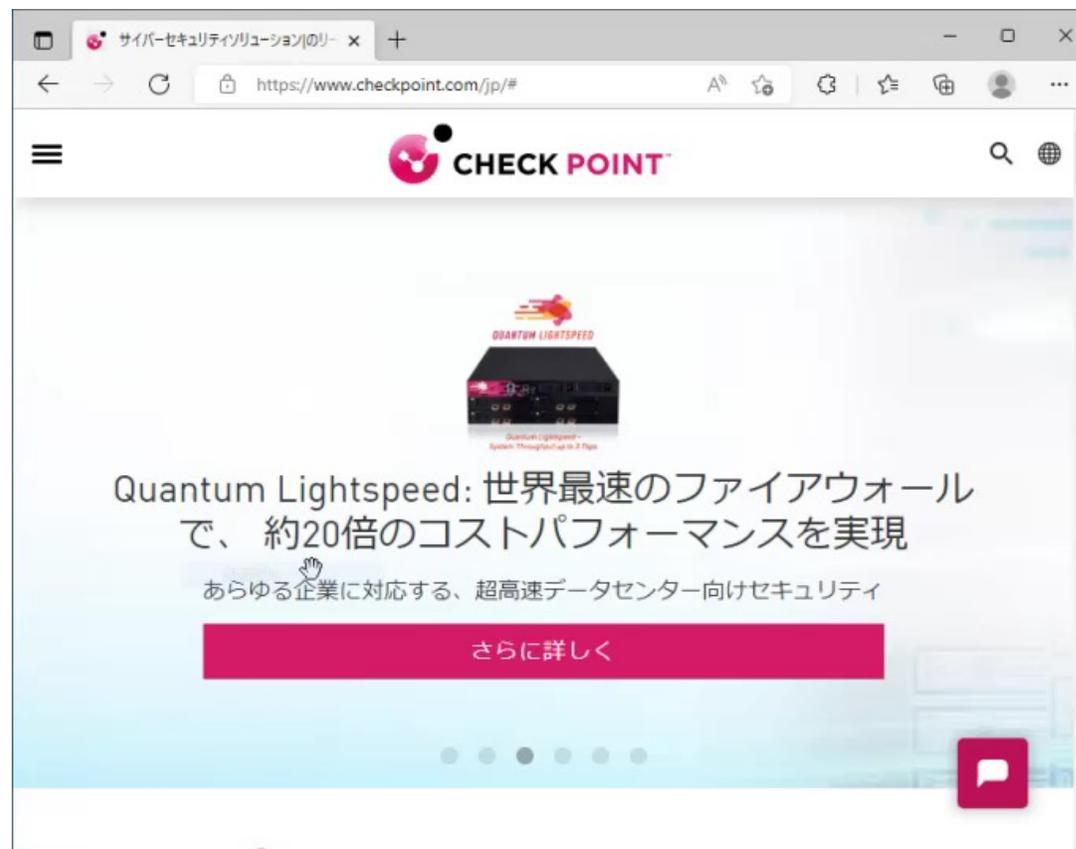
【参考】 Check Point アイコン の表示方法

- ブラウザにCheck Pointのアイコン  が表示されていない場合は、以下の動画を参考にして、表示させてください。

Check Point アイコンの表示方法 (Chrome)



Check Point アイコンの表示方法 (Edge)



【参考】オンラインインストール用インストーラ

- Overview > Operational Overview 上部の「Download Endpoint」からダウンロードします
- OS、クライアントバージョン、バーチャルグループを選択して、ダウンロードします
- Policy > Deployment Policy > Software Deployment の設定に従ってセキュリティ機能がインストールされます

The screenshot displays the Harmony Endpoint management console. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, PUSH OPERATIONS, ENDPOINT SETTINGS, and SERVICE MANAGEMENT. The main area shows the 'Operational Overview' page with a notification: 'To enable communication, make sure you have Endpoint client installed on all your devices' and a 'Download Endpoint' button. Below this, there are sections for 'ACTIVE ENDPOINTS' (3 Active), 'DESKTOPS' (0 Windows, 0 macOS, 0 Linux, 0 ChromeOS), 'LAPTOPS' (3 Windows, 0 macOS, 0 Linux, 0 ChromeOS), 'DEPLOYMENT STATUS' (3 Success, 0 In Progress, 0 Failed, 0 Not installed or Unknown), and 'HEALTH STATUS' (3 computers, No issues).

The 'Download Harmony Endpoint' dialog box is open, showing options for 'Quick install (Initial)'. It includes sections for Windows, Linux, and macOS, each with a 'Download version' dropdown, a 'Virtual group (optional)' dropdown, and a 'DOWNLOAD' button. The Windows section shows version 86.60.0186, Linux shows 'Latest', and macOS shows version 86.60.2568. All sections specify 'Any CPU (<2MB)'. A 'More versions' link is at the bottom left, and 'CANCEL' and 'OK' buttons are at the bottom right.

【演習】

- インストールパッケージを作成してください
 - バージョンは、最新バージョン以外を選択してください
- インストールパッケージをダウンロードしてください
- クライアントソフトウェアをインストールしてください

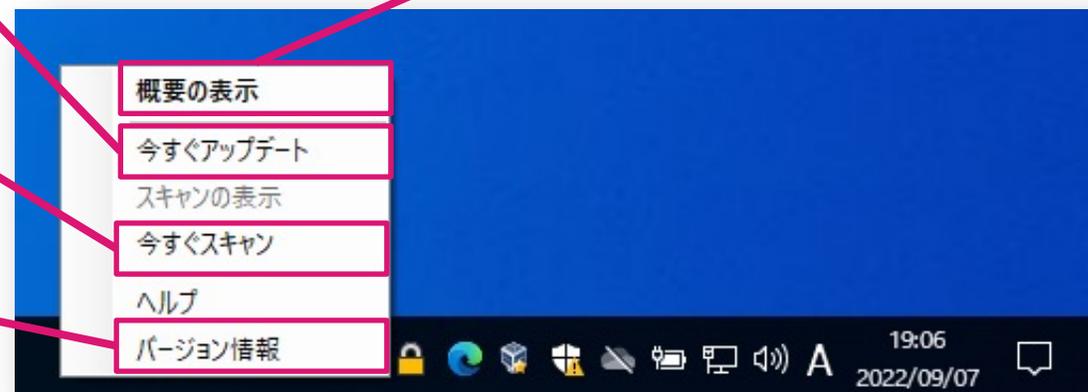
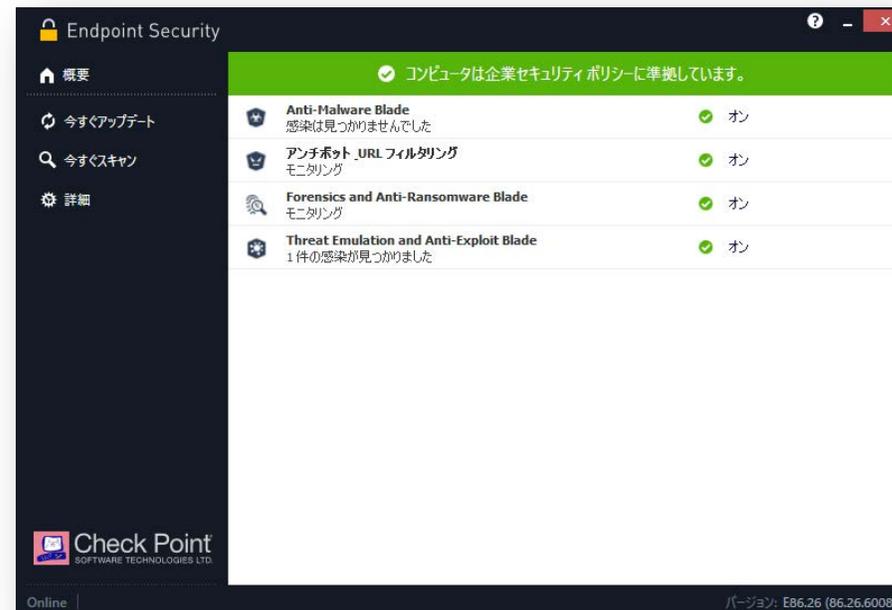
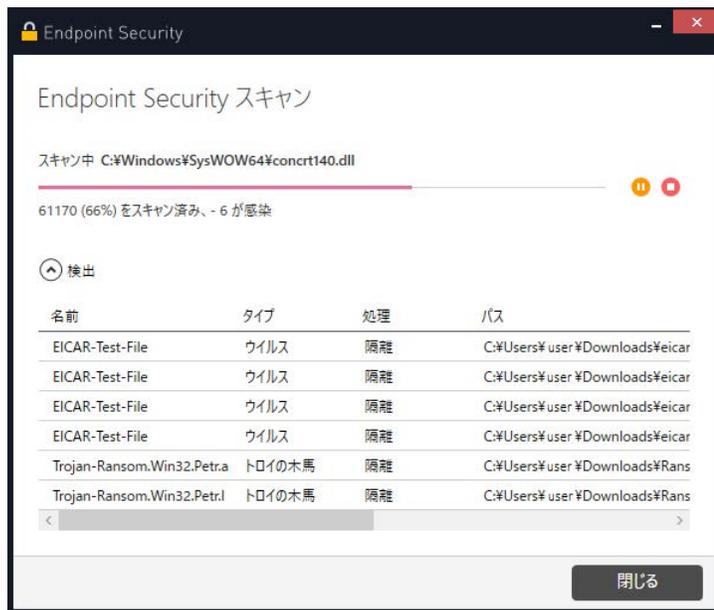
クライアントの UI

YOU DESERVE THE BEST SECURITY

クライアントの UI 概要（1 / 4）

- クライアントソフトウェアでは、各種情報を確認、収集できます
 - セキュリティ機能のステータス
 - セキュリティログ
 - クライアントソフトウェアのバージョン
 - セキュリティ Blade のバージョン
 - ポリシーのバージョン
 - テクニカルサポートに提供するログ（CPinfo）
- ポリシーと Anti-Malware のシグネチャを更新できます
- Anti-Malware による Scan を実施できます

クライアントの UI 概要 (2 / 4)



クライアントの UI 概要（3 / 4）：詳細

- 「ポリシーの表示」は、パソコンに適用されているポリシーバージョンを確認できます
- 「ログの表示」は、パソコンでのアクティビティを確認できます
- 「収集」は、テクニカルサポート用の情報（CPInfo）を収集します
 - CPInfo は、%UserProfile%\CPInfo に保存されます

The main screenshot shows the 'Endpoint Security' client interface. The 'Details' (詳細) window is open, displaying the 'Policy' (ポリシー) section. The 'Policy display' (ポリシーの表示) button is highlighted with a red box. The 'Log' (ログ) section is also visible, with the 'Log display' (ログの表示) button highlighted. The 'Collection' (収集) button is highlighted as well.

The 'Policy display' button points to a screenshot of the 'インストール済みポリシー' (Installed Policies) window, which shows a table of installed policies:

名前	タイプ	バージョン	日付	モード
CP-demo (Anti Bot)	アンチボット	33	9/9/2022 5:38:34 PM	接続
CP-demo (Anti Malware)	アンチマルウェア	33	9/9/2022 5:38:34 PM	接続
CP-demo (Forensics)	フォレンジック	33	9/9/2022 5:38:32 PM	接続
Default Common Client settings for the entire...	共通クライアント	5	8/26/2022 3:26:30 PM	接続

The 'Log display' button points to a screenshot of the 'Log Viewer' window, which shows a table of log events:

Local Time	UTC Time	Severity	Product	Event type	Action	Endpoint Addr...	Source	Destinatio...	Description	Rule
2022-09-09 17:10:54	2022-09-09 08:10:54	4	Forensics	Forensics Case Analysis		10.0.2.14			Endpoint Anti-Malware has pre...	
2022-09-09 17:15:21	2022-09-09 08:15:21	1	Anti-Malware	Infection		10.0.2.14			Endpoint Anti-Malware has pre...	
2022-09-09 17:19:40	2022-09-09 08:19:40	4	Forensics	Forensics Case Analysis		10.0.2.14			Endpoint Anti-Malware has pre...	
2022-09-09 17:19:35	2022-09-09 08:19:35	1	Anti-Malware	Infection		10.0.2.14			Endpoint Anti-Malware has pre...	

The 'Collection' button points to a screenshot of the 'Check Point Log Collection Tool' terminal window, which shows the current configuration:

```
Current Configuration:
Detail level..... <Extended>
Log files since..... <13/08/2022>
Upload to Check Point..... <Disabled>

Press 'c' to configure
Press 'e' to enable upload to Check Point
Press <Enter> to start
Press 'q' to quit
```

クライアントの UI 概要（4 / 4）：Blade

- 各 Blade をクリックすると、各 Blade での検出状況、ポリシーバージョンを確認できます

The image displays the Check Point Endpoint Security user interface. On the left, a sidebar menu shows navigation options: 概要 (Overview), 今すぐアップデート (Update Now), 今すぐスキャン (Scan Now), and 詳細 (Details). The main content area is divided into several panels:

- Overview Panel:** Shows a green status bar indicating the computer is compliant with enterprise security policies. Below it, a list of blades is shown, each with a status icon (green checkmark for 'On') and a brief description of detected threats.
- Anti-Malware Blade Detail:** Shows the current status (On), update information (e.g., 'アップデートはまだ行われていません'), and a table of detected infections.
- Anti-Bot URL Filtering Detail:** Shows the current status (On), version (8.68.62.6), and a table of detected threats.
- Forensics and Anti-Ransomware Blade Detail:** Shows the current status (On), version (33), and a table of analyzed cases.
- Threat Emulation and Anti-Exploit Blade Detail:** Shows the current status (On), version (33), and a table of detected threats.

感染名	パス
Trojan-Ranso...	C:\Users\%n...
FileCAD_Test...	C:\Users\%n...

保護の名前	実行アクション
Anti-Bot test.TC.f	Prevented

インシデント ID	インシデントのソース	脅威の名前	実行アクション	コソフデ
dc99955f-4f30-4adf-9e50-5fda7b0...	Harmony File Reputation	C:\Users\%...	隔離	高
24109ea19-56a2-4957-9c41-2ba39...	Harmony File Reputation	C:\Users\%...	隔離	高
7b41bc2a-53ea-489c-98ad-bf14d...	Harmony File Reputation	C:\Users\%...	隔離	高
a30f12d9-4ea1-4818-a4be-03097c...	Harmony File Reputation	C:\Users\%...	隔離	高
97151dca-1a2a-4e76-b628-881d89...	Harmony Browser Exten...	eicar.com	隔離	高
e567efc0-bb6f-42c4-b1bb-abfd85...	Harmony File Reputation	C:\Users\%...	隔離	高
f3f7735-361f-4d3e-befb-a9b9783...	Harmony File Reputation	C:\Users\%...	隔離	高
32bbd62d-cad7-48fe-8418-7b1368...	Harmony File Reputation	C:\Users\%...	隔離	高
74268058-b467-4a72-ba3f-165f32...	Harmony File Reputation	C:\Users\%...	隔離	高
9bf13182-cf5a-4adc-80af-201a73...	Harmony Browser Exten...	eicar.zip	隔離	高

インシデント ID	インシデントのソース	脅威の名前	実行アクション	コソフデ
dc99955f-4f30-4adf-9e50-5fda7b0...	Harmony File Reputation	C:\Users\%...	隔離	高
24109ea19-56a2-4957-9c41-2ba39...	Harmony File Reputation	C:\Users\%...	隔離	高
7b41bc2a-53ea-489c-98ad-bf14d...	Harmony File Reputation	C:\Users\%...	隔離	高
a30f12d9-4ea1-4818-a4be-03097c...	Harmony File Reputation	C:\Users\%...	隔離	高
97151dca-1a2a-4e76-b628-881d89...	Harmony Browser Exten...	eicar.com	隔離	高
e567efc0-bb6f-42c4-b1bb-abfd85...	Harmony File Reputation	C:\Users\%...	隔離	高
f3f7735-361f-4d3e-befb-a9b9783...	Harmony File Reputation	C:\Users\%...	隔離	高
32bbd62d-cad7-48fe-8418-7b1368...	Harmony File Reputation	C:\Users\%...	隔離	高
74268058-b467-4a72-ba3f-165f32...	Harmony File Reputation	C:\Users\%...	隔離	高
9bf13182-cf5a-4adc-80af-201a73...	Harmony Browser Exten...	eicar.zip	隔離	高

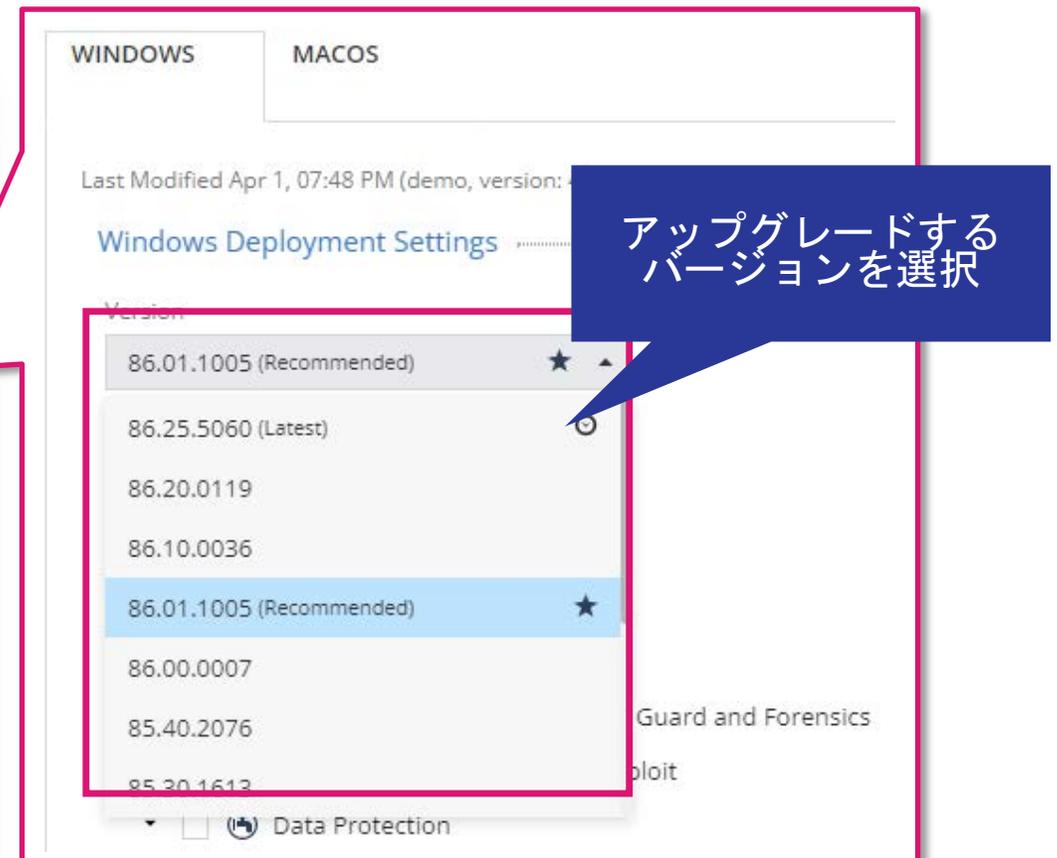
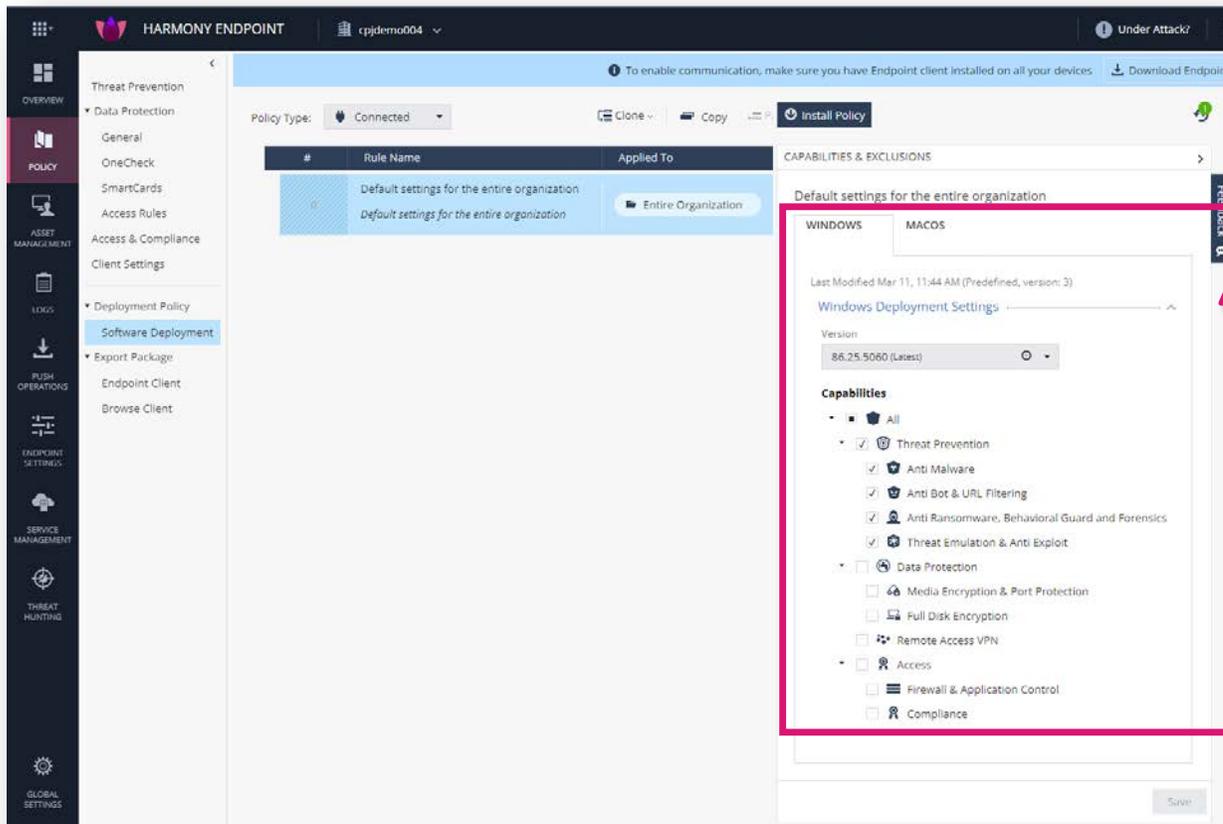
クライアントのアップグレード

YOU DESERVE THE BEST SECURITY

クライアントのアップグレード

Policy > Deployment Policy > Software Deployment

- クライアントソフトウェアをコンピュータに展開後に、機能の追加やクライアントのアップグレードがリモートから実施可能です
- ダウングレードはできません
- Save と、Install Policy を実行します



【演習】

- クライアントのバージョンを最新バージョンにアップグレードしてください

バーチャルグループによる管理

- バーチャルグループの概要
- バーチャルグループの作成
- バーチャルグループへのコンピュータの追加、削除
- バーチャルグループへのポリシーの適用

YOU DESERVE THE BEST SECURITY

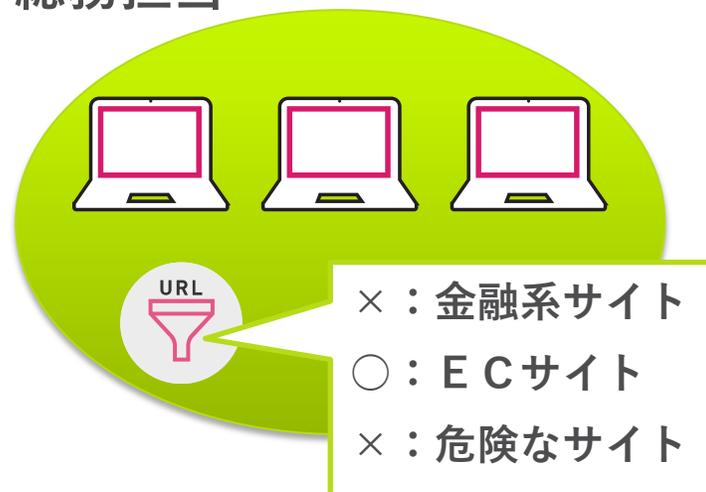
バーチャルグループの概要

- 組織や役職などに応じて、ポリシーやセキュリティ機能、クライアントのバージョンなどをコンピュータが所属するグループでカスタマイズすることができます
- Harmony Endpoint で作成するグループを、「バーチャルグループ」といいます
- OSやコンピュータ種別に応じて事前定義されたバーチャルグループを使用することもできます
- バーチャルグループは、インストールパッケージを作成する際に指定することも、クライアントをインストール後に追加、削除することもできます

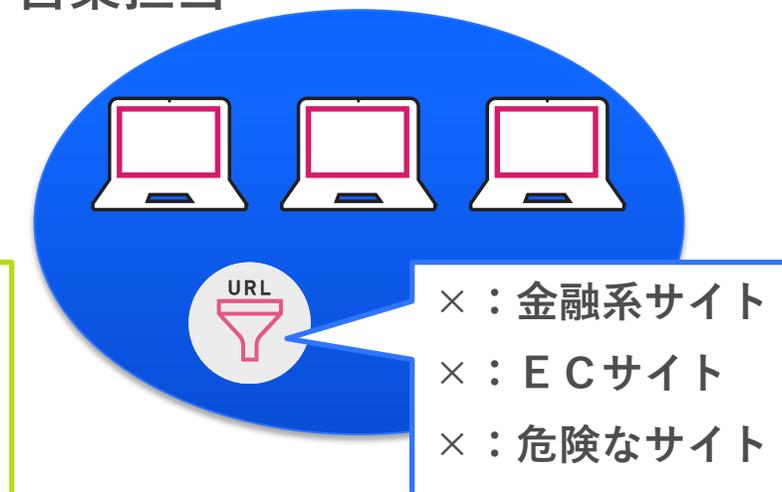
経営担当



総務担当



営業担当



バーチャルグループの作成（1 / 2）

- バーチャルグループの作成は、以下の2つの方法で可能です
 - Asset Management > Computers > Computer Actions
 - Asset Management > Organizational Tree

Asset Management > Computers > Computer Actions での作成方法

The screenshot shows the Harmony Endpoint console interface. The left sidebar has 'ASSET MANAGEMENT' highlighted. The main area shows 'Computers' selected in the left pane, and a table of computer assets. The 'Computer Actions' dropdown menu is open, with 'Create Virtual Group' highlighted. A callout box shows the 'CREATE VIRTUAL GROUP' dialog with 'demo2' entered in the Name field and 'Comment' in the Comment field.

Status	Computer Name	Endpoint Version	OS Build
<input type="checkbox"/>	ep	86.26.6008	10.0-17763-SP0.0-S
<input type="checkbox"/>	ep-demo2	86.50.0190	10.0-19043-SP0.0-S
<input type="checkbox"/>	ep-demo3	86.50.0190	10.0-19043-SP0.0-S

General Actions

- View Computer Logs
- Create Virtual Group**
- Create and Add to Virtual Group
- Add to Virtual Group
- Reset Computer Data
- Delete
- Recover
- Terminate

CREATE VIRTUAL GROUP

Name: demo2

Comment: Comment

CANCEL OK

バーチャルグループの作成 (2 / 2)

Asset Management > Organizational Tree > Actions での作成方法

The screenshot illustrates the steps to create a virtual group in the Harmony Endpoint console. The left sidebar shows the navigation menu with 'ASSET MANAGEMENT' selected. The main area displays the 'Organizational Tree' for the 'Entire Organization'. The 'Virtual Groups' folder is expanded, and the 'Actions' menu is open, with 'Create Virtual Group' highlighted. A dialog box titled 'CREATE VIRTUAL GROUP' is open, showing the 'Name' field with 'demo2' and a 'Comment' field with 'Comment'. The 'OK' button is highlighted.

バーチャルグループへのコンピュータの追加、削除（1 / 4）

- バーチャルグループ用のインストールパッケージを作成することで、インストール時にバーチャルグループに所属させることができます（後述）
- インストール後にバーチャルグループへの追加、削除を行えます
- バーチャルグループへの追加、削除は、1台ずつもしくは複数台まとめて行えます
- バーチャルグループへのコンピュータの追加、削除は、以下の2つの方法で可能です
 - Asset Management > Computers > Computer Actions
 - Asset Management > Organizational Tree

バーチャルグループへのコンピュータの追加、削除（2 / 4）

- コンピューター一覧でコンピュータを選択し、Computer Actions メニューから Add to Virtual Group を選択する
- 複数台のコンピュータを同時にバーチャルグループへ追加する時は、対象のコンピュータをすべて選択して、Computer Actions > Add to Virtual Group を選択する

Asset Management > Computers > Computer Actions での追加方法

The screenshot illustrates the steps to add computers to a virtual group in the HARMONY ENDPOINT interface. The interface is divided into several sections:

- ① コンピューターを選択**: The 'Computers' tab is selected in the left sidebar, and the 'Computers' table is visible. The first row, representing a computer named 'ep', is highlighted with a red box.
- ② クリック**: The 'Computer Actions' dropdown menu is open, and the 'Add to Virtual Group' option is highlighted with a red box.
- ③ 選択**: The 'Add to Virtual Group' option is selected in the context menu.
- ④ バーチャルグループを選択**: A dialog box titled 'ADD MEMBERS TO VIRTUAL GROUP' is open, showing a list of virtual groups. The 'Select virtual Group' dropdown is highlighted with a red box.

Status	Computer Name	Endpoint Version
<input checked="" type="checkbox"/>	ep	86.26.6008
<input type="checkbox"/>	ep-demo2	86.50.0190
<input type="checkbox"/>	ep-demo3	86.50.0190

Computer Actions Menu:

- General Actions
- View Computer Logs
- Create Virtual Group
- Create and Add to Virtual Group
- Add to Virtual Group
- Reset Computer Data
- Delete
- Recover
- Terminate
- Directory Scanner

Virtual Groups List:

- CP-demo
- All ChromeOs Desktops
- All ChromeOs Laptops
- All Desktops
- Eval
- Capsule Docs external users

バーチャルグループへのコンピュータの追加、削除（3 / 4）

- コンピューター一覧でコンピュータを選択すると、所属するバーチャルグループが表示される
 - 追加： + をクリックし、バーチャルグループの一覧から所属させるグループを選択
 - 削除：表示されたバーチャルグループを選択し、x をクリック

Asset Management > Computers での追加、削除方法

① コンピューターを選択

② 所属するバーチャルグループを表示

③ バーチャルグループを追加、削除

④ バーチャルグループの横にマウスオーバーした際に表示される +、- をクリック

追加 + x 表示切替

削除 表示切替

Status	Computer Name	Endpoint Version	OS Build	Device Type	Deployment
✓	ep	86.26.6008	10.0-17763-SP0.0-SMP	Laptop	Completed
✓	ep-demo2	86.50.0190	10.0-19043-SP0.0-SMP	Laptop	Completed
✓		86.50.0190	10.0-19043-SP0.0-SMP	Laptop	Completed

1 of 3 selected

General | LDAP

Display Name: ep | SAM Name: ep

Description: - | CN: CN=EP,OU=Domain

Controllers,DC=harmon...

10.0 (17763)

Number of

+ x 表示切替

Pre-defined Virtual Groups

Custom Virtual Group

- 20220629demo
- ✓ CP-demo
- DEMO0728

CANCEL OK

バーチャルグループへのコンピュータの追加、削除（4 / 4）

- Organizational Tree で Virtual Group を選択して、コンピュータを追加、削除する

Asset Management > Organizational Tree での追加方法

① Virtual Group を選択

② コンピュータを追加、削除する Virtual Group を選択

② + をクリック

③ Other Users/Computers を選択

④ 追加するコンピュータを選択

バーチャルグループへのポリシーの適用（1 / 2）

- バーチャルグループに適用するポリシーを作成する際は、既存のポリシーを複製し、適用するバーチャルグループを選択します
- Threat Prevention、Data Protection、Access & Compliance、Client Settings、Deployment Policy で適用するバーチャルグループを設定できます

① 複製元のポリシーを選択

② 「Clone」か、「Copy & Paste」をクリックして複製

「Clone」は、複製元のポリシーの真上か、真下に複製

「Copy & Paste」は、複製時に任意のポリシーを選択し、真上か、真下に複製

バーチャルグループへのポリシーの適用（2 / 2）

- 表示されたダイアログボックスで、ポリシーの名前と適用対象を設定します
- バーチャルグループ以外に、コンピュータや Active Directory の OU に適用できます
 - Active Directory の OU に適用できるのは、AD Scanners を設定した場合のみです

CLONE RULE

Name *

New Rule 1

ポリシーの名前を入力

Applied to ⓘ *

Search for entity...

Select from organization tree

適用対象を選択

Affected Devices (0)

Clone Configuration From

CANCEL OK

【演習】

- 任意の名前のバーチャルグループを作成してください。

ポリシーバージョンの確認

YOU DESERVE THE BEST SECURITY

ポリシーバージョンの確認：Threat Prevention

CAPABILITIES & EXCLUSIONS

CP-demo

24 Exclusions

Policy Mode: Custom

WEB & FILES PROTECTION | BEHAVIORAL PROTECTION | ANALYSIS & REMEDIATION

Last Modified Sep 9, 05:31 PM (yoshiyasun_EpMaa5_Only, version: 33)

URL Filtering

URL Filtering Mode: Prevent

Download Protection

Download Emulation & Extraction: Prevent

Credential Protection

Zero Phishing: Prevent

Password Reuse Protection: Prevent

Safe Search

Search Reputation: On

Save

Endpoint Security

概要

今すぐアップデート

今すぐスキャン

詳細

コンピュータは企業セキュリティポリシーに準拠しています。

Anti-Malware Blade: オン

31件の感染が見つかりました

現在のステータス

アップデートはまだ行われていません。
シグネチャバージョン: 202204131304
最終スキャン: 今日 15:33:54

CP-demo (Anti Malware), バージョン:33

感染

感染名	パス	感染状態	検出時間	処理時間	隔離
Trojan-Ranso...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい
Trojan-Ranso...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい
Trojan-Ranso...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい
Trojan-Ranso...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい
Trojan-Ranso...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい
ELICAR_Test_Fi...	C:\Users\nack%On...	削除	2022/09/09 1...	2022/09/09 1...	はい

再スキャン | 削除 | 復元

戻る | スキャンの表示 | 今すぐスキャン

Check Point SOFTWARE TECHNOLOGIES LTD.

Online | cpjdemo006-2c792ee1-hap21.epmgmt.checkpoint.com | バージョン: E86.26 (86.26.6008)

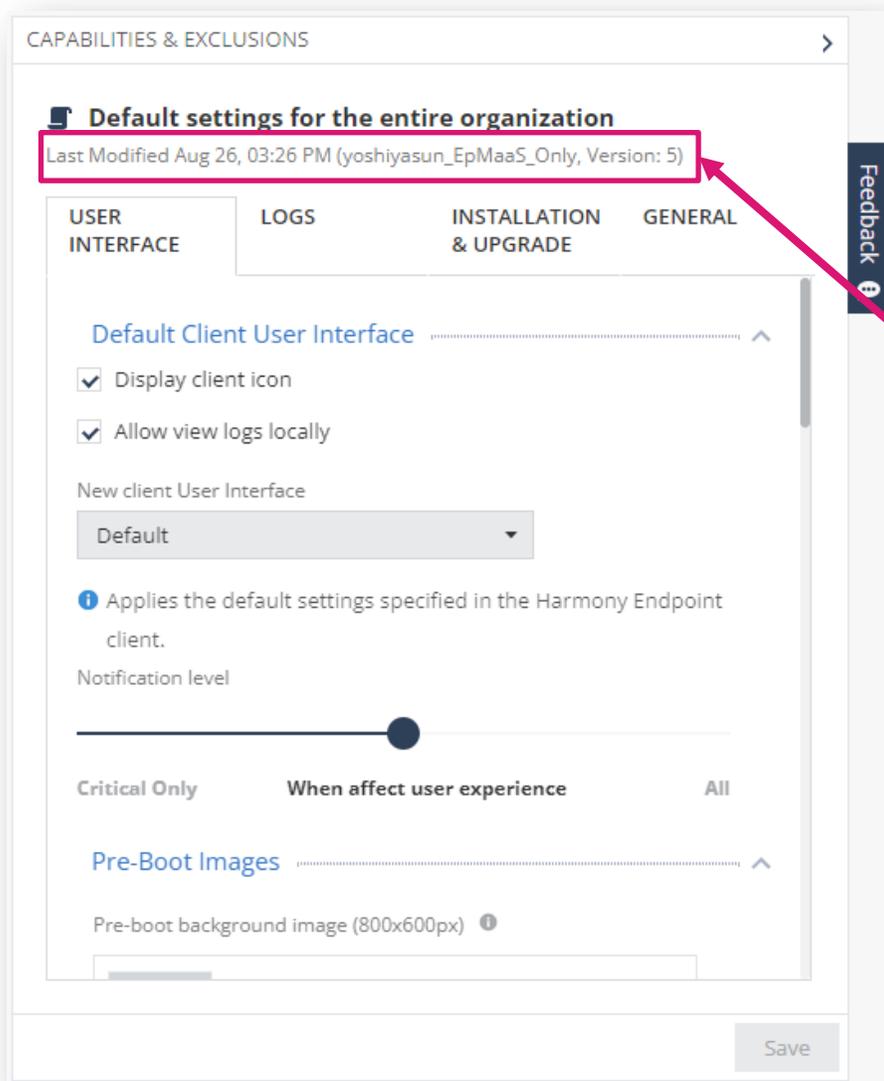
Endpoint Security

インストール済みポリシー

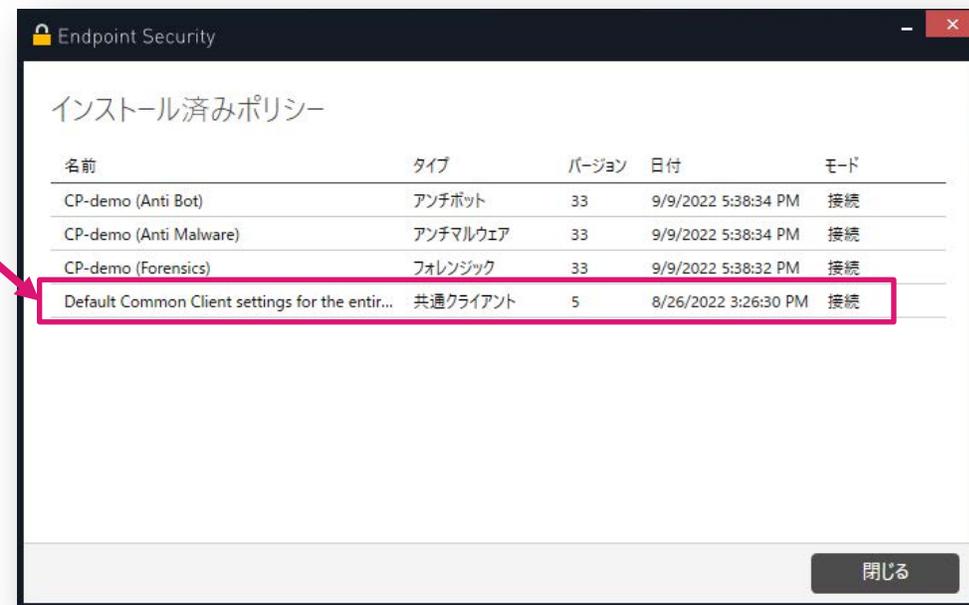
名前	タイプ	バージョン	日付	モード
CP-demo (Anti Bot)	アンチボット	33	9/9/2022 5:38:34 PM	接続
CP-demo (Anti Malware)	アンチマルウェア	33	9/9/2022 5:38:34 PM	接続
CP-demo (Forensics)	フォレンジック	33	9/9/2022 5:38:32 PM	接続
Default Common Client settings for the entir...	共通クライアント	5	8/26/2022 3:26:30 PM	接続

閉じる

ポリシーバージョンの確認：Client Settings



Client Settings のポリシーバージョンを確認する際は、クライアントソフトウェアで「概要の表示 > 詳細 > ポリシーの表示」を選択してください。



THREAT PREVENTION 設定

- 共通
- ダウンロード保護 (Threat Emulation、Threat Extraction)
- 認証情報の保護 (Zero-Phishing、Password Reuse Protection)
- アンチ・ランサムウェア

YOU DESERVE THE BEST SECURITY

ポリシーの設定

THREAT PREVENTION
共通

YOU DESERVE THE BEST SECURITY

Threat Prevention : 共通 (1 / 5)

Policy > Threat Prevention

- Threat Prevention では脅威対策機能に関する設定を構成します
 - Web & Files Protection
 - URL フィルタリング
 - ダウンロード保護 (サンドボックス、ファイル無害化)
 - 認証情報の保護 (ゼロ・フィッシング、企業パスワード保護)
 - 安全な検索 (セーフ・レピュテーション、セーフ・サーチ)
 - ファイル保護 (アンチ・マルウェア、サンドボックス)
 - Behavioral Protection
 - アンチ・ボット
 - 振る舞い検査
 - アンチ・ランサムウェア
 - アンチ・エクスプロイト
 - Analysis & Remediation
 - 攻撃解析 (フォレンジクス)
 - 修復

Threat Prevention : 共通 (2 / 5)

Policy > Threat Prevention

- バーチャルグループを使用して、組織ごとに異なるポリシーを設定できます
- コンピュータが複数のポリシーの適用対象になっている場合、若番のポリシーが適用されます

The screenshot displays the 'Policy' configuration page in the Check Point Harmony console. The interface is annotated with callouts and a red arrow to highlight key features:

- ポリシー一覧** (Policy List): A table listing policies and their application targets.
- ポリシーの適用対象** (Policy Application Targets): A callout pointing to the 'Applied To' column in the policy list.
- 脅威対策機能の状態** (Threat Prevention Function Status): A callout pointing to the status icons for various threat prevention capabilities.
- ポリシーごとの詳細設定** (Detailed Settings per Policy): A callout pointing to the configuration panel for a selected policy.
- ポリシー適用順** (Policy Application Order): A red arrow pointing downwards, indicating that policies are applied in ascending order of their index.

#	Rule Name	Applied To	Web & Files	Behavioral	Analysis
0	Exclusion	ep-demo2 ep-demo3	[Icons]	[Icons]	[Icons]
1	Eval	Eval	[Icons]	[Icons]	[Icons]
2	CP-demo	CP-demo	[Icons]	[Icons]	[Icons]
3	demo-point	demo-point	[Icons]	[Icons]	[Icons]
4	Default settings	Entire Organization	[Icons]	[Icons]	[Icons]
	Default settings				

Policy Configuration Panel (CAPABILITIES & EXCLUSIONS):

- Policy Mode: Custom
- Exclusions: 29 Exclusions
- WEB & FILES PROTECTION: URL Filtering Mode: Prevent
- BEHAVIORAL PROTECTION: Download Protection: Off
- ANALYSIS & REMEDIATION: Credential Protection: Zero Phishing: Prevent, Password Reuse Protection: Prevent

Threat Prevention : 共通 (3 / 5)

Policy > Threat Prevention

The screenshot displays the 'CAPABILITIES & EXCLUSIONS' section of a security policy configuration. It includes a 'Policy Mode' dropdown set to 'Custom', three main protection categories: 'WEB & FILES PROTECTION', 'BEHAVIORAL PROTECTION', and 'ANALYSIS & REMEDIATION'. Below these are sections for 'Safe Search' (with 'Search Reputation' and 'Force Safe Search' both set to 'On') and 'Files Protection' (with 'Anti-Malware Mode' set to 'Prevent' and 'Files Threat Emulation Mode' set to 'On'). An 'Advanced Settings' button is at the bottom. A 'Last Modified' timestamp is also visible.

例外設定を管理

Exclusions Center
Custom

事前定義された設定を選択

- Tuning
- Recommended
- Default
- Strict

脅威対策のカテゴリを選択

ポリシーのバージョンを表示

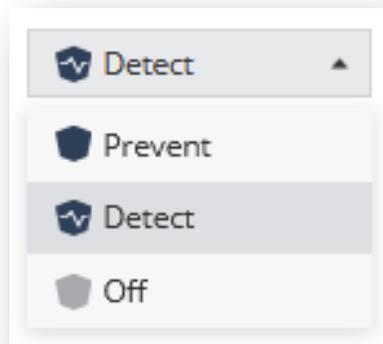
セキュリティ対策機能の動作モードを選択

セキュリティ対策機能の詳細を設定

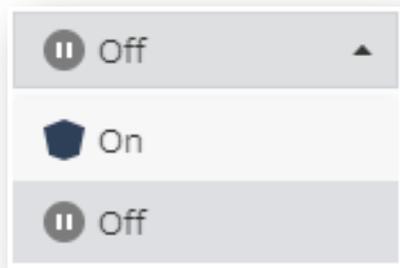
Threat Prevention : 共通 (4 / 5)

Policy > Threat Prevention

- 脅威に対する動作モードの設定方法は、2通りあります
 - 1) Prevent / Detect / Off
 - 2) On / Off



- 動作モードの選択肢①
 - Prevent : 脅威を阻止（ブロック）し、ログに記録
 - Detect : 脅威を検出し、ログに記録
 - Off : 機能を無効化

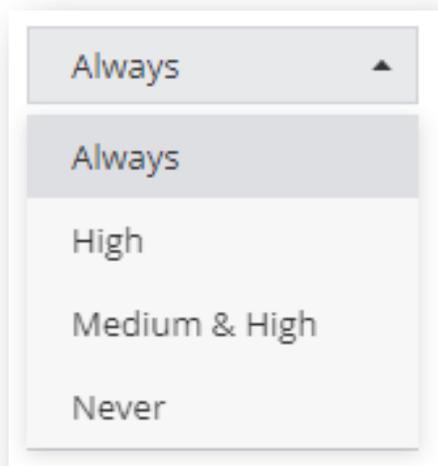


- 動作モードの選択肢②
 - On : 機能を有効化
 - Off : 機能を無効化

Threat Prevention : 共通 (5 / 5)

Policy > Threat Prevention

- Confidence Levelは、インシデントやファイルが悪意があることの確実性です。
- 「High」は、悪意があることがほぼ確実です。
- 「Medium」は、悪意がある可能性が非常に高いです。



- Confidence Level による動作の選択肢
 - Always : 常に実行
 - High : High の場合のみ実行
 - Medium & High : Medium と High の場合に実行
 - Never : 実行しません

ポリシーの設定

ポリシーの **SAVE** と **INSTALL**

ポリシーの Save と Install

Policy

- Web UI で設定・変更したポリシーは、ポリシーのインストールを行うまで、コンピュータに適用されません。変更を確定するにはポリシーをセーブして、インストールします
- セーブする前であれば、変更を取り消すことが可能です

Unsaved Rules 1

Install Policy

Unsaved Rules 1

- Save All Changes
- View Changes
- Discard Changes

変更内容の確認、破棄が可能

INSTALL POLICY

The following changes were made since the last policy installation. Review the changes and click on 'install' to install policy.

- Changed Rules Settings (1)
- Changed Rule Order and Assignments (2)

変更内容を適用

CANCEL INSTALL

Save

変更内容を保存

ポリシーの設定

THREAT PREVENTION
URL フィルタリング

YOU DESERVE THE BEST SECURITY

Threat Prevention : URL フィルタリング

Policy > Threat Prevention > Web & Files Protection > URL Filtering

- URL フィルタリングは、組織内でアクセスできるサイトを定義します
- Advanced Settings で、カテゴリの選択、ブラックリストの登録を構成します
- 各カテゴリは、さらに詳細なカテゴリの選択を構成できます

The image shows a screenshot of the Check Point Threat Prevention configuration interface, specifically the URL Filtering settings. The interface is divided into several sections, with red boxes highlighting key areas and blue callout boxes providing Japanese annotations.

Annotations:

- 動作モードを選択** (Select operation mode): Points to the "URL Filtering Mode" dropdown menu, which is currently set to "Detect".
- 事前定義されたカテゴリ** (Predefined categories): Points to the "Categories" section, which lists various predefined categories like "Bandwidth Consumption", "General Use", "Legal Liability", "Productivity Lost", "Security", and "Black list".
- ブラックリスト** (Blacklist): Points to the "Black list (0)" section, which allows for the registration of specific URLs to be blocked.
- Web サイトへのアクセスがブロックされた際に、エンドユーザの操作で警告を無視することを許可** (Allow user to dismiss the URL Filtering alert and...): Points to the checkbox "Allow user to dismiss the URL Filtering alert and...", which is checked.

Interface Elements:

- Left Panel:** "CAPABILITIES & EXCLUSIONS" section with "demo" and "EXCLUSIONS CENTER" tabs. It shows "Use Predefined Settings" (Default) and "Custom" options. The "WEB & FILES PROTECTION" tab is selected.
- URL Filtering Section:** Shows "URL Filtering Mode" set to "Detect" and "Download protection" set to "Prevent".
- Advanced Settings - WEB & FILES PROTECTION:** Contains the "URL Filtering" section with the "Allow user to dismiss the URL Filtering alert and..." checkbox checked.
- Categories List:** A table showing predefined categories with checkboxes for selection. The "Security" category is checked.
- Black list:** A section for managing a blacklist of URLs.

【演習】 URL フィルタリング

- 以下のカテゴリをブロック設定して、各カテゴリに該当する Web サイトへのアクセスがブロックされることを確認してください。
 - アルコール & タバコ
 - スポーツ
 - 翻訳
 - 旅行
- ブロック画面で、「詳細」をクリックし、ブロックサイトへのアクセス理由を選択すると、ブロックサイトへアクセスできることを確認してください。
 - 接続先が安全なサイトであることを確認した上でアクセスしてください。

ポリシーの設定

THREAT PREVENTION DOWNLOAD 保護

- Threat Emulation (Sandbox)
- Threat Extraction (無害化)

YOU DESERVE THE BEST SECURITY

Threat Prevention : Download 保護 (1 / 2)

Policy > Threat Prevention > Web & Files Protection > Download Protection

- Web ダウンロードに対するThreat Emulationと、Threat Extractionの設定を構成します
- 動作モードを「Detect」にした場合、ファイルへのアクセスを中断せずに Threat Emulation による検査のみ実施し、インシデントをログに記録します

The screenshot shows the 'CAPABILITIES & EXCLUSIONS' configuration page for 'demo'. The 'Download Protection' section is highlighted with a red box. The 'Download Emulation & Extraction' dropdown is set to 'Prevent'. The 'Advanced Settings' button is also highlighted. The right-hand pane shows the 'Supported files' and 'Emulation Environments' sections, both highlighted with red boxes. Annotations in blue boxes point to these sections and the 'Prevent' mode.

動作モードを選択

無害化の有効化と、モードの選択

無害化を無効化し、Sandboxでの検査完了までダウンロードを保留

無害化を無効化し、Sandboxでの検査完了前にダウンロードを許可

Sandbox、無害化機能で未サポートのファイルのダウンロード可否

Sandboxで検査するファイルサイズの上限

エミュレーションが実行されるOSイメージを選択

ファイルタイプごとのデフォルトのアクションを上書き

Threat Prevention : Download 保護 (2 / 2)

Policy > Threat Prevention > Web & Files Protection > Download Protection > Advance Settings

- Elements To Extract で、無害化を実施する要素を選択します
- Override Default Files Actions で、ファイル拡張子ごとの Threat Emulation と Threat Extraction の動作を構成します

Elements To Extract

ADVANCED SETTINGS - WEB & FILES PROTECTION

< Back Elements To Extract

Search 16 items

Name	Risk	Description
Custom Properties	1 Very-Low	Custom document properties
✓ Fast Save Data	1 Very-Low	Stored data for fast document saving
✓ Macros and Code	5 Critical	Microsoft Office macros and PDF JavaScript code
Summary Properties	1 Very-Low	Summary document properties
✓ Linked Objects	4 High	
✓ Sensitive Hyperlinks	3 Medium	Links to network/local file paths
✓ PDF URI Actions	3 Medium	Open Uniform Resource Identifier (URI) resources
✓ Embedded Objects	4 High	Files and objects embedded in documents
✓ PDF Launch Actions	4 High	Launch external applications

Override Default Files Actions

ADVANCED SETTINGS - WEB & FILES PROTECTION

< Back Override Default Files Actions

Search 81 items

File Extension	Description	File Action	Extraction Mode
PDF	Adobe acrobat document	Default (Emulate and Extrac	Irrelevant
DOC	Microsoft Word 97-2003 Document	Default (Emulate and Extrac	Irrelevant
DOCX	Microsoft Word Document	Default (Emulate and Extrac	Irrelevant
XLS	Microsoft Excel 97-2003 Worksheet	Default (Emulate and Extrac	Irrelevant
XLSX	Microsoft Excel Worksheet	Default (Emulate and Extrac	Irrelevant
PPT	Microsoft PowerPoint 97-2003 Present...	Default (Emulate and Extrac	Irrelevant
PPTX	Microsoft PowerPoint Presentation	Default (Emulate and Extrac	Irrelevant
EXE	Executable File	Default (Emulate)	Irrelevant
TAR	Tar Archive	Default (Emulate)	Irrelevant

【演習】 サンドボックス & ファイル無害化

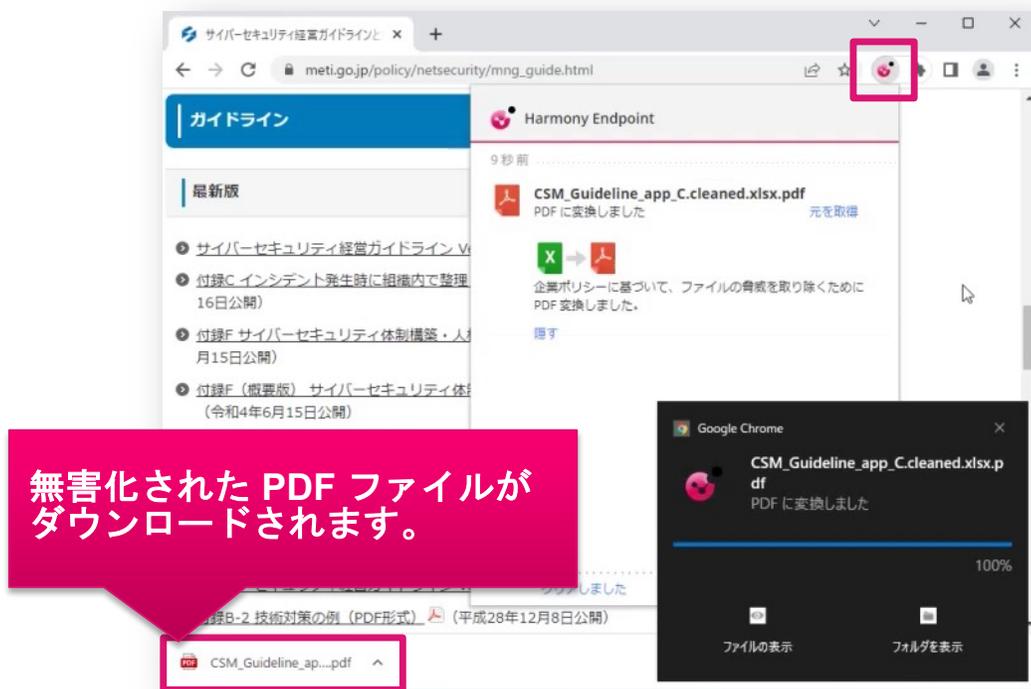
- Override Default Files Actions で、ファイル拡張子が、doc、xlsmの場合の File Action と、Extraction Mode を以下の様に設定して、動作の違いを確認してください

File Extention	File Action	Extraction Mode
doc	Emulate and Extract	Convert to PDF
xlsm	Emulate and Extract	Extract Elements

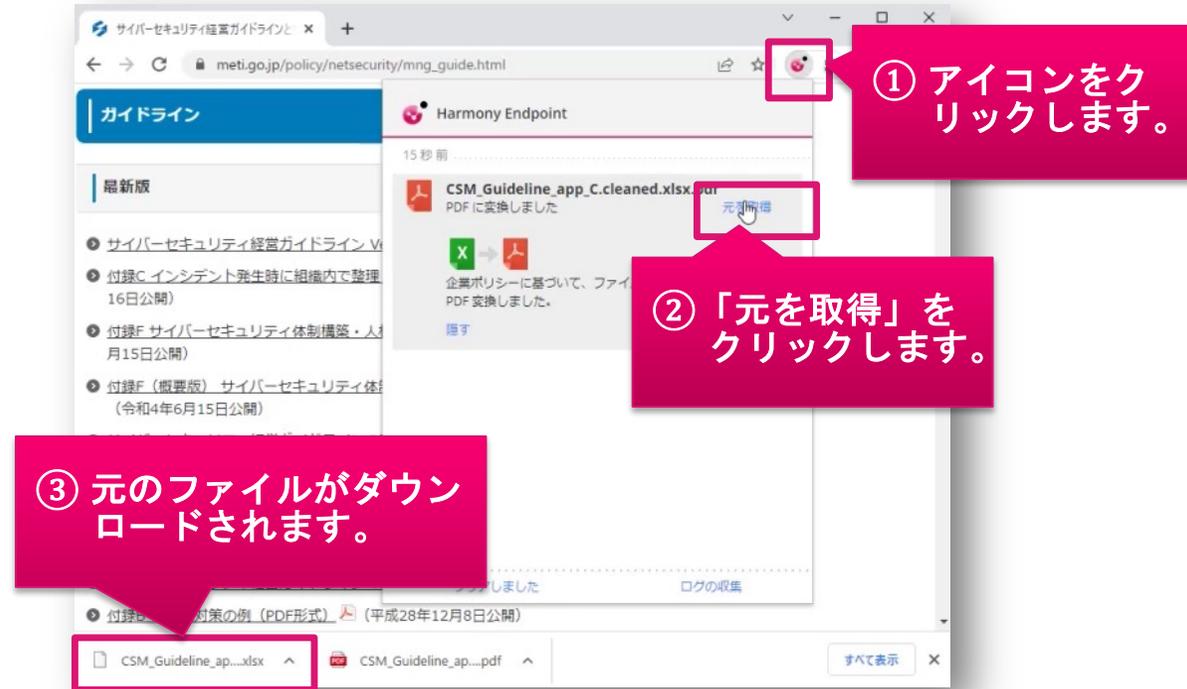
【参考】 サンドボックス & ファイル無害化の操作 (1 / 2)

- OfficeファイルやPDFファイルのダウンロード時に、ファイルの無害化を行います
- ファイルの無害化と併行して、クラウドのサンドボックスで元のファイルの検査を行います
- 検査が終了し、元のファイルの安全性が確認できたら、元のファイルを取得することが可能になります

ファイルの無害化

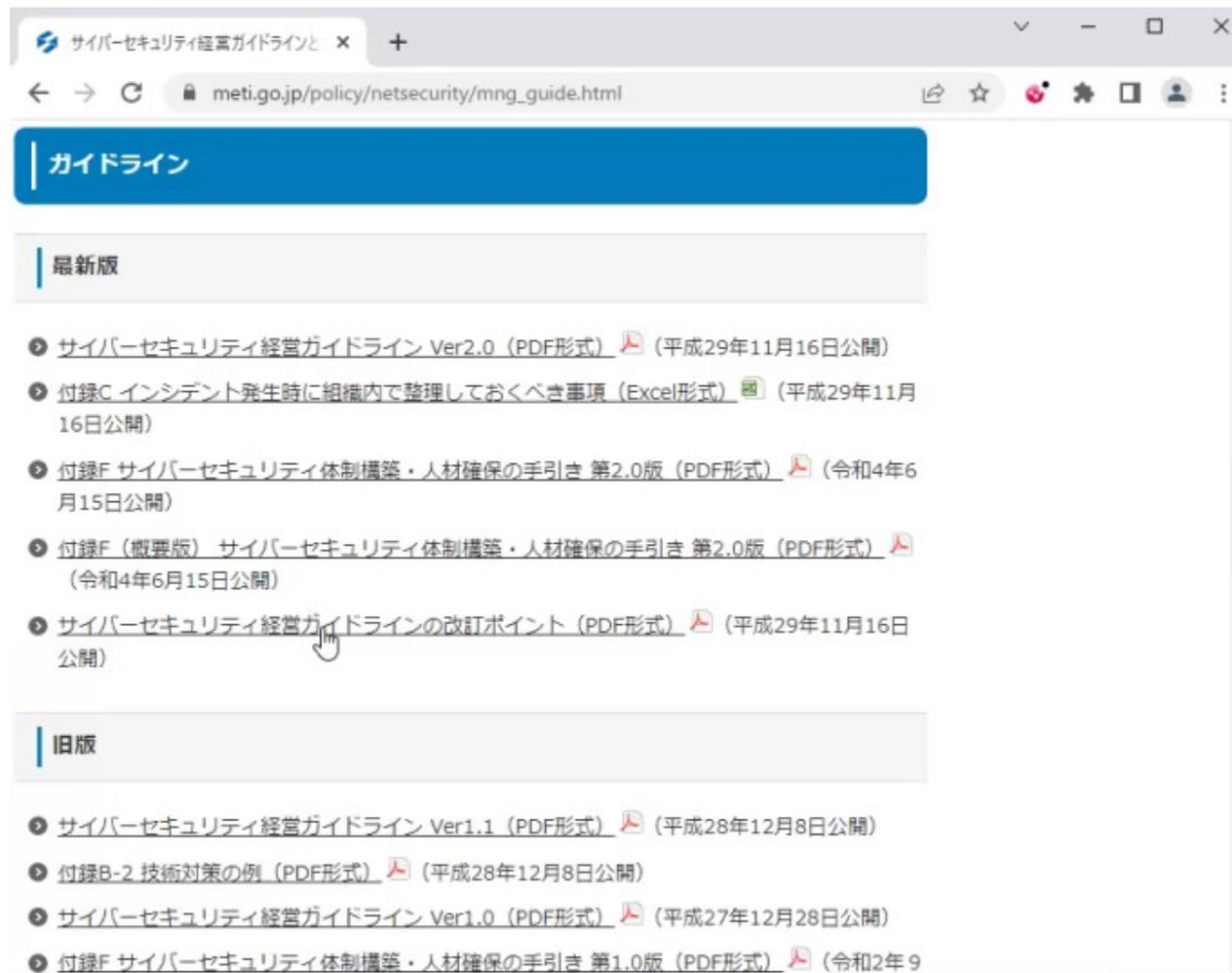


元のファイルのダウンロード



【参考】 サンドボックス&ファイル無害化の操作 (2 / 2)

サンドボックス&ファイル無害化の操作



The screenshot shows a web browser window with the URL meti.go.jp/policy/netsecurity/mng_guide.html. The page title is "サイバーセキュリティ経営ガイドライン" (Cybersecurity Management Guidelines). The main content is organized into sections: "ガイドライン" (Guidelines), "最新版" (Latest Version), and "旧版" (Older Versions). Under "最新版", there are five items listed, each with a download icon and a date. A mouse cursor is pointing at the fifth item, "サイバーセキュリティ経営ガイドラインの改訂ポイント (PDF形式)" (Revision Points of the Cybersecurity Management Guidelines (PDF format)), which was published on November 16, 2019. Under "旧版", there are four items listed, each with a download icon and a date, ranging from December 8, 2018, to September 2019.

Document Title	Format	Publication Date
サイバーセキュリティ経営ガイドライン Ver2.0	PDF形式	平成29年11月16日公開
付録C インシデント発生時に組織内で整理しておくべき事項	Excel形式	平成29年11月16日公開
付録F サイバーセキュリティ体制構築・人材確保の手引き 第2.0版	PDF形式	令和4年6月15日公開
付録F (概要版) サイバーセキュリティ体制構築・人材確保の手引き 第2.0版	PDF形式	令和4年6月15日公開
サイバーセキュリティ経営ガイドラインの改訂ポイント	PDF形式	平成29年11月16日公開
サイバーセキュリティ経営ガイドライン Ver1.1	PDF形式	平成28年12月8日公開
付録B-2 技術対策の例	PDF形式	平成28年12月8日公開
サイバーセキュリティ経営ガイドライン Ver1.0	PDF形式	平成27年12月28日公開
付録F サイバーセキュリティ体制構築・人材確保の手引き 第1.0版	PDF形式	令和2年9月

ポリシーの設定

THREAT PREVENTION
認証情報の保護

YOU DESERVE THE BEST SECURITY

Threat Prevention : 認証情報の保護

Policy > Threat Prevention > Web & Files Protection > Credential Protection

- Zero-Phishing は、Webサイトの様々な特性をチェックして、フィッシングサイトを検出します
- パスワードの再利用保護は、企業ドメインで利用されたパスワードのハッシュを記録し、同じパスワードを非企業ドメインで企業パスワードを使用しない様に警告します

demo EXCLUSIONS CENTER

Use Predefined Settings Default

Custom

WEB & FILES PROTECTION BEHAVIOR PROTECTION **動作モードを選択**

Credential protection

Zero Phishing Prevent

Password reuse protection Detect & Alert

Safe Search

Force Safe Search Off

Advanced Settings

ADVANCED SETTINGS - WEB & FILES PROTECTION

URL Filtering

Download Protection

Credential Protection

Threat Emulation

Files Protection

General

Signature

Scan

Allow user to dismiss the phishing alert and access the website

Send log on each scanned site

Allow user to abort phishing scans

Password Reuse Protection (0) | Edit

パスワードの再利用保護を適用するドメインを企業ドメインとして追加

【演習】 Zero-Phishing

- Google等で、“ログインページ”というキーワードで検索をして、Zero-Phishingの動作を確認してください

【参考】ゼロ・フィッシングの動作概要

正規のWebサイトへアクセスした際の動作概要

The screenshot shows the login page of Resona Bank. The browser address bar displays the URL `ib.resonabank.co.jp/IB/0102/SC_N_0102_010.aspx`. The page features the Resona Bank logo and a navigation menu. A prominent banner advertises 'ウイルス対策ソフト無料配布!' (Free virus protection software distribution!). Below this, the 'りそな銀行' (Resona Bank) logo is displayed. The login section is titled 'ログインIDをご入力ください。' (Please enter your login ID). It includes a text input field for the login ID, a checkbox for 'ソフトウェアキーボードを使用して入力する' (Use software keyboard for input), and a keyboard overlay with letters and numbers. A 'ヘルプ' (Help) button is visible in the top right corner.

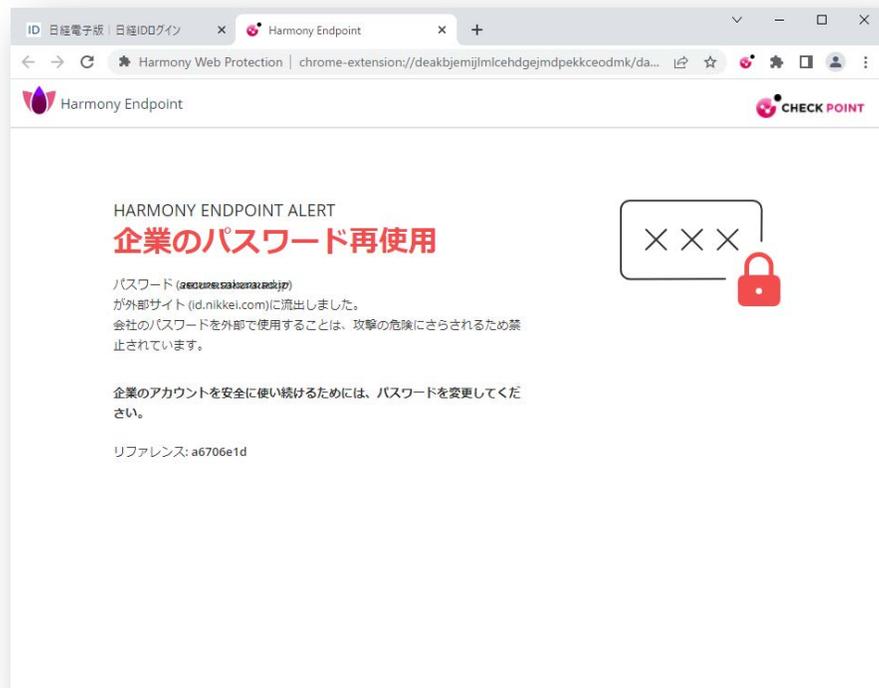
フィッシングサイトへアクセスした際の動作概要

The screenshot shows a phishing site designed to look like the Salesforce login page. The browser address bar displays the URL `salesforce.sbm-demo.xyz/zero-phishing`. The page has a yellow header with the text 'Demo Zero-Phishing Site!' and 'NON-PRODUCTION ENVIRONMENT AND FOR DEMO PURPOSES ONLY'. The Salesforce logo is prominently displayed in the center. Below the logo, there are input fields for 'Username' and 'Password', a blue 'Log In' button, and a 'Remember me' checkbox. The page layout and branding are highly similar to the legitimate Salesforce login page.

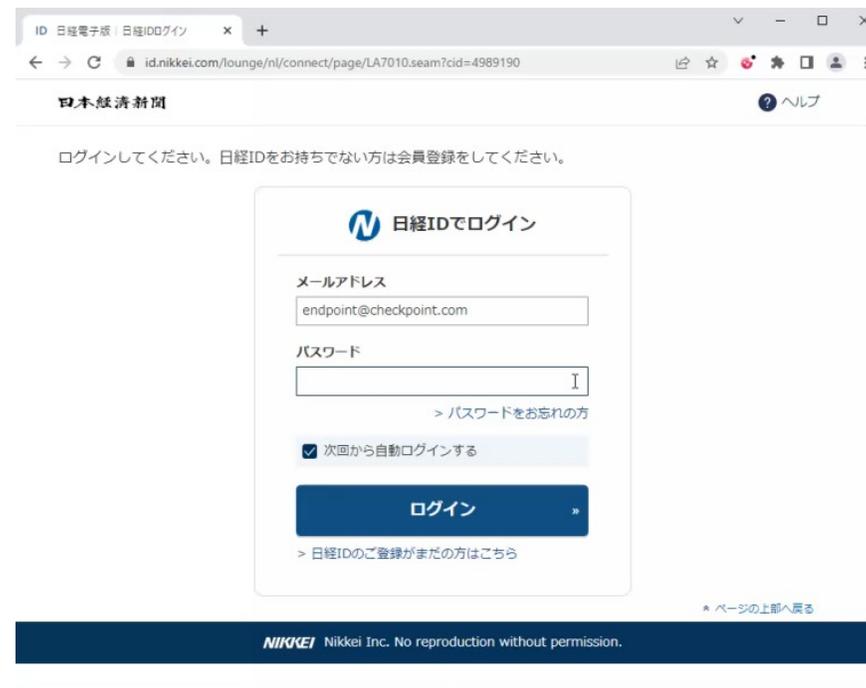
【参考】企業パスワード保護機能の動作概要

- 社内システムで使用しているパスワードを、インターネットのWebサイトで使用した際に、警告画面が表示されます。

企業パスワード保護の警告画面の例



企業パスワード保護の動作概要



ポリシーの設定

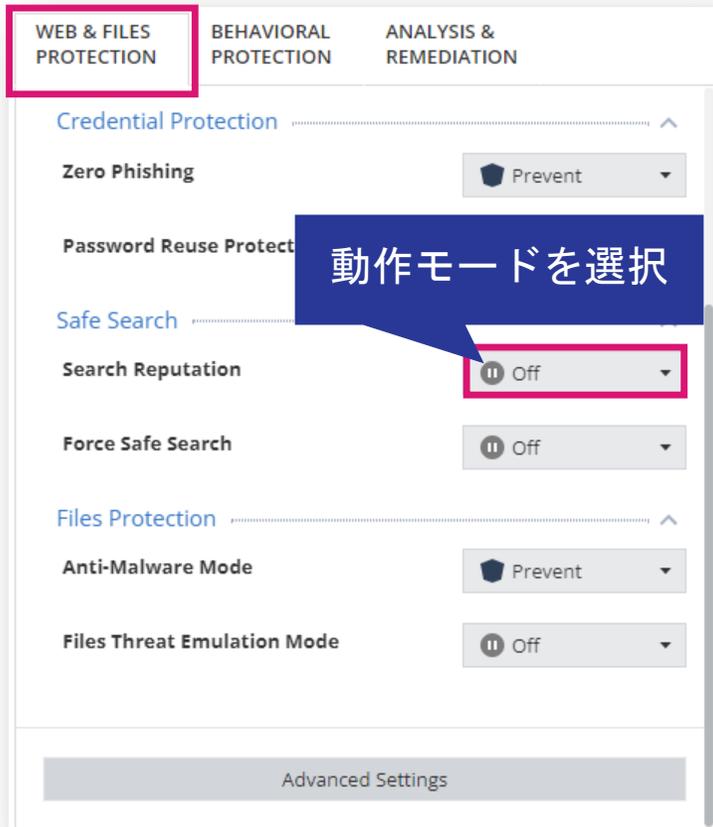
THREAT PREVENTION
安全な検索

YOU DESERVE THE BEST SECURITY

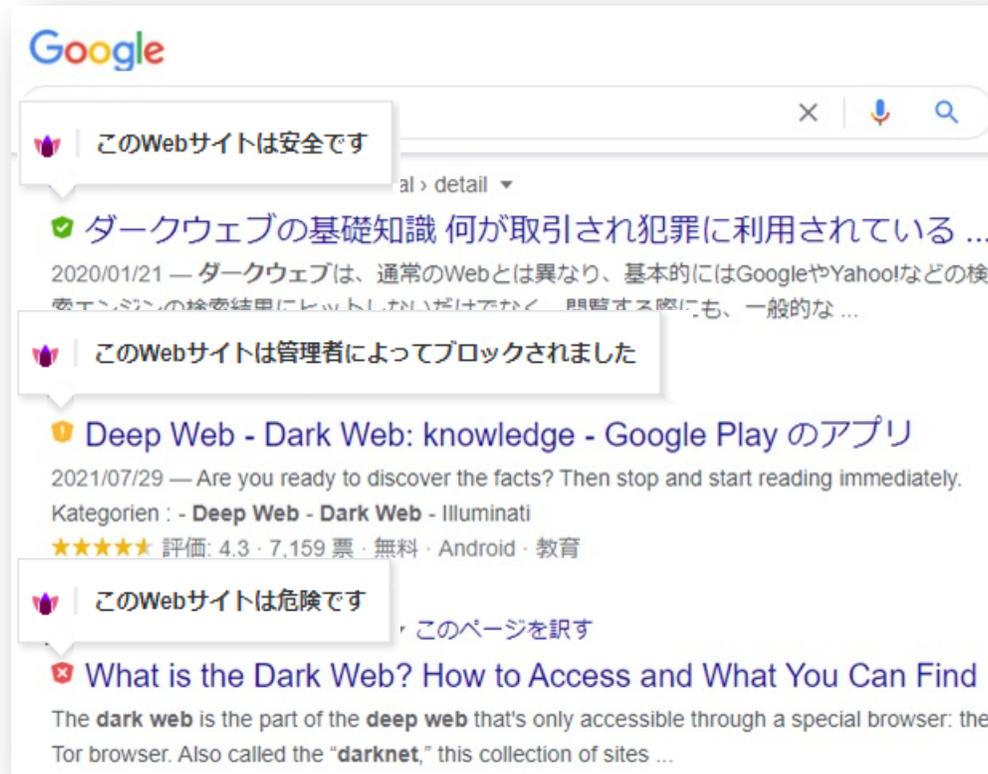
Threat Prevention : サーチ・レピュテーション

Policy > Threat Prevention > Web & Files Protection > Search Reputation

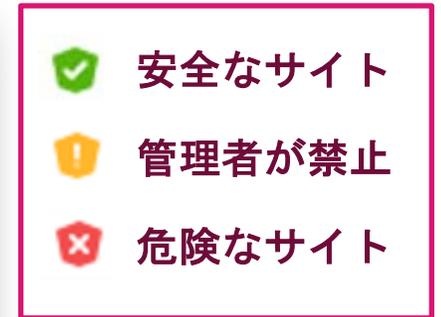
- Google 検索エンジンでの検索結果をURL のレピュテーションに基づいて分類します。
- この機能を有効にするには、[URL フィルタリング モード] を [Prevent] または [Detect] に設定してください。



検索結果例



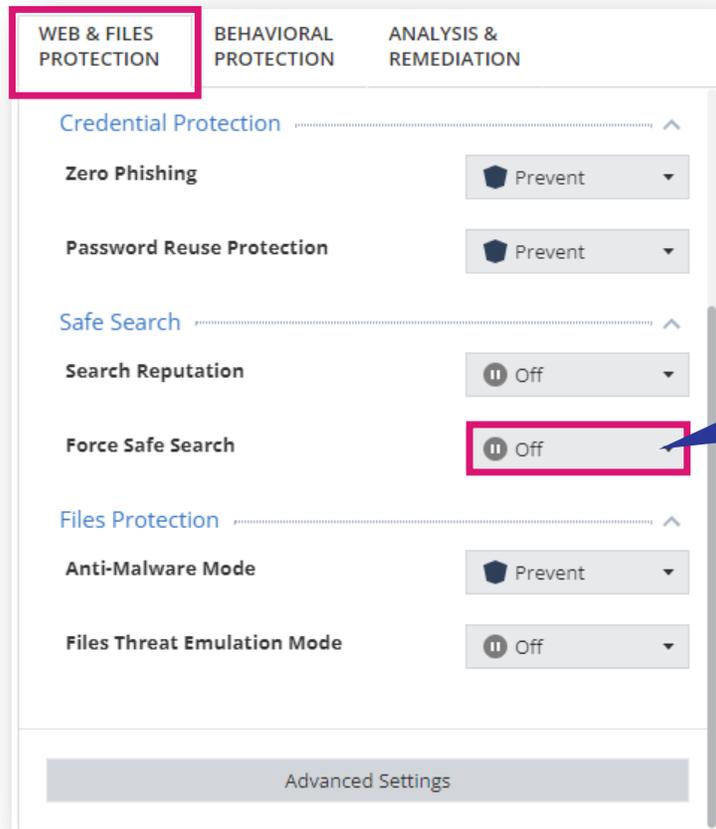
凡例



Threat Prevention : セーフ・サーチ

Policy > Threat Prevention > Web & Files Protection > Safe Search

- 検索エンジンでのセーフサーチ機能の適用を制御します
- この機能は、Google、Bing、Yahooでのセーフサーチをサポートしています。



動作モードを選択

【演習】 Search Reputation

- Google で任意のキーワードで検索をして、レピュテーションに基づく分類がされることを確認してください

ポリシーの設定

THREAT PREVENTION
ファイル保護

YOU DESERVE THE BEST SECURITY

Threat Prevention ファイル保護 (1 / 4)

Policy > Threat Prevention > Web & Files Protection > Files Protection

- マルウェア対策は、ワームやトロイの木馬、アドウェア、キーロガーなどあらゆる種類のマルウェアからコンピュータを保護します
- Files Threat Emulation は、コンピュータにあるファイルのエミュレーションを行います

The image shows the configuration interface for Threat Prevention. The main window is titled 'CAPABILITIES & EXCLUSIONS' and shows 'demo' as the selected policy. Under 'WEB & FILES PROTECTION', 'Files Protection' is selected. The 'Anti-Malware Mode' is set to 'Prevent' and 'Files Threat Emulation Mode' is set to 'On'. A callout bubble points to these settings with the text '動作モードを選択' (Select action mode). Below this, the 'Advanced Settings' button is highlighted. A second window, 'ADVANCED SETTINGS - WEB & FILES PROTECTION', is open, showing a table of file extensions and their actions. A callout bubble points to the table with the text 'ファイル拡張子ごとの動作を選択' (Select action for each file extension). The table lists various file extensions and their default actions, all set to 'Default (Emulate)'. The 'Threat Emulation' option in the left sidebar is also highlighted.

動作モードを選択

ファイル拡張子ごとの動作を選択

File Extension	Description	File Action
PDF	Adobe acrobat document	Default (Emulate)
DOC	Microsoft Word 97-2003 Document	Default (Emulate)
DOCX	Microsoft Word Document	Default (Emulate)
XLS	Microsoft Excel 97-2003 Worksheet	Default (Emulate)
XLSX	Microsoft Excel Worksheet	Default (Emulate)
PPT	Microsoft PowerPoint 97-2003 Presentation	Default (Emulate)
PPTX	Microsoft PowerPoint Presentation	Default (Emulate)
EXE	Executable File	Default (Emulate)
TAR	Tar Archive	Default (Emulate)

Threat Prevention ファイル保護 (2 / 4)

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings

ADVANCED SETTINGS - WEB & FILES PROTECTION

URL Filtering

Download Protection

Credential Protection

Threat Emulation

▼ Files Protection

General

Signature

Scan

Malware Treatment

Quarantine file if cure failed

Delete file if cure failed

Riskware Treatment

Treat as malware

Skip file

Threat Cloud Knowledge Sharing

Allow sending infection info and statistics to Check Point servers for analysis

Allow sending infected file samples to Check Point servers for analysis

Scan On Access

Detect unusual activity

Enable reputation service for files, web resources & processes

Connection timeout: 600 ms

Enable web protection

Mail Protection

Scan mail messages

Anti-Malware で修復に失敗したファイルへの動作を選択

リスクウェア（危険な可能性のある合法的なソフトウェア）の取り扱い方法を選択

Threat Cloud への情報共有の可否を選択

異常な挙動の監視を有効化するかを選択。信頼できるプロセスは監視しない

クラウドを使用したファイル、Web リソース、プロセスのレピュテーションの有効化を選択。PCの再起動後に有効

疑わしい Web サイトへのアクセスと悪意のあるスクリプトの実行防止を有効化するかを選択

電子メールがファイルとして保存される時に、電子メールの検査を有効化するかを選択

Threat Prevention ファイル保護 (3 / 4)

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings

Frequency

Update signatures every 4 hours

Signature update will fail after 60 seconds without server response

Signature Sources

First Priority: External Check Point Signature Server

Second Priority: N/A

Third Priority: N/A

Shared Signature Server

Set as shared signatures server

signature server path

シグネチャの更新間隔とタイムアウト時間

シグネチャの配信元

VDI 環境の非永続的な仮想デスクトップ向けの共有フォルダからのシグネチャ取得設定

Threat Prevention ファイル保護 (4 / 4)

Policy > Threat Prevention > Web & Files Protection > Files Protection > Advance Settings

ADVANCED SETTINGS - WEB & FILES PROTECTION

- URL Filtering
- Download Protection
- Credential Protection
- Threat Emulation
- Files Protection
 - General
 - Signature
 - Scan**

Perform Periodic Scan

Scan Periodic: Every Month

Day of week: Sunday

Day of month: 1

Randomize scan time

Start scan: 12:00

End scan: 12:00

Scan start hour: 12:00

Run initial scan after anti-malware blades installation

Allow user to cancel scan

Prohibit cancel scan if more than 30 Days passed since last successful scan

Scan Targets

Critical areas

Removable drives

Optical drivers

Unrecognized devices

Local drives

Network drives

Mail messages

Scan Target Exclusions

Skip archives and non executables

Do not scan files larger than 20 MB

定期スキャンの設定

定期的なスキャン実行の設定

スキャン対象の選択 (定期スキャンのみ)

スキャン対象の除外設定 (定期スキャンのみ)

【演習】 Anti-Malware

- 以下の Web ページからテストファイルをダウンロードして、Anti-Malware 等で検出することを確認してください
- <https://www.eicar.org/download-anti-malware-testfile/>

ポリシーの設定

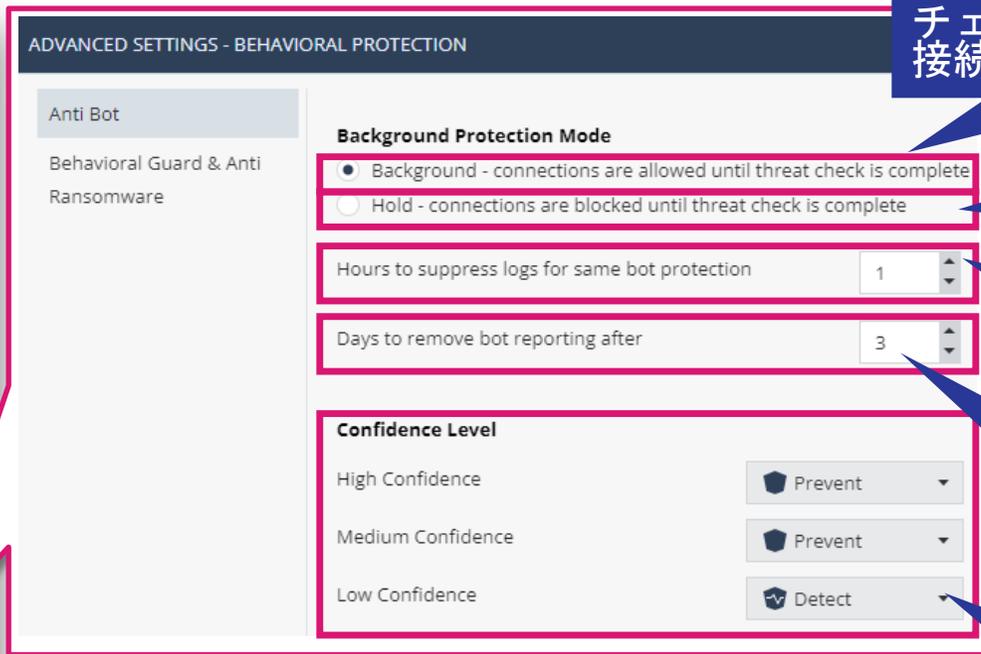
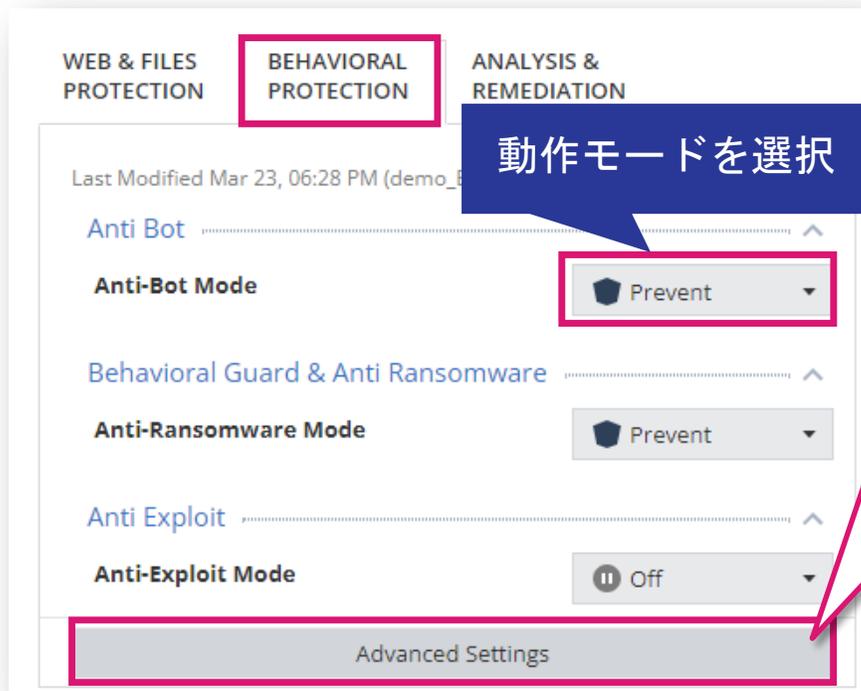
THREAT PREVENTION
ANTI-BOT

YOU DESERVE THE BEST SECURITY

Threat Prevention : Anti-Bot

Policy > Threat Prevention > Behavioral Protection > Anti Bot

- Anti-Botは、C&Cサーバへのボット通信をブロックすることで被害を防ぎ、機密情報が盗まれたり組織から送信されたりしないようにします
- ThreatCloudには、ボットを検出するためのアドレスと、ボットネットの通信パターンが含まれています



チェックが完了する前に、接続を許可 (デフォルト)

チェックが完了するまで、接続をブロック

同じボットのアクションをログに記録する間隔※

選択した日数が経過してもボットがC&Cサーバに接続しない時、感染報告を停止

ボット検出の確実性 (高/中/低) ごとのアクションを選択

※ デフォルトは、1時間。変更する場合は、時間数を選択

ポリシーの設定

**THREAT PREVENTION
BEHAVIORAL GUARD & ANTI-RANSOMWARE**

YOU DESERVE THE BEST SECURITY

Threat Prevention : Behavioral Guard & Anti Ransomware

Policy > Threat Prevention > Behavioral Protection > Behavioral Guard & Anti Ransomware

- 疑わしい動作がないか、ファイルとネットワークアクティビティを常に監視します。
- パソコンにハニーポットファイルを作成し、ファイルの変更を検出するとすぐに攻撃を停止します。

動作モードを選択

共有フォルダの保護の有効化

自動復旧でファイルをリストアする場所を指定

バックアップ領域のサイズと、バックアップの間隔※

ランサムウェア対策でバックアップファイルの種類とサイズ上限を指定

フォレンジックに使用するデータベースサイズ

※ バックアップを取得してから、バックアップ間隔で設定した時間が経過するまでは、バックアップを再取得しません。

【参考】 Anti-Ransomware のバックアップ対象ファイル拡張子（デフォルト）

- 3gp
- aif
- aiff
- asf
- avi
- bmp
- bpg
- csv
- dib
- dibl
- doc
- docb
- docm
- docx
- dot
- dotm
- dotx
- emf
- eps
- flv
- gam
- gif
- hdr
- heif
- htm
- html
- jfif
- jpegl
- jpg
- m4a
- m4v
- mov
- mp3
- mp4
- mpa
- mpeg
- mpg
- pbm
- pdf
- pgm
- png
- pnm
- pot
- potx
- ppm
- pps
- ppsx
- ppt
- pptm
- pptx
- prn
- ps
- rle
- rtf
- sldx
- swf
- tif
- tiff
- txt
- wav
- webp
- wma
- wmv
- wpd
- xlm
- xls
- xlsb
- xlsx
- xlt
- xltm
- xltx

※ バックアップ対象ファイルのサイズ上限の初期値は、25MBです

【参考】 Anti-Ransomware の動作概要



ポリシーの設定

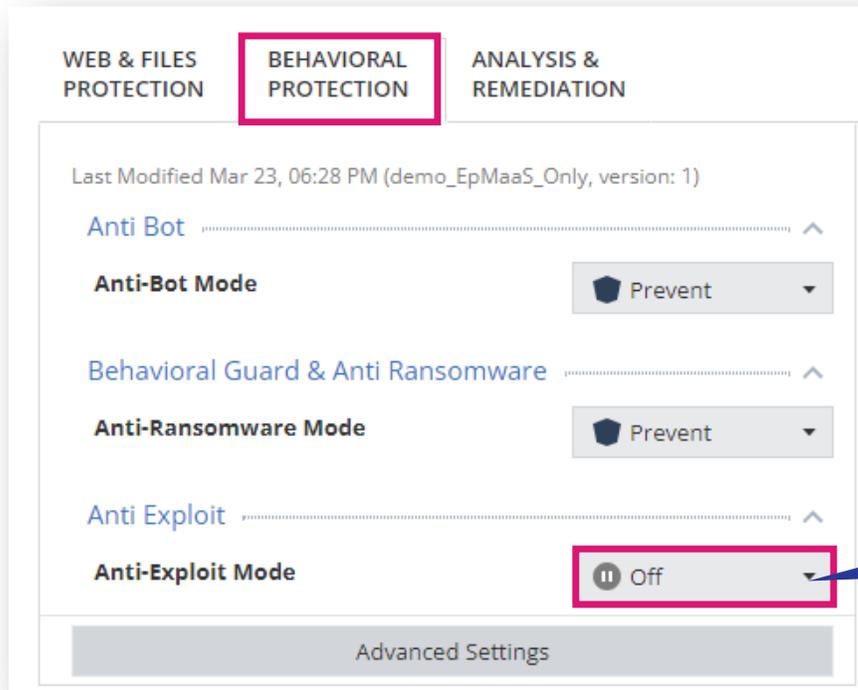
THREAT PREVENTION
ANTI-EXPLOIT

YOU DESERVE THE BEST SECURITY

Threat Prevention : Anti Exploit

Policy > Threat Prevention > Behavioral Protection > Anti Exploit

- Anti-Exploit は、ブラウザや Office のエクスプロイトベースの攻撃に対する保護を提供します。
- Anti-Exploit は悪意のあるペイロードのダウンロードまたは実行を防ぎます。
- Anti-Exploit は、検出時に悪用されているプロセスをシャットダウンし、フォレンジックレポートを生成します。



動作モードを選択

ポリシーの設定

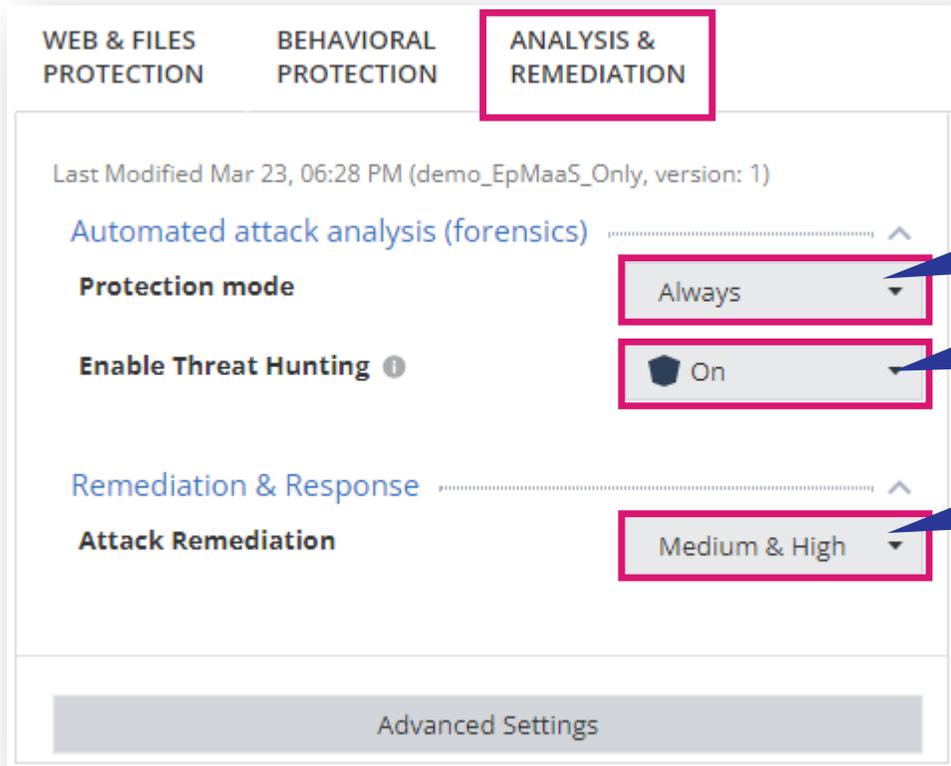
**THREAT PREVENTION
FORENSICS & REMEDIATION**

YOU DESERVE THE BEST SECURITY

Threat Prevention : Analysis & Remediation (1 / 2)

Policy > Threat Prevention > Analysis & Remediation

- Anti-RansomwareやBehavioral Guardなどによって悪意のあるイベントまたはファイルが検出されると、フォレンジック分析が自動的に開始されます
- File Remediationは、悪意のあるファイルを検出すると、ポリシーに基づいてそれらのファイルを自動的に隔離し、必要に応じて修正します



インシデントを分析するコンフィデンスレベル

Threat Huntingの有効／無効を選択

修復を実行するコンフィデンスレベル

Threat Prevention : Analysis & Remediation (2 / 2)

Policy > Threat Prevention > Analysis & Remediation

- File Quarantine（ファイル隔離）では、隔離されるファイルの設定を定義します。
- デフォルトでは、アイテムは 90 日間隔離され、ユーザーは隔離からアイテムを削除できます。
- File Remediation（ファイル修復）では、フォレンジックによって検出された攻撃に関連するファイルの処理をカテゴリごとに定義します。

ADVANCED SETTINGS - ANALYSIS & REMEDIATION

File Quarantine

File Quarantine Medium & High

Allow users to delete items from quarantine

Allow users to restore items from quarantine

Copy quarantine files to central location

Choose location

e.g. c:\Endpoint\default

Quarantine folder name

%ProgramData%\CheckPoint\Endpoint Security\Remediation\Quarantine

File Remediation

Malicious Files	Quarantine
Suspicious Files	Quarantine
Unknown Files	Quarantine
Trusted Files	Ignore

ファイルを隔離する際のコンフィデンスレベルを選択

隔離されたファイルの削除、復元をユーザに許可するか選択

隔離されたファイルのコピーの保存場所を指定

隔離フォルダの場所を指定

ファイルのカテゴリごとに動作を指定

除外設定

YOU DESERVE THE BEST SECURITY

除外設定の概要

- Harmony Endpointによる検査から特定のオブジェクトを除外できます
- 除外設定は、[ログ]のレコードから右クリックで作成するか、除外設定追加メニューで作成します
- 組織全体に適用することも、個別ルールに適用することもできます

機能	除外指定方法					
URL フィルタ	Domain/URL					
Anti-Malware	Infection by name	Process Path	File Path	Folder Path		
Threat Emulation	Domain	SHA-1 Hash	Folder Path			
Threat Extraction	Domain	SHA-1 Hash				
Zero Phishing	Domain					
Anti-Ransomware	Folder Path	Certificate	Protection Name	Process Path		
Behavioral Guard	Folder Path	Certificate	Protection Name	Process Path		
Anti-Bot	Domain	URL	Protection Name	Process	IP Range	
Anti-Exploit	Process Path	Protection Name				
Forensics - Quarantine	Certificate	File Path	Folder Path	MD5 Hash	SHA-1 Hash	File Extension
Forensics - Monitoring	Process Path	Certificate				

除外設定の方法：ログから作成

- Logs で表示されるログのレコードを右クリックする
- 織全体に適用する場合は、「Create Exclusion for All Rules」を選択する
- 個別のルールに適用する場合は、「Create Exclusion for Effective Rule」を選択する

Logs

① レコードを選択して右クリック

② 組織全体に適用する除外設定を作成

② 個別のルールに適用する除外設定を追加

Time	Blade	Action	Type	Severity
Aug 15, 2022 10:11:15 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 10:11:02 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:52:19 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:49:15 AM	Forensics	Prevent	Log	Critical
Aug 15, 2022 9:49:05 AM	Forensics	Prevent	Log	Critical
Aug 15, 2022 9:48:53 AM	Anti-Bot	Prevent	Log	Informational
Aug 15, 2022 9:41:04 AM	Threat Emulation	Allow	Log	Informational
Aug 15, 2022 9:38:30 AM	Endpoint Compliance	Detect	Log	High
Aug 15, 2022 9:37:53 AM	Endpoint Compliance	Inform User	Log	High
Aug 15, 2022 9:37:52 AM	Endpoint Compliance	Inform User	Log	High
Aug 15, 2022 9:35:27 AM	Endpoint Compliance	Detect	Log	High
Aug 15, 2022 9:34:57 AM	URL Filtering	Accept	Log	Informational
Aug 15, 2022 9:34:52 AM	Threat Emulation	Allow	Log	Informational
Aug 15, 2022 9:33:58 AM	Endpoint Compliance	Control	Log	Low
Aug 15, 2022 9:33:42 AM	Threat Emulation	Control	Log	Informational
Aug 15, 2022 9:33:27 AM	Endpoint Compliance	Log	Log	Informational
Aug 15, 2022 9:33:27 AM	Endpoint Compliance	Log	Log	Informational
Aug 15, 2022 9:33:17 AM	Endpoint Compliance	Log	Log	Informational
Aug 15, 2022 9:32:29 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:31:57 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:31:51 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:31:04 AM	Threat Extraction	Extract	Log	Informational
Aug 15, 2022 9:31:04 AM	Threat Extraction	Extract	Log	Informational
Aug 15, 2022 9:30:06 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:29:29 AM	Anti-Malware	Prevent	Log	Low
Aug 15, 2022 9:29:21 AM	URL Filtering	Accept	Log	Informational
Aug 15, 2022 9:28:18 AM	URL Filtering	Prevent	Log	Informational
Aug 15, 2022 9:28:04 AM	URL Filtering	Prevent	Log	Informational

除外設定の方法：編集メニューから作成（1 / 2）

- Policy > Threat Prevention > Global Exclusions で、組織全体に適用する除外設定を追加
- Policy > Threat Prevention > Policy Capabilities > Capabilities & Exclusions > Edit Exclusions で、ルールごとの除外設定を追加
- 除外設定を追加後は、Save と Install を実施する

組織全体に適用する除外設定を作成

#	Rule Name	Applied To	Web & Files	Behavioral	Analysis
0	Eval	Eval			
1	CP-demo	CP-demo			
2	demo-point	demo-point			
3	Default settings	Entire Organization			

個別のルールに適用する除外設定を追加

除外設定の方法：編集メニューから作成（2 / 2）

The screenshot displays the Check Point Harmony Endpoint interface. The main content area shows a table of exclusions with columns for 'Exclusion', 'Method', and 'Value'. A red callout box labeled '① クリック' (Click) points to an asterisk icon in the 'Exclusion' column of the first row.

Two 'NEW EXCLUSION' dialog boxes are overlaid on the screen. The left dialog box is titled 'NEW EXCLUSION' and contains the following fields:

- 'Exclusion' dropdown menu: 'Anti Bot -> URL Filtering exclusions' (highlighted by a red callout box labeled '② 除外設定のカテゴリを選択' - Select the exclusion category).
- 'Method' dropdown menu: 'Domain/URL'.
- 'Value' text input field: (highlighted by a red callout box labeled '③ 除外内容を入力' - Enter exclusion content).
- 'Add to all rules' checkbox: unchecked.
- 'CANCEL' and 'OK' buttons at the bottom.

The right dialog box is also titled 'NEW EXCLUSION' and shows a list of exclusion categories in a scrollable area, with 'Anti Bot -> URL Filtering exclusions' selected at the top.

At the bottom right of the interface, there are 'Cancel' and 'OK' buttons.

【演習】 除外設定

- Anti-Malware の除外設定で、テストファイル（eicar）を除外するルールを作成し、検出されなくなることを確認してください。

コンピュータの隔離、解放

YOU DESERVE THE BEST SECURITY

隔離方法その1：Asset Management 画面からの端末の隔離、解放

Asset Management > Computers > Computer Actions > Forensics & Remediation > Isolate Computer

- リモートから端末の隔離、解放を実行できます。
- 端末の隔離をするためには、Firewall Bladeが必要です。

The screenshot illustrates the process of isolating a computer through the HARMONY ENDPOINT interface. The interface is divided into several sections:

- ASSET MANAGEMENT:** The sidebar on the left has 'ASSET MANAGEMENT' selected.
- Computers Table:** The main area displays a table of computers. The 'Status' column for the selected computer (CP-DEMO) has a checkmark in a box, indicating selection.
- Computer Actions:** A dropdown menu is open, showing various actions. The 'Forensics & Remediation' option is selected, and the 'Isolate Computer' option is highlighted.
- PUSH OPERATION CREATION DIALOG:** A dialog box titled 'Isolate Computer' is open on the right. It contains a 'Comment' field, a 'User Notification' section with a checked 'Inform user with notification' option, and a 'Scheduling' section with the text 'Operation will be executed immediately'. At the bottom, there are 'Cancel' and 'Create' buttons.

Annotations in blue callouts indicate the steps:

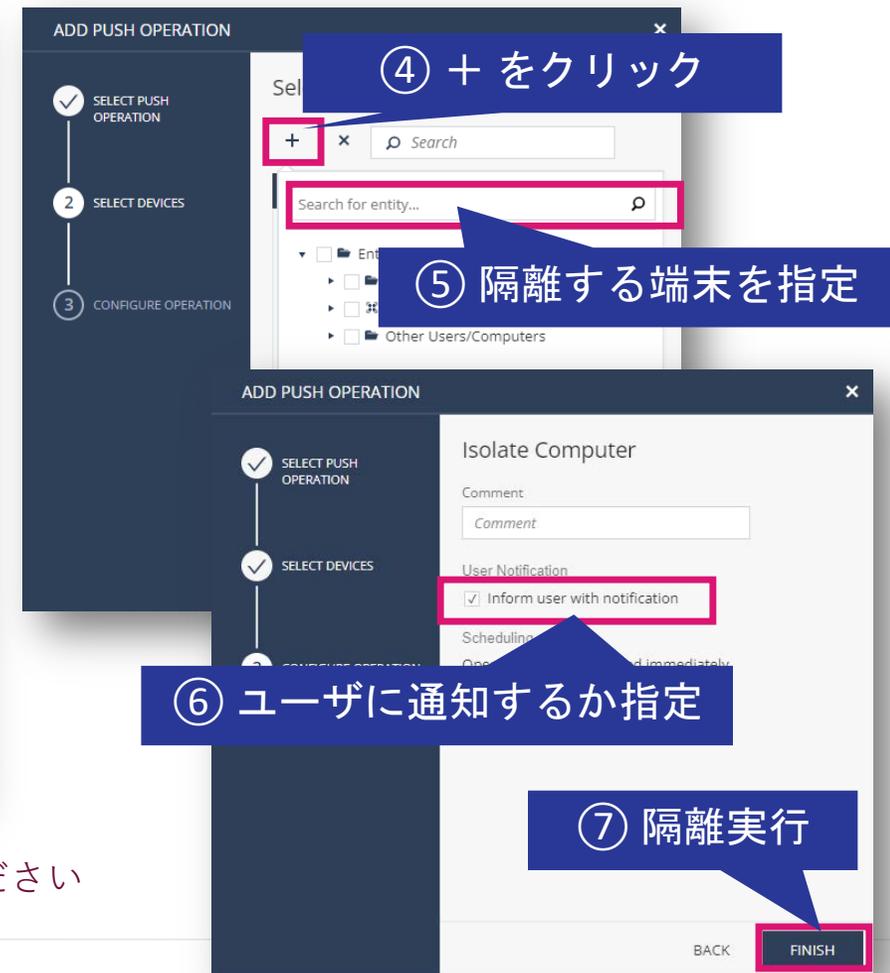
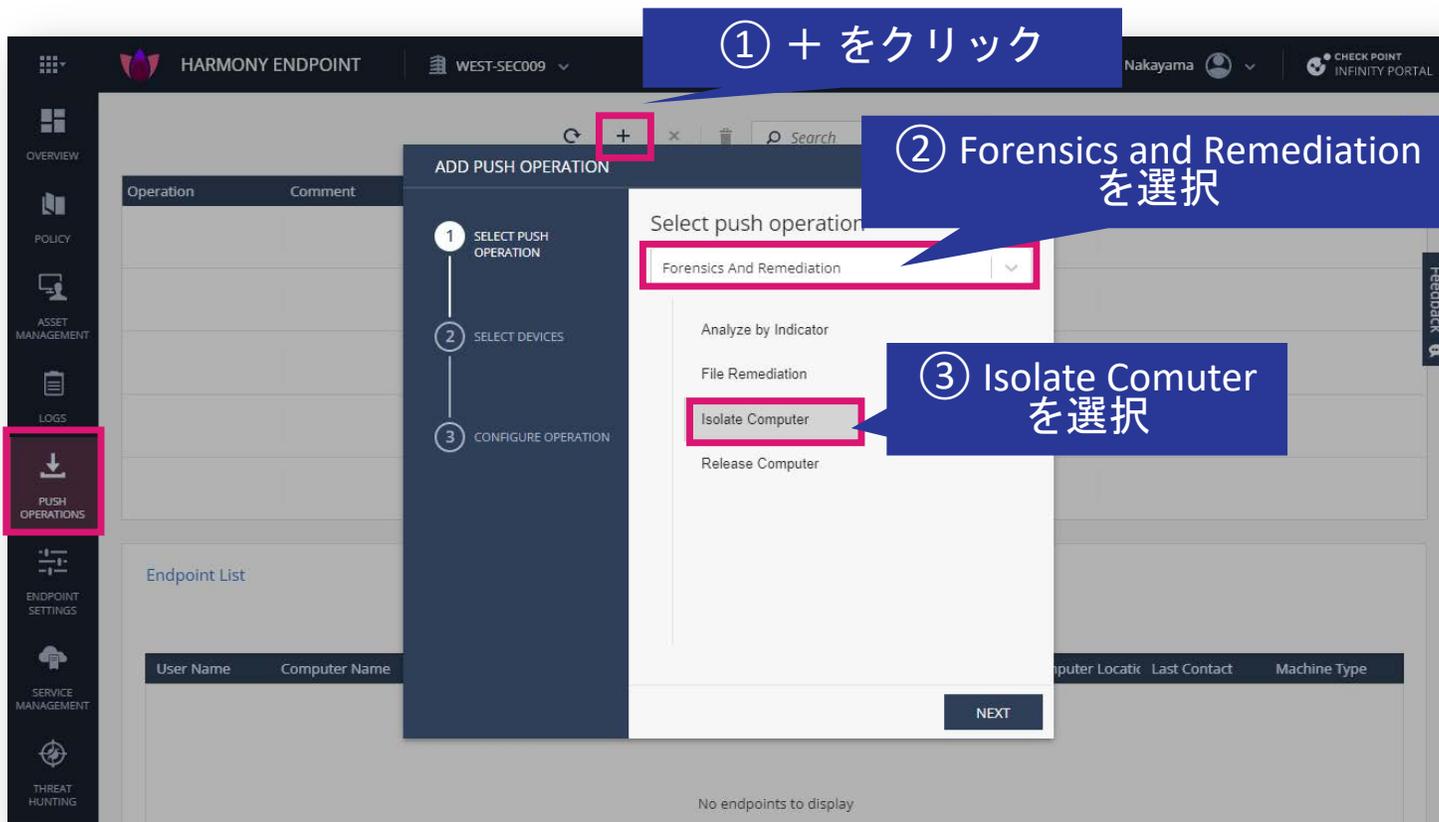
- ① 隔離する端末を選択
- ② Computer Actions をクリック
- ③ Forensics and Remediation をクリック
- ④ Isolate Computer をクリック
- ⑤ 隔離実行

※ 端末を解放する際は、Computer Actions > Forensics & Remediations > Release Computer Isolation を選択してください。

隔離方法その2：Push Operations 画面からの端末の隔離、解放

Push Operations

- リモートから端末の隔離を実行できます。
- 端末の隔離をするためには、Firewall Bladeが必要です。



※ 端末を解放する際は、Forensics & Remediations > Release Computer を選択してください

遠隔操作の状況確認

Push Operations

- Push Operations で遠隔操作の状況を確認

The screenshot displays the Harmony Endpoint management interface. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, PUSH OPERATIONS (highlighted with a red box), ENDPOINT SETTINGS, and SERVICE MANAGEMENT. The main content area is divided into two sections. The top section, titled '遠隔操作の状況' (Remote Operation Status), shows a table of operations. The bottom section, titled 'Endpoint List', shows a table of endpoint details. Both tables have their first rows highlighted with a red box.

遠隔操作の状況

Operation	Comment	Pushed To	Status	Admin Name	Advanced Settings	Created On	Active Until
Isolate Computer		CP-DEMO	Pushing to clients	yoshiyasun_EpMaaS_Only	View Advanced Settings...	10 Jun 2022 06:53 pm	11 Jun 2022 06:53 pm
Uninstall Client		Lab-13	Pushing to clients	yoshiyasun_EpMaaS_Only	View Advanced Settings...	10 Jun 2022 04:45 pm	11 Jun 2022 04:45 pm
Release Computer Isolation		CP-DEMO	Completed	yoshiyasun_EpMaaS_Only	View Advanced Settings...	10 Jun 2022 01:36 pm	11 Jun 2022 01:36 pm
Isolate Computer		CP-DEMO	Completed	yoshiyasun_EpMaaS_Only	View Advanced Settings...	10 Jun 2022 11:45 am	11 Jun 2022 11:45 am
Release Computer Isolation		CP-DEMO	Completed	yoshiyasun_EpMaaS_Only	View Advanced Settings...	10 Jun 2022 07:36 am	11 Jun 2022 07:36 am

Previous Page 1 of 2

Endpoint List

User Name	Computer Name	Operation Status	Operation Status Descriptio	Operation Output	Sent To Endpoint On	Status Update Received On
nack	CP-DEMO	Succeeded	success		10 Jun 2022 06:59 pm	10 Jun 2022 06:59 pm

Asset Management 画面での端末の状況確認

Asset Management > Computers

- Host Isolation 表示に切り替えることで、端末の隔離状況を表示可能

The screenshot shows the HARMONY END interface. The left sidebar has 'ASSET MANAGEMENT' highlighted. The main area shows 'Computers' selected in the organizational tree. The 'Columns' dropdown is set to 'Host Isolation'. A table displays the isolation status for two computers: CP-DEMO (Isolated) and Lab-13 (Not Isolated).

表示モードを [Host Isolation] に切り替え

コンピューターの隔離状況を確認

Status	Computer Name	Endpoint Version	Isolation Status	Last Connection
<input checked="" type="checkbox"/>	CP-DEMO	86.26.6008	Isolated	10 Jun 2022 06:58 pm
<input type="checkbox"/>	Lab-13	86.26.6008	Not Isolated	03 Jun 2022 01:02 pm

【演習】コンピュータの隔離、開放

- コマンドプロンプトを起動して以下のコマンドを実行してください
 - ping -t 8.8.8.8
- コンピュータの隔離と解放を行い、ping の応答の変化を確認してください

ログの表示

YOU DESERVE THE BEST SECURITY

ログの表示 (1 / 2)

Logs > New Tab Catalog > Favorites (もしくは、Logs) > Logs

- New Tab Catalog から表示したいログ、ビュー、レポートを選択します
- デフォルトでは、Logs が表示されます (その他のログ等を見たい場合は、**+** を押して New Tab Catalog を表示させます)

The image shows two screenshots of the Check Point Harmony Endpoint console. The left screenshot displays the 'New Tab Catalog' with a grid of categories: Audit Logs, Access Control, Audit Overview, Threat Prevention, and General Overview. A blue callout box points to the 'Logs' category with the text '表示するカテゴリを選択' (Select the category to display). Another blue callout box points to the '+' icon in the top right of the catalog with the text '表示するログを選択' (Select the log to display). The right screenshot shows the 'Logs' view with a table of log entries. A blue callout box points to the 'Logs' category in the left sidebar with the text '表示するログを選択'.

Time	Blade	Action	Severity	Confidence L...	Machine Name	Protection T...	Protection Name	Malware Act...
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low	Low	Endpoint3	Generic	DOS/ICAR_Test_File	
Mar 30, 2022 9:09:10 AM	Endpoint Compliance	Detect	Me...	N/A	Endpoint3			
Mar 30, 2022 9:08:20 AM	Full Disk Encryption		Me...	N/A	Endpoint3			
Mar 30, 2022 9:08:19 AM	Full Disk Encryption		Me...	N/A	Endpoint3			
Mar 30, 2022 9:07:21 AM	Endpoint Compliance	Inform User	Crit...	N/A	Endpoint3			
Mar 30, 2022 9:07:17 AM	Endpoint Compliance		High	N/A	Endpoint3			
Mar 30, 2022 1:09:18 AM	Anti-Malware		Low	N/A	Endpoint3			
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.exe	Trojan", "beh
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.exe	Trojan", "beh
Mar 30, 2022 12:58:44 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.exe	Trojan", "beh
Mar 30, 2022 12:58:39 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.exe	Trojan", "beh
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:58:11 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:58:00 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:57:48 AM	Forensics	Prevent	High	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:57:47 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:57:43 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:57:38 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:57:36 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Em...	Gen.SB.dll	Trojan
Mar 30, 2022 12:56:02 AM	Forensics	Prevent	High	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:50 AM	Forensics	Prevent	High	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:38 AM	Forensics	Prevent	High	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:26 AM	Forensics	Prevent	High	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:14 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:13 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File Reputation	Gen.Rep.exe	
Mar 30, 2022 12:55:08 AM	Forensics	Prevent	Crit...	High	Endpoint3	Static File Anal...	Gen.MLSA	

ログの表示 (2 / 2)

事前定義されたビューの一覧

お気に入りへ登録可能

Favorites	Name	Category	Last Viewed	Created by
★	Access Control	Access Control	22 minutes ago	Check Point
★	Active Users	Access Control		Check Point
★	Application Categories	Access Control		Check Point
★	Applications and Sites	Access Control		Check Point
★	Audit Overview	General		Check Point
★	Content Awareness	Access Control		Check Point
★	Cyber Attack View - Endpoint	Threat Prevention	3 days ago	Check Point
★	Cyber Attack View - Endpoint	Threat Prevention		Check Point
★	Cyber Attack View - Gateway	Threat Prevention		Check Point
★	Cyber Attack View - Mobile	Threat Prevention		Check Point
★	Data Loss Prevention (DLP)	Access Control		Check Point
★	General Overview	General		Check Point
★	High Bandwidth Applications	Access Control		Check Point
★	High Risk Applications and Sites	Access Control		Check Point
★	Important Attacks	Threat Prevention		Check Point
★	Infected Hosts	Threat Prevention		Check Point
★	Infinity Threat Prevention Dashboard	Threat Prevention		Check Point
★	License Status	General		Check Point
★	MITRE ATT&CK	Threat Prevention		Check Point
★	MTA Live Monitoring	General		Check Point
★	MTA Overview	General		Check Point
★	MTA Troubleshooting	General		Check Point
★	Remote Access	Access Control		Check Point
★	Security Checkup Summary	General		Check Point
★	Security Incidents	Threat Prevention	3 days ago	Check Point
★	Threat Prevention	Threat Prevention		Check Point
★	Web Extension Security Dashboard	General		Check Point

表示種別を選択

事前定義されたビューの一覧

事前定義されたレポートの一覧

お気に入りへ登録可能

Favorites	Name	Category	Last Viewed	Created by
★	Application and URL Filtering	Access Control	2 weeks ago	Check Point
★	Cloud Services	Access Control		Check Point
★	Compliance Blade	Compliance		Check Point
★	Content Awareness	Access Control		Check Point
★	Correlated Events	General		Check Point
★	Data Loss Prevention (DLP)	Access Control		Check Point
★	DDOS Protector	Threat Prevention		Check Point
★	Detailed User Activity	Access Control		Check Point
★	GDPR Security Report	General		Check Point
★	IntelliStore	Threat Prevention		Check Point
★	Intrusion Prevention System (IPS)	Threat Prevention		Check Point
★	License Inventory	General		Check Point
★	Mobile Security Checkup	General		Check Point
★	Network Activity	Access Control		Check Point
★	Network Security	General		Check Point
★	Security Checkup - Advanced	General		Check Point
★	Security Checkup - Anonymized	General		Check Point
★	Security Checkup - SaaS	General		Check Point
★	Security Checkup - Statistics	General		Check Point
★	Threat Emulation	Threat Prevention		Check Point
★	Threat Extraction	Threat Prevention		Check Point
★	Threat Prevention	Threat Prevention		Check Point
★	User Activity	Access Control		Check Point

表示種別を選択

事前定義されたレポートの一覧

ログの表示：一覧表示・詳細表示 (1 / 2)

The screenshot displays the Harmony Endpoint console interface. On the left, a sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS (highlighted), PUSH, SETTINGS, SERVICE MANAGEMENT, THREAT HUNTING, and Global Settings. The main area is divided into three sections:

- Statistics:** A bar chart titled 'Sessions Timeline' showing activity for Wed 23, Sat 26, and Tue 29. Below it, a 'Blade' filter section lists various security components with their respective percentages (e.g., Endpoint Compliance at 28.6%, Anti-Malware at 22.54%).
- Log Table:** A table with columns for Time, Blade, Action, Severity, Protection Type, Protection Name, and File Name. It lists numerous log entries, such as 'Detect' actions for 'gen.win.trojan' and 'DOS/EICAR_Test_File'.
- Card:** A detailed view of a selected log entry, showing 'Log Info' (Origin, Time, Blade, etc.), 'Policy' (Action, Date, Name), and 'Protection Details' (Severity, Confidence Level, Malware Action).

Annotations in blue callouts provide additional context:

- A callout pointing to the 'New Tab Catalog' button states: **事前定義された数多くのビュー、レポートを選択して表示できます** (You can select and display many predefined views and reports).
- A callout pointing to the log table states: **一覧表示。ダブルクリックでログの詳細を表示。ログの詳細からフォレンジックレポートを表示可能** (List view. Double-click to display log details. Forensic reports can be displayed from log details).
- A callout pointing to the Card section states: **詳細表示** (Detailed view).
- A callout pointing to the filter section states: **ログの表示条件を選択** (Select log display conditions).

ログの表示：一覧表示・詳細表示（2 / 2）

- 一覧表示されたログの詳細を表示できます

The screenshot displays the Check Point Harmony Endpoint interface. The main window shows a list of logs with columns for Time, Blade, Action, and Severity. A blue callout box with the text "エンTRIESをダブルクリックして、詳細を表示" (Double-click the entries to display details) points to a log entry. A red box highlights this entry, and a red arrow points to a detailed view card on the right. The card shows Log Info (Origin, Time, Blade) and DETAILS (Log Info, Policy, Protection Details, Forensics Report).

Time	Blade	Action	Severity
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low
Mar 30, 2022 9:09:10 AM	Endpoint Compliance	Detect	Medium
Mar 30, 2022 9:08:20 AM	Full Disk Encryption	Detect	Medium
Mar 30, 2022 9:08:19 AM	Full Disk Encryption	Detect	Medium
Mar 30, 2022 9:07:21 AM	Endpoint Compliance	Inform User	Critical
Mar 30, 2022 9:07:17 AM	Endpoint Compliance	Detect	High
Mar 30, 2022 1:09:18 AM	Anti-Malware	Detect	Low
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High
Mar 30, 2022 12:58:44 AM	Threat Emulation	Prevent	Low
Mar 30, 2022 12:58:39 AM	Threat Emulation	Prevent	High
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High
Mar 30, 2022 12:58:11 AM	Forensics	Prevent	High
Mar 30, 2022 12:58:00 AM	Forensics	Prevent	High
Mar 30, 2022 12:57:48 AM	Forensics	Prevent	High
Mar 30, 2022 12:57:47 AM	Threat Emulation	Prevent	Low
Mar 30, 2022 12:57:43 AM	Threat Emulation	Prevent	High
Mar 30, 2022 12:57:38 AM	Threat Emulation	Prevent	Low
Mar 30, 2022 12:57:36 AM	Threat Emulation	Prevent	High
Mar 30, 2022 12:56:02 AM	Forensics	Prevent	High
Mar 30, 2022 12:55:50 AM	Forensics	Prevent	High
Mar 30, 2022 12:55:38 AM	Forensics	Prevent	High
Mar 30, 2022 12:55:26 AM	Forensics	Prevent	High
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	Low
Mar 30, 2022 12:55:22 AM	Threat Emulation	Prevent	High
Mar 30, 2022 12:55:14 AM	Threat Emulation	Prevent	Low
Mar 30, 2022 12:55:13 AM	Threat Emulation	Prevent	High
Mar 30, 2022 12:55:08 AM	Forensics	Prevent	Critical

Log Info

- Origin: cpjdemo002-d69e771e-hap2
- Time: Mar 30, 2022 11:34:53 PM
- Blade: SmartEvent Client

Card

Prevent Forensics Oct 30, 2020 11:31:21 AM

DETAILS

Log Info

- Origin: CheckPointKitta-b14818cb-hap1
- Time: Oct 30, 2020 11:31:21 AM
- Blade: Forensics
- Triggered By: Endpoint Anti-Bot
- Product Family: Endpoint
- Type: Log
- Attack Status: Blocked
- Event Type: Forensics Case Analysis

Policy

- Action: Prevent
- Policy Date: Sep 15, 2020
- Policy Name: Default Forensics settings
- Policy Version: 1
- Log Server IP: 164.100.1.8

Protection Details

- Severity: Critical
- Confidence Level: Medium
- Malware Action: Communication with C&C

Traffic

- Source: ip-192-168-100-5.ec2.internal (192.168.100.5)
- Source User Name: aduser1
- Machine Name: DESKTOP-M5E17GCad.example.com

Forensics Report

Open the Forensics Report

ログの表示：期間指定

- 指定した期間でログを絞り込むことができます

The screenshot displays the 'Select a time filter' dialog in the Check Point log viewer. At the top left, a dropdown menu is set to 'Last 7 Days'. Below this, a table of preset filters is shown, with 'Last 7 Days' highlighted in blue. The table includes options like 'Today', 'Yesterday', 'This Week', 'This Month', 'This Year', 'Last Hour', 'Last 24 Hours', 'Last Week', 'Last 30 Days', 'Last Month', 'Last 365 Days', and 'Last Year'. Below the table, there are sections for 'Relative Time Range', 'Date Range', and 'Date and Time Range'. At the bottom, there are filters for 'Threat Emulation' (2.94%) and 'Severity' (Low, 41.18%). The main log area shows several entries with timestamps, severity levels (Critical), and source/destination information.

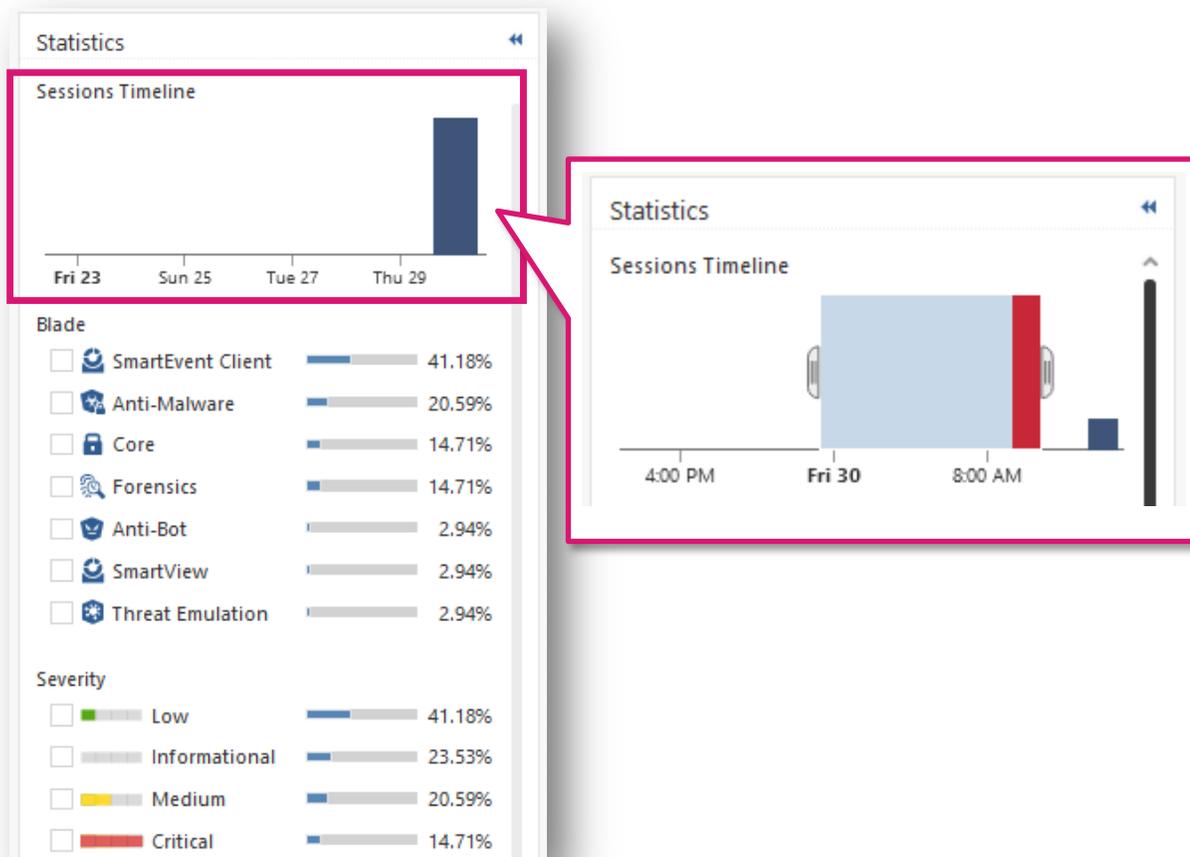
Time Filter	Relative Time Range
Today	(Oct 30, 2020)
Yesterday	(Oct 29, 2020)
This Week	(Since Oct 26, 2020)
This Month	(Since Oct 1, 2020)
This Year	(Since Jan 1, 2020)
Last Hour	(Since 2:25 PM)
Last 24 Hours	(Since Oct 29, 2020 3:25 PM)
Last 7 Days	(Since Oct 23, 2020)
Last Week	(Oct 19, 2020 - Oct 25, 2020)
Last 30 Days	(Since Sep 30, 2020)
Last Month	(Sep 2020)
Last 365 Days	(Since Oct 31, 2019)
Last Year	(2019)

指定した期間でログを絞り込み

時間で指定することも可能

ログの表示： Statistics パネル

- 簡単な統計情報が表示されます
- チェックボックスをクリックすると、それぞれの項目で簡単にフィルタをかけることができます
- タイムライン上で表示期間を選択することも可能です



ログの表示：カラム指定

- ログのカラム表示を変更できます

タイトルバーの上で、右クリック

表示プロファイルを選択

The screenshot displays a log table with columns: Time, Blade, Action, Severity, and a multi-column section for details. A context menu is open over the table, showing a list of display profiles. The 'Endpoint' profile is selected, and its sub-menu is also open, showing 'Anti-Exploit' as the selected option.

Time	Blade	Action	Severity	Profile	Severity	File Name	Protection	Malware Act...	File Name
Mar 30, 2022 9:09:10 AM	Endpoint Complia...	Detect	Me...	Endpoint	High	File System Emulation			
Mar 30, 2022 9:08:20 AM	Full Disk Encryption		Me...	Endpoint	High	File System Emulation			
Mar 30, 2022 9:08:19 AM	Full Disk Encryption		Me...	Endpoint	High	File System Emulation			
Mar 30, 2022 9:07:21 AM	Endpoint Complia...	Inform ...	Cri...	Endpoint	High	File System Emulation			
Mar 30, 2022 9:07:17 AM	Endpoint Complia...		High	Endpoint	High	File System Emulation			
Mar 30, 2022 1:09:18 AM	Anti-Malware		Low	Endpoint	High	File System Emulation			
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High	Endpoint	High	File System Emulation			48d3aa
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High	Endpoint	High	File System Emulation			00031
Mar 30, 2022 12:58:44 AM	Threat Emulation	Prevent	Low	Endpoint	High	File System Emulation			ee2cc-1
Mar 30, 2022 12:58:39 AM	Threat Emulation	Prevent	Low	Endpoint	High	File System Emulation			00031
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High	Endpoint	High	File System Emulation	Gen.SB.dll	Trojan	7e2b1bbff
Mar 30, 2022 12:58:11 AM	Forensics	Prevent	High	Endpoint	High	File System Emulation	Gen.SB.dll	Trojan	f000025

ログの表示：キーワードでの検索

- キーワードを入力して、ユーザ名やコンピュータ名などでログを絞り込むことができます

Mar 30, 2022 Endpoint3

Time	Blade	Action	Severity	Confidence Le...	Machine Na...	Protection Type	Protection Name	Malware Act...	File Name
Mar 30, 2022 2:13:21 PM	Forensics	Detect	Low	Low	Endpoint3	Generic	gen.win.trojan		backdoor.msil.tyupkin.a.vir
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low	Low	Endpoint3	Generic	DOS/EICAR_Test_File		eicar_com.zip
Mar 30, 2022 9:09:10 AM	Endpoint Compliance	Detect	Me...	N/A	Endpoint3				
Mar 30, 2022 9:08:20 AM	Full Disk Encryption		Me...	N/A	Endpoint3				
Mar 30, 2022 9:08:19 AM	Full Disk Encryption		Me...	N/A	Endpoint3				
Mar 30, 2022 9:07:21 AM	Endpoint Compliance	Inform User	Cri...	N/A	Endpoint3				
Mar 30, 2022 9:07:17 AM	Endpoint Compliance		High	N/A	Endpoint3				
Mar 30, 2022 1:09:18 AM	Anti-Malware		Low	N/A	Endpoint3				
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.exe	Trojan", "behavior	14e48d3aa7b9058c56882eb61fa40cf1f5261
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.exe	Trojan", "behavior	f_000031
Mar 30, 2022 12:58:44 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.exe	Trojan", "behavior	f57ee2cc-1a44-498a-bd23-0c8defb2dd6d.tr
Mar 30, 2022 12:58:39 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.exe	Trojan", "behavior	f_000031
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	7e2b1bbffa7f05e7bf57ee60d162ef1e6f83b2
Mar 30, 2022 12:58:11 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	f_000035
Mar 30, 2022 12:58:00 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	f_000034
Mar 30, 2022 12:57:48 AM	Forensics	Prevent	High	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	2826815873d90ad38c5aeed57c09385d6ac
Mar 30, 2022 12:57:47 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	ed8c6b08-f914-4231-9e64-699fcab522a3.tr
Mar 30, 2022 12:57:43 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	f_000035
Mar 30, 2022 12:57:38 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	f_000034
Mar 30, 2022 12:57:36 AM	Threat Emulation	Prevent	Low	High	Endpoint3	File System Emulati...	Gen.SB.dll	Trojan	3d14a9c7-e1a7-44aa-8adf-4044e9a04c50.tr

クエリ言語の概要

- クエリ言語を使用すると、条件に従ってログから選択したレコードのみを表示できます
- 複雑なクエリを作成するには、ブール演算子、ワイルドカード、フィールド、範囲を使用します
- 基本的なクエリ構文は次のとおりです

```
[<Field>:] <Filter Criterion>
```

ほとんどのキーワードやクエリ条件で、大文字小文字は区別されませんが、一部例外があります
クエリ結果に期待される結果が表示されない場合、大文字小文字を変更してみます
例：source:<X>は、大文字小文字が区別されます。Source:<X>では一致しません

- 1つのクエリに複数の条件を含めるには、ブール演算子を使用します

```
[<Field>:] <Filter Criterion> {AND | OR | NOT} [<Field>:] <Filter Criterion> ...
```

複数の基準値を持つクエリを使用する場合、ANDは自動的に暗黙指定されるため、追加する必要はありません
必要に応じて、ORまたはその他のブール演算子を入力します

クエリ言語の概要

- 1単語の文字列の例
 - Alice
 - inbound
 - 192.168.2.1
 - some.example.com
 - dns_udp
- フレーズの例
 - "Alice Pleasance Liddell"
 - "Log Out"
 - "VPN-1 Embedded Connector"
- IPアドレス
 - ログクエリで使用されるIPアドレスは、1単語としてカウントされます
 - 192.168.2.1
 - 2001:db8::f00:d
 - ワイルドカード '*'文字と標準のネットワークサブネットマスクを使用して、範囲内のIPアドレスに一致するログを検索することもできます
 - src:192.168.0.0/16
 - src:192.168.2.0/24
 - src:192.168.2.*
 - 192.168.*

クエリ言語の概要

- NOT 値
 - 次のとおり、ログクエリのキーワードでNOT<Field>値を使用して、フィールドの値がクエリの値ではないログを検索できます
 - `NOT <field>: <value>`
 - NOT src:192.168.2.100
- ワイルドカード
 - クエリで標準のワイルドカード文字（*および?）を使用して、ログレコードの変数文字または文字列を照合できます
 - ‘*’ は、文字列と一致します
 - ‘?’ は、1文字に一致します
 - Ali* は、Aliceや、Alia、Alice Pleasance Liddellなどが一致します
 - Ali? は、AliaやAlisなどが一致しますが、AliceやAlice Pleasance Liddellなどは一致しません

クエリ言語の概要

- フィールドキーワード
 - フィルタ条件のキーワードとして、事前定義されたフィールド名を使用できます

`<field name>:<values>`

- source:192.168.2.1
- action:(Reject OR Block)

Keyword	Keyword Alias	Description
severity		Severity of the event
app_risk		Potential risk from the application, of the event
Protection		Name of the protection
protection_type		Type of protection
confidence_level		Level of confidence that an event is malicious
action		Action taken by a security rule
blade	product	Software Blade
destination	dst	Traffic destination IP address, DNS name or Check Point network object name
origin	orig	Name of originating Security Gateway
service		Service that generated the log entry
source	src	Traffic source IP address, DNS name or Check Point network object name
user		User name
Rule		Rule Number

- フィールド名を使用しない場合、いずれかのフィールドが条件に一致するレコードが表示されます

クエリ言語の概要

- ブール演算子
 - ブール演算子AND、OR、およびNOTを使用して、複数条件を持つフィルターを作成できます
 - 数のブール式を括弧で囲むことができます
 - ブール演算子なしで複数の条件を入力すると、AND演算子が暗黙指定されます
 - 括弧なしで複数の基準を使用する場合、OR演算子はAND演算子の前に適用されます
- 例
 - blade:"application control" AND action:block
 - 192.168.2.133 10.19.136.101
 - 192.168.2.133 OR 10.19.136.101
 - (blade: Firewall OR blade: IPS OR blade:VPN) AND NOT action:drop
 - source:(192.168.2.1 OR 192.168.2.2) AND destination:17.168.8.2

クエリ言語の概要

Mar 30, 2022 Search

Time	Blade	Action	Severity	Confidence Le...	Protection T...	Protection Na...	File Name
Mar 30, 2022 2:13:21 PM	Forensics	Detect	Low	Low	Generic	gen.win.trojan	backdoor.msil.tyupkin.a.vir
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low	Low	Generic	DOS/EICAR_Test...	eicar_com.zip
Mar 30, 2022 9:09:10 AM	Endpoint Compliance	Detect	Medium	N/A			
Mar 30, 2022 9:08:20 AM	Full Disk Encryption		Medium	N/A			
Mar 30, 2022 9:08:19 AM	Full Disk Encryption		Medium	N/A			

Mar 30, 2022 blade:forensics

Time	Blade	Action	Severity	Confidence...	Protection Type	Protection Name	File Name
Mar 30, 2022 2:13:21 PM	Forensics	Detect	Low	Low	Generic	gen.win.trojan	backdoor.msil.tyupkin.a.vir
Mar 30, 2022 2:13:06 PM	Forensics	Detect	Low	Low	Generic	DOS/EICAR_Test_File	eicar_com.zip
Mar 30, 2022 12:59:02 AM	Forensics	Prevent	High	High	File System Emulation	Gen.SB.exe	14e48d3aa7b9058c56882eb
Mar 30, 2022 12:58:50 AM	Forensics	Prevent	High	High	File System Emulation	Gen.SB.exe	f_000031
Mar 30, 2022 12:58:23 AM	Forensics	Prevent	High	High	File System Emulation	Gen.SB.dll	7e2b1bbffa7f05e7bf57ee60

Mar 30, 2022 blade:forensics AND severity:Critical

Time	Blade	Action	Severity	Confidence Level	Protection Type	Protection Name	File Name
Mar 30, 2022 12:55:08 AM	Forensics	Prevent	Critical	High	Static File Analysis	Gen.MLSA	581cf8c1-4f20-4abf-97e7-8895a0117b40.tmp
Mar 30, 2022 12:54:35 AM	Forensics	Prevent	Critical	High	File Reputation	Gen.Rep.dll	unconfirmed 344285.crdownload

フォレンジックレポート

YOU DESERVE THE BEST SECURITY

フォレンジックレポートの生成と表示

- インシデント発生時には、フォレンジックレポートが自動的に生成されます
- インシデント・ログの Forensics Report > Open the Forensics Report からアクセス可能です
- フォレンジックレポートは、次の質問に対する回答を提供します
 - どのようにしてシステムに入りましたか？
 - 感染はまだ存在していますか、それとも除去されましたか？
 - どんな被害が発生しましたか？

Card

Prevent Threat Emulation Mar 30, 2022 12:58:44 AM

DETAILS

Protection File System
Type: Emulation

Forensics Report

Open the Forensics Report

Download the Forensics Report

Forensics Details

Verdict: Malicious

Resource: C:\User\oads\1458c568

フォレンジックレポートを表示

フォレンジックレポートをZIP形式でダウンロード

SandBlast Forensics

OVERVIEW GENERAL ENTRY POINT REMEDIATION BUSINESS IMPACT SUSPICIOUS ACTIVITY INCIDENT DETAILS

CLEANED status Anti-Bot test malware family CRITICAL severity Endpoint Anti-Bot triggered by

http://www.threat-cloud.com/test/files/HighConfidenceBot.M... Anti-Bot test.TC.f protection name Bruce remote user

ATTACK STATS What sort of connections and processes were involved?

Remote Logon Internal 1 Malicious Processes 1 Script Processes

BUSINESS IMPACT What was the potential damage done?

2 Data Changes 1 Data Loss

ATTACK TYPES What were the attacks types seen or prevented?

bot infostealer trojan

ENTRY POINT How did it enter the system?

Bruce was remotely logged in via RDP. Incident was traced back to an execution or copy in explorer

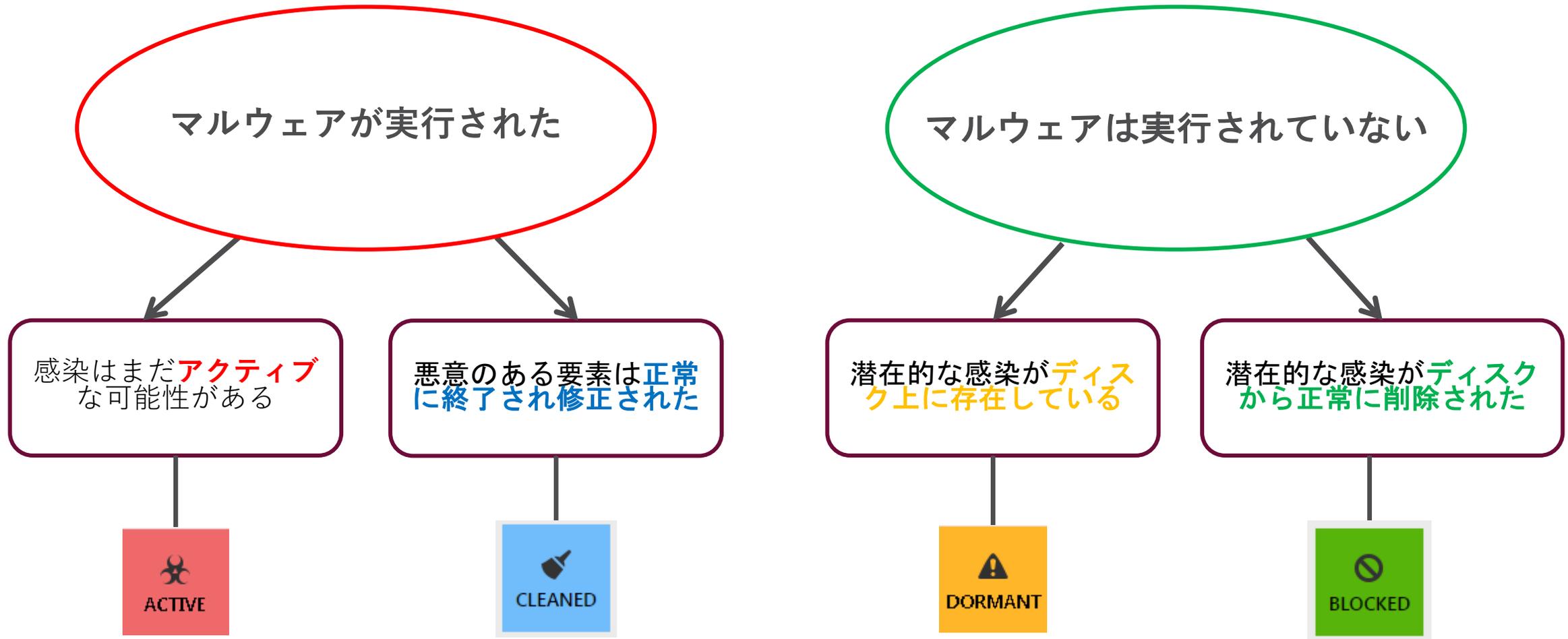
REMIEDIATION Were all incident created elements removed?

100% 17/17 terminated processes 100% 7/7 quarantined/deleted files

INCIDENT DETAILS (17 processes) How do I analyze further?

HELP? INCIDENT RESPONSE TEAM 24/7/365 CONSULTING

インシデントのステータス (1 / 2)



インシデントのステータス（2 / 2）

- 攻撃分析中に、修復プロセスを実行しています。インシデントの判断（または現在のコンピュータのステータス）は、このプロセスの結果によって異なります
- **Active:**
 - 悪意のあるプロセスが実行され、システムが感染しました
 - プロセスまたは攻撃の他の要素の終了と隔離は、ポリシーで無効になっているか、失敗しています
- **Cleaned:**
 - 悪意のあるプロセスが実行され、システムが感染しましたが、攻撃要素の終了と隔離が成功しました
 - システムがまだ損傷している可能性があります
- **Dormant:**
 - 悪意のあるプロセスは実行されませんでしたでしたが、システムは感染していました
 - 検出されたファイルの隔離に失敗しました
- **Blocked:**
 - 悪意のあるプロセスは実行されませんでした。
 - 検出されたすべてのファイルの隔離に成功しました
 - 攻撃は即座にブロックされ、システムは感染していなかったため、被害はありませんでした

フォレンジックレポート：Overview

- Overview で攻撃の全体像を把握することができます
- 各項目をドリルダウンするか、画面上部のメニューバーからアイコンを選択することで詳細な情報を表示することができます

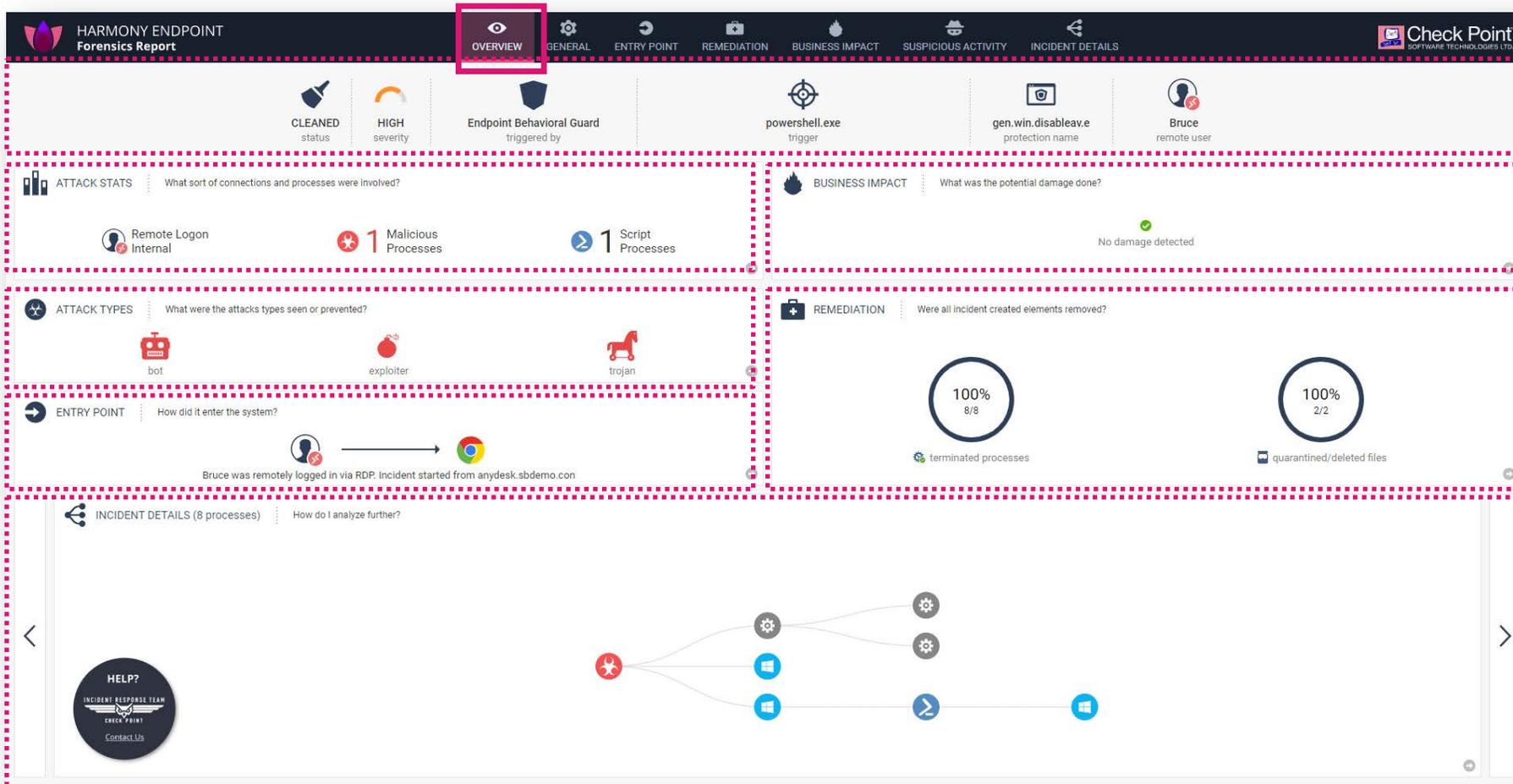
攻撃概要

攻撃統計

攻撃タイプ

侵入経路

プロセスツリー



被害状況

修復状況

フォレンジックレポート：General

- インシデントと検出に関する一般的な情報を表示します
- 一般的な情報には、時間、コンピュータ名、ドメイン、ユーザー名、OS、IDが含まれます
- 検出の詳細には、トリガーが含まれます：時間、プロセス、PID、トリガーを送信したAP

The screenshot displays the SandBlast Forensics interface for an incident. The top navigation bar includes tabs for OVERVIEW, GENERAL (selected), ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The main content is divided into three sections:

- ATTACK INFORMATION:** Shows Malware Family: Anti-Bot test. A row of icons includes bot, infostealer, and trojan.
- GENERAL DETAILS:** A table of incident information:

Incident ID:	b6a13402-7105-4a4b-8d85-b14dacc6f9b9	Analysis Time:	12/10/2021, 6:36:32 PM	Client Version:	84.50.7526
PC Name:	PROTECTED-USER	Machine Type:	Desktop	OS:	Windows 10
Machine Roles:	Microsoft Print to PDF, Microsoft XPS Document Writer, WCF Services, TCP Port Sharing, Media Features, Windows Media Player, SMB 1.0/CIFS Automatic Removal, Remote Differential Compression API Support, .NET Framework 4.8 Advanced Services, Windows Search, Windo...				
Domain:	SBdemo.com	IP Address:	10.128.0.12		
User Name:	SBDEMO\Bruce	User SID:	S-1-5-21-867849086-1392971733-3836376186-1106	Logon Time:	12/10/2021, 3:50:16 PM
Logon Type:	Remote Desktop Protocol (RDP)	Remote PC:	BOAZ-GAR-JUMP-S	Remote IP:	10.128.0.14 (Internal)
- DETECTION DETAILS:** A table of detection information:

Description:	Endpoint Anti-Bot prevented access to URL: http://www.threat-cloud.com/test/files/HighConfidenceBot.html	Protection Name:	Anti-Bot test.TC.f		
Trigger Matched:	http://www.threat-cloud.com/test/files/HighConfidenceBot.html	Trigger Time:	12/10/2021, 6:36:21 PM		
Trigger Actual:	http://www.threat-cloud.com/test/files/HighConfidenceBot.html	Trigger Type:	URL		
Trigger Process:	c:\users\bruce\documents\oem471b.exe	Trigger PID:	5700		
Trigger Args:					
Trigger App:	Endpoint Anti-Bot	Trigger Rep:	Malicious	Trigger MD5:	N/A
Mode:	Prevent	Confidence:	High	Severity:	Critical
- ATTACK STATS:** A summary of attack statistics:

remote (RDP) logons	malicious connections	suspicious connections	unclassified connections	malicious processes	suspicious processes	unclassified processes	unsigned processes	script processes	windows os processes	malicious files	suspicious files
1	0	0	0	1	0	1	3	1	5	1	0

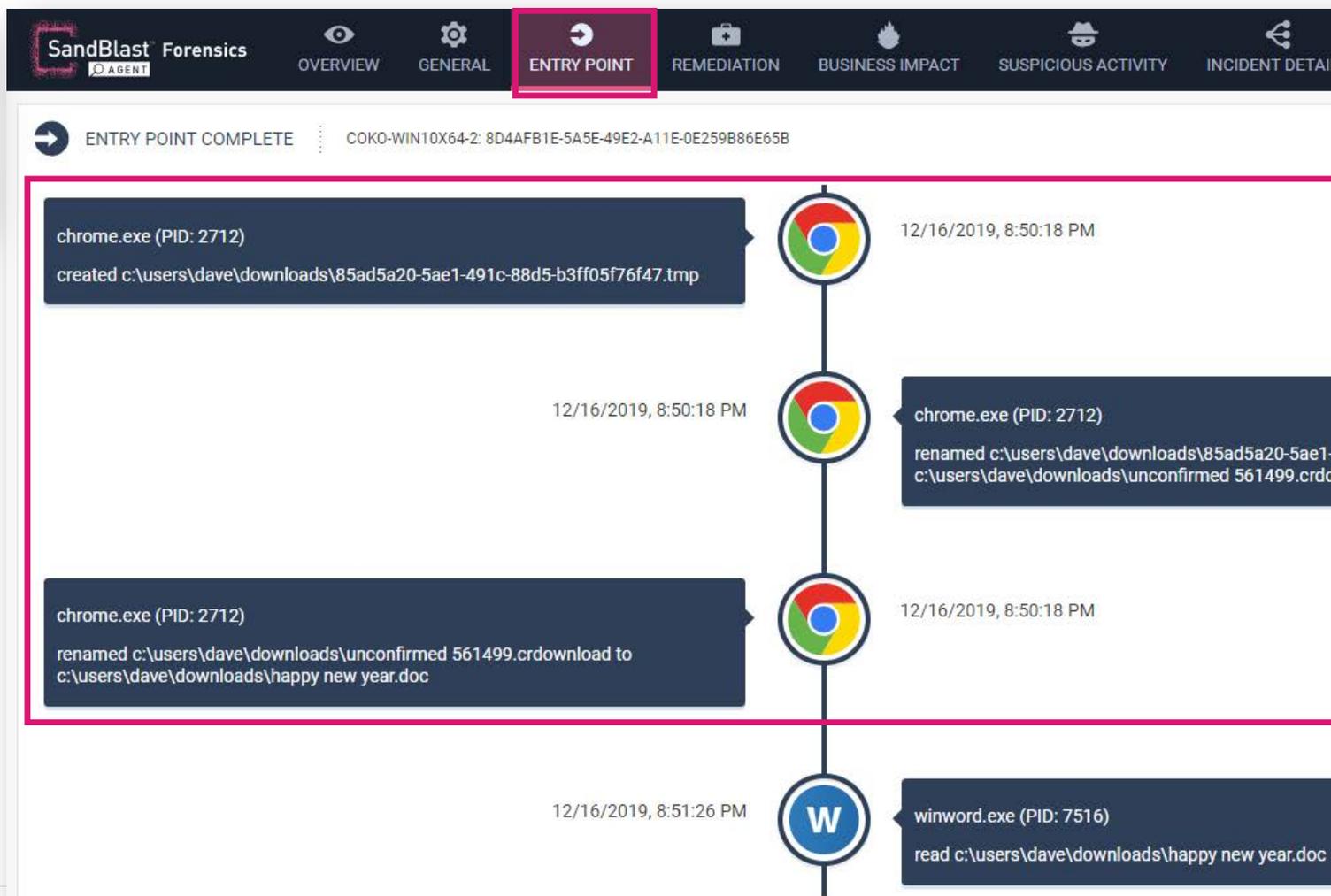
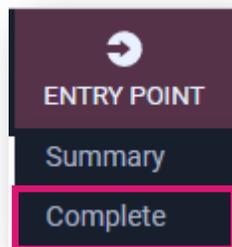
フォレンジックレポート：Entry Point - Summary

- Entry Point は、攻撃者がマルウェアを展開することに成功した弱点を示すことで、セキュリティに潜む脆弱なベクターを明らかにする可能性があります

The screenshot displays the SandBlast Forensics interface. On the left, a sidebar menu includes 'ENTRY POINT', 'Summary', and 'Complete'. The main content area shows the 'ENTRY POINT SUMMARY' for a specific incident. The summary is visualized as a flowchart with two nodes connected by a vertical line. The top node, representing 'chrome.exe (PID: 2712)', shows the action 'renamed [85ad5a20-5ae1-491c-88d5-b3ff05f76f47.tmp] to [happy new year.doc]' at 12/16/2019, 8:50:18 PM. The bottom node, representing 'winword.exe (PID: 7516)', shows the action 'read [happy new year.doc]' at 12/16/2019, 8:51:26 PM. The interface includes a top navigation bar with various tool icons and the Check Point logo.

フォレンジックレポート：Entry Point - Complete

- Entry Point は、攻撃者がマルウェアを展開することに成功した弱点を示すことで、セキュリティに潜む脆弱なベクターを明らかにする可能性があります



エントリポイントは、完全なビューで表示され、Summaryには表示されない複数のステージで構成されていることが分かります

フォレンジックレポート：Remediation

- Remediation は、ファイルの修復状況（削除、隔離）や、プロセスの停止状況を表示します

REMEDIATION POLICY PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

Remediation: Enabled: Incident remediation is enabled by policy for Endpoint Anti-Bot with confidence (High).

Malicious: Terminate and Quarantine

Suspicious: Terminate and Quarantine

Unknown: Terminate and Quarantine

Trusted: Terminate

REMEDIATION DETAILS PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

This section describes all the remediation actions that were taken.

▼ **Already Deleted Files: 3 deleted**

These are files that were already deleted before the analysis completed.

Reputation	File Name	File Path	MD5	Status
?	oem471b.exe	c:\users\bruce\documents\oem471b.exe	7c114e4c2b3c402499533f2b6a65027b	🗑️
?	oem5496.bat	c:\users\bruce\appdata\local\temp\oem5496.bat		🗑️
?	__psscscriptpolicytest_j35iavai.5pf.ps1	c:\users\bruce\appdata\local\temp__psscscriptpolicytest_j35iavai.5pf.ps1		🗑️

▼ **Quarantined Files: 4 quarantined**

These are files that have been quarantined by SBA.

Reputation	File Name	File Path	MD5	Status
⚠️	bot.exe	c:\users\bruce\documents\received files\bot.exe	36bb9bdded3a80e75890838385cae58e	🔒
?	oem4719.exe	c:\users\bruce\appdata\local\temp\oem4719.exe	da0b3bab43e17b842b5d52a509c0add2	🔒
?	oem471a.exe	c:\programdata\oem471a.exe	da0b3bab43e17b842b5d52a509c0add2	🔒
?	oem471c.exe	c:\users\bruce\appdata\roaming\microsoft\windows\start menu\programs\startup\oem471c.exe	7c114e4c2b3c402499533f2b6a65027b	🔒

▶ **Already Terminated Processes: 16 terminated**

▼ **Terminated Processes: 1 terminated**

フォレンジックレポート：Business Impact

- Business Impactは、コンピュータおよびコンピュータに直接接続されている他のデバイス（外部ストレージデバイス、ネットワーク共有など）のデータを侵害するためにマルウェアによって行われた損害またはアクションを表示します
- ビジネスへの影響のセクションは、修正と復元が行われた後に更新されます

The screenshot displays the SandBlast Forensics interface. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT (selected), SUSPICIOUS ACTIVITY, and INCIDENT DETAILS. The main content area shows a report for a specific user (PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9) under the BUSINESS IMPACT section. It lists two categories of events: Data Tampering (2 events) and Data Loss (1 event). The Data Tampering section shows a table of user files that were modified or deleted, including file names, paths, actions (Write/Delete), and event times. The Data Loss section shows a table of user files that were likely accessed, including file names, paths, actions (Read), and event times.

BUSINESS IMPACT (2 categories, 3 events) PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

These are potentially important events that have business impact.

▼ **Data Tampering (2 events)**

User files that were modified or deleted in the incident.

File Name	File Path	Action	Event Time
avt_local.png	c:\users\bruce\AppData\Local\lan messenger\lan messenger\avt_local.png	Write	12/10/2021, 3:50:52 PM
avt_42010a800016admin.png	c:\users\bruce\AppData\Local\lan messenger\lan messenger\cache\avt_42010a800016admin.png	Delete	12/10/2021, 3:51:03 PM

Showing 1 to 2 of 2 entries

▼ **Data Loss (1 event)**

User files that were likely accessed in the incident.

File Name	File Path	Action	Event Time
companysecret.doc	c:\users\bruce\documents\companysecret.doc	Read	12/10/2021, 6:36:19 PM

Showing 1 to 1 of 1 entries

フォレンジックレポート：Suspicious Activity（1 / 3）

- MITRE ATT & CK™ Matrix ビューは、攻撃と疑わしいアクティビティを MITRE ATT & CK™ Framework の戦術と手法にマッピングして表示します

MITRE ATT&CK™ Matrix: PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon Internal 1 event	Command-Line Interface 2 events	Registry Run Keys / Startup Folder 4 events	Bypass User Account Control 1 event	Bypass User Account Control 1 event		Application Window Discovery 5 events	Third-party Software 1 event	Data from Local System 1 event	Commonly Used Port 6 events		Data Encrypted for Impact 2 events
Valid Accounts 1 event	Execution through API 13 events	Scheduled Task 3 events	Scheduled Task 3 events	File Deletion 2 events		Process Discovery 4 events			Listening Port 1 event		
	Execution through Module Load 5 events	Valid Accounts 1 event	Valid Accounts 1 event	Modify Registry 12 events		Remote System Discovery 1 event			Uncommonly Used Port 279 events		
	Local WMI Execution 1 event		Vertical Privilege Escalation 15 events	Scripting 3 events							
	PowerShell			Valid Accounts							

フォレンジックレポート：Suspicious Activity（2 / 3）

- Suspicious Events ビューは、悪意のあるアクティビティを示すさまざまなカテゴリで構成され、重大度レベルごとに整理して表示します

The screenshot shows the SandBlast Forensics interface. The top navigation bar includes tabs for OVERVIEW, GENERAL, ENTRY POINT, REMEDIATION, BUSINESS IMPACT, SUSPICIOUS ACTIVITY (selected), and INCIDENT DETAILS. The main content area displays 'SUSPICIOUS ACTIVITY (30 categories, 386 events)' for a specific user. It lists several event categories with their respective counts and severity levels (indicated by colored dots):

- Vertical Privilege Escalation (15 events)
- System Security Policy Change (1 event)
- Data Encrypted for Impact (2 events)
- Listening Port (1 event)
- Remote System Discovery (1 event)
- Command-Line Interface (2 events)

Two detailed event entries are shown in a table format:

Description	Time
bot.exe (PID: 5608) modified HKU\s-1-5-21-867849086-1392971733-3836376186-1106\hku\software\microsoft\windows\currentversion\policies\ A process changed a policy setting that affects the system security.	12/10/2021, 6:36:16 PM
lmc.exe (PID: 788) modified avt_local.png in c:\users\bruce\appdata\local\lan messenger\lan messenger lmc.exe (PID: 788) modified avt_42010a800016admin.png in c:\users\bruce\appdata\local\lan messenger\lan messenger\cache	12/10/2021, 3:50:52 PM 12/10/2021, 3:51:03 PM

フォレンジックレポート：Suspicious Activity（3 / 3）

- Network Events ビューは、攻撃で発生したネットワークイベント（外部、内部へのネットワーク接続）を表示します

Network Connections Map | PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacc6f9b9

World map showing activity from the United States and Unknown regions.

Country	Benign	Unknown	Suspicious	Malicious
United States	1	1	0	1
Unknown	4	1	0	0

Previous 1 Next

Network Activity | PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacc6f9b9

URLs (2) Domains (2) IPs (6)

Show 100 Reputation: All Search:

Rep	Malware Family	Risk	URL	IP	Type	Country
1			http://dropbox-docs.com/download/stage2.exe	10.128.0.22	Internal	Unknown
100	Anti-Bot test		http://www.threat-cloud.com/test/files/HighConfidenceBot.html	209.87.209.71	External	United States

Previous 1 Next

フォレンジックレポート： Incident Details（1 / 3）

- Tree ビューは、攻撃に使用されたプロセスのプロセスツリーと各プロセスの詳細を表示します

The screenshot displays the SandBlast Forensics interface in 'TREE VIEW' mode. The top navigation bar includes 'OVERVIEW', 'GENERAL', 'ENTRY POINT', 'REMIEDIATION', 'BUSINESS IMPACT', 'SUSPICIOUS ACTIVITY', and 'INCIDENT DETAILS'. The main area shows a process tree for a 'PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacc6f9b9'. The tree includes processes like 'lmc.exe 788', 'bot.exe 64', 'bot.exe 5608', and several 'schtasks.exe' and 'conhost.exe' processes. A blue callout box points to the tree with the text 'プロセスツリーを表示'. Another blue callout box points to a selected 'bot.exe 5608' process with the text '各プロセスをクリックして、プロセスの表示を下段に表示'. A third blue callout box points to the details pane at the bottom with the text 'プロセスの詳細を表示'. The details pane for 'bot.exe' shows the following information:

Category	Value
Process Name	bot.exe
Path	c:\users\bruce\documents\received files\bot.exe
Start Time	12/10/2021, 6:36:15 PM
Close Time	12/10/2021, 6:36:17 PM
Created By	c:\program files (x86)\lan messenger\lmc.exe
Parent Chain	smss.exe (PID : 304 Date : 10-Dec-2021 03:15:47) -->smss.exe (PID : 8396 Date : 10-Dec-2021 06:50:11) -->winlogon.exe (PID : 7748 Date : 10-Dec-2021 06:50:12) -->userinit.exe (PID : 1724 Date : 10-Dec-2021 06:50:26) -->explorer.exe (PID : 12144 Date : 10-Dec-2021 06:50:26)
Arguments	
PID	5608
Duration	1s 452ms
Created By PID	788

フォレンジックレポート： Incident Details（2 / 3）

- Tree Timelineビューは、攻撃に使用されたプロセスのプロセスツリーをタイムラインで表示します

The screenshot displays the SandBlast Forensics interface in the 'INCIDENT DETAILS' section. The main area shows a 'TREE TIMELINE VIEW (17 processes)' for a 'PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacd6f9b9'. The timeline spans from 12/10/2021, 3:50:47 PM to 12/10/2021, 6:36:16 PM. A process tree is visible with nodes for 'lmc.exe 788', 'bot.exe 64', 'bot.exe 5608', 'schtasks.exe 3772', and 'conhost.exe 6716'. Each node includes a brief description of its activity, such as 'Attack Start, Listening Port Dropped Executable, Uncommonly Used Port Modify Registry...' for lmc.exe and 'Persistence, Registry Run Keys / Startup Folder Vertical Privilege Escalation, Dropped Executable System Security Policy Change...' for bot.exe 5608. A blue callout box points to the tree with the text '各プロセスをクリックして、プロセスの表示を下段に表示'. Below the timeline, a detailed view for 'lmc.exe' is shown, including its path, start time, and parent chain.

プロセスツリーをタイムライン表示

各プロセスをクリックして、プロセスの表示を下段に表示

プロセスの詳細を表示

Process Name	Path	Start Time	Close Time	PID	Duration	Created By	Created By PID
lmc.exe	c:\program files (x86)\lan messenger\lmc.exe	12/10/2021, 3:50:47 PM		788			0

Parent Chain: smss.exe (PID : 304 Date : 10-Dec-2021 03:15:47) -->smss.exe (PID : 8396 Date : 10-Dec-2021 06:50:11) -->winlogon.exe (PID : 7748 Date : 10-Dec-2021 06:50:12) -->userinit.exe (PID : 1724 Date : 10-Dec-2021 06:50:26) -->explorer.exe (PID : 12144 Date : 10-Dec-2021 06:50:26)

フォレンジックレポート： Incident Details (3 / 3)

- Script & Shortcut Content ビューは、AMSIや、WmiGet、ショートカット、インシデントの一部であったコンテンツなどを表示するために使用されます

SandBlast Forensics AGENT

OVERVIEW GENERAL ENTRY POINT REMEDIATION BUSINESS IMPACT SUSPICIOUS ACTIVITY INCIDENT DETAILS

Check Point SOFTWARE TECHNOLOGIES LTD.

SCRIPT & SHORTCUT CONTENT PROTECTED-USER: b6a13402-7105-4a4b-8d85-b14dacad6f9b9

This view is used to display AMSI, WmiGet, Shortcut and other content that was part of the incident. Click on the row of interest to view its contents.

File/Process Name	Args	Type
powershell.exe (11312)	-c \$proc=([WMICLASS]ROOT\CIMV2:win32_process).Create('C:\Users\bruce\Documents\oem471B.exe')	AMSI

AMSI content for: powershell.exe (11312)

```
$proc=([WMICLASS]ROOT\CIMV2:win32_process).Create('C:\Users\bruce\Documents\oem471B.exe')  
  
win32_process.GetObject();  
win32_process.GetObject();  
Win32_Process.GetObject();  
Win32_Process.GetObject();  
SetPropValue.CommandLine("C:\Users\bruce\Documents\oem471B.exe");
```

選択

詳細を表示

フォレンジックレポート：凡例

Graph Legends

-  Process is known to be malicious
-  Reputation is not known for process
-  Process is trusted operating system process
-  Process has damage events
-  Process has different privilege level than start
-  Process is currently selected

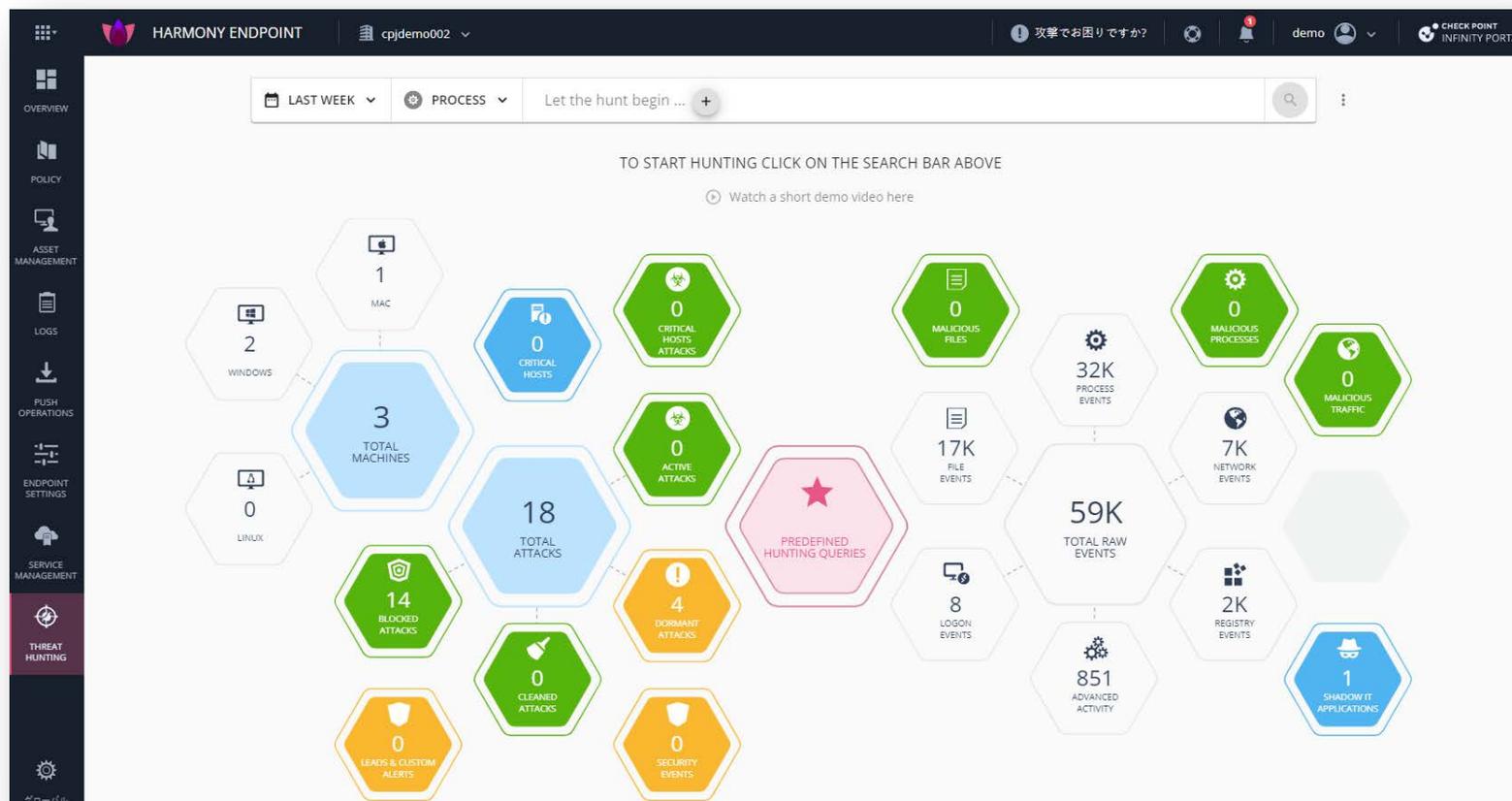
-  Parent Process X executing Parent Process Y
-  Selected Process Y 's backing file was created by X
-  Selected Process X created the file backing Y
-  Process X injected into Process Y
-  Link between 2 different Sub-Trees. Select process Y to see the real relationship.

THREAT HUNTING

YOU DESERVE THE BEST SECURITY

Threat Hunting の概要 (1 / 2)

- Threat Hunting は、エンドポイントからすべてのイベントを収集し、調査するツールです
- イベントには、良性のデータと悪意のある可能性のあるデータの両方が含まれます
- Threat Hunting により、すべてのイベントを完全に可視化して、攻撃の全範囲を理解し、ステルス攻撃を明らかにすることができます
 - ※ データ保持期間は、デフォルトで7日間です (オプション購入で最長1年まで延長できます)



Threat Hunting の概要 (2 / 2)

- Threat Hunting には、次の利点があります
 - アラートだけでなく、すべてのエンドポイントのすべてのイベントに対する完全な可視性
 - 攻撃の全範囲の調査
 - 疑わしいアクティビティを明らかにする
 - 複数の修復アクションによる、疑わしいアクティビティの修復
 - 調査、ハンティング、修復を簡単にする
- 発見されたイベントに対して以下の修復を行えます
 - プロセスを強制終了
 - ファイルを隔離
 - コンピュータを隔離
 - フォレンジックを利用して攻撃を分析
 - フォレンジック分析によって検出されたプロセスを強制終了
 - フォレンジック分析によって検出されたファイルを隔離

ハンティング画面の概要 (1 / 2)

- 事前定義された条件や、カスタム条件により組織に潜む脅威を探索します

簡単操作によるカスタムクエリ

事前定義されたクエリ

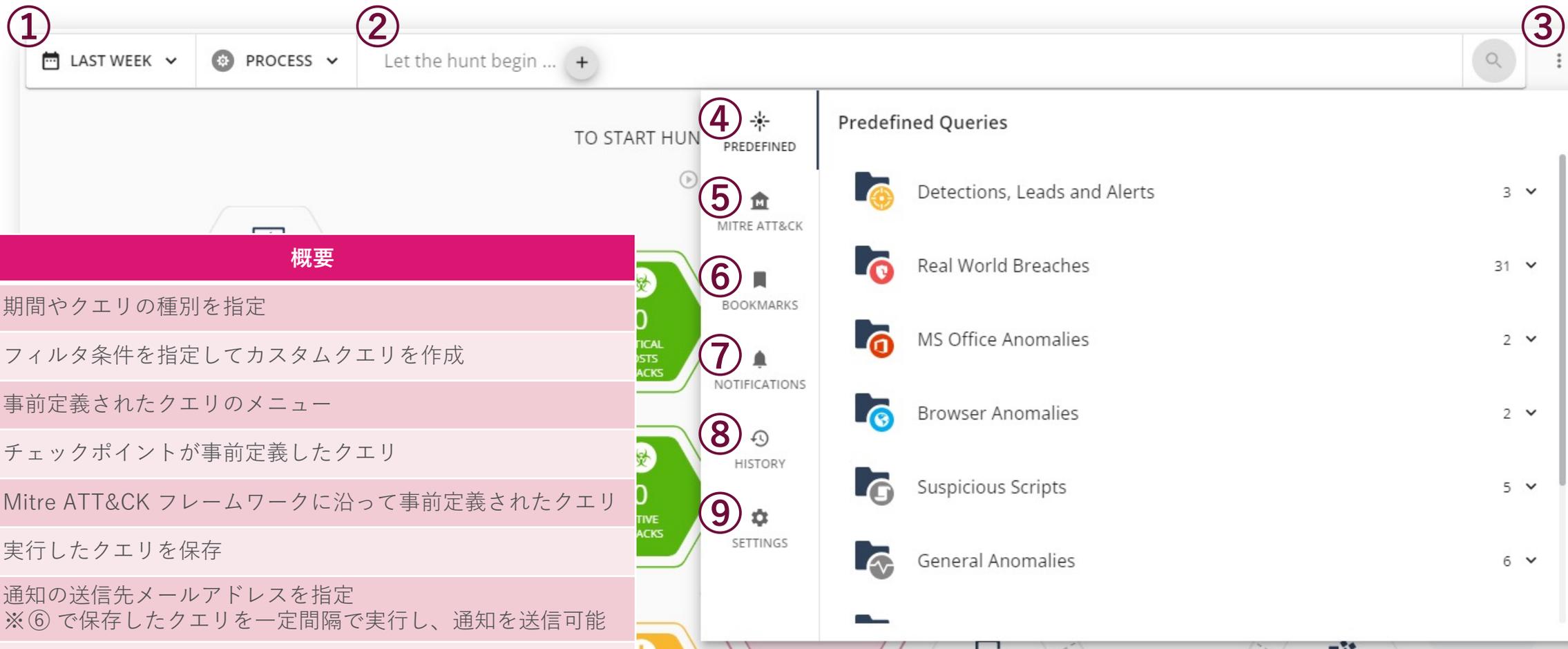
組織への攻撃の概要を表示

ドリルダウンで一覧表示

各レコードの詳細表示

Overview of the hunting interface showing a dashboard with various metrics and a search bar. The dashboard includes metrics for Windows, MAC, Critical Hosts, Malicious Files, Malicious Processes, Malicious Traffic, Total Machines, Process Events, File Events, Network Events, Active Attacks, Blocked Attacks, Dormant Attacks, Cleaned Attacks, Leads & Custom Alerts, and Security Events. A sidebar on the right lists predefined queries. A detailed view of a detection event is shown at the bottom, including fields for Trigger, Asset, and Additional Information.

ハンティング画面の概要 (2 / 2)



項番	概要
①	期間やクエリの種別を指定
②	フィルタ条件を指定してカスタムクエリを作成
③	事前定義されたクエリのメニュー
④	チェックポイントが事前定義したクエリ
⑤	Mitre ATT&CK フレームワークに沿って事前定義されたクエリ
⑥	実行したクエリを保存
⑦	通知の送信先メールアドレスを指定 ※⑥ で保存したクエリを一定間隔で実行し、通知を送信可能
⑧	使用したすべてのクエリを確認
⑨	UI の見た目を設定

Threat Hunting : 期間の指定

- Threat Hunting する期間を、Last Day、Last 2 Days、Last Week、Custom から指定可能です
※ 但し、データの保存期間は、標準では7日間です

The screenshot shows the Threat Hunting interface. At the top, there is a dropdown menu for 'LAST DAY' which is currently expanded to show options: 'Last Day', 'Last 2 Days', 'Last Week', and 'Custom'. Below this, there is a 'Select specific dates' dialog box with two calendar views for April 2022. The first calendar shows the date '4' selected, and the second calendar shows the date '4' selected. The time range is set from 12:00 AM to 11:59 AM. The dialog box has 'CANCEL' and 'FILTER' buttons. A blue callout box points to the 'Custom' option and the date selection dialog, containing the text: 「Custom」を選択し、任意の期間を設定することも可能 ※ 但し、データの保存期間は、標準では7日間。 The background of the interface shows various security metrics: '1 WINDOWS', '0 MALICIOUS FILES', '52K', '0 MALICIOUS PROCESSES', and '0'.

Threat Hunting : クエリ種別、フィルタ条件の指定

- クエリ種別には、プロセスや検知イベント、ファイル、ネットワーク接続などを指定します
- フィルタ条件には、プロセスやファイルの名称・ハッシュ値、ドメイン名、IPアドレスなどを指定します

The screenshot displays a Threat Hunting interface with three callouts:

- クエリ種別を指定** (Specify query type): Points to a dropdown menu on the left with the following options: Process, Detection Event, File, Network, Registry, Logon, Script, Remote Execution, Advanced Activity, Indirect Execution, and Email.
- フィルタ条件を追加** (Add filter condition): Points to a '+' button in the top navigation bar.
- フィルタ条件を指定** (Specify filter condition): Points to the 'Add Filter' dialog box, which contains:
 - Indicator: Process Name
 - Operator: Is
 - Value field: Add a single value... (with a dropdown arrow)
 - Label: Process name
 - Buttons: CANCEL and ADD

The background dashboard shows various metrics: 2 WINDOWS, 0 CRITICAL HOSTS, 0 ACTIVE ATTACKS, 25K FILE EVENTS, 14K NETWORK EVENTS, and 277K. A search bar and a 'Let the hunt begin...' button are also visible at the top.

(参考) フィルタ条件のキー

Activity Details
Activity Name
Activity Target PID
Activity Target Directory
Activity Target Name
Activity Type
Browser Name
Browser Version
Process Start Time
Detection Attack Status

Detection Trigger Process
Detection Attack User Domain
Detection Attack User Name
Detection Creating Process Start Time
Detection Creating Process PID
Detection Description
Detection Email Attachment

Detection Email Delivery Date
Detection Email Embedded URL
Detection Email Sender
Detection Email ID
Detection Email Subject
Detection Email Recipient
Detection Enforcement
Detection Entry Point Process

Detection Entry Point File MD5
Detection Entry Point File Name
Detection Entry Point Network
Detection Entry Point Browser Tab
Detection General Info
Detection Impersonated Brand
Detection Impersonated Domain

Detection Impersonated Type
Detection Confidence
Detection Report ID
Detection Severity
Detection Trigger Path
Detection Malware Family
Detection Protection Name
Detection Protection Type
Detection Remediation Policy

Detection Remediation Policy
Detection Third Party
Detection Trigger MD5
Detection Triggered By
Domain Classification
Email Attachments Count
Email BCC
Email CC
Email From
Email Message Id

Email Message Id
Number Of Recipients
Email Server Name
Source country
Email Status
Email Subject
Email To
Email Direction
Email URLs Count
Logon Event

Execution Details
Execution Name
Execution Target PID
Execution Target Directory
Execution Target Name
Execution Type
File Classification
File Directory
File MD5
File Name

New File Directory
New File Name
File Operations
File Path
File Signer
File Size
File Type
Gateway Blade
Host IPs
Host MACs

Host Type
Logon Account Type
Logon ID
Logon Origin
Machine Name
Network Bytes Received
Network Bytes Sent
Network Connection Direction
Network Dest IP
Network Dest Port

Network Email Display URL
Network Domain
Network HTTP Method
Network Is Listening
Network Path
Network Protocol
Network Referer
Network Status Code
Network Src IP
Network Src Port

Network Src Port
Network Sensor
Network URL
Network User Agent
OS Name
OS Version
Original File Classification
Parent Process Args
Parent Process Directory
Parent Process Integrity Level

Process Signer Is Invalid
Logon Session
Process MD5
Process Name
Process Original Name
Parent PID
Process Path
Process Signer
Process Trusted Signer
Product Version

Registry Key
Registry New Data
Registry Old Data
Registry Operations
Registry Value
Remote Ip Address
Remote Machine Name
Logon Event ID
Remote Execution Type
Logon Type

Connection Count
Logon User Domain
Logon User Name
Reputation Risk
Script Data
User Name

Threat Hunting：事前定義されたクエリ

- 事前定義されたクエリを使用することで簡単に脅威をハンティングすることができます

Query Category	Count	Action
Detections, Leads and Alerts	3	^
Active attacks Attacks detected by the endpoint client that are still active on the device		▶ ▼
Attacks detected All attacks detected by the endpoint client		▼
Alerts detected All user defined alerts detected by our notification service		▼
Real World Breaches	31	▼
MS Office Anomalies	2	▼

Query Category	Count	Action
Browser Anomalies	2	▼
Suspicious Scripts	5	▼
General Anomalies	6	▼
Persistence	5	▼
Shadow IT	2	▼
Reputation	3	▼

Threat Hunting : MITER ATT & CKダッシュボード

- MITER ATT & CKダッシュボードは12のカテゴリに分けられ、各カテゴリは攻撃のステージです
- 各カテゴリには、複数の攻撃手法が含まれています。テクニックをクリックすると、テクニックの説明と事前定義されたクエリのリストが表示されたウィンドウが開きます。クエリを実行して、特定の手法の実装が使用されたイベントのリストを取得します
- 悪意のある、疑わしい、または良性であるかどうかに関係なく、すべての生のイベントをMITRE TTPにマップします

The screenshot shows the MITRE ATT&CK (Beta) dashboard. At the top, there is a navigation bar with a back arrow, the text 'MITRE ATT&CK (Beta)', a refresh icon, 'Last Loaded 6:48:47 PM', and a calendar icon with 'LAST WEEK' and a dropdown arrow. Below the navigation bar is a grid of 12 categories, each with a colored vertical bar on its left side. The categories and their associated techniques are as follows:

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Valid Accounts T1078	Software Deployment Tools T1017	Accessibility Features T1015	DLL Search Order Hijacking T1038	File System Logical Offsets T1006	Credential Dumping T1003	System Service Discovery T1007	Application Deployment Software T1017	Data from Local System T1005	Commonly Used Port T1043	Data Compressed T1002	Data Destruction T1485
Replication Through Removable Media T1091	Windows Remote Management T1028	Shortcut Modification T1023	Process Injection T1055	Obfuscated Files or Information T1027	Input Capture T1056	Query Registry T1012	Windows Remote Management T1028	Input Capture T1056	Application Layer Protocol T1071	Data Encrypted T1022	Service Stop T1489
External Remote Services T1133	Service Execution T1035	Modify Existing Service T1031	Bypass User Access Control T1088	DLL Search Order Hijacking T1038	Brute Force T1110	System Network Configuration Discovery T1016	Remote Desktop Protocol T1076	Email Collection T1114	Multilayer Encryption T1079	Exfiltration Over Command and Control Channel T1041	Inhibit System Recovery T1490
Drive-by Compromise T1189	Windows Management Instrumentation T1047	Path Interception T1034	Access Token Manipulation T1134	Process Injection T1055	Private Keys T1145	Remote System Discovery T1018	Windows Admin Shares T1077	Screen Capture T1113	Remote File Copy T1105		Resource Hijacking T1496
Spearphishing Attachment T1193	Scheduled Task/Job T1053	Logon Scripts T1037	Sudo T1169	Indicator Removal on Host T1070	Credentials in Registry T1214	System Owner/User Discovery T1033	Remote File Copy T1105		Multi-hop Proxy T1188		

Threat Hunting : 修復

- 発見されたイベントに対して、プロセスの停止やファイルの隔離などの修復を行えます

The screenshot displays the Check Point Harmony Endpoint console. The main area shows a detection event for Trojan-Ransom.Win32.Locky.d. The event details are as follows:

DETECTION EVENT INFORMATION		ASSET		ADDITIONAL INFORMATION		TIME	
Trigger	locky.b64	User	nack	Name	b2.exe	Date	09/09/2022
Triggered By	Endpoint Anti-Malware	Machine	EP-DEMO2	Args			

DETECTION DETAILS		ASSET DETAILS		PROCESS DETAILS	
Trigger Path	c:\users\nack\documents\becky2\631...	User	nack	Name	b2.exe
Triggered By	Endpoint Anti-Malware	Machine	EP-DEMO2	Directory	c:\program files (x86)\rimarts\b2
Attack Status	Active	OS Name	Windows	Full Path	c:\program files (x86)\rimarts\b2\b2.exe
Trigger Process	c:\program files (x86)\rimarts\b2\b2.e...	Host Type	VirtualMachine	Start Time	2022-09-09T17:02:20.429
Attack User Domain	EP-DEMO2	OS Version	Microsoft Windows 10 Enterprise Evaluation (10...	Args	
Attack User Name	nack	Product Version	86.26.6008	PID	8432
Protection Name	Trojan-Ransom.Win32.Locky.d	Domain Name	DomainNameNotFound	MD5	3a3848ca63b94ad04cfd4a4a4ce33172c
Trigger MD5	7a8290fdfad2a7b06fc03491932ae8e9	Host IPs	fe80::84fd:e643:4ee0:96d%13, 10.0.2.14	Classification	Benign
Severity	Critical	Host MACs	080027CEF971	Reclassification	Benign
Confidence	High			Detections	VirusTotal 0 out of 69
Enforcement	Prevent			Signed By	RimArts Inc.
Attack Root	b2.exe			Parent Name	explorer.exe
Entry Point	explorer.exe			Parent MD5	7a413ddd10e81adb6bb5d5e38f399d08

A context menu is open over the event, listing the following actions:

- Terminate Process
- Quarantine File
- Trigger Forensic Analysis
- Isolate Machine
- View Forensics Report
- Download Forensics Report

アラート通知設定

YOU DESERVE THE BEST SECURITY

アラート通知設定（1 / 4）

Threat Hunting

- 事前設定した条件で Threat Hunting を定期実行し、新規にイベントを発見した際に、管理者に通知できます
- Threat Hunting 画面で、通知したいイベントと通知先メールアドレスを設定します

アラート通知フロー



アラート通知設定（2 / 4）：アラート通知宛先設定

Threat Hunting

- Threat Hunting の Notifications に、アラートの通知先メールアドレスを設定します
- テナントの管理者からアラートの通知先を選択します

① メニューを開きます

② NOTIFICATIONS を選択します

③ テナントに登録されているユーザから、通知の送信先を選択します。

アラート通知設定（3 / 4）：アラート通知イベント設定

Threat Hunting

- 管理者に通知するイベントの条件を設定します
- 検索窓の ☆ マークをクリックし、検索条件を Bookmark に登録します
- Bookmark に登録された検索条件で定期的に Threat Hunting が行われます
- 検知した攻撃の状態（Detection Attack Status）や、検出したBlade（Detection Triggered by）、Severity（Detection Severity）などを検索条件に設定できます

① Threat Hunting の条件を Bookmark に登録します

② 名前、重要度、タグを設定します

③ チェックボックスにチェックを入れます

+ Create Shared Bookmark

Shared - available to all system users
 Private - available only to you

Name Importance

Select or create tag name

Send E-mail notifications to mailing list for any new hits

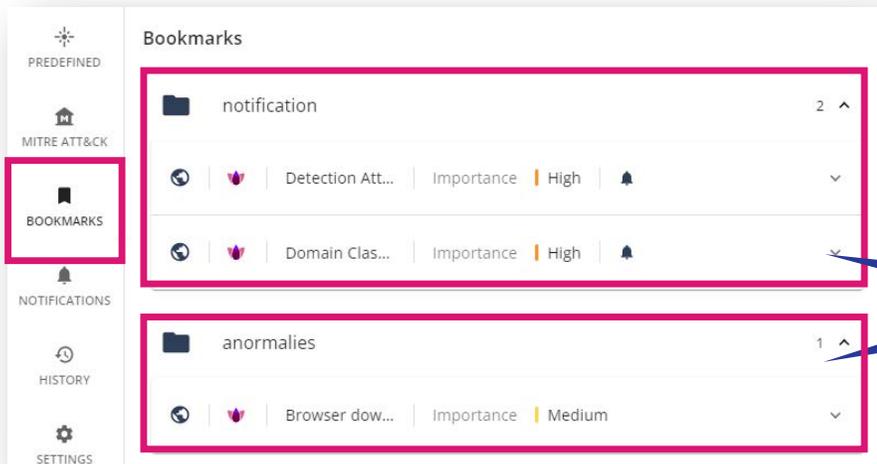
CANCEL SAVE

Low
Medium
High
Critical

アラート通知設定（3 / 4）：アラート通知イベント設定

Threat Hunting

- Bookmark への登録時に「Tag」を設定すると、Bookmark がタグごとにまとめて表示されます



Bookmark は、タグごとにまとめて表示されます

アンインストールパスワードの設定

YOU DESERVE THE BEST SECURITY

アンインストールパスワードの設定

Policy > Client Settings > Install & Upgrade > Uninstall Settings

- コンピュータの管理者がHarmony Endpointをアンインストールできない様に、アンインストールパスワードを設定します
- Push Operations でアンインストールをする場合は、アンインストールパスワードは不要です

The screenshot displays the Check Point Harmony Endpoint management console. The left sidebar shows the navigation menu with 'POLICY' and 'Client Settings' highlighted. The main content area shows the 'CLIENT UNINSTALL PASSWORD SETTINGS' dialog box, which is open and contains the following fields and options:

- Password:** A text input field with a masked password (dots) and a clear icon.
- Confirm Password:** A text input field with a masked password (dots) and a clear icon.
- Change the password for all rules where the default password was not changed**
- CANCEL** and **OK** buttons at the bottom.

The background shows the 'INSTALLATION & UPGRADE' settings page, which includes the following sections:

- Default settings for the entire organization:** Last Modified Feb 8, 12:38 PM (yoshiyasun_EpMaa5_Only, Version: 3)
- USER INTERFACE** tab is selected.
- Default Installations and Upgrades:**
 - Enable the user to postpone the client installation or upgrade**
 - Default reminder interval:** 30 min(s)
 - Force installation and automatically restart after:** 48 hour(s)
 - Maximum delay in download of packages:** 4 hour(s)
- Uninstall settings:** A section containing the **Agent Uninstall Password** field.

クライアントのアンインストール

YOU DESERVE THE BEST SECURITY

PUSH OPERATIONS

YOU DESERVE THE BEST SECURITY

Asset Management 画面からのアンインストール

Asset Management > Computers > Computer Actions > Agent Settings > Uninstall Client

- リモートからクライアントソフトウェアをアンインストールできます。

The screenshot illustrates the process of uninstalling a client from the Asset Management interface. The interface is divided into several sections:

- ASSET MANAGEMENT:** The sidebar on the left has 'ASSET MANAGEMENT' selected.
- Computers:** The main table lists computers. The 'CP-DEMO' computer is selected, and its 'Computer Actions' menu is open.
- Computer Actions:** The 'Agent Settings' option is selected, and the 'Uninstall Client' option is highlighted.
- PUSH OPERATION CREATION DIALOG:** The dialog is titled 'Uninstall Client' and contains the following options:
 - Comment:** A text input field with the placeholder 'Comment'.
 - User Notification:** Inform user with notification, Allow user to postpone operation.
 - Scheduling:** Execute operation immediately, Schedule operation for: [calendar icon].

Five numbered callouts indicate the steps:

- ① アンインストールする端末を選択 (Select the terminal to be uninstalled)
- ② Computer Actions をクリック (Click Computer Actions)
- ③ Agent Settings をクリック (Click Agent Settings)
- ④ Uninstall Client をクリック (Click Uninstall Client)
- ⑤ Create をクリック (Click Create)

Push Operations 画面からのアンインストール

Push Operations

- リモートから端末のクライアントソフトウェアをアンインストールできます。

The screenshot displays the 'ADD PUSH OPERATION' workflow in the Check Point Harmony Endpoint console. The interface includes a sidebar with navigation options like Overview, Policy, Asset Management, Logs, and Push Operations. The main area shows a table of operations and a detailed view of the 'Uninstall Client' operation. The workflow is annotated with seven numbered steps:

- ① + をクリック (Click +)
- ② Agent Settings を選択 (Select Agent Settings)
- ③ Uninstall Client を選択 (Select Uninstall Client)
- ④ + をクリック (Click +)
- ⑤ 端末を指定 (Specify endpoint)
- ⑥ ユーザに通知するか指定 (Specify if notify user)
- ⑦ アンインストール実行 (Execute uninstall)

遠隔操作の状況確認

Push Operations

- Push Operations で遠隔操作の状況を確認

The screenshot displays the Harmony Endpoint management interface. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, PUSH OPERATIONS (highlighted with a red box), ENDPOINT SETTINGS, and SERVICE MANAGEMENT. The main content area is divided into two sections. The top section, titled '遠隔操作の状況' (Remote Operation Status), shows a table of push operations. The bottom section, titled '端末ごとの状況、結果' (Status and Results by Device), shows a table of endpoint details for a specific operation.

遠隔操作の状況

Operation	Comment	Pushed To	Status	Admin Name	Advanced Settings	Created On	Active Until
Uninstall Client		CP-DEMO	Pushing to clients	[Redacted]	View Advanced Settings...	10 Jun 2022 07:18 pm	11 Jun 2022 07:18 pm
Release Computer Isolation		CP-DEMO	Completed	[Redacted]	View Advanced Settings...	10 Jun 2022 07:09 pm	11 Jun 2022 07:09 pm
Isolate Computer		CP-DEMO	Completed	[Redacted]	View Advanced Settings...	10 Jun 2022 06:53 pm	11 Jun 2022 06:53 pm
Uninstall Client		Lab-13	Pushing to clients	[Redacted]	View Advanced Settings...	10 Jun 2022 04:45 pm	11 Jun 2022 04:45 pm
Release Computer Isolation		CP-DEMO	Completed	[Redacted]	View Advanced Settings...	10 Jun 2022 01:36 pm	11 Jun 2022 01:36 pm

Page 1 of 3

端末ごとの状況、結果

User Name	Computer Name	Operation Status	Operation Status Descriptio	Operation Output	Sent To Endpoint On	Status Update Received O
nack	CP-DEMO	Waiting For Endpoint			10 Jun 2022 07:18 pm	10 Jun 2022 07:18 pm

Asset Management 画面での端末の状況確認

Asset Management > Computers

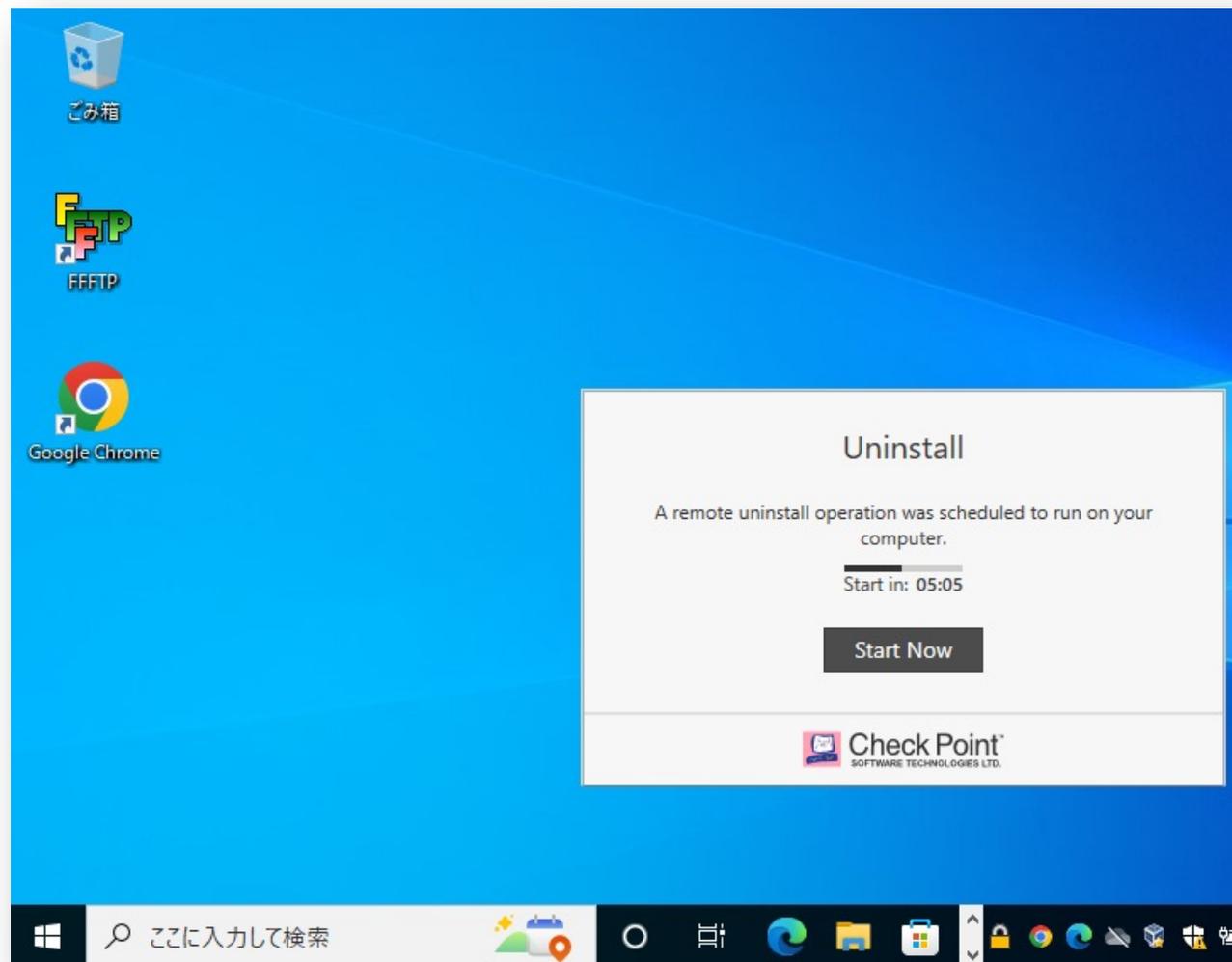
- Host Isolation 表示に切り替えることで、端末の隔離状況を表示可能

表示モードを [Deployment] に切り替え

Status	Computer Name	Endpoint Version	OS Build
<input type="checkbox"/>	Lab-13	86.26.6008	10.0-19043-SP0.0-SMP

アンインストールした端末 (今回の例では、CP-DEMO) が表示されないことを確認

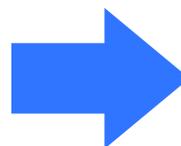
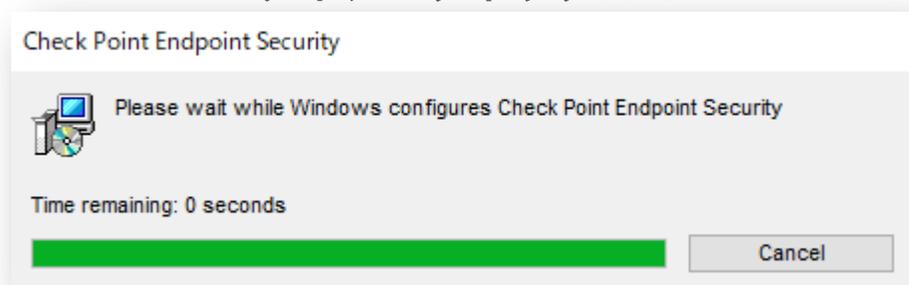
<参考> クライアントへの通知画面



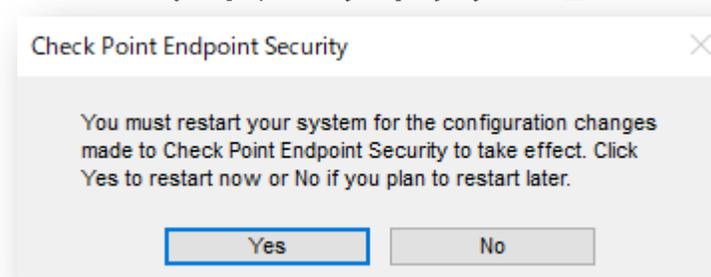
クライアントアンインストール時の注意事項

- 再起動を促すダイアログボックスが表示されるまで、パソコンのシャットダウンや再起動などを行わないでください

ダイアログボックス-1



ダイアログボックス-2



コントロールパネル

YOU DESERVE THE BEST SECURITY

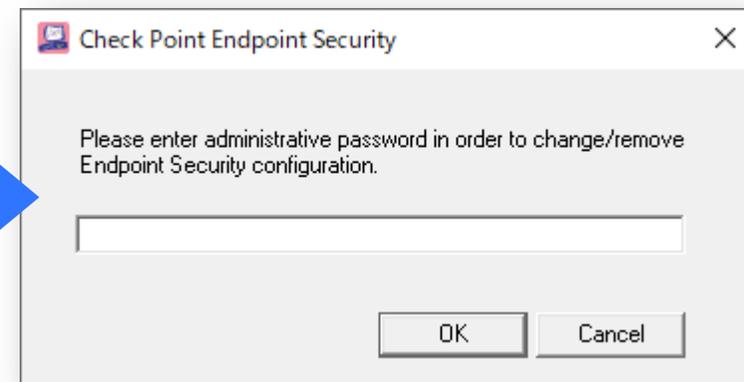
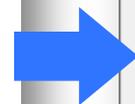
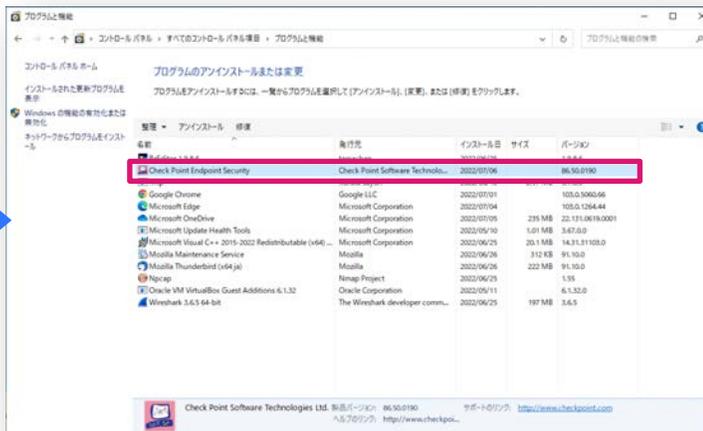
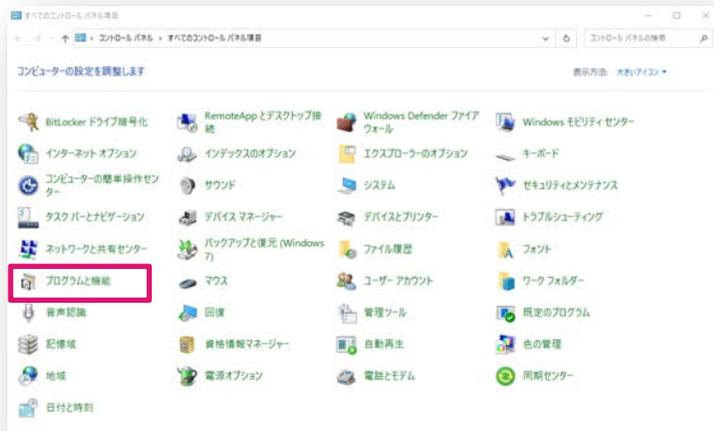
コントロールパネルからのアンインストール

- コントロールパネルの「プログラムと機能」を開きます
- 「Check Point Endpoint Security」を選択して、「アンインストール」をクリックします
- アンインストールパスワードを入力します
- 再起動を促すダイアログボックスが表示されたら、Yes を押して再起動してください

コントロールパネル

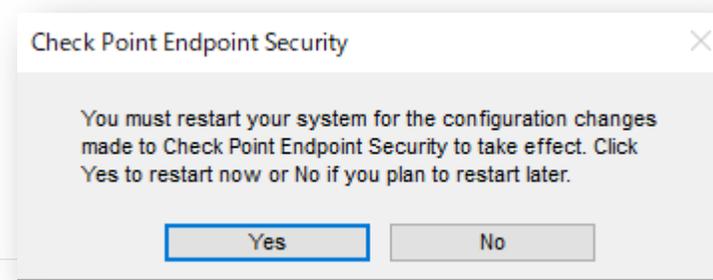
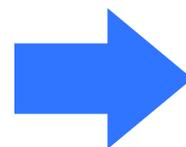
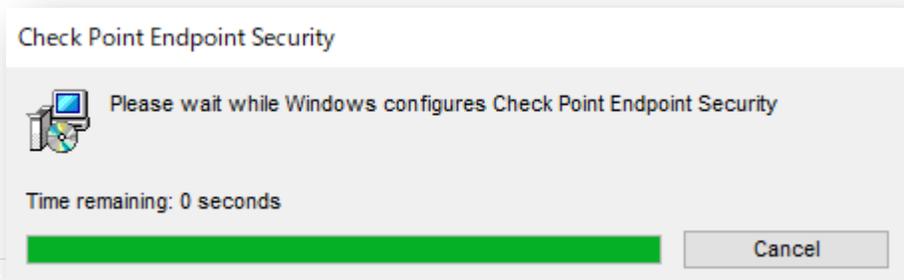
プログラムと機能

アンインストールパスワード



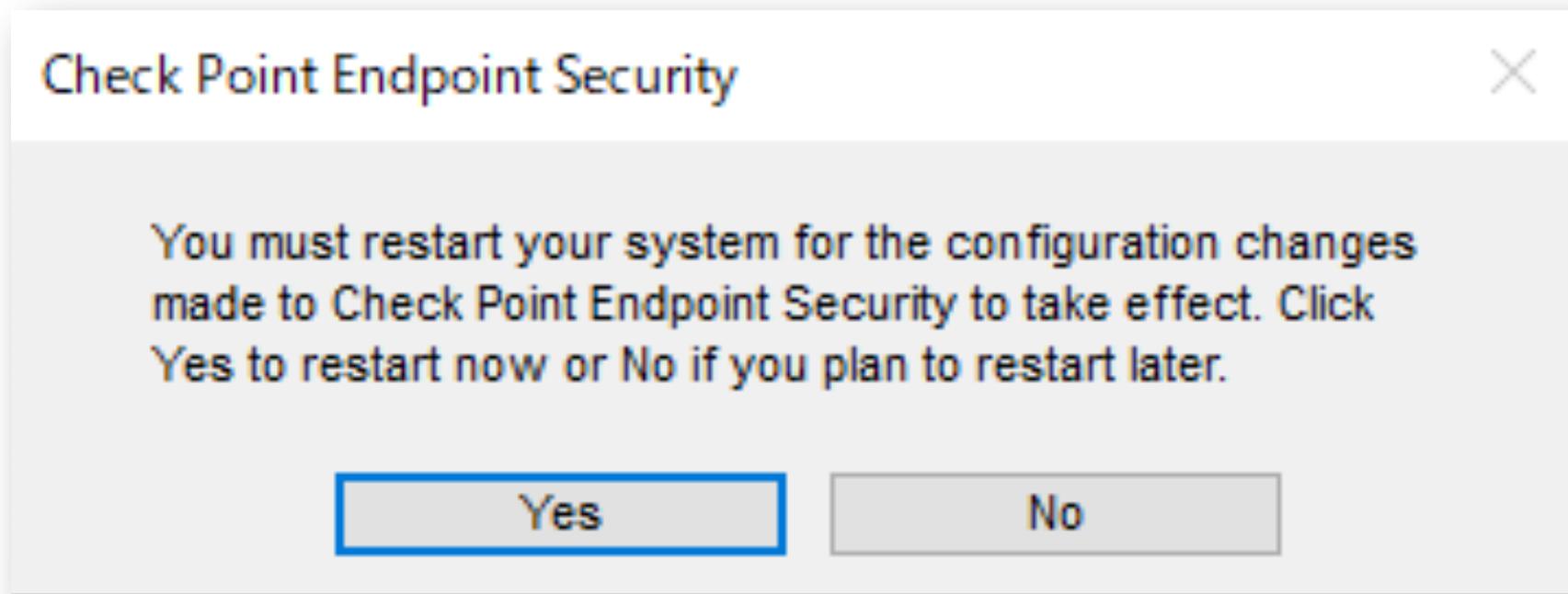
ダイアログボックス-1

ダイアログボックス-2



クライアントアンインストール時の注意事項

- 再起動を促すダイアログボックスが表示されるまで、パソコンのシャットダウンや再起動などを行わないでください





Thank You

YOU DESERVE THE BEST SECURITY