



HARMONY BROWSE

ハンズオントレーニングガイド

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

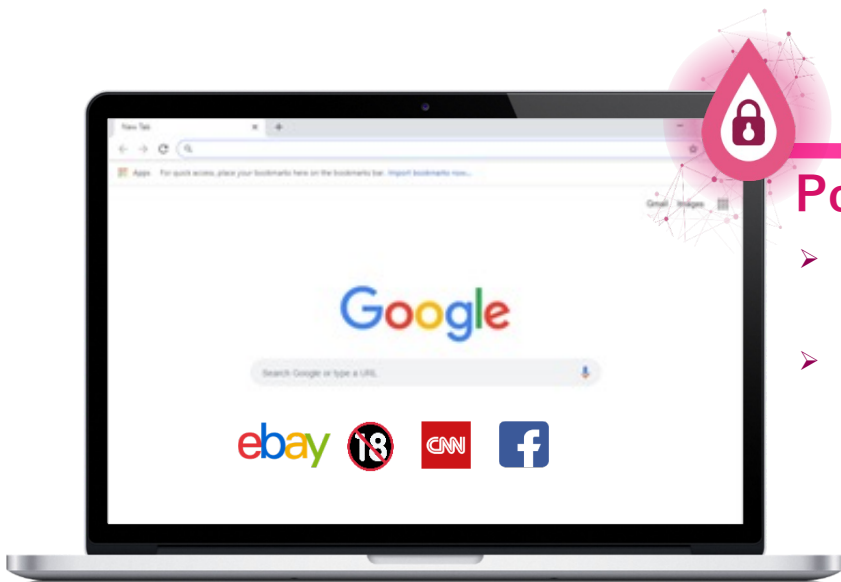
- Harmony Browse の概要
- 設定画面の概要
- クライアントのインストール
 - バーチャルグループの作成
 - インストールパッケージのダウンロード
- Threat Prevention 設定
 - URL フィルタリング
 - サンドボックス&ファイル無害化
 - ゼロ・フィッシング
- ログの表示

YOU DESERVE THE BEST SECURITY

HARMONY BROWSE の概要

YOU DESERVE THE BEST SECURITY

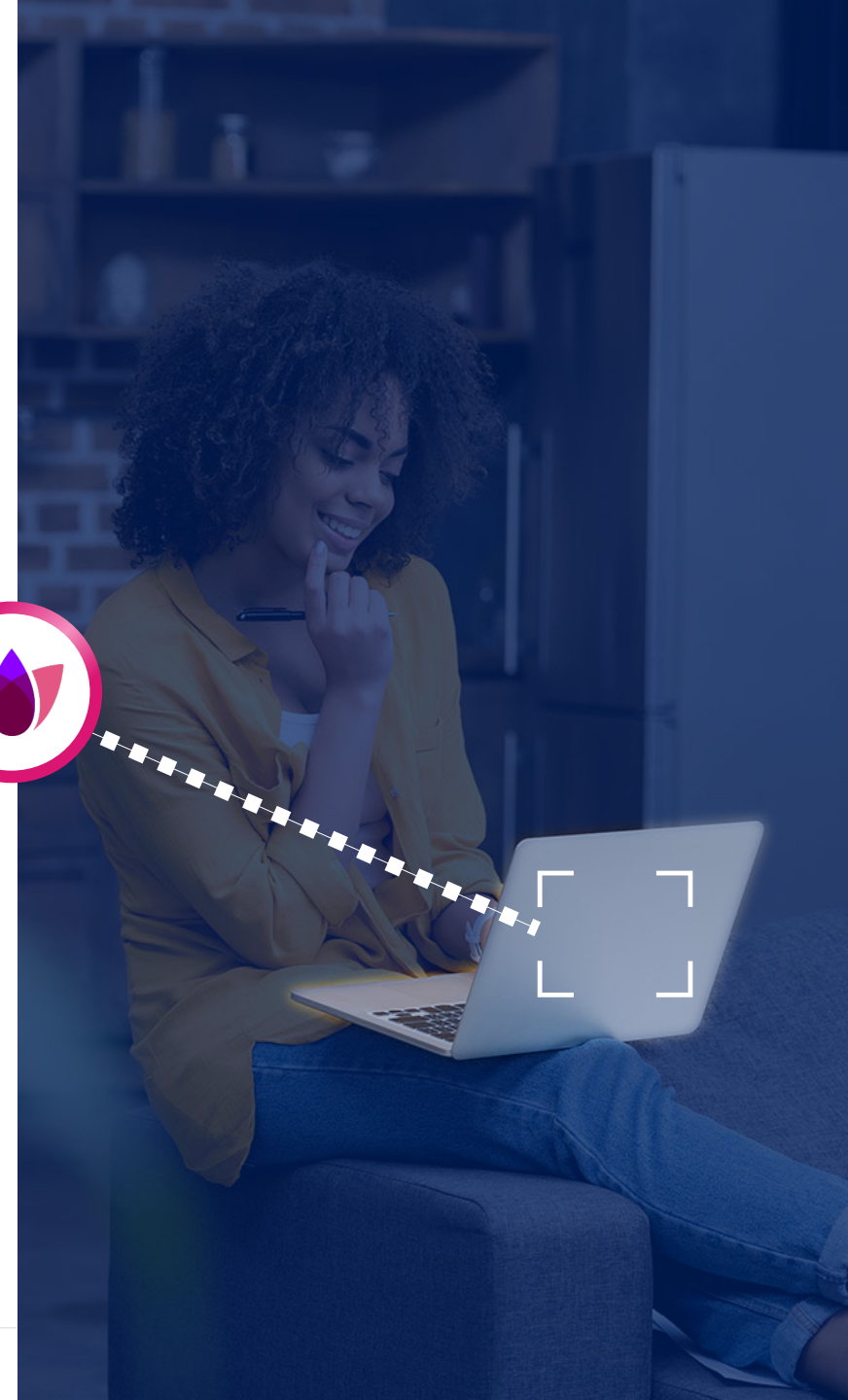
安全なブラウザ利用



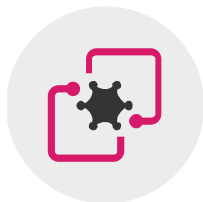
Powered by Nano Agents

- あらゆるブラウザのセキュリティを確保
- SSLトラフィックの100%を検査

- ・ マルウェアダウンロードを防止
- ・ フィッシングを防止
- ・ 企業で使用するパスワードの流出を防止
- ・ リスクあるサイトへのアクセスを防止

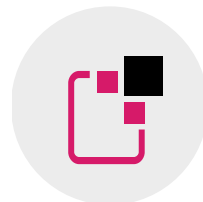


Harmony Endpoint が提供する先進の防御技術



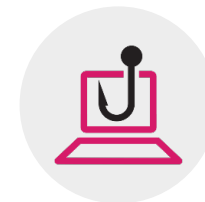
サンドボックス

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

検知 & 防止：サンドボックス（Threat Emulation）

サンドボックスの必要性

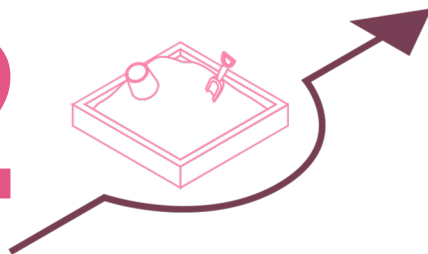
次世代型サンドボックスにより、未知の脅威や高度な脅威へも対応

1



攻撃者は、未知の脅威を使いシグネチャーベースのセキュリティ機能をバイパスします

2



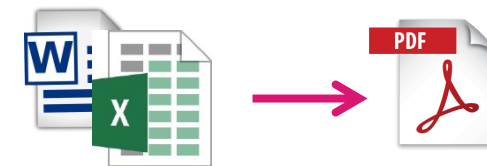
攻撃者は、回避技術を使って、第一世代のサンドボックスをバイパスします

検知 & 防止：ファイル無害化（Threat Extraction）

無害化された安全なファイルをユーザに届け、セキュリティと生産性を両立

- ✓ Webダウンロードするファイルが対象
- ✓ 2つのモードを選択可能
 - ・ PDF変換（100%無害化）
 - ・ マクロや埋め込みオブジェクトを削除
- ✓ 内容を維持し、ユーザに迅速にファイルを提供

Option1 – PDF変換

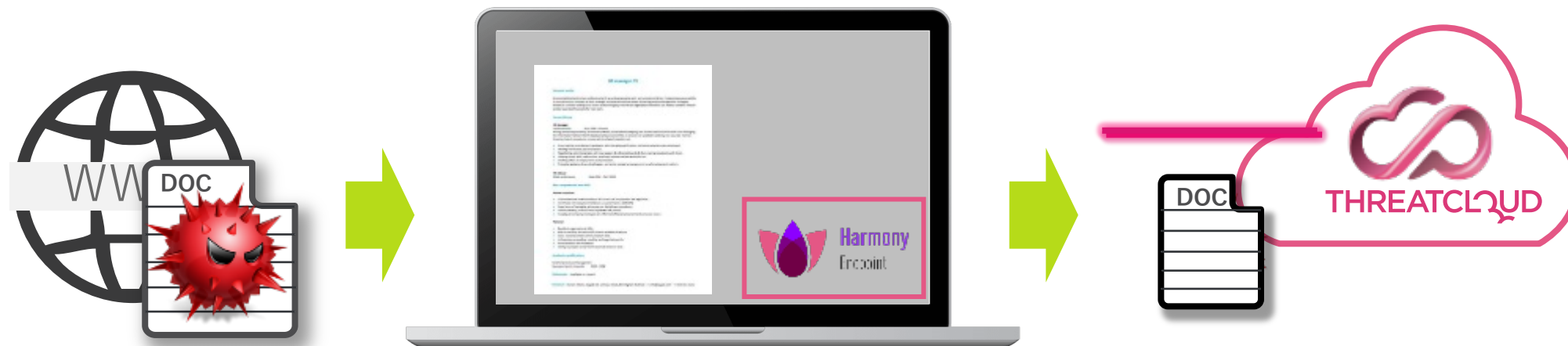


Option2 – 悪用可能なコンテンツ除去



サンドボックス & ファイルの無害化の動作イメージ

ユーザの生産性に影響を与えることなく、悪意のあるダウンロードをブロック



1

WEB ダウンロードを
Harmony Endpoint
が検出

2

アクティブなコンテンツ
を取り除いたファイルを
ユーザへ提供
(ファイル無害化)

3

バックグラウンドで
オリジナルファイルを
サンドボックスで
検査し安全性を確保

検知 & 防止：ゼロ・フィッシング

リアルタイムにフィッシングサイトを検出し、認証情報の漏洩を防止

- ✓ ゼロデイのフィッシングサイトをブロック
- ✓ Webサイト上の不審な要素を検査
- ✓ 検査終了までID/Passwordの入力を無効化

会員ID: Scanning.....

パスワード: Scanning by Zero Phishing



[パスワードを忘れた方はこちら](#)

- ✓ IPLレピュテーション
- ✗ URLの類似性
- ✗ タイトルの類似性
- ✗ 視覚的な類似性
- ✗ 文章の類似性
- ✓ ドメインレピュテーション
- ✓ よく似た文字列
- ✗ 画像のみのページ
- ✗ 複数の最上位ドメイン
- ✗ よく似たファビコン






SBlab LTD. - Anydesk Download x +

Not secure | anydesk.sbdemo.com/download/index.htm?lang=en&user=Bruce&jwt=Oisjaiz8...

SBlab AnyDesk Enterprise Download

 Custom SBlab Build  Full Remote Access  Advanced Security (FIPS 140-2)


Please fill the needed details in order to download your secure installer:

Domain:

Username:

Password:

E-Mail:



To get your custom build:

Mail SBlab IT Department No Items

1:19 PM 4/14/2022



他社製品を利用して、機能面で不安があります。

更新時期がまだ先なのですが、手軽にエンドポイントのセキュリティを強化する方法はありますか？

YOU DESERVE THE BEST SECURITY

Harmony Browse によるセキュリティ強化

Harmony Browse で SSL を可視化し、Web セキュリティを強化できます

サンドボックス、ファイル無害化、ゼロ・フィッシング、URL フィルタリングなど

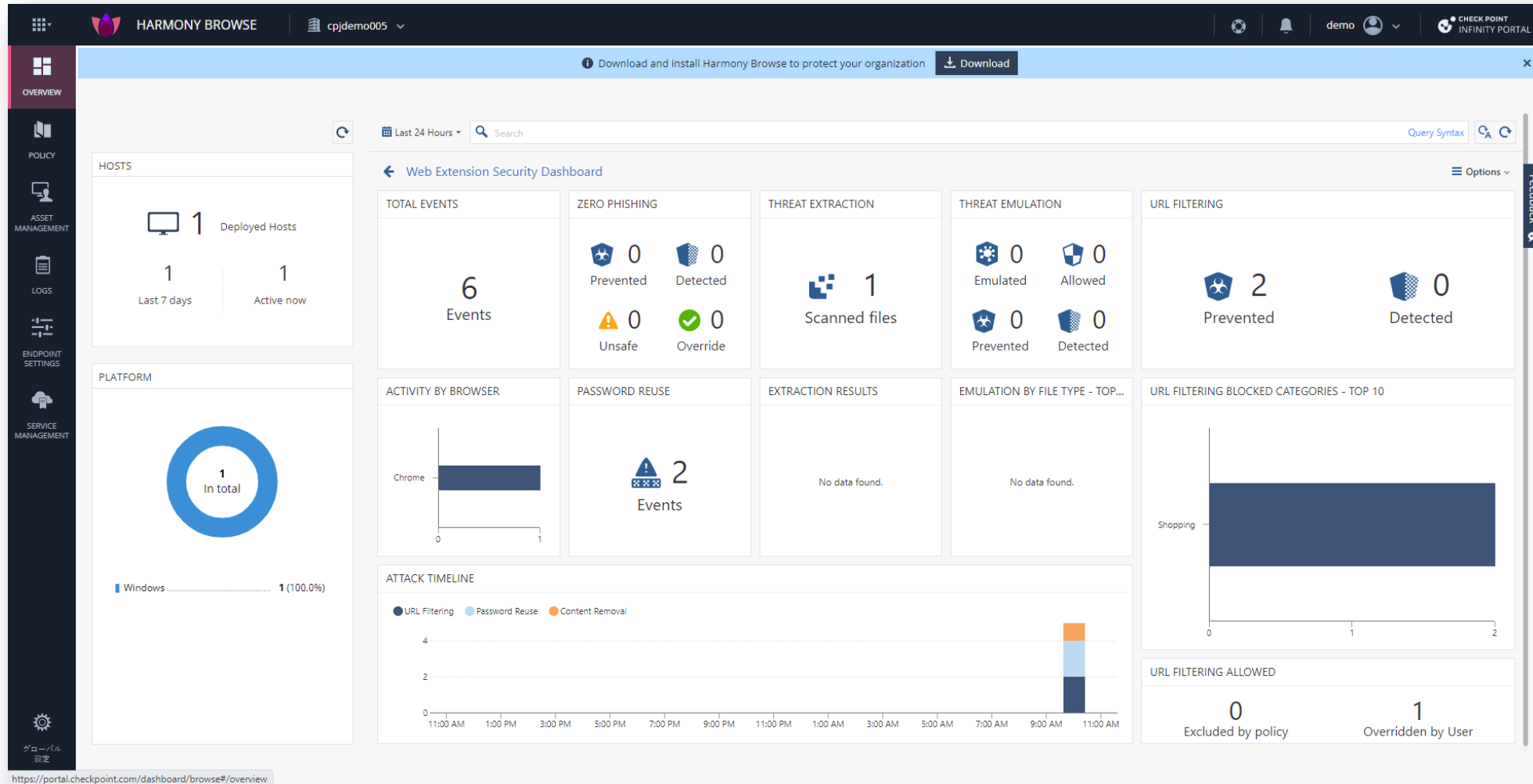
| 機能リスト | Harmony パッケージ | Harmony Basic | Harmony Advanced | Harmony Complete | Harmony Browse |
|---------------------------------------------------------------------------------------|---------------|---------------|------------------|------------------|----------------|
| 攻撃対象領域の削減: エンドポイント ファイアウォール、アプリケーション制御、 コンプライアンス、ポート防御、VPN | | + | + | + | |
| 攻撃防御: アンチウイルス、静的分析、ファイルレピュテーション、次世代アンチウイルス、 アンチマルウェア | | + | + | + | |
| 継続的な防御: アンチ ランサムウェア、振る舞い防御、アンチボット、アンチエクスプロイト | | + | + | + | |
| 攻撃調査と対応: フォレンジック収集、インシデント可視化、MITREマッピング、脅威ハンティング、 自動化された攻撃チェーンの完全無害化、暗号化ファイルの復元 | | + | + | + | |
| Threat Intelligence: ThreatCloud™による自動 IoCとIoAクラウド共有 | | + | + | + | |
| 安全なインターネットブラウジング: ゼロ・フィッシング、企業パスワードの再利用防止、 URL フィルタリング、SSL 可視化、悪質なサイト防御 | | + | + | + | + |
| Web ダウンロード保護: サンドボックス、ファイル無害化 | | | + | + | + |
| データ保護: ホスト暗号化、メディア暗号化 | | | | + | |

設定画面の概要

YOU DESERVE THE BEST SECURITY

Overview

HarmonyBrowseクライアントに関する概要をグラフィカルに表示



Policy

脅威対策、ユーザーインターフェースのカスタマイズなどを構成

The screenshot displays the 'HARMONY BROWSE' interface for a user named 'cpjdemo005'. The left sidebar contains navigation options: OVERVIEW, POLICY (highlighted), and MA. The main area shows a table of rules under the 'Threat Prevention' section. A callout points to the 'POLICY' menu item with the text '設定項目を選択' (Select setting items). Another callout points to the table with the text 'グループごとにポリシーを構成' (Configure policies by group). A third callout points to the 'CAPABILITIES & EXCLUSIONS' panel with the text 'ポリシーの詳細を構成' (Configure policy details). The table has the following data:

| # | Rule Name | Applied To | Web & Files |
|---|----------------------------------------------------------------------------------------------|---------------------|-------------|
| 0 | Default settings for the entire organization Default settings for the entire organization | Entire Organization | |

The 'CAPABILITIES & EXCLUSIONS' panel shows settings for 'Default settings for the entire organization'. It includes options for 'Use Predefined Settings' (Default) and 'Custom'. Under 'WEB & FILES PROTECTION', the following settings are visible:

- URL Filtering: URL Filtering Mode is set to 'Prevent'.
- Download protection: Download Emulation & Extraction is set to 'Prevent'.
- Credential protection: Zero Phishing is set to 'Prevent' and Password reuse protection is set to 'Detect & Alert'.
- Safe Search: Force Safe Search is set to 'Off'.

Asset Management

コンピュータ名、バージョン、バーチャルグループなどの情報を表示

The screenshot displays the 'ASSET MANAGEMENT' section of the Check Point Harmony Browse interface. The main area shows a table of computers with columns for Status, Computer Name, Endpoint Version, OS Build, Virtual Group, Device Type, Deploy Time, Last Connection, and Last Logged In User. A callout box labeled '概要表示' (Summary View) points to this table. To the right, a 'FILTERS' sidebar allows for filtering by Computer Name, Active status, Domain Name, Agent Installed, Endpoint version, Operating System, Device Type, Deploy Time, OS Build, Last Connection, Last Logged In User, Virtual Groups, and Package Version. A callout box labeled '一覧表示の条件選択' (Filter Selection for Summary View) points to this sidebar. Below the table, a detailed view for the selected computer 'DESKTOP-02CEUVB' is shown, with a callout box labeled '詳細表示' (Detailed View) pointing to it. The detailed view includes fields for General (Display Name, Description), LDAP (SAM Name, CN), Operating System (Windows 10.0 Enterprise Evaluation Edition), OS Version (10.0-19043-SP0.0-SMP), and Member of (All Laptops, All Windows Laptops).

| Status | Computer Name | Endpoint Version | OS Build | Virtual Group | Device Type | Deploy Time | Last Connection | Last L |
|--------|-----------------|-------------------|----------------------|---------------------|-------------|----------------------|----------------------|--------|
| ✓ | DESKTOP-02CEUVB | BROWSE_90.08.7417 | 10.0-19043-SP0.0-SMP | All Laptops+ 1 more | Laptop | 30 May 2022 10:22 am | 30 May 2022 11:44 am | nack |

1 of 1 selected

General

Display Name
DESKTOP-02CEUVB

Description
-

LDAP

SAM Name
DESKTOP-02CEUVB

CN
-

Operating System
Windows 10.0 Enterprise Evaluation Edition

OS Version
10.0-19043-SP0.0-SMP

Member of

- All Laptops
- All Windows Laptops

Logs

コンピュータで検出されたアクティビティを表示

The screenshot displays the Check Point Harmony Browse interface. The top navigation bar includes the 'HARMONY BROWSE' title and a search bar labeled 'クエリ検索バー'. The left sidebar contains navigation options: '期間' (Period), '統計 & 簡易フィルタ' (Statistics & Simple Filters), 'POLICY', 'ASSET MANAGEMENT', 'LOGS', 'ENDPOINT SETTINGS', and 'SERVICE MANAGEMENT'. The main content area is divided into three sections: 'Statistics' on the left, a central table of logs, and a 'ログ詳細' (Log Details) panel on the right. The 'ログ一覧' (Log Overview) label points to the central table. The 'オプション' (Options) label points to the 'Options' dropdown in the top right. The 'ログ詳細' label points to the right-hand panel.

期間

クエリ検索バー

ログ詳細

オプション

統計 & 簡易フィルタ

ログ一覧

| Time | Source User Na... | B. | Matched Catego... | A. | Resource |
|--------------------------|-------------------|----|-------------------|----|-------------------------------------------------------------------------------------------------------|
| May 30, 2022 10:38:35 AM | nack | | | | https://secure.sakura.ad.jp/auth/login?url=https%3A%2F%2Fsecure.sakura.ad.jp%2Fmenu%2Ftop%2Findex.php |
| May 30, 2022 10:38:21 AM | nack | | | | https://secure.sakura.ad.jp/auth/login?url=https%3A%2F%2Fsecure.sakura.ad.jp%2Fmenu%2Ftop%2Findex.php |
| May 30, 2022 10:36:44 AM | nack | | Shopping | | https://www.amazon.co.jp/ |
| May 30, 2022 10:36:27 AM | nack | | Shopping | | https://www.amazon.com/ |
| May 30, 2022 10:35:42 AM | nack | | Shopping | | https://www.amazon.com/ |
| May 30, 2022 10:31:20 AM | nack | | | | http://www.checkpoint.sc/eval/sample2.xlsm |

ログ詳細

オプション

ログ一覧

統計 & 簡易フィルタ

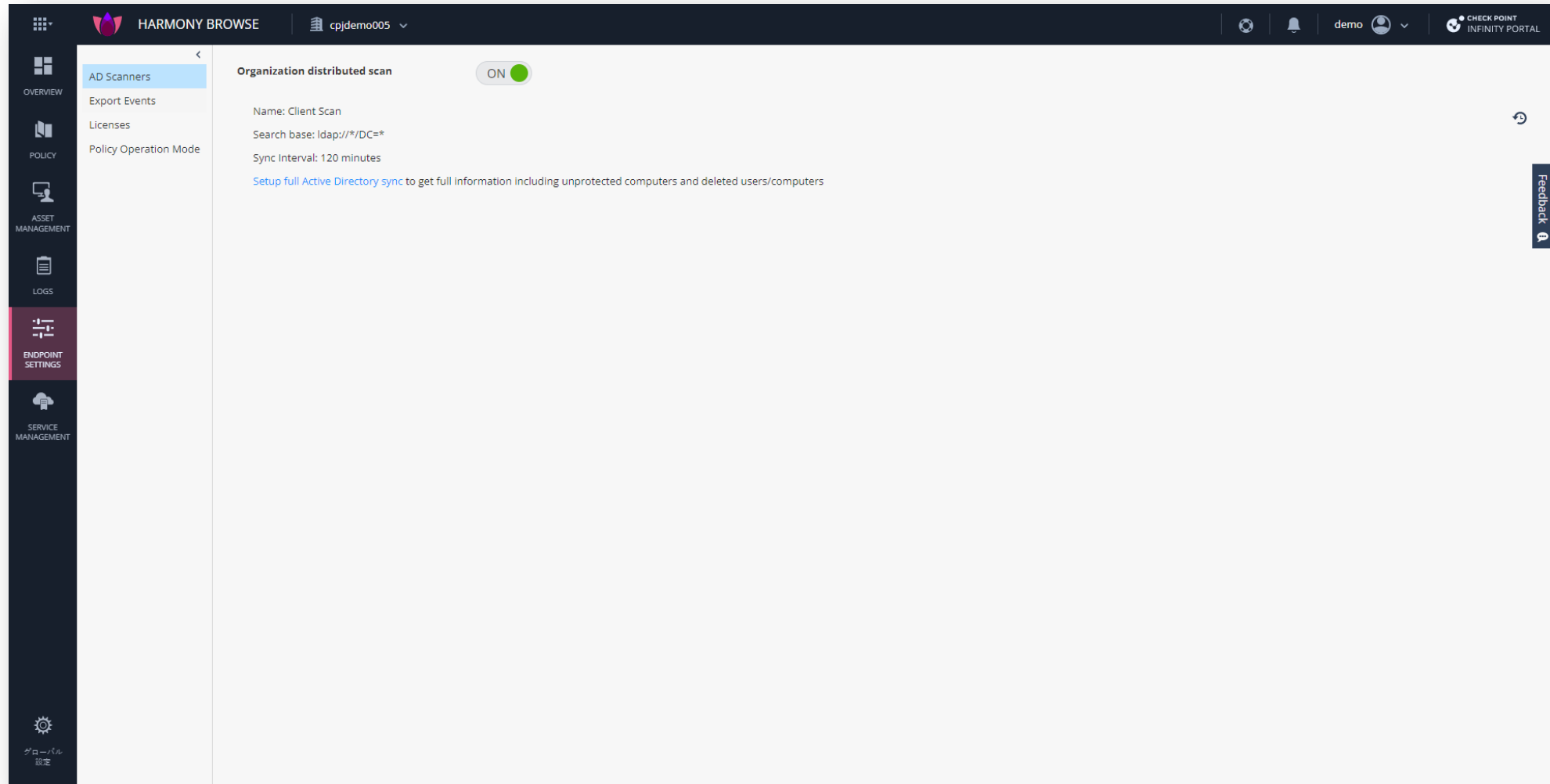
期間

クエリ検索バー

オプション

Endpoint Settings

ログのエクスポート、ライセンス管理など



Service Management

サービスステータスを管理

The screenshot displays the Harmony Browse web interface. The top navigation bar includes the 'HARMONY BROWSE' logo, a dropdown menu for 'cpjdemo005', and user information 'demo'. The left sidebar contains navigation options: OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, ENDPOINT SETTINGS, SERVICE MANAGEMENT (highlighted), and グローバル設定 (Global Settings). The main content area is divided into two sections. The top section, titled 'Service Status', shows a 'Running' status with a green play button icon. It lists the following details: Account Name: cpjdemo005, Service version: 81.10.9.110, Web version: 8.27.0:8.27.0-sba4b, Connection Token: cpjdemo005-3c67b77c-hap2, Hosting Site: Europe, Purpose: Product Evaluation, Launch Time: 20 May 2022 | 10:58, Fingerprint: View Details, and SmartView URL: https://cpjdemo005-3c67b77c... The bottom section, titled 'Install Harmony Browse Client', provides instructions: 'To install the Harmony Browse Client, go to Overview Page and click the Download Agent button.' It includes a screenshot of a browser's download bar with a 'Download Agent' button circled. Below this, there is a link to 'Set SmartView Administrator Password'.

クライアントのインストール

- バーチャルグループの作成
- インストールパッケージのダウンロード

YOU DESERVE THE BEST SECURITY

バーチャルグループの作成

Asset Management > Operational Tree > Install & Upgrade > Uninstall Settings

- 組織ごとにポリシーやパッケージをカスタマイズする場合、バーチャルグループを作成します
- 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

The screenshot displays the Harmony Endpoint console interface. On the left sidebar, the 'ASSET MANAGEMENT' menu is highlighted. The main area shows the 'Organizational Tree' with 'Virtual Groups' selected. An 'Actions' menu is open, with 'Create Virtual Group' highlighted. A dialog box titled 'CREATE VIRTUAL GROUP' is shown, containing a 'Name' field with the value 'demo2' and a 'Comment' field with the placeholder text 'Comment'. The dialog has 'CANCEL' and 'OK' buttons at the bottom.

インストールパッケージのダウンロード

Overview

The screenshot displays the Check Point Harmony Browse console interface. A modal window titled "DOWNLOAD HARMONY BROWSE" is open, showing download options for three components: Windows, macOS, and AD Client. Each component has a "Download version" dropdown set to "Latest" and a "DOWNLOAD" button. The "AD Client" version is specifically set to "86.25.5060". A red box highlights the "Download" button in the top right of the console, with a red arrow pointing to the modal window. The background console shows a sidebar with navigation options like OVERVIEW, POLICY, ASSET MANAGEMENT, LOGS, ENDPOINT SETTINGS, and SERVICE MANAGEMENT. The main area displays "HOSTS" (1 Deployed Hosts), "PLATFORM" (1 in total, 100.0% Windows), and various security metrics like THREAT EMULATION, URL FILTERING, and EMULATION BY FILE TYPE.

THREAT PREVENTION 設定

- URL フィルタリング
- Threat Extraction (無害化)
- ゼロ・フィッシング

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 / 4)

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
 - Web ダウンロード時のサンドボックスとファイル無害化
 - フィッシング対策
 - 企業パスワード保護
 - セーフサーチの有効化

Threat Prevention : 共通 (2 / 4)

Policy > Threat Prevention

- バーチャルグループを使用して、組織ごとに異なるルールを設定できます
- コンピュータが複数のバーチャルグループに所属している場合、若番のポリシーが適用されます

Annotation: ポリシー一覧 (Policy List)

Annotation: 挙動監視 (Behavioral Monitoring)

Annotation: 分析と修復 (Analysis and Remediation)

Annotation: ポリシーごとの設定の詳細 (Detailed Settings for Policy)

Annotation: ポリシー適用順 (Policy Application Order)

| # | Rule Name | Applied To | Web & Files | Behavioral | Analysis |
|---|----------------|---------------|-------------|------------|----------|
| 0 | macOS | macOS | [Icons] | [Icons] | [Icons] |
| 1 | Windows Server | Windows Se... | [Icons] | [Icons] | [Icons] |
| 2 | demo | demo | [Icons] | [Icons] | [Icons] |
| 3 | demo3 | demo3 | [Icons] | [Icons] | [Icons] |

Annotation: 適用するバーチャルグループ (Virtual Groups to Apply)

Annotation: Web アクセス、ファイルアクセス対策 (Web Access, File Access Protection)

Annotation: CAPABILITIES & EXCLUSIONS (Capabilities & Exclusions)

Annotation: EXCLUSIONS CENTER (Exclusions Center)

Annotation: WEB & FILES PROTECTION (Web & Files Protection)

Annotation: BEHAVIORAL PROTECTION (Behavioral Protection)

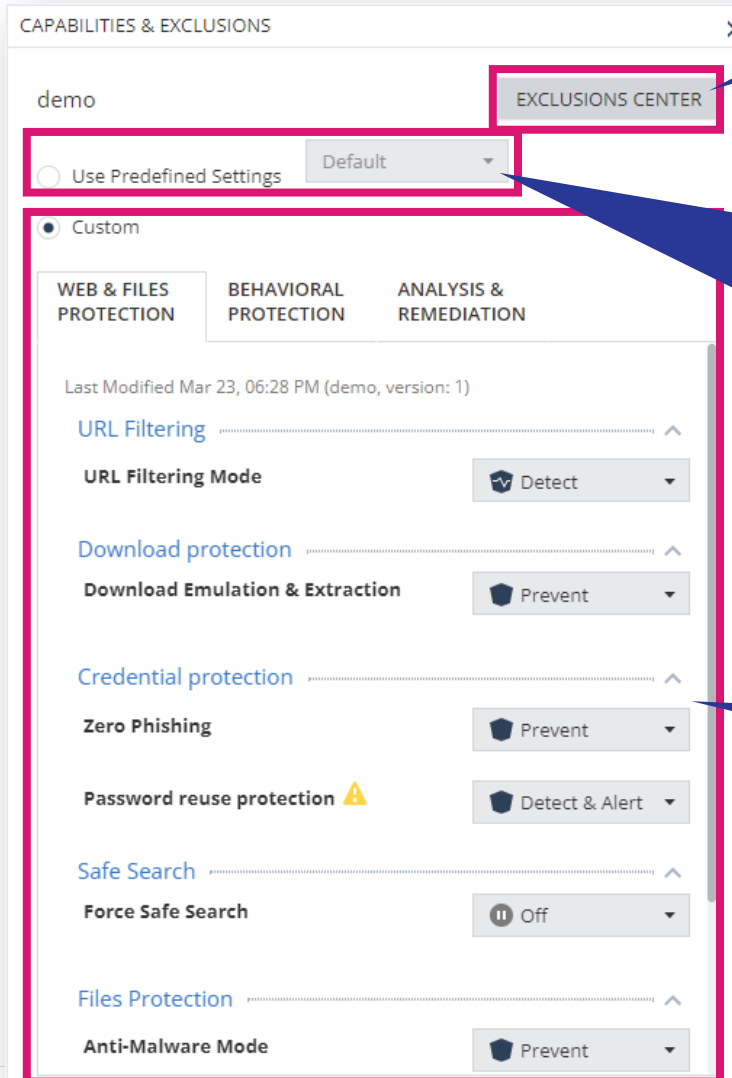
Annotation: ANALYSIS & REMEDIATION (Analysis & Remediation)

Annotation: Automated attack analysis (forensics) (Automated attack analysis (forensics))

Annotation: Protection mode (Protection mode)

Threat Prevention : 共通 (3 / 4)

Policy > Threat Prevention



すべての例外設定を管理

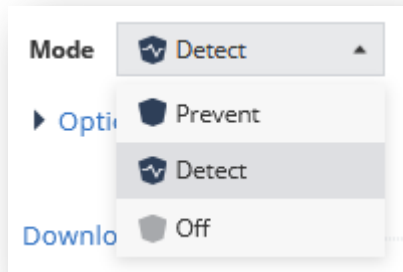
事前定義された設定

- Tuning
- Recommended
- Default
- Strict

各項目ごとの詳細な設定

Threat Prevention : 共通 (4 / 4)

Policy > Threat Prevention



- 各機能では脅威に対して動作モードを選択できます
 - 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

ポリシーの設定

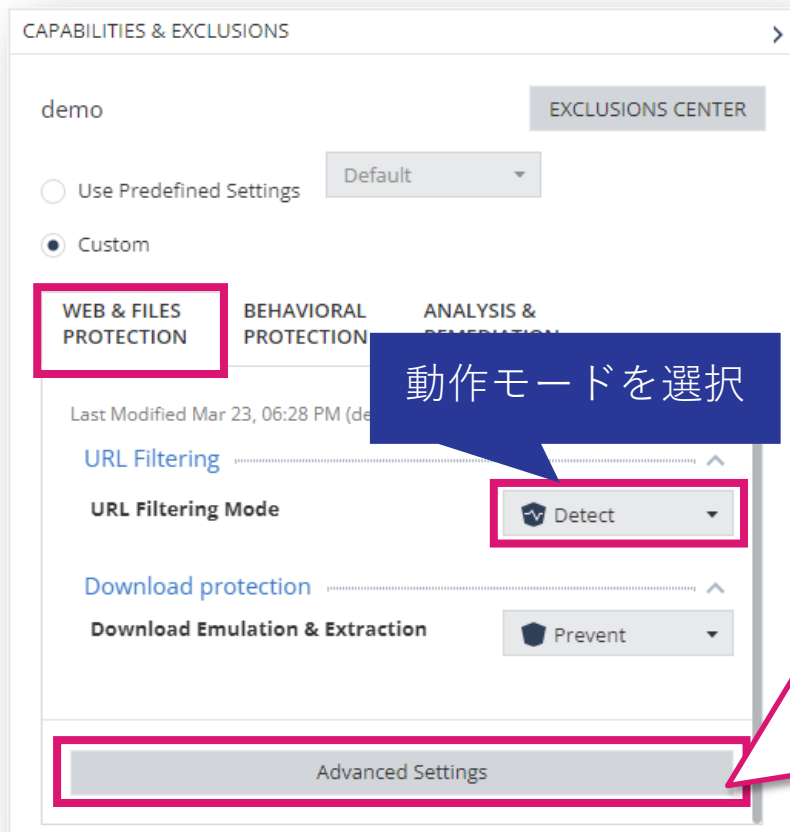
THREAT PREVENTION URL フィルタリング

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



動作モードを選択

このスクリーンショットは「ADVANCED SETTINGS - WEB & FILES PROTECTION」の「URL Filtering」セクションを示しています。設定には「Allow user to dismiss the URL Filtering alert and」がチェックされています。下部には「Categories」セクションがあり、「Security (10)」が選択されています。右側には「Black list (0)」と「Edit...」ボタンが表示されています。右側のパネルには「Categories」リストがあり、「Alcohol & Tobacco」から「Education」までの項目がリストアップされています。

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

事前定義されたカテゴリ

ブラックリスト

【演習】 URL フィルタリング

- URL フィルタリングのモードを「Prevent」にしてください
- Alcohol & Tobacco のカテゴリを禁止して、URLフィルタリングの動作を確認してください
- 「Allow user to dismiss the URL Filtering alert and access the website」にチェックを入れた時と、外した時のエンドユーザのブロック画面の違いを確認してください
- ブラックリストに Web サイトを登録して、ブロックされることを確認してください

ポリシーの設定

THREAT PREVENTION DOWNLOAD 保護

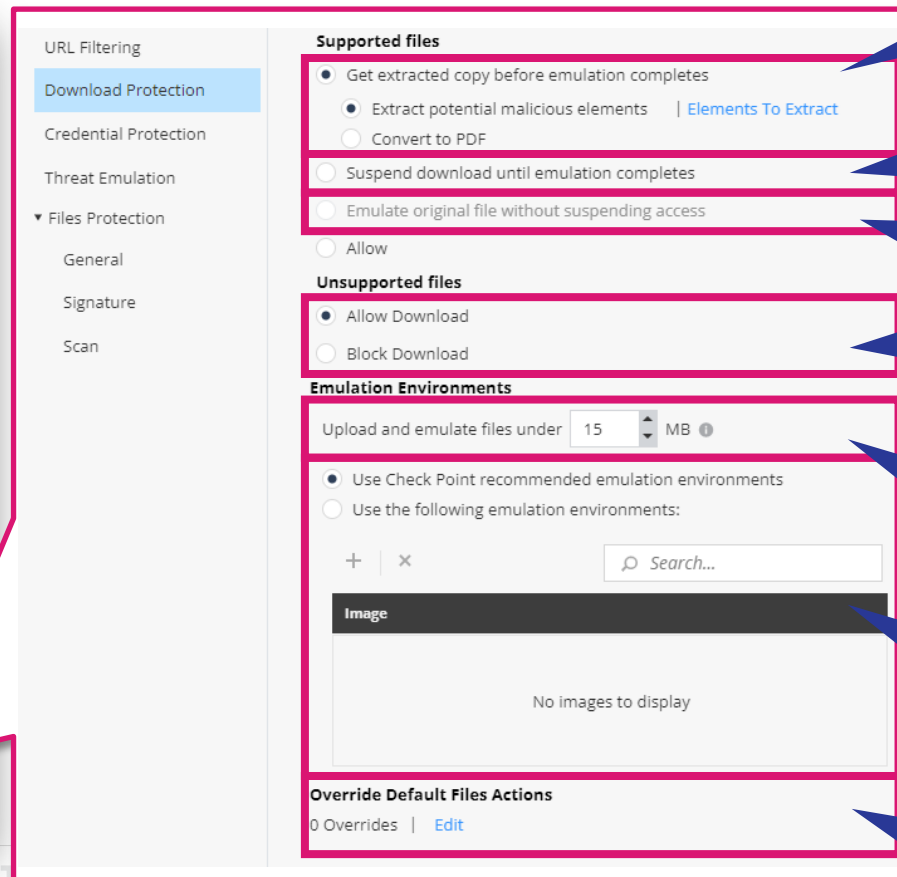
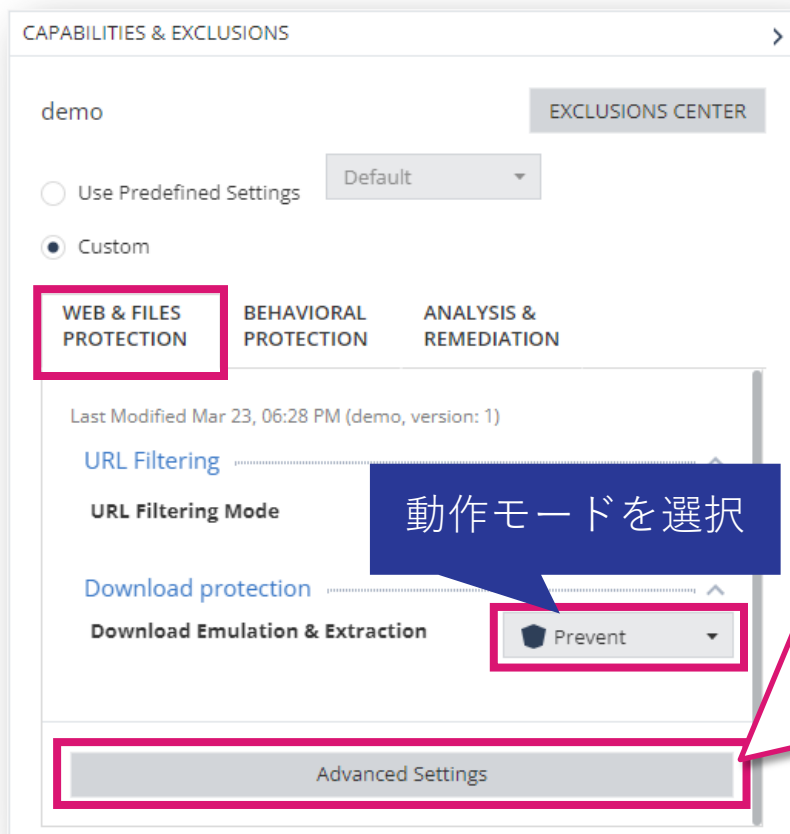
- Threat Emulation (Sandbox)
- Threat Extraction (無害化)

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



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、docx、xls、xlsx 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 | Download URL |
|----------------|-------------------------|------------------|----------------------------------------------------------------------------------------------|
| doc | Emulate and Extract | Convert to PDF | www.checkpoint.sc/eval/sample1.doc |
| xlsm | Emulate and Extract | Extract Elements | www.checkpoint.sc/eval/sample1.xlsm |
| xls | Emulate | — | www.checkpoint.sc/eval/sample1.xls |
| xlsx | Emulate without Suspend | — | www.checkpoint.sc/eval/sample1.xlsx |

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

CAPABILITIES & EXCLUSIONS

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】ゼロ・フィッシング

- www.amazon.com 等へアクセスして、認証情報を入力する際に、フィッシングサイトの検査が実施されることを確認してください
- salesforce.sbm-demo.xyz/zero-phishing へアクセスして、認証情報の入力がブロックされることを確認してください

ログの表示

YOU DESERVE THE BEST SECURITY

ログの表示

Logs

The screenshot displays the Check Point Logs interface with several callouts:

- 期間** (Period): Points to the "Last 7 Days" dropdown menu.
- クエリ検索バー** (Query Search Bar): Points to the search input field.
- 統計 & 簡易フィルタ** (Statistics & Simple Filters): Points to the "Statistics" sidebar containing a "Sessions Timeline" bar chart and filter sections for "Blade", "Severity", and "Action".
- ログ詳細** (Log Details): Points to the "Log Info" section in the right-hand "Card" pane.
- ログ一覧** (Log List): Points to the main table of log entries.
- オプション** (Options): Points to the "Options" menu in the top right corner.

| Time | B.. | Severity | A.. | Origin | Source | User | Destination | Service |
|-------------------------|------|---------------|------|-------------------------|-------------|------|-------------|---------|
| Sep 2, 2021 12:55:15 PM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:15:22 PM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:13:49 PM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:03:28 PM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:03:22 PM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:02:55 PM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 12:02:52 PM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 11:53:22 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 11:53:20 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:54:12 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:54:03 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:53:27 AM | Info | Medium | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:53:27 AM | Info | Informational | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:42:39 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:19:03 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:17:32 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:09:32 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 10:06:34 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 192.168.1.4 | | | |
| Sep 2, 2021 10:06:13 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 9:52:11 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 9:35:49 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 9:24:23 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 9:22:46 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 8:47:00 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 8:44:34 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 8:42:56 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |
| Sep 2, 2021 7:50:24 AM | Info | Low | Info | cpalldemo-fd1bc249-hap1 | 10.61.0.6 | | | |

一覧表示・詳細表示

- 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 console interface. On the left, there is a navigation sidebar with sections like Overview, Policy, Asset Management, Logs, Push Operations, Endpoint Settings, Service Management, Threat Hunting, and Global Settings. The main area is titled 'Logs' and shows a table of log entries. A blue callout box with white text says 'エンタリをダブルクリックして、詳細を表示' (Double-click the entry to display details). A red box highlights a specific log entry: 'Mar 30, 2022 12:59:02 AM', 'Forensics', 'Prevent', 'High', 'High', 'Endpoint3', 'File System Em...', 'Gen.SB.exe', and 'Trojan, "be...'. To the right, a 'Card' window provides detailed information for this event, including Log Info (Origin: cpjdemo002-d69e771e-hap2, Time: Mar 30, 2022 11:34:53 PM, Blade: SmartEvent Client), 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), and Traffic (Source: ip-192-168-100-5.ec2.internal (192.168.100.5), Source User Name: aduser1, Machine Name: DESKTOP-M5E17GCad.example.com). A 'Forensics Report' link is also visible at the bottom of the card.

| Time | Blade | Action | Severity | Endpoint | File System Em... | Gen.SB.exe | Trojan, "be... |
|--------------------------|----------------------|-------------|----------|-----------|----------------------|-------------|----------------|
| Mar 30, 2022 2:13:06 PM | Forensics | Detect | Low | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 9:09:10 AM | Endpoint Compliance | Detect | Medium | Endpoint3 | Full Disk Encryption | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 9:08:20 AM | Full Disk Encryption | Detect | Medium | Endpoint3 | Full Disk Encryption | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 9:08:19 AM | Full Disk Encryption | Detect | Medium | Endpoint3 | Full Disk Encryption | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 9:07:21 AM | Endpoint Compliance | Inform User | Critical | Endpoint3 | Full Disk Encryption | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 9:07:17 AM | Endpoint Compliance | Inform User | High | Endpoint3 | Full Disk Encryption | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 1:09:18 AM | Anti-Malware | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 12:58:44 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 12:58:39 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.exe | Trojan, "be... |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:58:11 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:58:00 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:57:48 AM | Forensics | Prevent | High | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:57:47 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:57:43 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:57:38 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:57:36 AM | Threat Emulation | Prevent | Low | Endpoint3 | File System Em... | Gen.SB.dll | Trojan, "be... |
| Mar 30, 2022 12:56:02 AM | Forensics | Prevent | High | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:50 AM | Forensics | Prevent | High | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:38 AM | Forensics | Prevent | High | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:26 AM | Forensics | Prevent | High | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:22 AM | Threat Emulation | Prevent | Low | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:22 AM | Threat Emulation | Prevent | Low | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:14 AM | Threat Emulation | Prevent | Low | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:13 AM | Threat Emulation | Prevent | Low | Endpoint3 | File Reputation | Gen.Rep.exe | Trojan, "be... |
| Mar 30, 2022 12:55:08 AM | Forensics | Prevent | Critical | Endpoint3 | Static File Anal... | Gen.MLSA | Trojan, "be... |

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

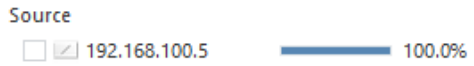
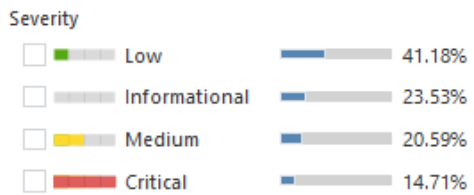
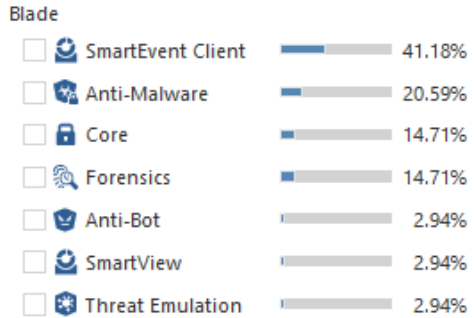
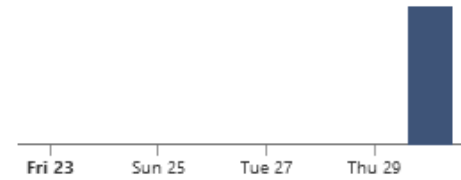
The screenshot displays the 'Select a time filter' dialog box in the Check Point management console. At the top left, a dropdown menu is set to 'Last 7 Days'. Below this, a grid of preset time filters is shown, with 'Last 7 Days' highlighted in blue. The grid includes options like 'Today', 'Yesterday', '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 grid, there are sections for 'Relative Time Range', 'Date Range', and 'Date and Time Range'. At the bottom of the dialog, there are filters for 'Threat Emulation' (2.94%) and 'Severity' (Low, 41.18%). The background shows a list of logs with columns for time, severity, and source.

| 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

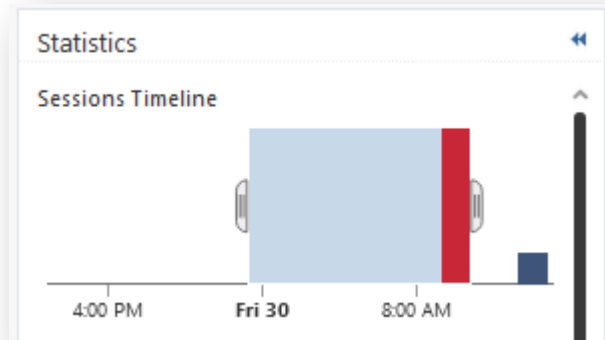
時間で指定することも可能

Sessions Timeline



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



クエリ：キーワード

- 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 | 2826815873d90ad38c5aeeed57c09385d6ac |
| 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：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 security log table with columns: Time, Blade, Action, Severity, and a multi-column section for details. A context menu is open over the table, listing various 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 System Emulation | Protection... | Malware Act... | File Name |
|--------------------------|----------------------|------------|----------|-------------------|-----------------------|-----------------------|---------------|----------------|-----------|
| Mar 30, 2022 9:09:10 AM | Endpoint Complia... | Detect | Me... | Profile Editor... | | | | | |
| Mar 30, 2022 9:08:20 AM | Full Disk Encryption | | Me... | Automatic | | | | | |
| Mar 30, 2022 9:08:19 AM | Full Disk Encryption | | Me... | Access Control | | | | | |
| Mar 30, 2022 9:07:21 AM | Endpoint Complia... | Inform ... | Cri... | Endpoint | | | | | |
| Mar 30, 2022 9:07:17 AM | Endpoint Complia... | | High | Management | | | | | |
| Mar 30, 2022 1:09:18 AM | Anti-Malware | | Low | Mobile | | | | | |
| Mar 30, 2022 12:59:02 AM | Forensics | Prevent | High | Threat Prevention | | | | | |
| Mar 30, 2022 12:58:50 AM | Forensics | Prevent | High | High | File System Emulation | | | | |
| Mar 30, 2022 12:58:44 AM | Threat Emulation | Prevent | Low | High | File System Emulation | | | | |
| Mar 30, 2022 12:58:39 AM | Threat Emulation | Prevent | Low | High | File System Emulation | | | | |
| Mar 30, 2022 12:58:23 AM | Forensics | Prevent | High | High | File System Emulation | | Gen.SB.dll | Trojan | 7e2b1bbff |
| Mar 30, 2022 12:58:11 AM | Forensics | Prevent | High | High | File System Emulation | | Gen.SB.dll | Trojan | f.000025 |

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"
- 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 | | イベントの重大度 |
| app_risk | | アプリケーションからの潜在的なリスク |
| Protection | | 保護の名前 |
| protection_type | | 保護のタイプ |
| confidence_level | | イベントが悪意のあるものである確かさ |
| action | | セキュリティルールによって実行されるアクション |
| blade | product | ソフトウェアブレード (セキュリティ機能) |
| destination | dst | トラフィックの宛先IPアドレス、DNS名、またはチェックポイントネットワークオブジェクト名 |
| origin | orig | 発信元のセキュリティゲートウェイの名前 |
| service | | ログエントリを生成したサービス |
| source | src | トラフィックの送信元IPアドレス、DNS名、またはチェックポイントネットワークオブジェクト名 |
| user | | ユーザー名 |

- 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 |



THANK YOU

YOU DESERVE THE BEST SECURITY