MENLO SECURITY

Browsing Forensics 概要

セキュリティチーム、インシデント対応チームおよびコンプライアンスチームがこれまで見逃していた重要な情報を提供

フィッシングやその他の脅威などの最新の攻撃の多くがブラウザ経由で行われていることは、今やほとんどのセキュリティチームの共通認識です。先進的な攻撃者は組織内に足掛かりを構築するためのさまざまな方法を編み出し、ランサムウェアへの感染や機密情報の流出などを引き起こしています。

これらの攻撃の多くがブラウザから始まっていることが攻撃の根本原因を突き止めることを難しくしており、それがセキュリティチームやインシデント対応チームにとっての長年の課題でした。多くの調査担当者は、ネットワークセキュリティツールやセキュアWebゲートウェイ、その他のクラウドセキュリティプラットフォーム、EDR（Endpoint Detection and Response）ツールからの記録の分析、あるいはユーザーのデバイス自体の検査など、さまざまなツールとプロセスを駆使して実際のイベントの状況をまとめています。

これらのツールから得られるログは、特定の結論を示唆する場合もありますが、それらは曖昧であることも多く、確実な結論には至らない場合も少なくありません。確実な答えを得るために、対応チームは多くの場合、ダウンロードや認証情報の漏洩など、過去の特定のアクションに関する個人の記憶に頼らざるを得ません。数日または数週間前に発生したイベントを再現するために、メールやインタビューを通じてユーザーとやり取りする必要があるのです。このプロセスには時間がかかり、ただでさえ忙しいセキュリティチームにとって大きな負担となっています。それでも、漏洩の範囲や攻撃の背後にある動機については依然として不透明です。攻撃を開始したサイトは長期間存続しないよう設計されているため、脅威ハンターであっても追跡は非常に困難です。

セキュリティチームの54%が、セキュリティオペレーションにおける重要な課題として可視性を挙げています[1]

（調査）回答者の63%が、過去3年間で攻撃対象が拡大したと回答しました

（調査）回答者の51%が、過去12か月間に第三者によるデータ侵害やその他のセキュリティインシデントを経験したと回答しました

リスクとコンプライアンス活動を連携させていない**（調査対象）企業の84%**が、過去24ヶ月間にサプライチェーンの中断を経験しました

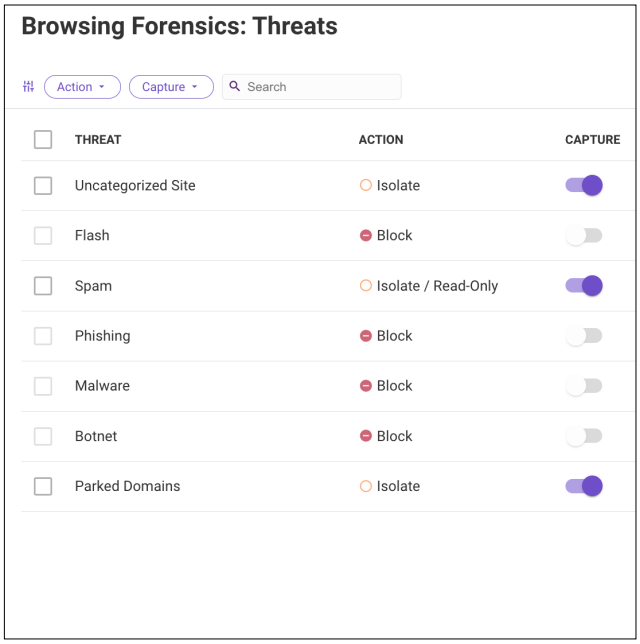
Menlo Secure Enterprise Browserソリューション

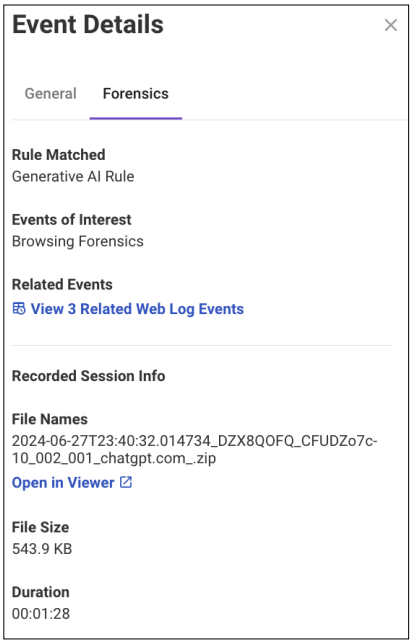
Menlo Secure Enterprise Browserソリューションは、問題解決のための最初の重要な一歩です。多くのメリットを提供しますが、ユーザーは使い慣れたブラウザを変更する必要はありません。Menlo Securityなら、管理対象でも対象外でも、すべてのブラウザをエンタープライズレベルの充分なセキュリティ対策が施された「セキュアエンタープライズブラウザ」に変えることができます。さらにBrowsing Forensicsが追加されたことで、これまでは取得できなかった重要な情報を収集できるようになりました。

Browsing Forensicsが必要な理由

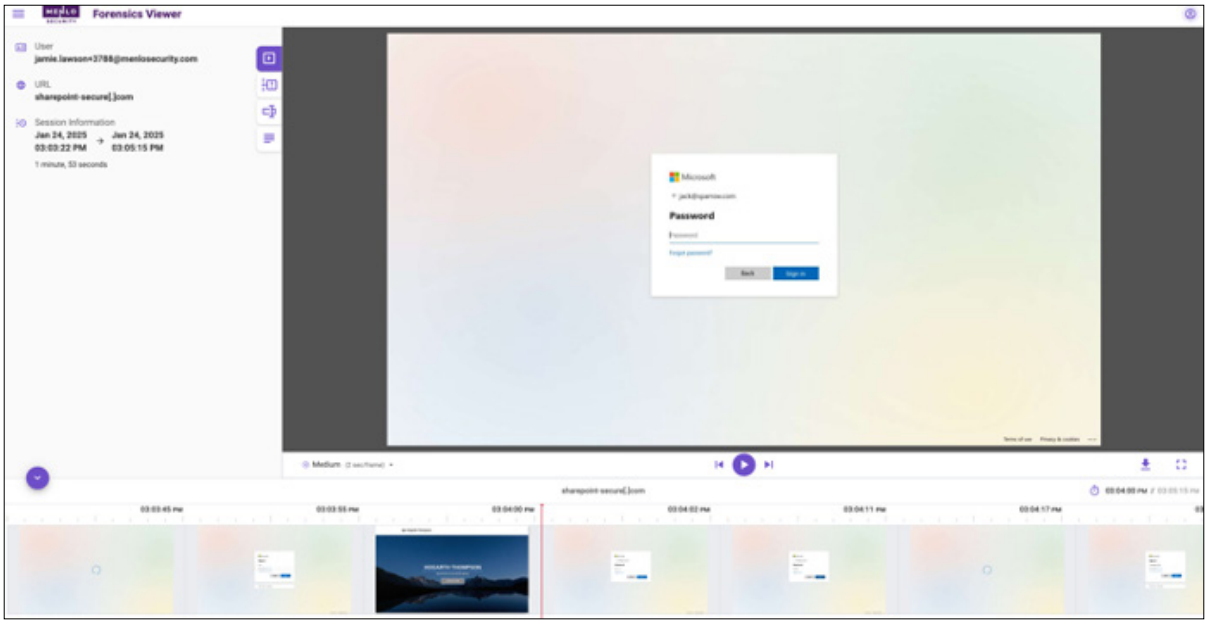
Menlo Securityが提供するBrowsing Forensicsは、ポリシーで定義されたブラウジングセッションをキャプチャし、セキュリティインシデントや監査/コンプライアンス問題、そしてその他のイベントを分析する担当者をサポートします。セッションをキャプチャする基準は、WebサイトのカテゴリーやSaaSアプリなど幅広く設定でき、Menlo Secure Application Accessと組み合わせることで、ドメイン、ユーザー、さらにはプライベートアプリケーションなどで絞り込むことができます。管理者はどのアプリケーションやサイト、ユーザーのアクションをキャプチャするかに加えて、セッション記録の一部としてキャプチャされるコンテンツを定義することができます。これには画面キャプチャ、ユーザー入力、ページリソースの詳細を記録するオプションが含まれており、調査目標やコンプライアンス要件を満たすことができます。これらのフォレンジックにより、チームはセキュリティ、監査/コンプライアンス、HR、その他のイベントを迅速かつ効率的に調査できます。

キャプチャされたセッションは、お客様が指定したクラウドストレージに安全に転送され、プライバシー、アクセス制御、安全性が確保されます。Browsing Forensicsは、AWSとAzureの両方のストレージオプションをサポートしており、Menlo Securityはこれらのロケーションへの書き込み専用のアクセスのみを行います。記録されたセッションには、イベントのサポートデータを含むBrowsing Forensicsログエントリが含まれており、記録にワンクリックでアクセスできます。この機能はMenlo logs APIを通じても利用でき、イベントアナリストはワンクリックで必要なコンテンツにアクセスできます。ログはほぼリアルタイムにAPIから利用できるため、調査ワークフローに組み込んで即座に利用できます。

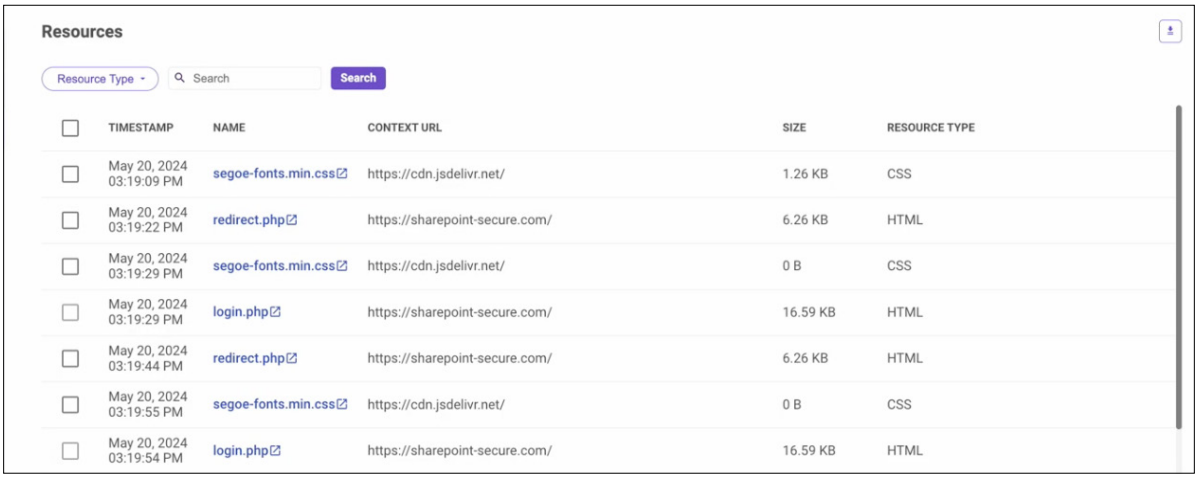




Browsing Forensics Viewerは、記録されたセッションのコンテンツを表示し、イベントを即座に可視化します。アナリストはこのビューアーを使用して効率的に調査を行い、イベントに関連する問題を解決したり、ユーザーの意図を推測したりできます。スクリーンショット、フォレンジックフロー、ユーザー入力、そしてページリソースのコンテンツを含むセッションの表示画面は、曖昧さを取り除いて高い精度を提供するため、確定的な調査を行うことが可能です。



Browsing Forensicsは、リソース自体に関する詳細情報も豊富に提供します。セキュリティチームは、JS、CSS、HTMLなどのリソースや、リソースのキャプチャ元のURLを即座に確認することができます。脅威ハンターは、リクエストとレスポンスを記録することでタイムリーに仕事を進めることができ、元のサイト自体が稼働を停止した場合でも、リソースは保持されます。



user-drawer-client-js-b5ea635a.js

```
import"./faceplate-switch-input-2b6f1293.js";import{_ as e,n as t,h as s,s as o,x as i}from"./icon-9159655c.js";import{bA as n,fc as r,$ as a,a0 as c,fd as d,
bB as l,fe as h,ff as p,fg as y,fh as m}from"./shell-5f065dde.js";import{u}from"./community-colors-563aae7f.js";import{D as f}from"./display-theme-7e251d41.
js";import"./checked-input-element-461606dd.js";import"./faceplate-input-1061e0c3.js";import"./input-element-93db3599.js";import"./form-common-utils-5eba1c1d.
js";import"./constants-3cb22c9a.js";let b=class extends o{constructor(){super(...arguments),this.enabled=!1,this.country=""}handler(e){e.preventDefault(),n
({country:this.country,name:r,value:this.enabled?"false":"true"}),window.location.reload()}render(){return i`<div @click="${this.handler}" @keypress="${this.
handler}">
  <slot></slot>
  </div>`}};e([t({type:Boolean})],b.prototype,"enabled",void 0),e([t({type:String})],b.prototype,"country",void 0),b=e([s("shreddit-modmode-setter")],b);let
  k=class extends o{constructor(){super(...arguments),this.enabled=!1,this.country="",this.cookieDomain="",this.sync=!1}async connectedCallback(){super.
  connectedCallback(),this.sync&&this.syncCookieToUserPreference()}async syncCookieToUserPreference(){try{const{data:e}=await a({operation:c.
  IdentityUserPreferences,variables:{includeNightMode:!0}}),t=e.identity?.preferences?.isNightModeE this: this ll==t)return;t!==this.enabled&&(this.enabled=t,
  this.updateClientStyles(),this.setCookie(),this.reportMismatch())}catch{}}setCookie(){n({country:this.country,name:d,value:this.enabled?f.Darkmode:f.
  Lightmode,options:{...l,domain:this.cookieDomain||void 0}})}async setUserPreference(){await a({operation:c.UpdateAccountPreferences,variables:{input:
  {isNightModeEnabled:this.enabled}}})}updateClientStyles(){u({isDarkMode:this.enabled});const e=this.querySelector("faceplate-switch-input");e&&(e.
  checked=this.enabled)}reportMismatch(){const e=h(this.country)&&!p(),t={cookies_enabled:navigator.cookieEnabled&&!e?"true":"false"};y({type:m.Counter,
  name:"shreddit_darkmode_preference_mismatches",value:1,labels:t})}async handler(e){e.preventDefault(),this.enabled=!this.enabled,this.updateClientStyles(),
  this.setCookie(),await this.setUserPreference()}handleKeypress(e){"Enter"!==e.key&&"Space"!==e.key||this.handler(e)}render(){return i`<div @click="${this.
  handler}" @keypress="${this.handleKeypress}">
  <community-colors></community-colors>
  <slot></slot>
  </div>`}};e([t({type:Boolean,reflect:!0})],k.prototype,"enabled",void 0),e([t({type:String})],k.prototype,"country",void 0),e([t({type:String,
  attribute:"cookie-domain"})],k.prototype,"cookieDomain",void 0),e([t({type:Boolean})],k.prototype,"sync",void 0),k=e([s("shreddit-darkmode-setter")],k);
//# sourceMappingURL=user-drawer-client-js-b5ea635a.js.map
```

推測を含まない、お客様が必要とする可視性を提供

インシデントの診断と解決のためにどれだけの時間がかかるのかは、非常に重要なポイントです。Browsing Forensicsをセキュリティワークフローに組み込むことは、時間の短縮と精度の向上に役立ち、最終的には外部に露出される期間を短縮し、よりよい成果をあげることができます。

また、Browsing Forensicsを使用してユーザーが機密データや新しいサイトとどのようにやり取りするかを観察することで、全体的なセキュリティレベルとITポリシーを簡単に改善することもできます。たとえば、生成AIサイトにアクセスするユーザーのセッションを記録しておけば、社内チームがユーザーに適切なアドバイスを提供できます。また、コントラクタやパートナー、その他のサードパーティによるアクセスを監視し、Secure Application Accessにより適切に制御することもできます。

Browsing Forensicsを使用することで、曖昧さのないデータに基づいてアクセスをカスタマイズし、攻撃の根本原因を突き止めるまでに必要な時間を短縮し、安全なアプリケーションアクセスを可能にし、コンプライアンスを維持（および実証）するなど、さまざまなことが可能になります。

これが、Menlo Browsing Forensicsです。人々の働き方を安全に守る方法について、詳しくはmenlosecurity.jpをご覧いただくか、japan@menlosecurity.comまでメールでお問い合わせください。

メンロ・セキュリティ・ジャパン株式会社
住所：〒100-0004 東京都千代田区大手町 1-6-1 大手町ビル 4F FINOLAB
Webサイト：https://www.menlosecurity.jp
お問い合わせ先：japan@menlosecurity.com