MENLO SECURITY

Browsing Forensics Executive Brief

Get the vital information that your security, incident response, and compliance/audit teams have been missing

By this time, most security teams are well aware of the fact that the browser has become ground zero for many of today's most powerful attacks, including phishing and other threats. Sophisticated attackers have discovered a myriad of ways to establish a beachhead in the enterprise, resulting in ransomware, loss of sensitive information, and more.

Finding the source of these attacks, which often begin in the browser, has eluded security and incident response teams for years. Typically, investigators have depended on a multitude of tools and processes to piece together the actual event's picture, which can involve analyzing records from network security tools, secure web gateways or other cloud security platforms, or endpoint detection and response (EDR) tools, as well as inspecting the user's device itself.

While the logs from these tools might suggest a likely conclusion, their results are often ambiguous. For firm answers, response teams often need to engage with users through email or interviews to reconstruct an event that may have occurred days or weeks earlier, relying on individuals' recollection of a single, specific action, such as a download or credential exposure. The entire process consumes time, demands focused attention from overwhelmed security teams, and still leaves a level of uncertainty regarding the exposure and the motives behind it. Threat hunters are presented with a similarly difficult job, as the sites from which an attack begins don't remain live for long, by design.

54% of security teams describe visibility as a key challenge in SecOps[1]

63% of (survey) respondents say the size of their attack surface has increased in the past three years[2]

51% of (survey) respondents said that they experienced a third-party data breach or other security incident in the last 12 months[3]

84% (of companies surveyed) who have not connected risk and compliance activities experienced a supply chain disruption in the last 24 months[4]

[1] https://swimlane.com/blog/top-soc-analyst-challenges/

[2] 2023 State of Threat Detection, Vectra AI

[3] https://www.prevalent.net/blog/2024-third-party-risk-management-study/

[4] https://hyperproof.io/it-compliance-benchmarks/

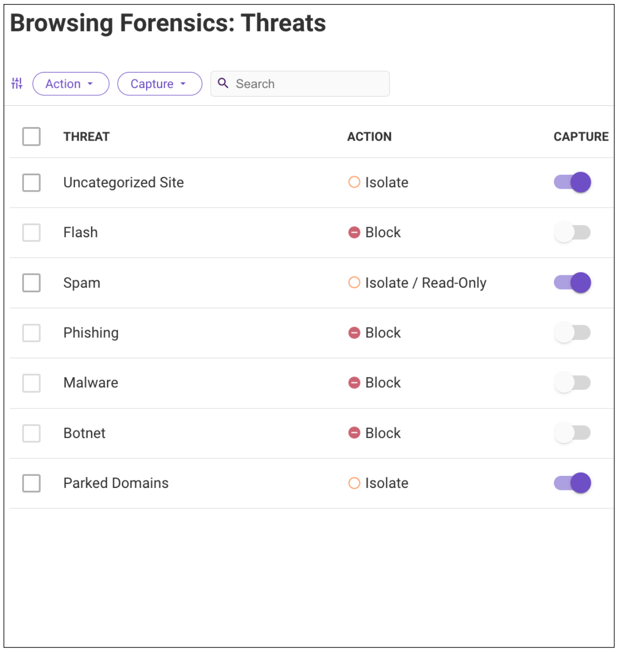
The Menlo Secure Enterprise Browser

The Secure Enterprise Browser, from Menlo Security, is a vital first step, providing a host of benefits without the need to change the browsers that your users know and love. Instead, with Menlo, you can make every browser, managed or unmanaged, into a Secure Enterprise Browser. And now, with the addition of Browsing Forensics, you can deliver vital information that has been beyond reach in the past.

Why Browsing Forensics?

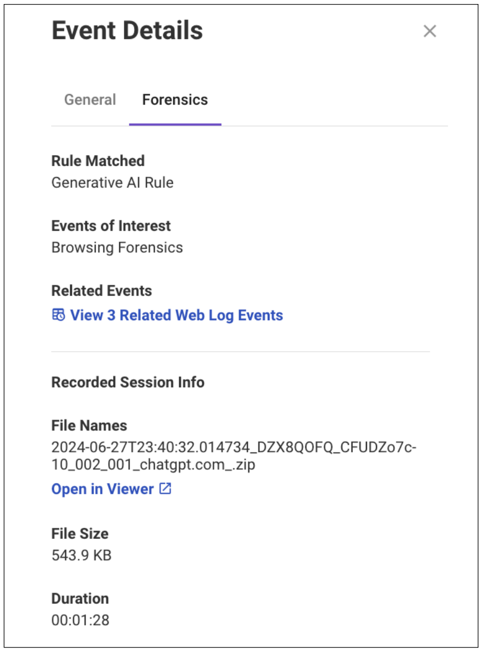
Browsing Forensics from Menlo Security captures policy-defined browser sessions to support investigators as they analyze security incidents, audit/compliance issues, and other events. Criteria to capture sessions can be broad, such as website categories or SaaS apps, and can be refined by domain, user, or even private applications. In addition to which application, site, or user actions are captured, the administrator can define what content is captured as part of the session recording. This includes the option to record screen captures, user inputs, and details of the page resources to meet investigatory goals and compliance requirements. These forensics empower teams to quickly and efficiently investigate security, audit/compliance, HR, and other events.

The captured sessions are then securely transferred to a cloud-storage location defined by the customer, ensuring privacy, access control, and safety. Browsing Forensics supports both AWS and Azure storage options, and Menlo has write-only access to these locations. Each captured session has a Browsing Forensics log entry containing supporting data from the event and providing convenient one-click access to the Browsing Forensics captures. This functionality is also available via the Menlo logs API, providing event analysts with access to necessary content with just one click. Logs are available from the API in near-real time, facilitating immediate consumption and incorporation into the investigatory workflow.



Browsing Forensics: Threats

□	THREAT	ACTION	CAPTURE
□	Uncategorized Site	○ Isolate	●
□	Flash	● Block	○
□	Spam	○ Isolate / Read-Only	●
□	Phishing	● Block	○
□	Malware	● Block	○
□	Botnet	● Block	○
□	Parked Domains	○ Isolate	●



Event Details

Rule Matched
Generative AI Rule

Events of Interest
Browsing Forensics

Related Events
View 3 Related Web Log Events

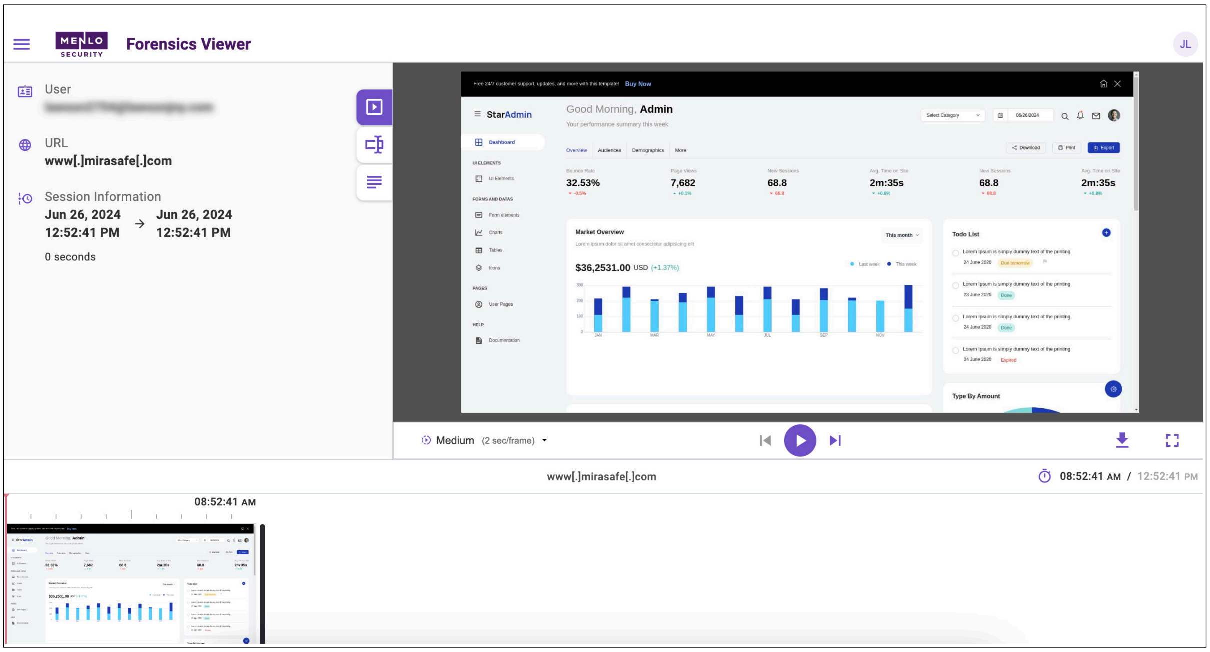
Recorded Session Info

File Names
2024-06-27T23:40:32.014734_DZX8QOFQ_CFUDZo7c-10_002_001_chatgpt.com_.zip
Open in Viewer

File Size
543.9 KB

Duration
00:01:28

The Browsing Forensics Viewer presents the content of the captured session, making it easy to immediately visualize the event. Analysts can use the viewer to efficiently conduct research and resolve issues surrounding events, as well as to infer user intent. Views of the session, including screenshots, user inputs, and page resource content, provide a high degree of accuracy, removing ambiguity and helping to ensure a conclusive investigation.



Forensics Viewer

User
[redacted]

URL
www[.]mirasafe[.]com

Session Information
Jun 26, 2024 12:52:41 PM → Jun 26, 2024 12:52:41 PM
0 seconds

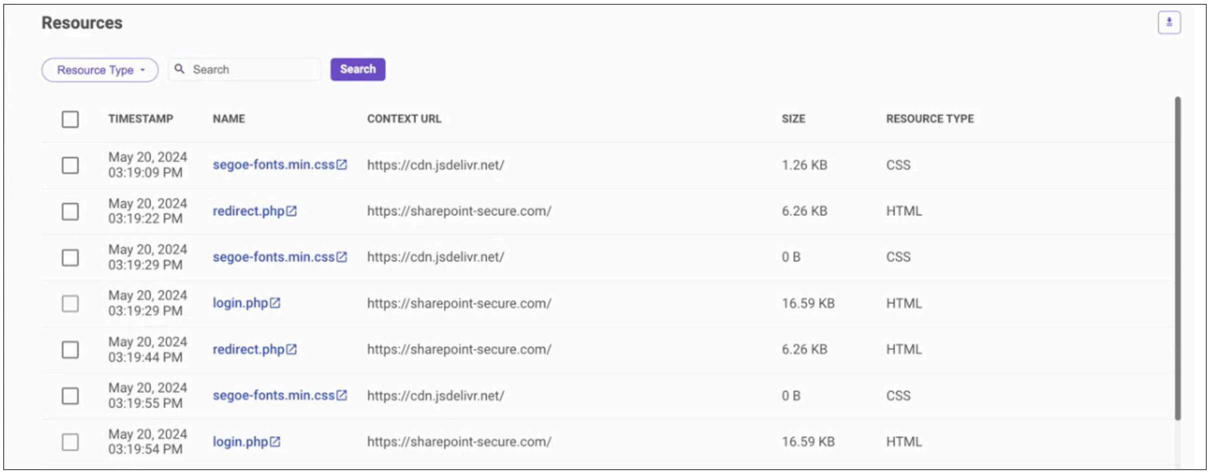
Medium (2 sec/frame)

www[.]mirasafe[.]com

08:52:41 AM / 12:52:41 PM

08:52:41 AM

Browsing Forensics also presents rich details about the resources themselves. Security teams can quickly see the recorded resources, including JS, CSS, and HTML, as well as the URL from which the resources were captured. Threat hunters can do their job in a timely fashion by capturing network requests and responses, and the resources are retained even if the site itself is no longer live.

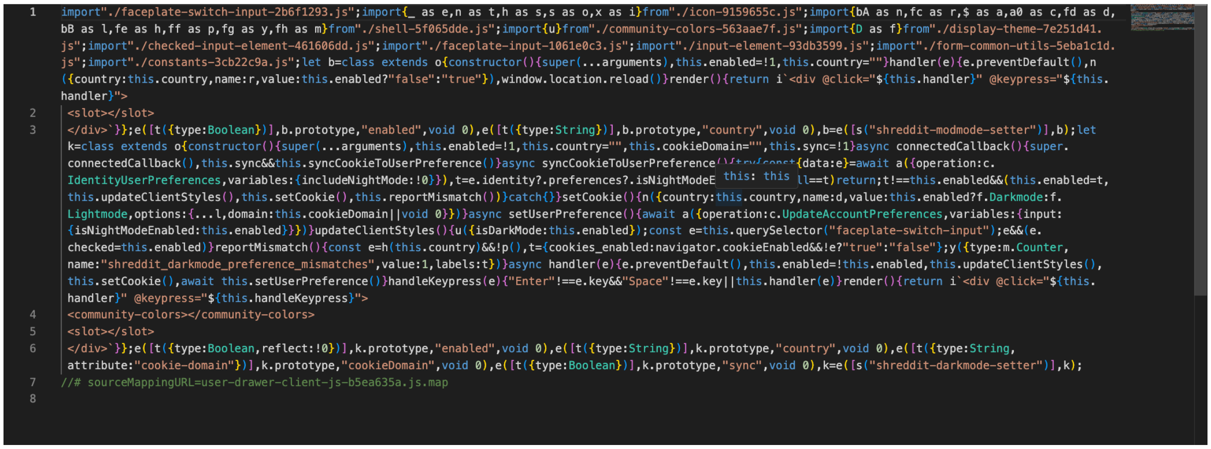


Resources

Resource Type ▾ | Search | Search

□	TIMESTAMP	NAME	CONTEXT URL	SIZE	RESOURCE TYPE
□	May 20, 2024 03:19:09 PM	segoe-fonts.min.css	https://cdn.jsdelivr.net/	1.26 KB	CSS
□	May 20, 2024 03:19:22 PM	redirect.php	https://sharepoint-secure.com/	6.26 KB	HTML
□	May 20, 2024 03:19:29 PM	segoe-fonts.min.css	https://cdn.jsdelivr.net/	0 B	CSS
□	May 20, 2024 03:19:29 PM	login.php	https://sharepoint-secure.com/	16.59 KB	HTML
□	May 20, 2024 03:19:44 PM	redirect.php	https://sharepoint-secure.com/	6.26 KB	HTML
□	May 20, 2024 03:19:55 PM	segoe-fonts.min.css	https://cdn.jsdelivr.net/	0 B	CSS
□	May 20, 2024 03:19:54 PM	login.php	https://sharepoint-secure.com/	16.59 KB	HTML

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
```

Menlo Security delivers the visibility you need without console swiveling or guesswork

The time it takes to diagnose and resolve an incident is critical. Incorporating Browsing Forensics into a security workflow plays a pivotal role in reducing time and enhancing accuracy, ultimately resulting in a shorter exposure window and improved outcomes.

Browsing Forensics also makes it simple to refine overall security and IT policy by observing how users interact with sensitive data or new sites. Session captures of users accessing GenAI sites, for example, can help internal teams deliver better advice to users. You will also be able to easily monitor access from contractors, partners, or other third parties, and enable appropriate controls with Secure Application Access.

With Browsing Forensics, you can custom tailor access based on non-ambiguous data, reduce the time needed to get to the root of an attack, enable secure application access, maintain (and demonstrate) compliance, and more.

Menlo Browsing Forensics. Now you know.

To learn more about securing the ways people work, visit menlosecurity.com or email us at ask@menlosecurity.com.

MENLO
SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

© 2024 Menlo Security, All Rights Reserved.