

CyberArk Labs Secure AI Agents Workshop – Privacy Policy

Last modified: 26.03.26

This Privacy Policy explains how information about you is collected, used, and disclosed by CyberArk Software Ltd. (a Palo Alto Networks Company) and its affiliated entities (“CyberArk”, “we”, “our”, or “us”) when you access or use the CyberArk Labs Secure AI Agents Workshop (the “Workshop”).

By accessing and registering the Workshop, you agree to the terms of this Privacy Policy. For more information about CyberArk data practices and safeguards, please review [CyberArk Privacy Notice](#).

1. Personal Information We Collect

The following information may be collected to enhance your participation in the Workshop:

Category	Data Elements	Purpose
Account Data	Identifiers such as full name, email address, self-selected username and password, and residency.	Enable sign-up, login, and participation in the Workshop
Team Association	Optional team association (internal instance only)	Internal organizational grouping
User Inputs	Prompts, exploit attempts, challenge solutions, and other text inputs	Enable participation in Workshop challenges and exercises
Technical Data	Browser type and version; operating system details; basic system configuration	Security, stability, and performance of the Workshop
Usage Analytics	Timestamps and challenge interactions; general usage analytics	Operational monitoring and performance optimization
Cookies (Strictly Necessary)	Session continuity cookies; load handling cookies; security cookies	Maintain session functionality, system reliability, and security

2. Use of Information

CyberArk shall use your personal information strictly for the following purposes:

- Provide and operate the Workshop
- Improve the workshop experience and challenge design

- Conduct cybersecurity and AI-safety research
- Support CyberArk's commercial defensive capabilities
- Detect, prevent, and investigate misuse of the Workshop
- To propose participants with related services and information we think you would find interesting.

CyberArk does **not** train commercial AI models using Workshop submissions unless such information is fully anonymized and aggregated for research or security purposes.

3. Sharing of Information

4. Legal Basis for Processing

For individuals in the EEA, UK, or Switzerland, CyberArk relies on:

- **Legitimate interests** – to operate and secure the Workshop, conduct research, improve features, and support the Workshop.
- **Legal obligations** – where applicable laws require processing.

5. International Data Transfers

Information may be processed in the United States, the EU, or other countries where CyberArk operates.

Where required, transfers are supported by **Standard Contractual Clauses** or other legally recognized safeguards.

6. Your Rights

Because CyberArk cannot identify participants from anonymized or pseudonymous data, we may not be able to fulfill certain requests (e.g., access, deletion) unless you provide additional context that allows us to locate your submissions.

If you believe that the information you submitted could indirectly identify you, you may request:

- Access the information we maintain within our control about you;
- Correction of any such information if you believe that it is inaccurate or missing;
- Deletion of all or some of your information. Note that deleting some of your information may prevent you from using the Workshop.
- Restriction or Objection of processing, in case you believe that there is no longer a legal basis for the processing of your information.

To submit a request, contact:

privacy-request@cyberark.com

For your own security, we may request additional information to identify you and ensure you're eligible for requesting the above requests with respect to your information, and help locate your data.

7. External Links

The Workshop may contain links to external websites or CyberArk corporate pages. These websites operate under their own privacy notices. CyberArk is not responsible for third-party practices.

8. Security

We maintain administrative, technical, and physical safeguards to protect information processed through the Workshop as specified in the [CyberArk Privacy Notice](#) including:

- **Encryption in transit and at rest**
Data is protected using industry-standard encryption mechanisms while transmitted between user devices and the Workshop, and while stored within CyberArk-controlled systems. This helps prevent unauthorized access or interception of data.
- **Access controls**
Access to systems processing Workshop data is restricted to authorized personnel only, based on role-based access controls and the principle of least privilege. Administrative access is logged and subject to periodic review.
- **Monitoring and intrusion prevention**
CyberArk employs continuous monitoring and automated security controls designed to detect, prevent, and respond to unauthorized access, misuse, or anomalous activity affecting the Workshop.
- **Vulnerability and risk management**
The Workshop is subject to ongoing security risk management processes, including vulnerability scanning, remediation, and regular security assessments, to identify and mitigate potential security risks in a timely manner.

9. Children

The Workshop is not intended for individuals under 18, and CyberArk does not knowingly collect information from children.

10. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The “Last modified” date above reflects the latest version. Any updates shall be effective as the date of publication.

Contact Us at privacy-request@cyberark.com