Exabeam Operational Hardening

Exabeam Security Management Platform - Version SMP 2020

Publication date October 30, 2020

Exabeam
1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We’d love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Community.
Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2020 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.
Table of Contents

1. Exabeam Hardening ................................................................................................................. 4
2. How To Enable Cross-Site Request Forgery Protection .............................................................. 5
3. How To Enable Cross-Origin Resource Sharing Protection ......................................................... 7
1. Exabeam Hardening

The Exabeam Security Management Platform (SMP) has enabled security features by default that provide stricter controls and data protection. Two examples of what Exabeam has built protection against include Cross-Site Request Forgery (CSRF) and Cross-Origin Resource Sharing (CORS). A default set of filters are defined and enabled in Exabeam configurations. This improves the default security of the environment for all Exabeam services.

For Exabeam SaaS deployments that use Exabeam Advanced Analytics as your Exabeam Cloud Connector identity provider (IdP), Exabeam will update Cloud Connector to v.2.5.86 or later.

No manual configuration is needed for deployments with the following versions or later, as these protections are enabled by default:

- Exabeam Advanced Analytics i53.6
- Exabeam Data Lake i34.6

**IMPORTANT**

This security enhancement has been enabled by default:

- Data Lake i34.6 and i35
- Advanced Analytics i53.6 and i54.5

It is not enabled by default in:

- Data Lake i33 or earlier
- Advanced Analytics i52 or earlier

Please follow the hardening guidelines. At the earliest opportunity, please upgrade to a currently supported version of Advanced Analytics and Data Lake.
2. How to Enable Cross-Site Request Forgery Protection

Cross-Site Request Forgery (CSRF) attacks are web-based vulnerabilities where attackers trick users with trusted credentials to commit unintended malicious actions. CSRF attacks change the states of their targets rather than steal data. Examples include changing account emails and changing passwords.

CSRF protection is available for Exabeam Advanced Analytics and Data Lake and previously inactive. Older versions of Advanced Analytics and Data Lake may manually harden or upgrade to a hardened supported version (Advanced Analytics i53.6 or later and Data Lake i34.6 or later) to enable the security configuration by default.

For information about enabled versions, see Exabeam Hardening.

These protections may affect API calls to the Exabeam SMP; please review customs scripts and APIs used by your organization. Please follow instructions given in Step 1c to conform your scripts.

To enable CSRF protection, apply the following:

1. For all deployments, the `/opt/exabeam/config/common/web/custom/application.conf` file at each master host needs to be configured to enable CSRF protection at service startup.
   a. Edit the following parameters in the CONF file:

   ```
   csrf.enabled=true
   csrf.cookie.secure=true
   csrf.cookie.name="CSRF_TOKEN"
   ```

   b. Restart `web-common` to enable CSRF protection.

   ```
   . /opt/exabeam/bin/shell-environment.bash
   web-common-restart
   ```

   **NOTE**
   Log ingestion will not be interrupted during the restart. `web-common` can take up to 1 minute to resume services.

   c. API calls to Exabeam that utilize POST requests using types `application/x-www-form-urlencoded`, `multipart/form-data` and `text/plain` are affected by CSRF configurations. Ensure API clients have headers that has Csrf-Token set to value nocheck. Continue with the next step.

2. For Advanced Analytics using Case Manager or Incident Responder, edit `/opt/exabeam/code/soar-python-action-engine/soar/integrations/exabeamaa/connector.py`.
   a. Find the entry `self._session = SoarSession(base_url=apiurl, timeout=timeout, verify=False)` and replace with:

   ```
   self._session = SoarSession(base_url=apiurl, timeout=timeout, verify=False, headers={'Csrf-Token': 'nocheck'})
   ```
b. Restart services.

```
sudo systemctl restart exabeam-soar-python-action-engine-web-server
sudo systemctl restart exabeam-soar-python-action-engine
```

3. If SAML is configured, the IdP’s domain needs to be explicitly added to the CORS origins and then apply the new configuration. Please follow steps given in How to Enable Cross-Origin Resource Sharing Protection.
3. How to Enable Cross-Origin Resource Sharing Protection

Cross-Origin Resource Sharing (CORS) is a browser standard which allows for the resources or functionality of a web application to be accessed by other web pages originating from a different domain. CORS protection is available for Exabeam Advanced Analytics and Data Lake and enabled by default in Data Lake i34.6 or Advanced Analytics i53.6 and later versions. Older versions of Advanced Analytics and Data Lake may manually harden or upgrade to a hardened supported version (Advanced Analytics i53.6 or later and Data Lake i34.6 or later) to enable the security configuration by default.

For information about enabled versions, see Exabeam Hardening.

To manually enable CORS protection when it is not enabled by default, apply the following:

1. For all deployments, the /opt/exabeam/config/common/web/custom/application.conf file at each master host needs to be configured to enable CORS protection at service startup. Edit webcommon.service.origins parameter the CONF file to match your Exabeam service domain:

   ```
   webcommon.service.origins = ["https://*.exabeam.<your_organization>.com:<listener_port>",
    <...additional_origins...>]
   ```

   Here’s an example with 2 service origins:

   ```
   webcommon.service.origins = ["https://*.exabeam.org-name.com", "https://*.exabeam.org-name.com:8484"]
   ```

2. Restart web-common to enable CORS protection.

   ```
   . /opt/exabeam/bin/shell-environment.bash
   web-common-restart
   ```

   **NOTE**
   Log ingestion will not be interrupted during the restart. `web-common` can take up to 1 minute to resume services.