

CloudSOC™ Tech Note

GitHub
Securlet

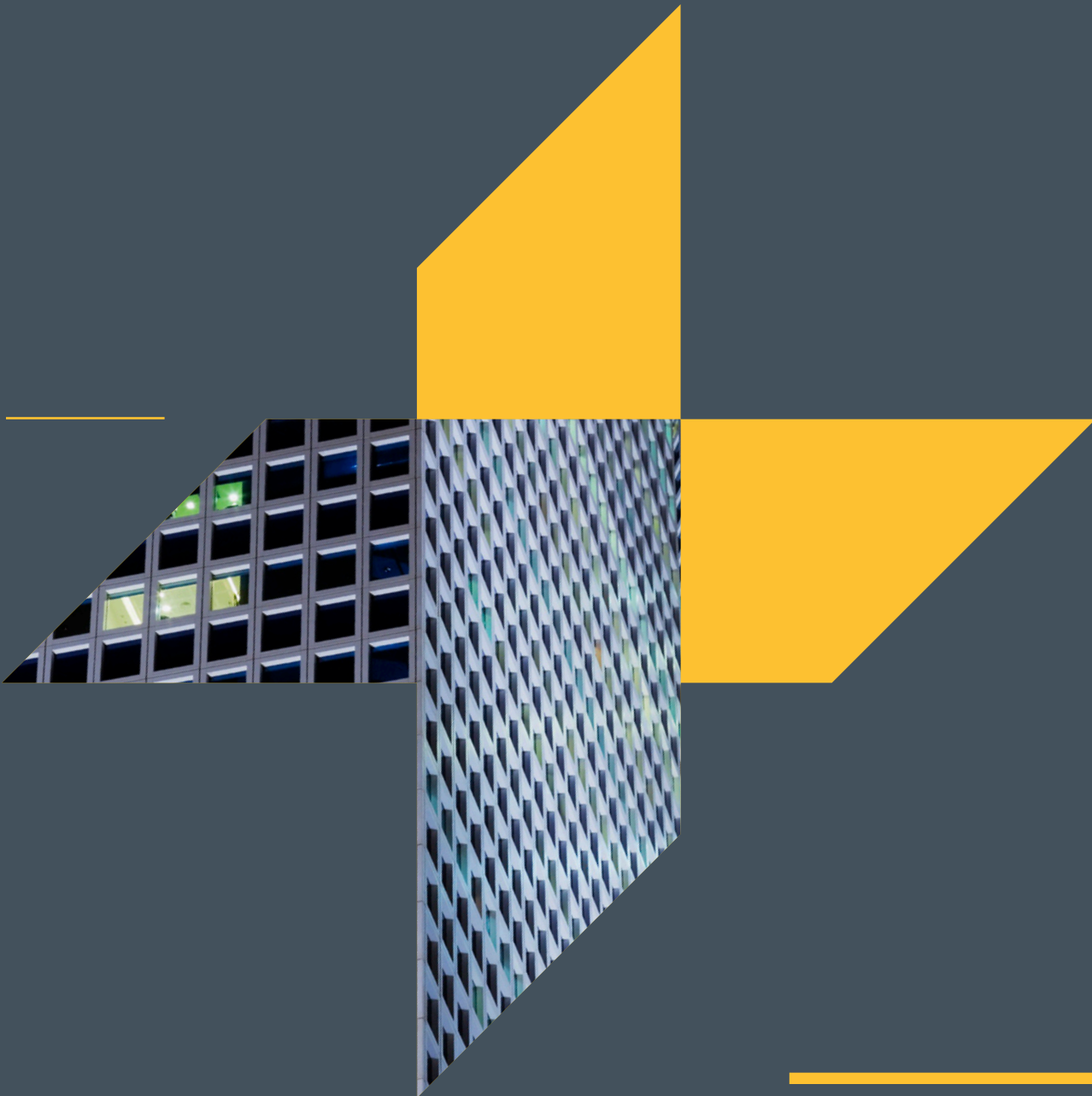


Table of Contents

[Introduction](#)

[Prerequisites](#)

[Enabling the GitHub Securlet](#)

[Activating additional GitHub accounts](#)

[Using the GitHub Securlet dashboard](#)

[Common activation issues](#)

[Securlet halt cases](#)

[Supported activities](#)

[Revision history](#)

Introduction

This tech note describes how to set up the GitHub Securlet™ on CloudSOC™.

The GitHub Securlet:

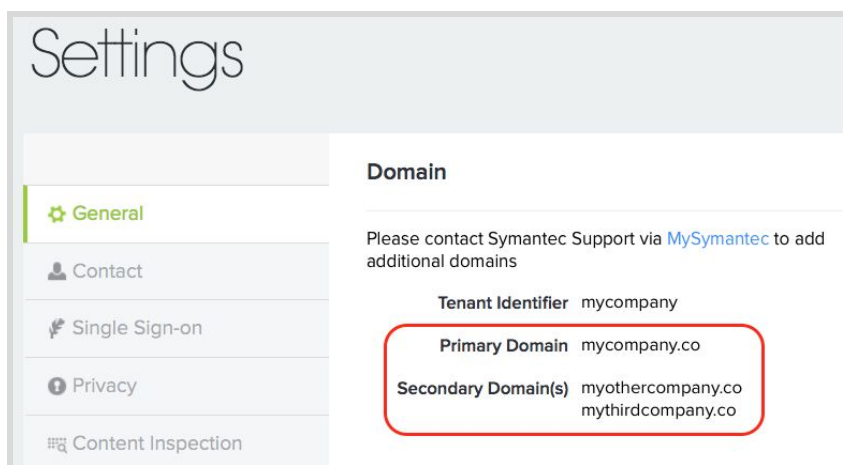
- Imports your organization's users from GitHub.
- Imports GitHub user activity data for investigation and forensics purposes

Note: Unlike some other CloudSOC Securlets, the GitHub Securlet does not let you create Access Monitoring via Securlets or Data Exposure via Securlets policies for GitHub in the CloudSOC Protect app.

Prerequisites

To activate the GitHub Securlet on your CloudSOC account:

- You must have Administrator privilege on your CloudSOC account.
- You must have Administrator privilege on your GitHub organization.
- You must have membership in your organization's Owners team at GitHub
- The email address you use as the username for the administrator login on your GitHub account must be exactly the same as the email address that you use as your CloudSOC username. Furthermore, this email address must be within the primary or secondary domains listed for your CloudSOC account. To confirm, login to CloudSOC, choose **<username>** > **Settings** > **General**, and check your domains as shown below.

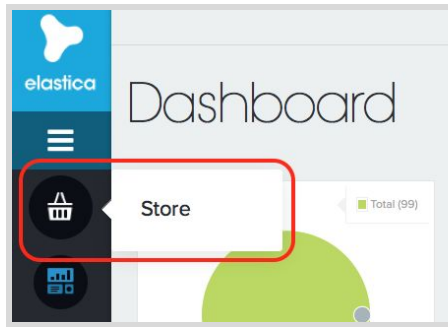


If necessary, contact Symantec Support via MySymantec to add additional secondary domains.

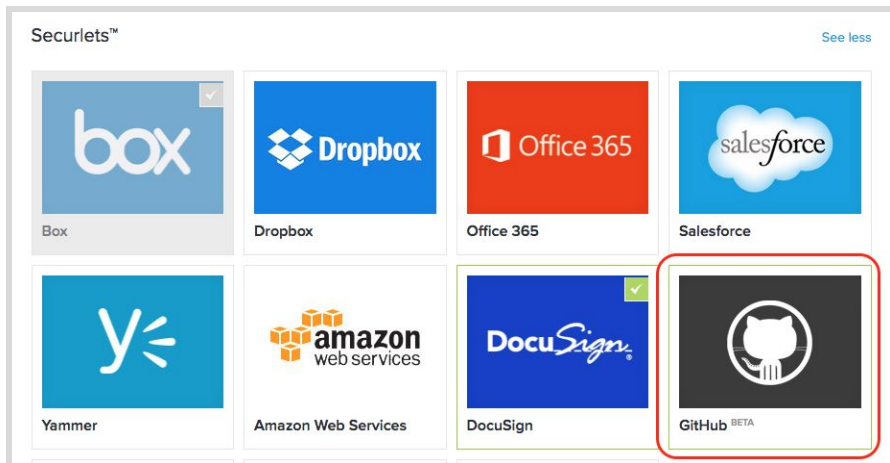
Enabling the GitHub Securlet

This section describes how to enable the GitHub Securlet for a single GitHub account.

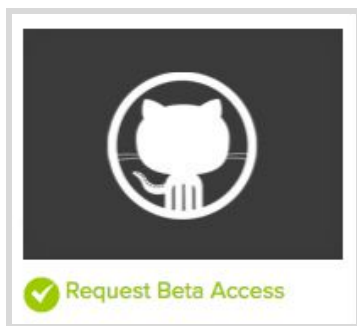
1. Login to CloudSOC using your administrator credentials.
2. Open the CloudSOC Store by clicking **Store** on the left side navigation bar.



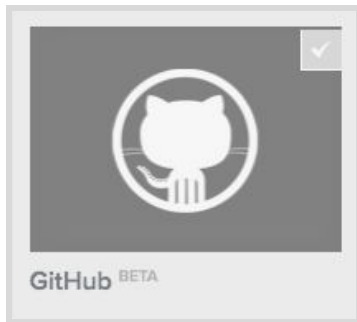
3. In the Store, scroll down to the Securlets area and click **See More**. Then locate the tile for the GitHub Securlet as shown below.



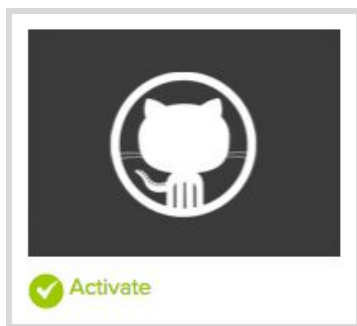
4. On the tile for GitHub, click **Request Beta Access**.



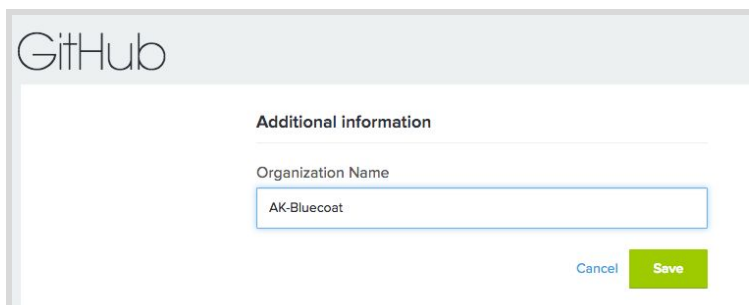
CloudSOC sends an activation request to the CloudSOC team for the GitHub Securlet. CloudSOC disables (grays out) the tile while your activation request is pending.



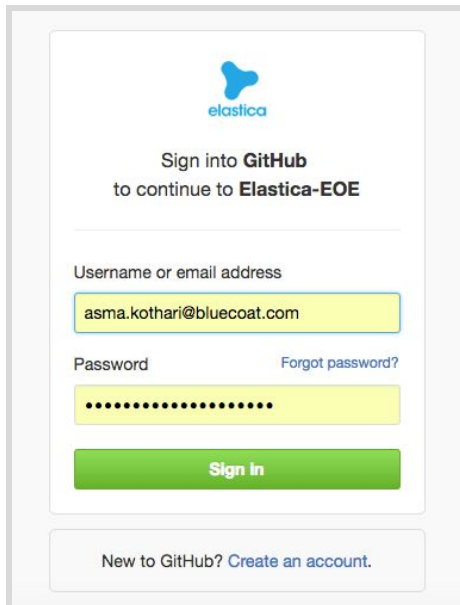
When the CloudSOC team approves the activation request, CloudSOC activates the tile and changes the button label to **Activate** as shown below. During weekday business hours Pacific time, activation usually takes a minute. Contact Symantec Support via MySymantec if the activation takes unusually long.



5. Click **Activate**. CloudSOC prompts you to provide your Organization Name at GitHub.
6. Enter your organization name at GitHub and click **Save** as shown below.

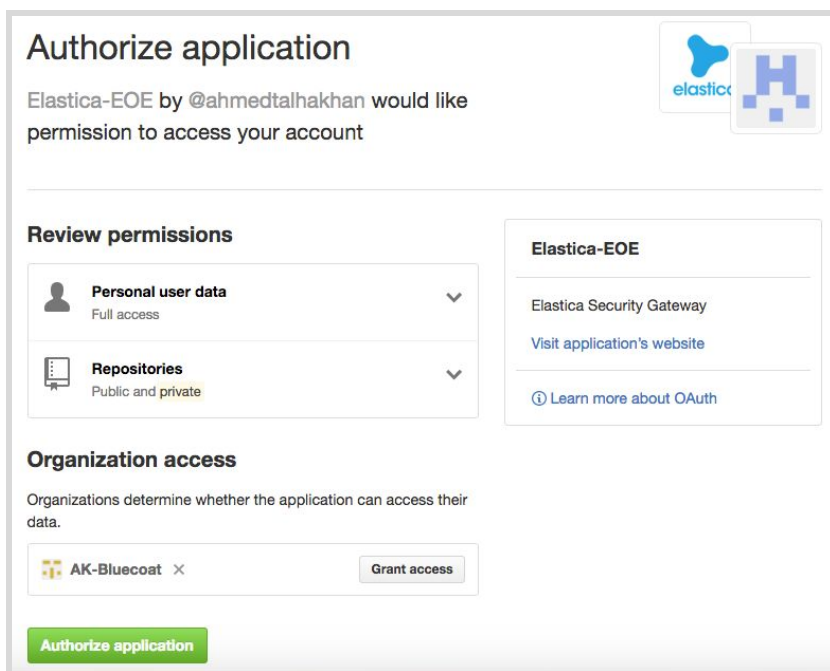
A screenshot of a GitHub web form. At the top left is the GitHub logo. Below it is a section titled "Additional information". Under this section is a label "Organization Name" followed by a text input field. The input field contains the text "AK-Bluecoat". At the bottom right of the form are two buttons: "Cancel" and "Save".

7. If you are not already logged in to your GitHub account, CloudSOC redirects you to the GitHub login page. Login to your GitHub Account as shown below.



The image shows a GitHub login page. At the top, the Elastica logo is displayed. Below it, the text reads "Sign into GitHub to continue to Elastica-EOE". There are two input fields: "Username or email address" with the value "asma.kothari@bluecoat.com" and "Password" with masked characters. A "Forgot password?" link is next to the password field. A green "Sign in" button is below the fields. At the bottom, there is a link "New to GitHub? Create an account."

GitHub opens the Authorize Application window as shown below.



The image shows the GitHub "Authorize application" window. At the top, it says "Elastica-EOE by @ahmedtalhahkhan would like permission to access your account". Below this, there are two sections: "Review permissions" and "Organization access".

Review permissions

- Personal user data**: Full access
- Repositories**: Public and private

Organization access

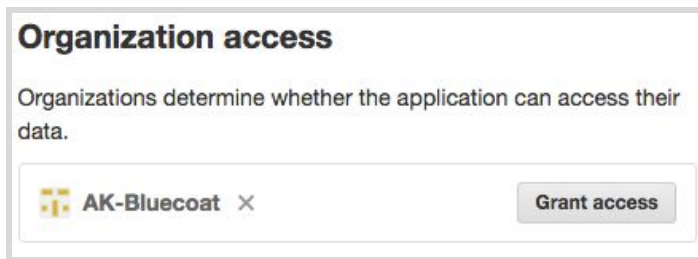
Organizations determine whether the application can access their data.

AK-Bluecoat × Grant access

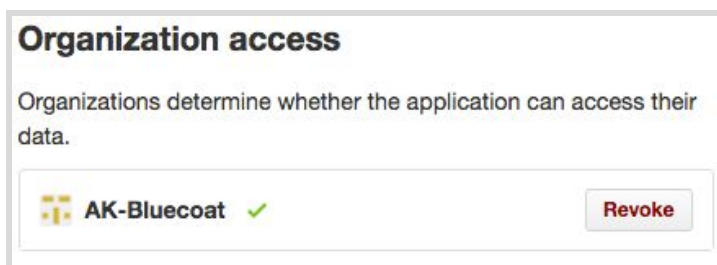
At the bottom, there is a green "Authorize application" button.

On the right side, there is a sidebar for "Elastica-EOE" with links: "Elastica Security Gateway", "Visit application's website", and "Learn more about OAuth".

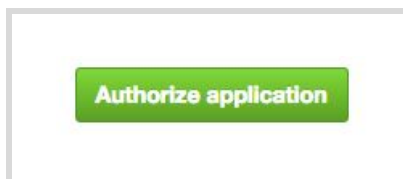
- Review permissions required by the Securlet and click **Grant Access** for your organization.



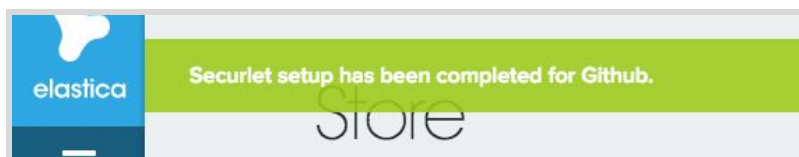
GitHub shows you a green check next to your organization name once you have granted access.



- Click **Authorize Application**.



You are redirected back to the CloudSOC Store page, where CloudSOC displays the green banner shown below.

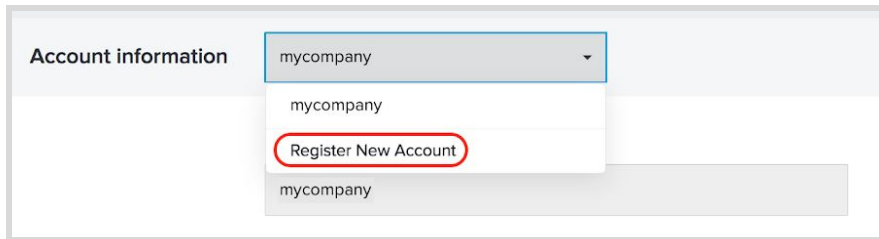


You have completed the Securlet setup for GitHub. CloudSOC starts scanning your GitHub resources.

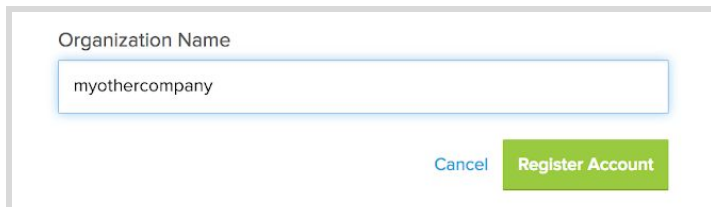
Activating additional GitHub accounts

The Github Securlet supports multiple Github accounts. To add an additional Github account after activating the Securlet:

1. In the CloudSOC Store, navigate to the Securlets area, and on the GitHub tile click **Configure**.
2. From the Account Information menu, choose **Register New Account** as shown below.

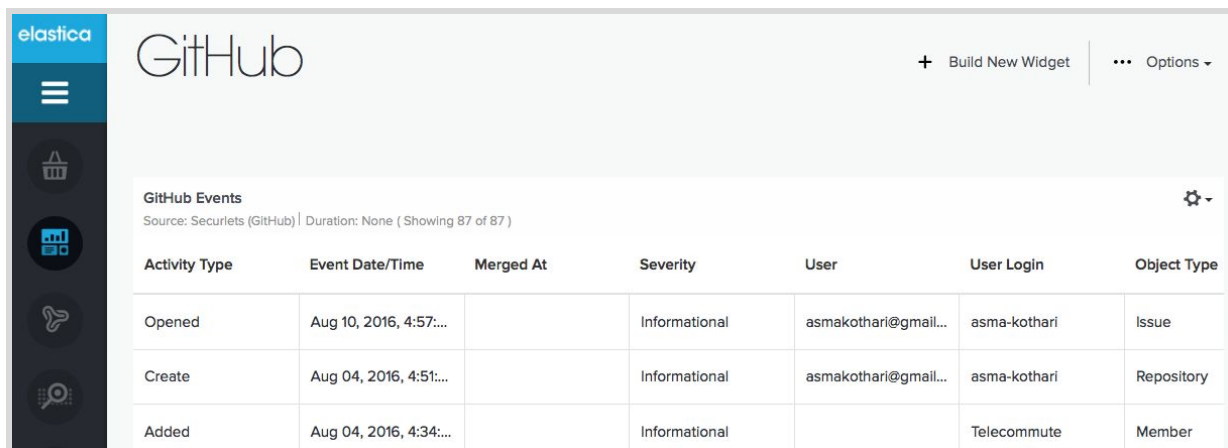


3. Enter the new account information and click **Register Account**.

A screenshot of a web form. It features a text input field labeled 'Organization Name' with the text 'myothercompany' entered. Below the input field are two buttons: a blue 'Cancel' button and a green 'Register Account' button.

Using the GitHub Securlet dashboard

The GitHub Securlet has a customizable dashboard that shows you metrics for your GitHub account. The default dashboard is a table showing raw data for all GitHub events as shown below. To open the dashboard, in CloudSOC choose **Securlet > GitHub**.



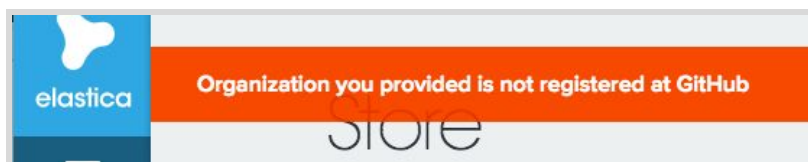
| Activity Type | Event Date/Time | Merged At | Severity | User | User Login | Object Type |
|---------------|------------------------|-----------|---------------|----------------------|--------------|-------------|
| Opened | Aug 10, 2016, 4:57:... | | Informational | asmakothari@gmail... | asma-kothari | Issue |
| Create | Aug 04, 2016, 4:51:... | | Informational | asmakothari@gmail... | asma-kothari | Repository |
| Added | Aug 04, 2016, 4:34:... | | Informational | | Telecommute | Member |

You can customize the dashboard by adding up to 12 pre-defined and custom widgets as described in the CloudSOC Tech Note *Customizing CloudSOC Dashboards*.

Common activation issues

This section describes how CloudSOC responds to the common failures while enabling the securlet for GitHub and how to address them.

- CloudSOC responds with a banner reading **INVALID ORGANIZATION: Organization you provided is not registered at GitHub** as shown below



Try reactivating the securlet with the correct name of organization registered at GitHub.

- CloudSOC responds with a banner reading **ORGANIZATION ACCESS REQUIRED: Please grant access to your organization** as shown below.

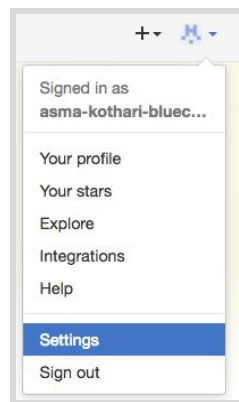


This issue might be have either of two causes:

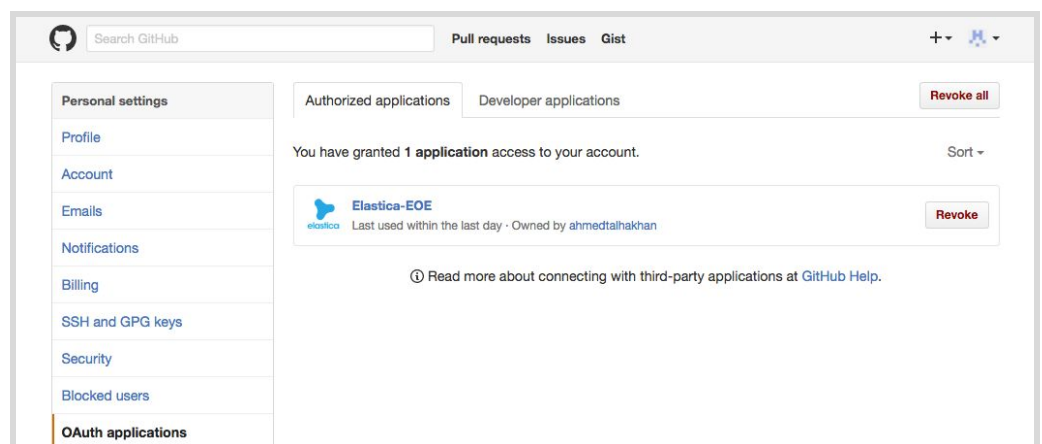
- **You granted access, but did not manage it as described in step #9.**

Follow these steps to address the problem:

1. Go to your GitHub account **settings**.

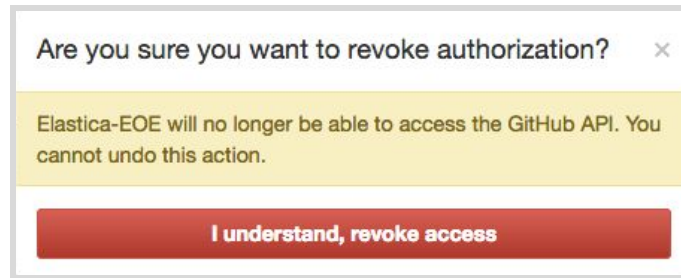


2. Navigate to **OAuth Applications**.



3. On the entry for the Securlet, click **Revoke**.

4. Click **I Understand, revoke access** as shown below.



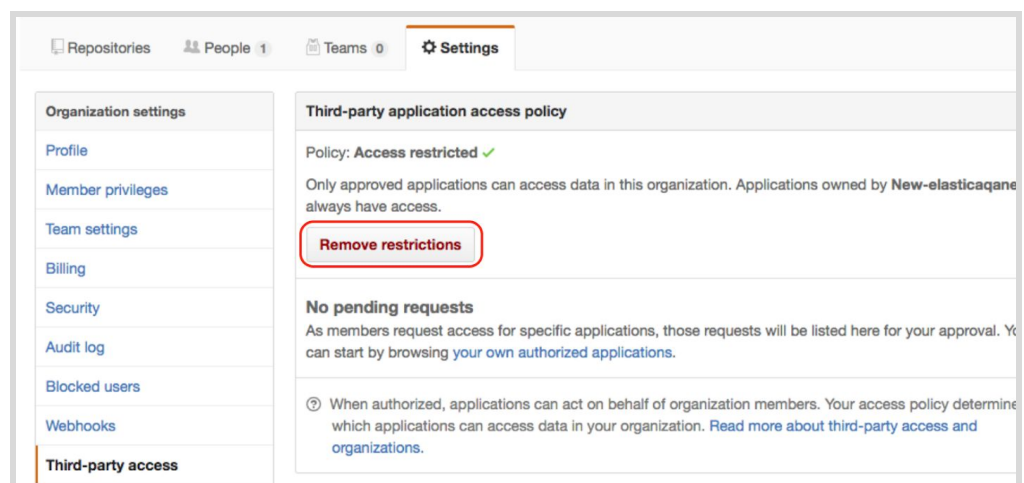
5. Go back to CloudSOC and repeat the procedure in [Enabling the GitHub Securlet](#).

In that procedure, take care to grant access to your organization before you authorize the Securlet application.

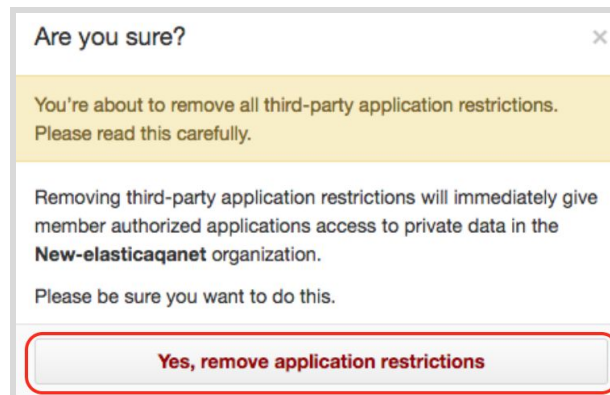
- **You are enabling CloudSOC on an additional GitHub account.**

Follow these steps to address the problem:

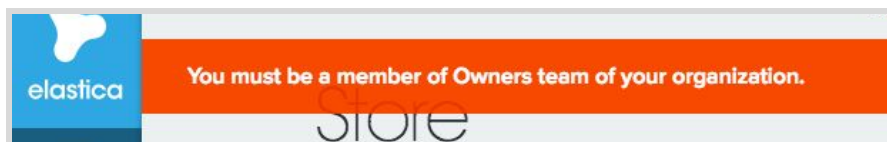
1. In your company's GitHub account, navigate to **Settings > Third-party access** and click **Remove Restrictions** as shown below.



2. When GitHub prompts you to confirm, click **Yes, remove application restrictions** as shown below.



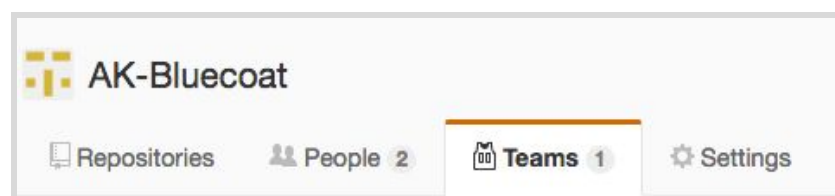
3. Go back to the section [Activating additional GitHub accounts](#) and repeat the activation procedure.
- CloudSOC responds with a banner that reads "**You must be a member of Owners team of your organization**" as shown below.



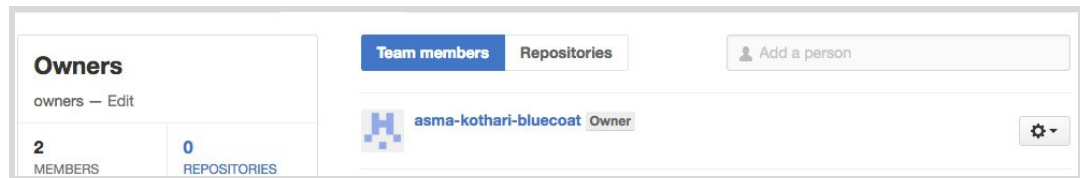
You probably tried to activate the securlet without having membership in your organization's Owners team, and you do not have administrative rights for the organization.

If you are an admin for your organization, follow this procedure to make yourself a member of the Owners team and then reactivate the securlet:

1. Go to **teams** of your organization.



2. Add yourself to the **Owners** team if you are not a member of it.

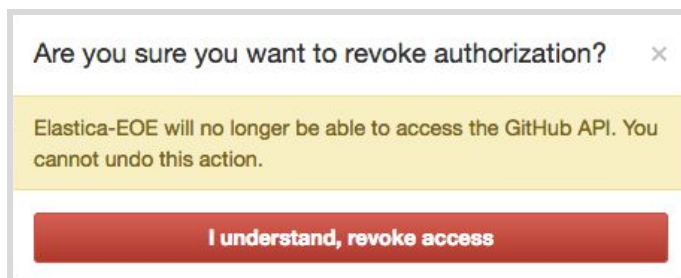


3. Go back to CloudSOC and follow the steps for [Enabling the GitHub Securlet](#).

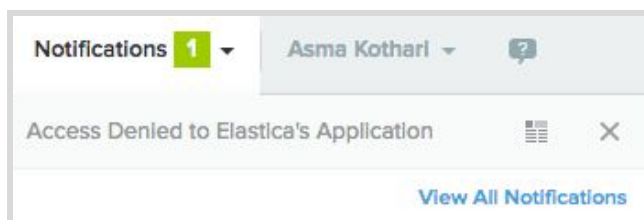
Securlet halt cases

This section describes how CloudSOC responds to the common errors for an enabled securlet.

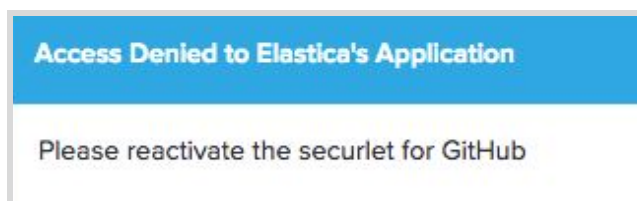
- Revoking access to the Securlet application halts the securlet for GitHub.



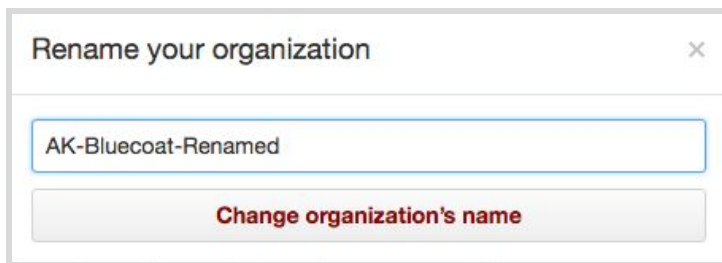
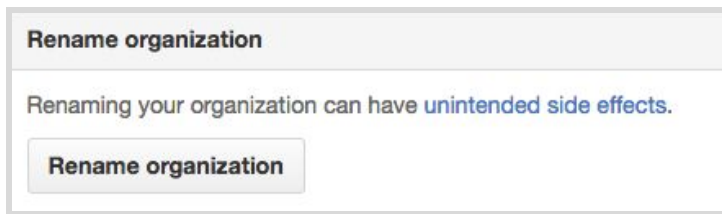
CloudSOC notifies you as shown below with the message "**Access Denied to Elastica's Application.**"



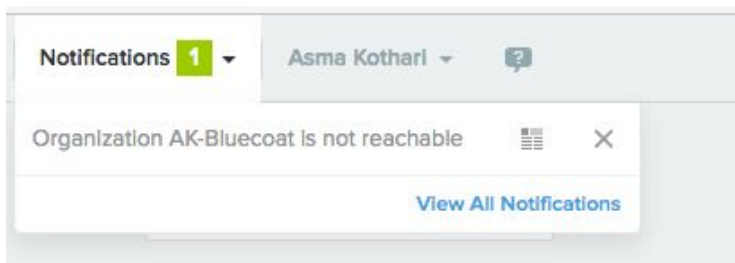
Details of the notification direct you to **reactivate the securlet**.



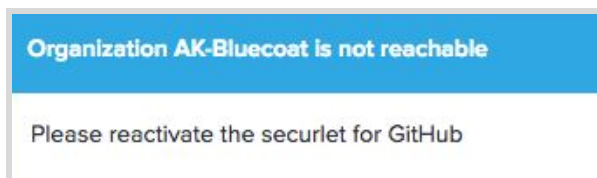
- Renaming your organization at GitHub halts the securlet.



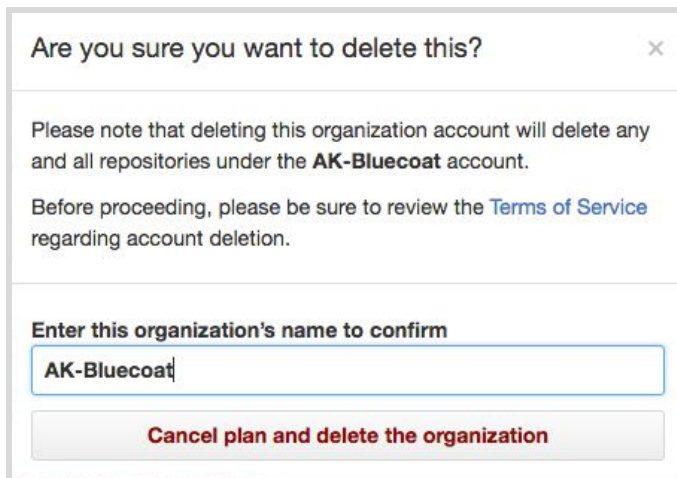
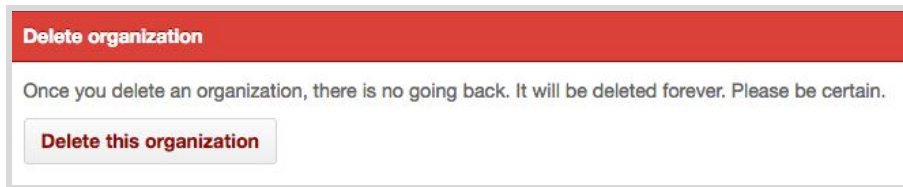
CloudSOC notifies you that the organization is not reachable as shown below.



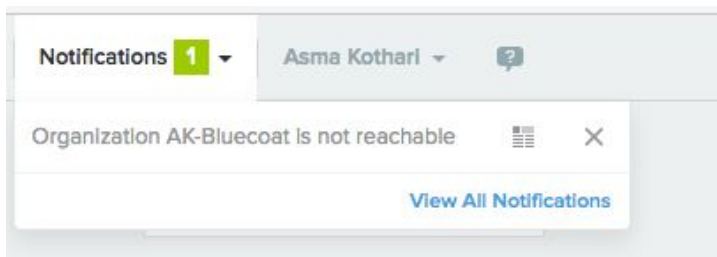
Details of the notification direct you to reactivate the securlet as shown below.



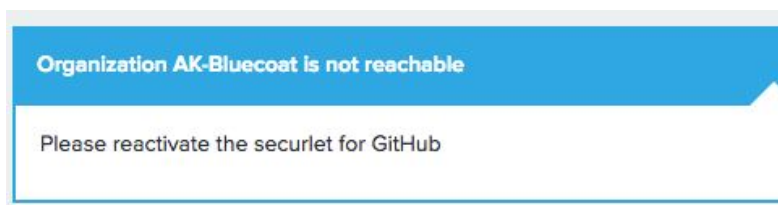
- Deleting your organization from GitHub halts the securlet.



CloudSOC notifies you that the organization is not reachable as shown below.



Details of the notification direct you to reactivate the securlet for the organization at GitHub.



Supported activities

The following table lists all of the objects and activities that are tracked by the GitHub Securlet.

| Object | Activity |
|---------------|---|
| Branch | Create |
| | Delete |
| Commit | Push |
| Issue | Assigned (Does not appear as a separate event, updated assignees appear in the next event of issue) |
| | Closed |
| | Edited |
| | Labeled (Does not appear as a separate event, updated labels appear in the next event of issue) |
| | Opened |
| | Reopened |
| | Unassigned (Does not appear as a separate event, updated assignees appear in the next event of issue) |
| | Unlabeled (Does not appear as a separate event, updated labels appear in the next event of issue) |
| Issue Comment | Create |
| | Delete |
| Member | Added (to repository) |
| Page | Build |
| Pull Request | Assigned (Does not appear as a separate event, updated assignees appear in the next event of issue) |
| | Closed (Without Merging) |
| | Edited |
| | Merged & Closed |
| | Opened |
| | Reopened |
| | Unassigned (Does not appear as a separate event, updated assignees appear in the next event of issue) |

| Object | Activity |
|--------|----------|
|--------|----------|

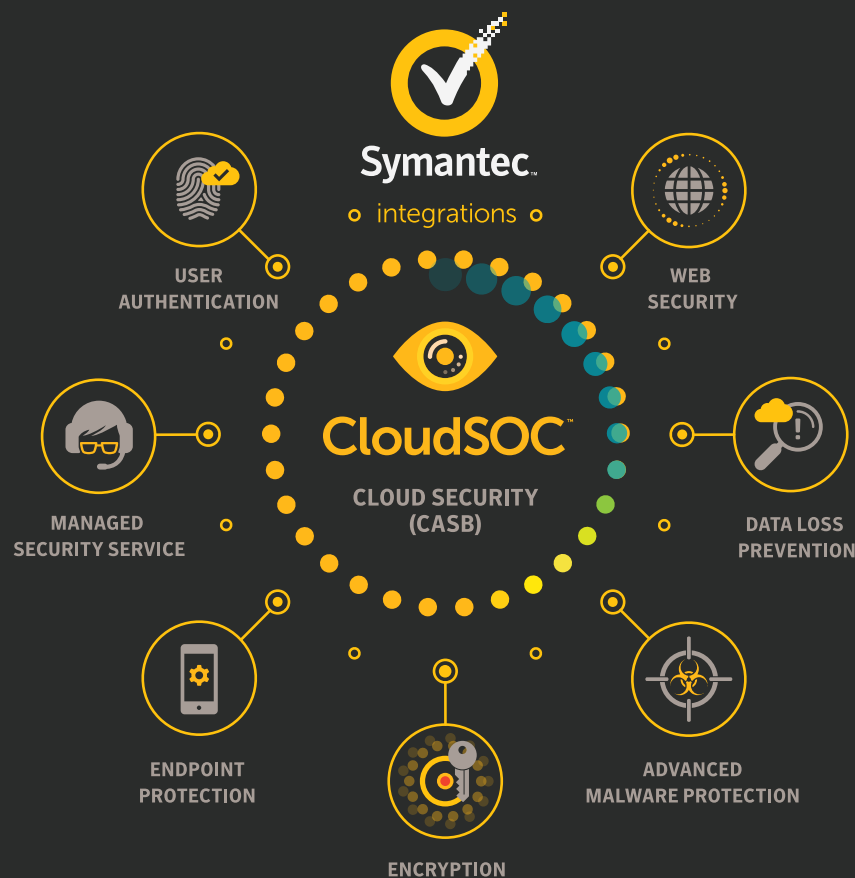
| | |
|-------------------------|-----------------|
| Pull Request Comment | Create |
| | Delete |
| Release | Publish |
| Repository | Create |
| | Delete |
| | Deploy |
| | Fork |
| | Privatize |
| | Publicize |
| | Watch (Starred) |
| Tag | Create |
| | Delete |
| Wiki Page | Create |
| | Update |

Revision history

| Date | Version | Description |
|-----------------|---------|---|
| 29 August 2016 | 1.0 | Initial release |
| 13 September | 1.1 | Minor changes |
| 9 November 2016 | 2.0 | Address multi-account support, new objects and activities, Add admin login domain prerequisite |
| 9 March 2017 | 3.0 | Address Securlet Dashboard |
| 16 March 2017 | 3.1 | Add note about Protect policies |
| 12 June 2017 | 3.2 | Add admin login email prerequisite |
| 23 June 2017 | 3.3 | Clarify prerequisites |
| 17 May 2018 | 3.4 | Minor changes and formatting updates |
| 23 May 2018 | 3.5 | Update support references |

Get better security with less complexity

Deploy an enterprise security system that integrates with your existing web, endpoint, data center, user, and information security solutions, and avoid the complexity and challenges of managing a standalone cloud solution. A Symantec security system with CloudSOC makes deployment easier, allows you to share policies and intelligence across solutions, and enables a user-centric and information-centric approach to security.



For more info on Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems, visit go.symantec.com/casb



symantec.com +1 650-527-8000

About CloudSOC

Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against data loss and compliance violations, and investigation of historical account activity for post-incident analysis.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.