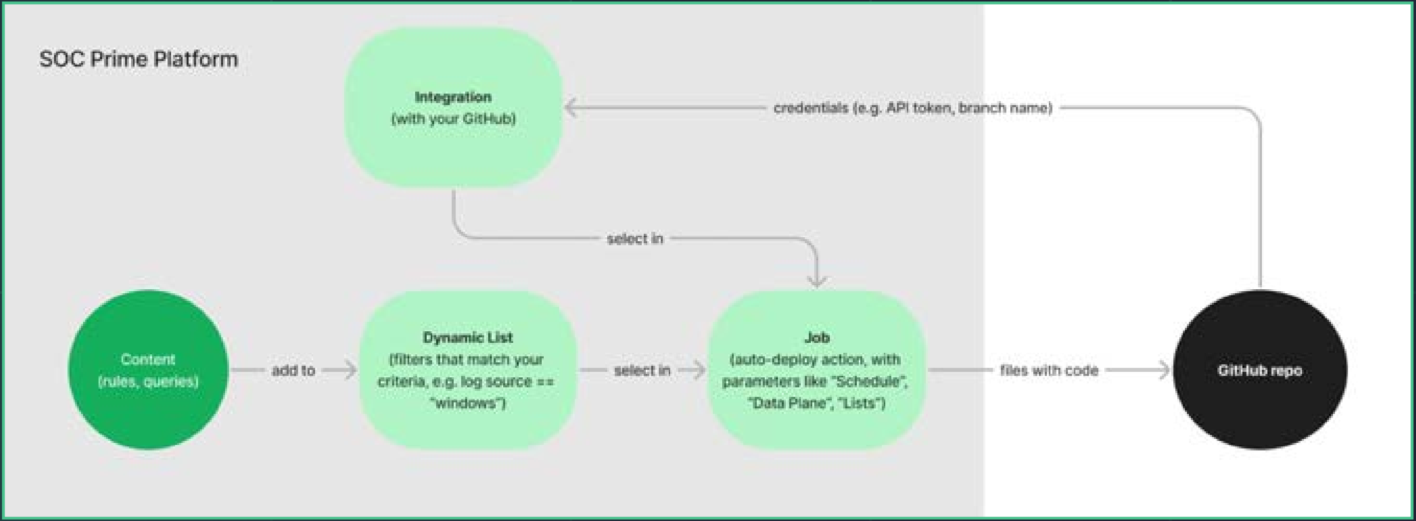
SOC PRIME

Stream Detection Content from SOC Prime Platform to Your Private GitHub Repository

You can continuously push detection content from the SOC Prime Platform to a GitHub repository.

On SOC Prime Platform:

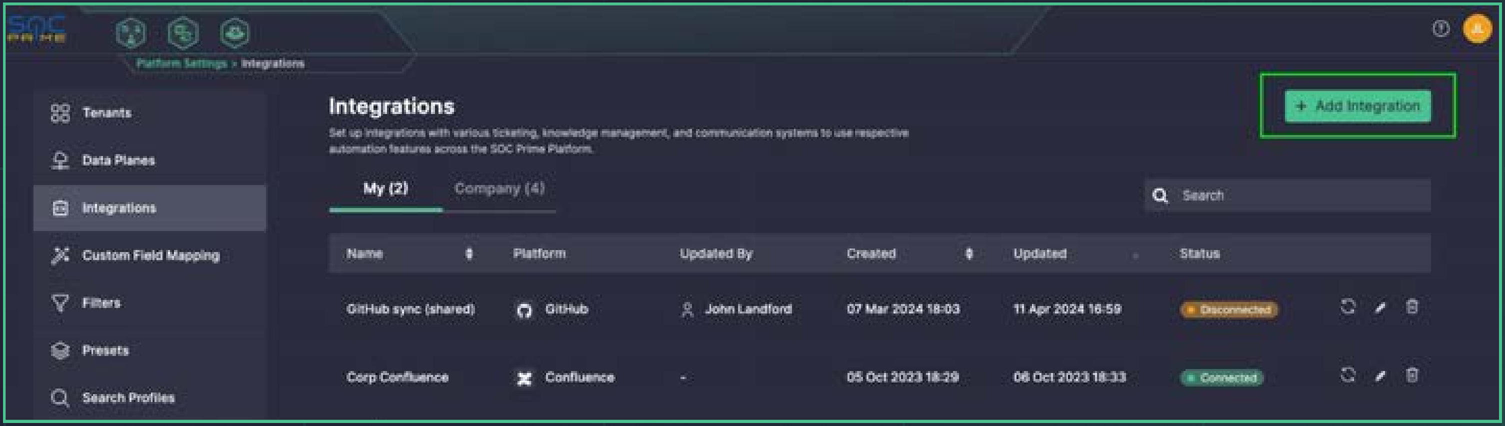
1. Set up an integration with your GitHub.
2. Create a Dynamic Content List based on your content selection criteria. For example, all content to detect activity related to CVEs for Windows.
3. Configure and run a Job that pushes the content added to the List on GitHub. New rules that match the List criteria will be pushed automatically.


SOC Prime Platform
Integration
(with your GitHub)
credentials (e.g. API token, branch name)
select in
Content
(rules, queries)
add to
Dynamic List
(filters that match your criteria, e.g. log source == "windows")
select in
Job
(auto-deploy action, with parameters like "Schedule", "Data Plane", "Lists")
files with code
GitHub repo

Let's look into each step:

Set up an integration with your GitHub

1. Go to **Platform Settings** > Integrations and click **Add Integration**.

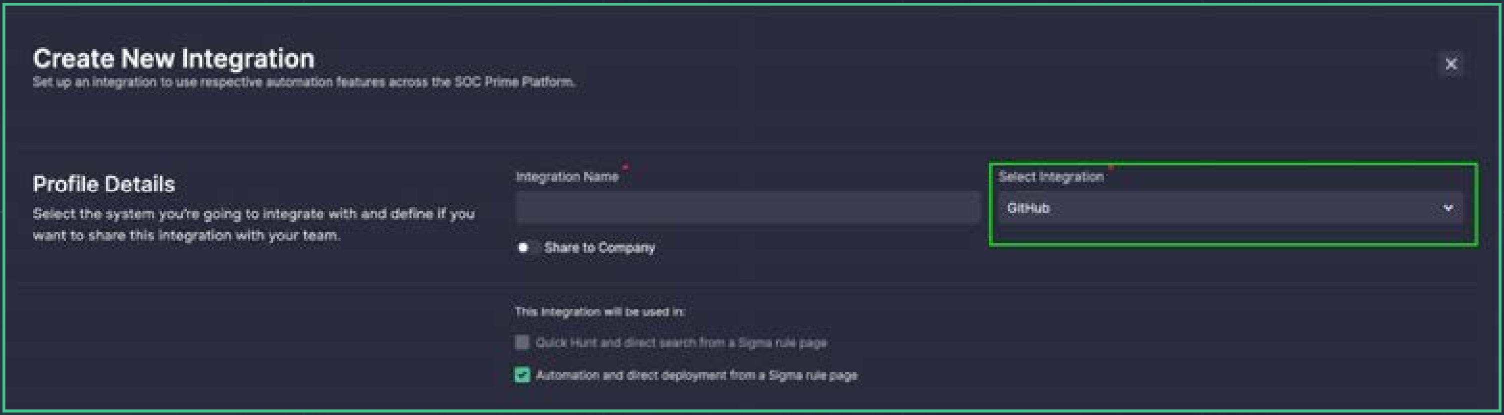


Integrations

Set up integrations with various ticketing, knowledge management, and communication systems to use respective automation features across the SOC Prime Platform.

Name	Platform	Updated By	Created	Updated	Status
GitHub sync (shared)	GitHub	John Landford	07 Mar 2024 18:03	11 Apr 2024 16:59	Disconnected
Corp Confluence	Confluence	-	05 Oct 2023 18:29	06 Oct 2023 18:33	Connected

2. In the modal that appears, name your Integration and select **GitHub** in the **Select Integration** dropdown. Keep the checkbox **Automation and direct deployment from a Sigma rule page** selected.



Create New Integration

Set up an integration to use respective automation features across the SOC Prime Platform.

Profile Details

Select the system you're going to integrate with and define if you want to share this integration with your team.

Integration Name *

● Share to Company

Select Integration *

GitHub

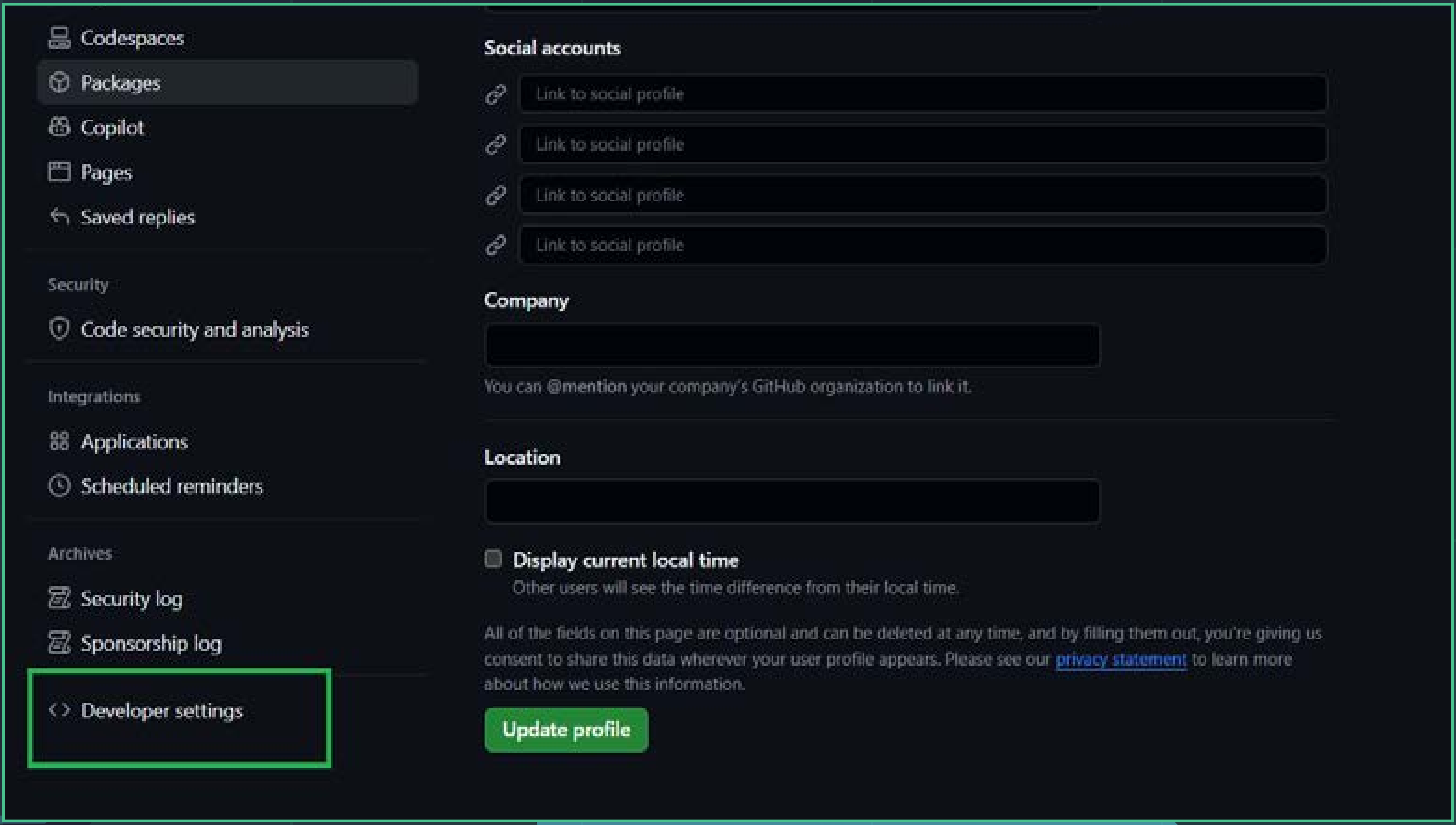
This integration will be used in:

□ Quick Hunt and direct search from a Sigma rule page

☑ Automation and direct deployment from a Sigma rule page

3. Then, configure the parameters:

- **Repository**: Provide the name of your repository. Note that the integration is supported only for private repositories.
- **GitHub Token**: Provide your personal access token. You can learn how to create it here. Basically, you need to:
    1. Click your account icon in the upper right corner > **Settings** > **Developer Settings**.



Social accounts

Link to social profile

Link to social profile

Link to social profile

Link to social profile

Company

You can @mention your company's GitHub organization to link it.

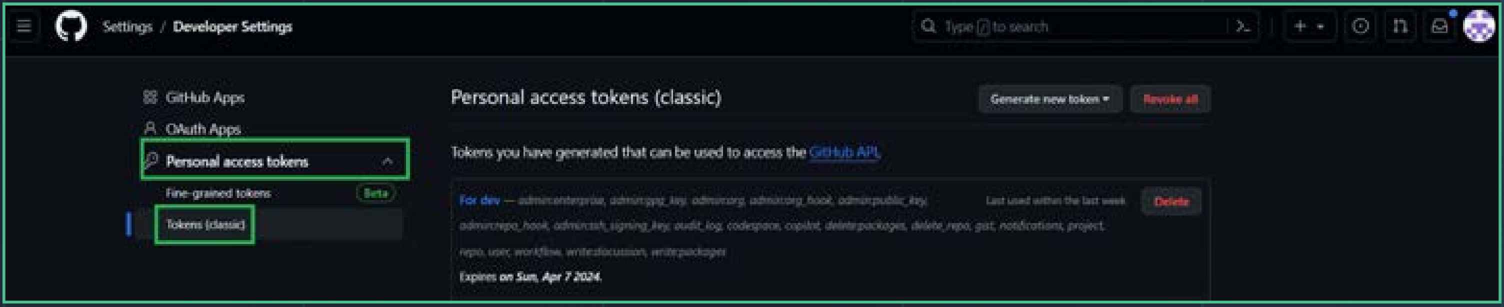
Location

□ Display current local time

Other users will see the time difference from their local time.

All of the fields on this page are optional and can be deleted at any time, and by filling them out, you're giving us consent to share this data wherever your user profile appears. Please see our privacy statement to learn more about how we use this information.

2. Go to **Personal access tokens** > **Tokens (classic)**.



Personal access tokens (classic)

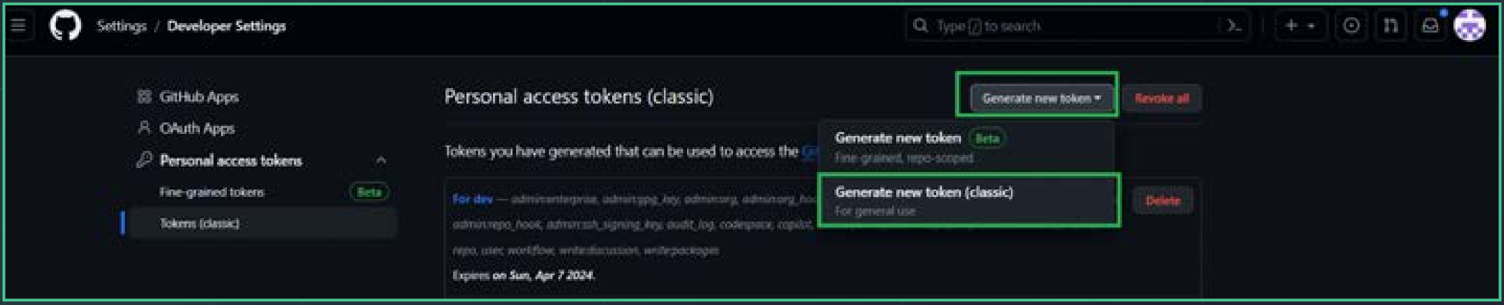
Tokens you have generated that can be used to access the GitHub API.

For dev — admin:enterprise, admin:gpg_key, admin:org, admin:org_hook, admin:public_key, admin:repo_hook, admin:ssh_signing_key, audit_log, codespace, copilot, delete:packages, delete_repo, gist, notifications, project, repo, user, workflow, write:discussion, write:packages

Last used within the last week

Expires on Sun, Apr 7 2024.

3. Click **Generate new token** > **Generate new token (classic)**.



Personal access tokens (classic)

Tokens you have generated that can be used to access the Gi

For dev — admin:enterprise, admin:gpg_key, admin:org, admin:org_hoo

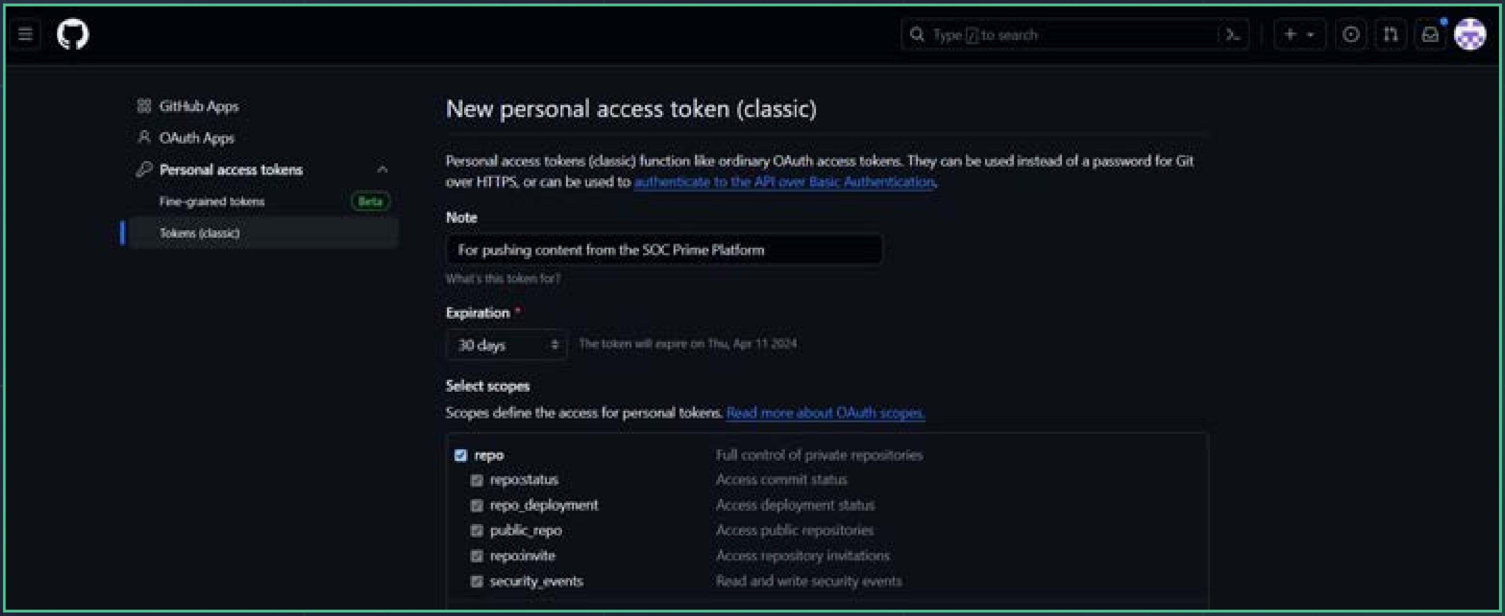
admin:repo_hook, admin:ssh_signing_key, audit_log, codespace, copilot,

repo, user, workflow, write:discussion, write:packages

Expires on Sun, Apr 7 2024.

4. Enter your GitHub account password if prompted.

5. Configure the key parameters:
    a. Note
    b. Expiration
    c. Scopes



New personal access token (classic)

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

Note

For pushing content from the SOC Prime Platform

What's this token for?

Expiration *

30 days

The token will expire on Thu, Apr 11 2024

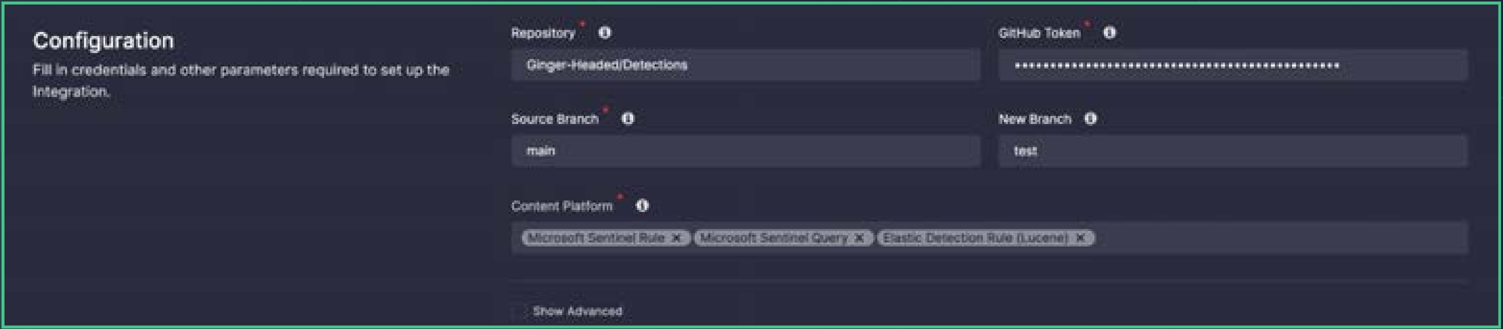
Select scopes

Scopes define the access for personal tokens. Read more about OAuth scopes.

☑ repo	Full control of private repositories
☑ repo:status	Access commit status
☑ repo_deployment	Access deployment status
☑ public_repo	Access public repositories
☑ repo:invite	Access repository invitations
☑ security_events	Read and write security events

6. Click **Generate token**.

- **Source Branch**: The name of the branch to pull content from.
- **New Branch**: The name of the branch to push content to. Leave this field empty to commit directly to the source branch.
- **Content Platform**: Content formats you're going to work with in Automation. Additionally, the tabs of selected platforms on a rule page will include the **Push to GitHub** button. Currently, we support:
  - Microsoft Sentinel Rule
  - Microsoft Sentinel Query
  - Elastic Detection Rule (Lucene)
  - Elastic Detection Rule (EQL)
  - Elastic Watcher
  - Elastic Saved Search
  - Chronicle Security Rule
  - Falcon LogScale Alert
  - Splunk Alert
  - Sumo Logic Query
  - LimaCharlie



Configuration

Fill in credentials and other parameters required to set up the Integration.

Repository *: Ginger-Headed/Detections

GitHub Token *: ••

Source Branch *: main

New Branch: test

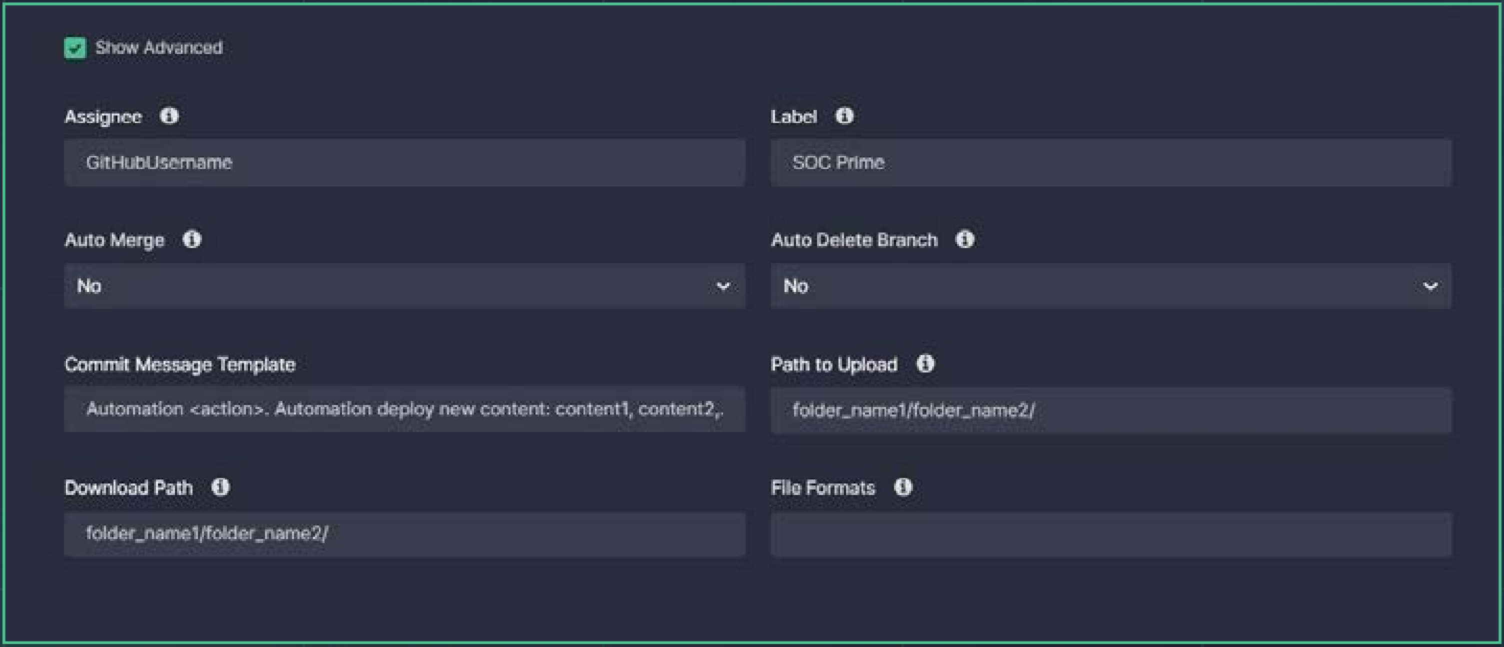
Content Platform *: Microsoft Sentinel Rule ✕ | Microsoft Sentinel Query ✕ | Elastic Detection Rule (Lucene) ✕

Show Advanced

4. These parameters are enough for pushing content. You can also configure advanced settings:

- Set the **Show Advanced** checkbox if you want to make optional advanced settings:
  - **Assignee**: The name of the GitHub user pull requests are assigned to
  - **Label**: Add a GitHub label that will be attached to pull requests
  - **Auto Merge**: Choose whether you want to merge pull requests automatically
  - **Auto Delete Branch**: Choose whether you want to automatically delete the branch after the pull request is merged (when **Auto Merge** is enabled)
- **Commit Message Template**: Provide a template for a commit message.
- **Path to Upload**: Provide the path to the folder the content should be uploaded to. If no value is entered, the root folder indicated in the **New Branch** field is used.

- **Download Path**: Provide the path to the folder the content should be downloaded from. If no value is entered, the root folder indicated in the **Source Branch** field is used.
- **File Formats**: Choose file formats of the content you're going to push to your repository.



☑ Show Advanced

Assignee: GitHubUsername

Label: SOC Prime

Auto Merge: No

Auto Delete Branch: No

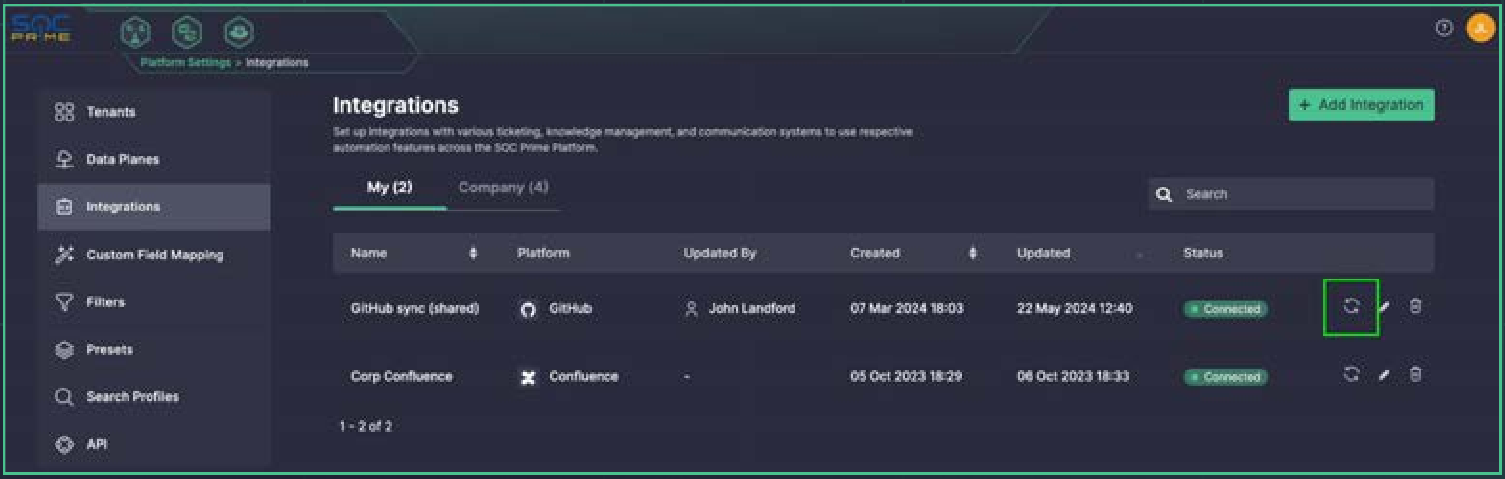
Commit Message Template: Automation <action>. Automation deploy new content: content1, content2,.

Path to Upload: folder_name1/folder_name2/

Download Path: folder_name1/folder_name2/

File Formats:

5. The Integration you've created should be displayed on the **Integrations** page. Click the **Check Connection** button to verify the connection to your GitHub repository.



Integrations

Set up integrations with various ticketing, knowledge management, and communication systems to use respective automation features across the SOC Prime Platform.

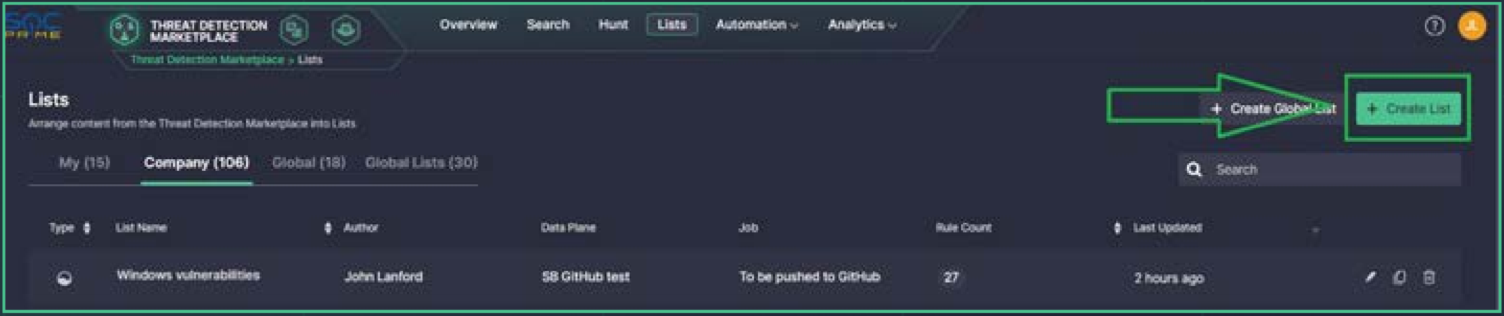
Name	Platform	Updated By	Created	Updated	Status
GitHub sync (shared)	GitHub	John Landford	07 Mar 2024 18:03	22 May 2024 12:40	Connected
Corp Confluence	Confluence	-	05 Oct 2023 18:29	06 Oct 2023 18:33	Connected

1 - 2 of 2

Create a Dynamic Content List

A Dynamic Content List defines the criteria for selecting content on the SOC Prime Platform. To create a list:

1. Go to Threat Detection Marketplace > Lists and click **Create List.**

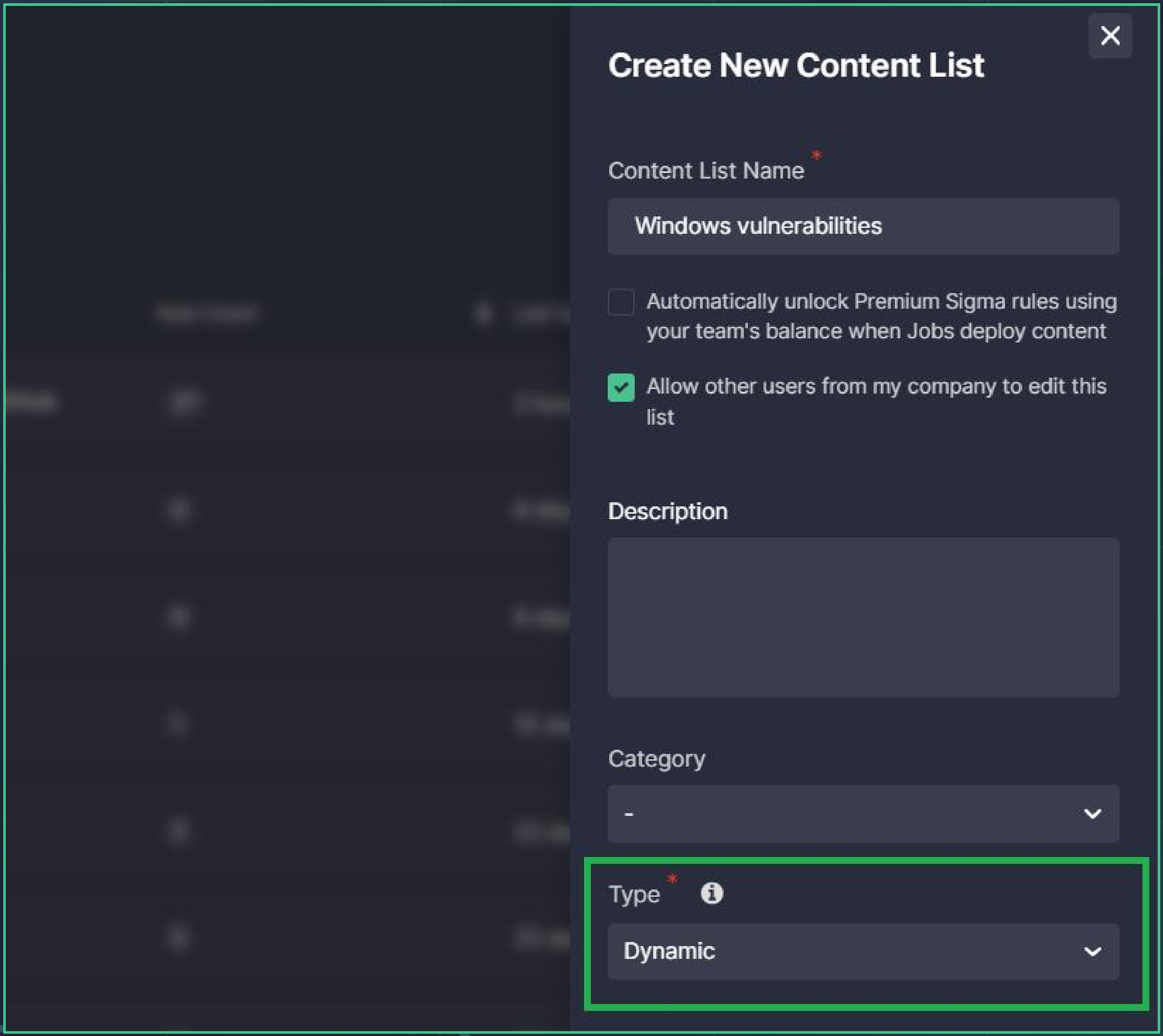


Lists

Arrange content from the Threat Detection Marketplace into Lists

Type	List Name	Author	Data Plane	Job	Rule Count	Last Updated
◒	Windows vulnerabilities	John Lanford	SB GitHub test	To be pushed to GitHub	27	2 hours ago

2. In the modal that appears, name your List and select **Type**: Dynamic.



Create New Content List

Content List Name *

Windows vulnerabilities

□ Automatically unlock Premium Sigma rules using your team's balance when Jobs deploy content

☑ Allow other users from my company to edit this list

Description

Category

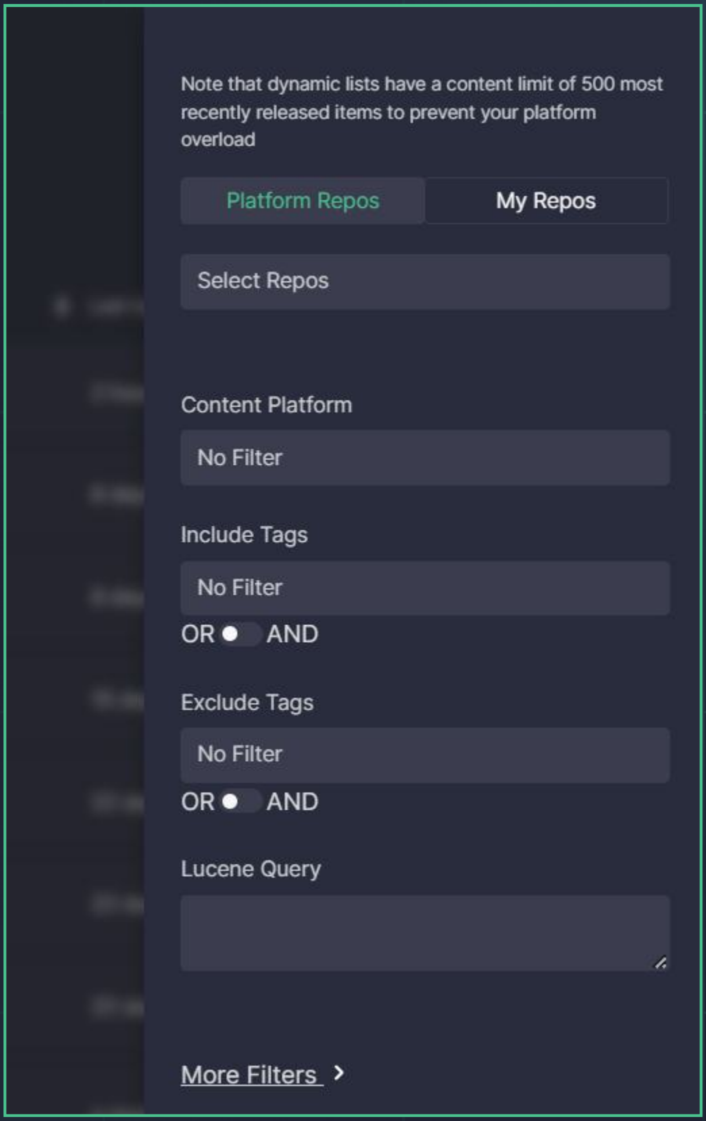
-

Type *

Dynamic

3. Set the parameters to select content. For example, you can build a Lucene search for all rules that include CVE as part of their name and select a **Sigma product**: Windows. The configurations are very flexible, so you can try different approaches.

4. Click **Save Changes**.



Note that dynamic lists have a content limit of 500 most recently released items to prevent your platform overload

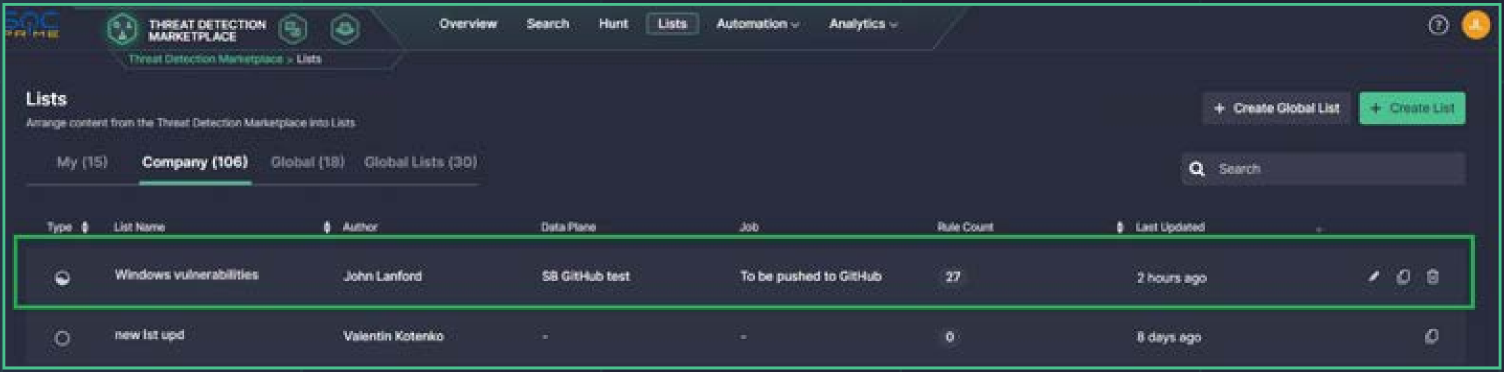
Content Platform
No Filter

Include Tags
No Filter
OR ● AND

Exclude Tags
No Filter
OR ● AND

Lucene Query

5. The list you've created should appear on the **Lists** page.



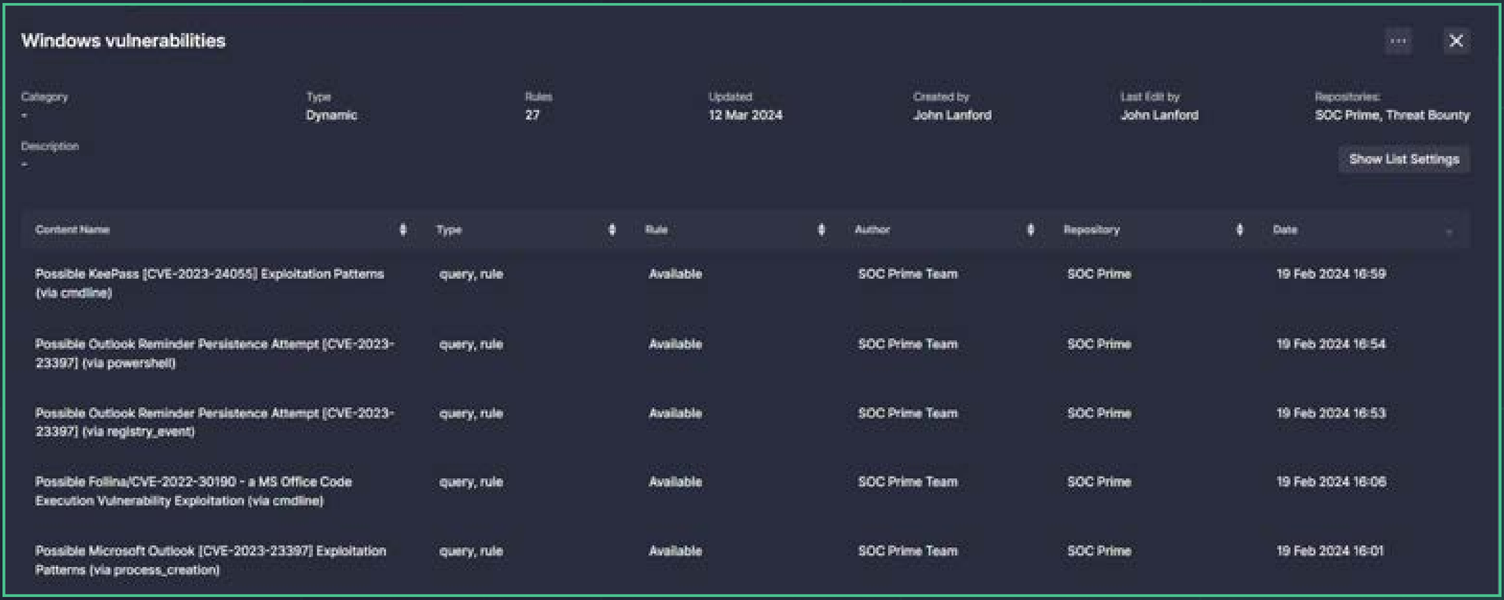
Lists

Arrange content from the Threat Detection Marketplace into Lists

My (15) | Company (106) | Global (18) | Global Lists (30)

Type	List Name	Author	Data Plane	Job	Rule Count	Last Updated
◒	Windows vulnerabilities	John Lanford	SB GitHub test	To be pushed to GitHub	27	2 hours ago
○	new lst upd	Valentin Kotenko	-	-	0	8 days ago

You can click it to check what rules are included currently.



Windows vulnerabilities

Category	Type	Rules	Updated	Created by	Last Edit by	Repositories:
-	Dynamic	27	12 Mar 2024	John Lanford	John Lanford	SOC Prime, Threat Bounty

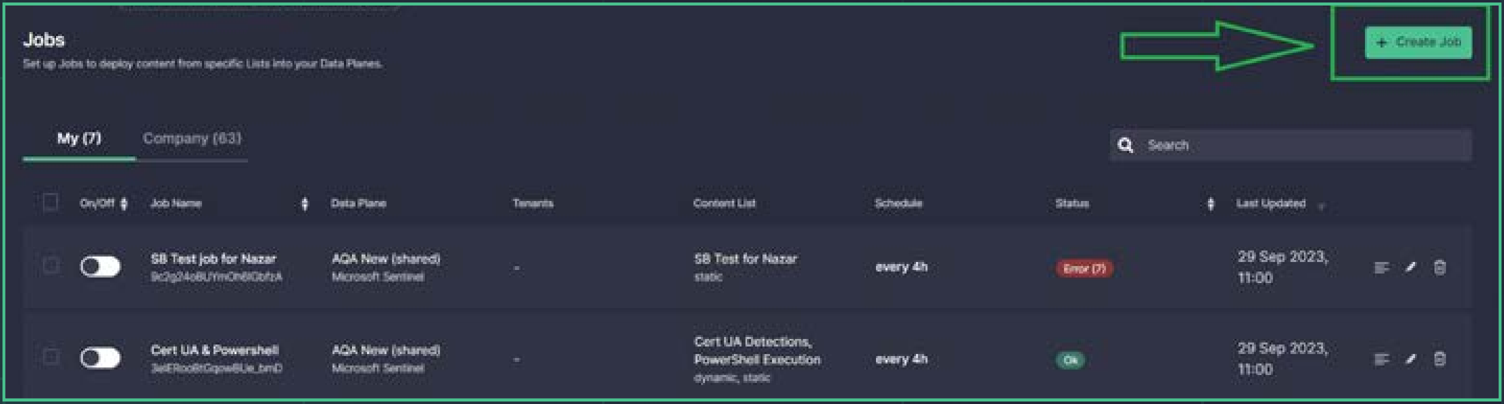
Description
-

Content Name	Type	Rule	Author	Repository	Date
Possible KeePass [CVE-2023-24055] Exploitation Patterns (via cmdline)	query, rule	Available	SOC Prime Team	SOC Prime	19 Feb 2024 16:59
Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via powershell)	query, rule	Available	SOC Prime Team	SOC Prime	19 Feb 2024 16:54
Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via registry_event)	query, rule	Available	SOC Prime Team	SOC Prime	19 Feb 2024 16:53
Possible Follina/CVE-2022-30190 - a MS Office Code Execution Vulnerability Exploitation (via cmdline)	query, rule	Available	SOC Prime Team	SOC Prime	19 Feb 2024 16:06
Possible Microsoft Outlook [CVE-2023-23397] Exploitation Patterns (via process_creation)	query, rule	Available	SOC Prime Team	SOC Prime	19 Feb 2024 16:01

Configure and Run a Job

A Job pushes the content selected using the List into the GitHub repository configured in the Data Plane. To create and run a Job:

1. Go to Threat Detection Marketplace > **Automation** > Jobs and click **Add Job**.



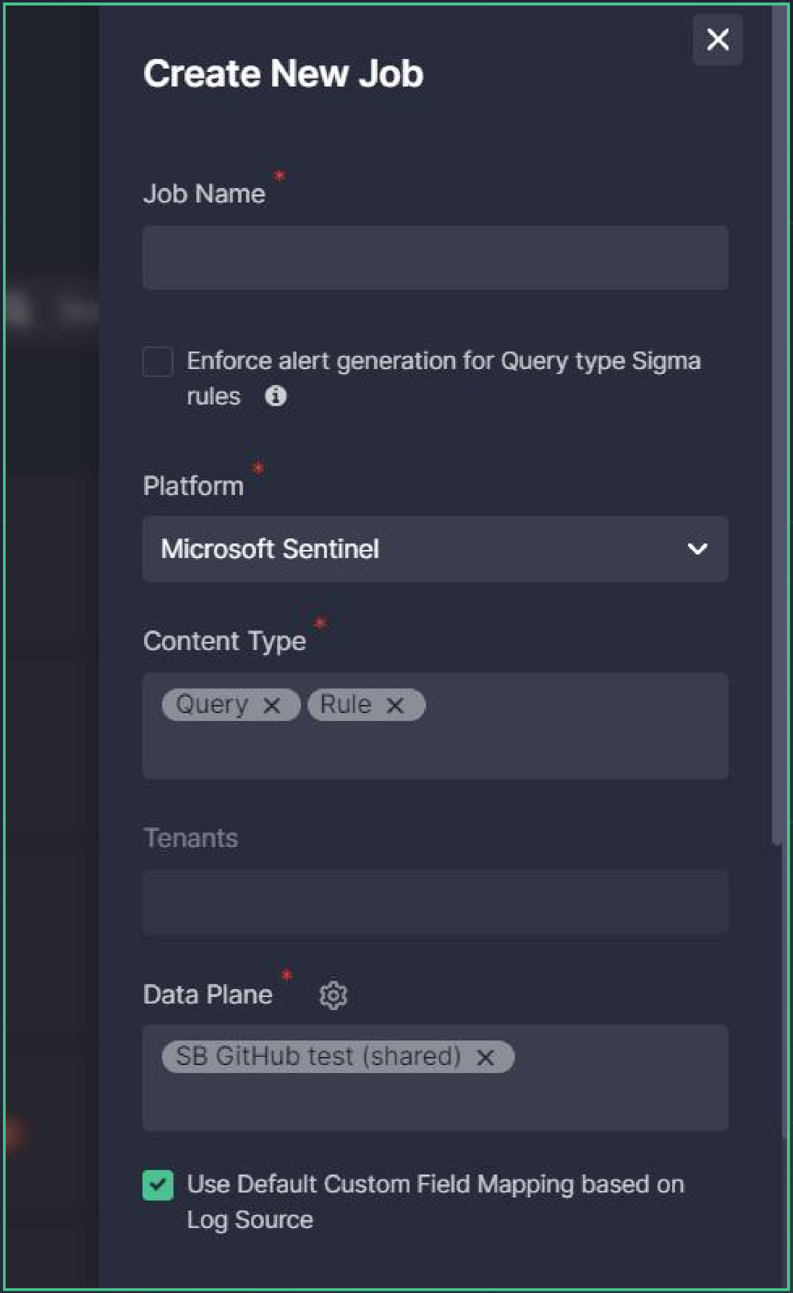
Jobs

Set up Jobs to deploy content from specific Lists into your Data Planes.

□	On/Off	Job Name	Data Plane	Tenants	Content List	Schedule	Status	Last Updated
□	○	SB Test job for Nazar 9c2g24o8UYmOn6lGbfzA	AQA New (shared) Microsoft Sentinel	-	SB Test for Nazar static	every 4h	Error (7)	29 Sep 2023, 11:00
□	○	Cert UA & Powershell 3eERooBtGqow8Ue_bmD	AQA New (shared) Microsoft Sentinel	-	Cert UA Detections, PowerShell Execution dynamic, static	every 4h	Ok	29 Sep 2023, 11:00

2. In the modal that appears, name your Job and select the platform and content type (they should match the content type selected in your GitHub Data Plane).

3. Then, select your GitHub Data Plane.



Create New Job

Job Name *

□ Enforce alert generation for Query type Sigma rules

Platform *: Microsoft Sentinel

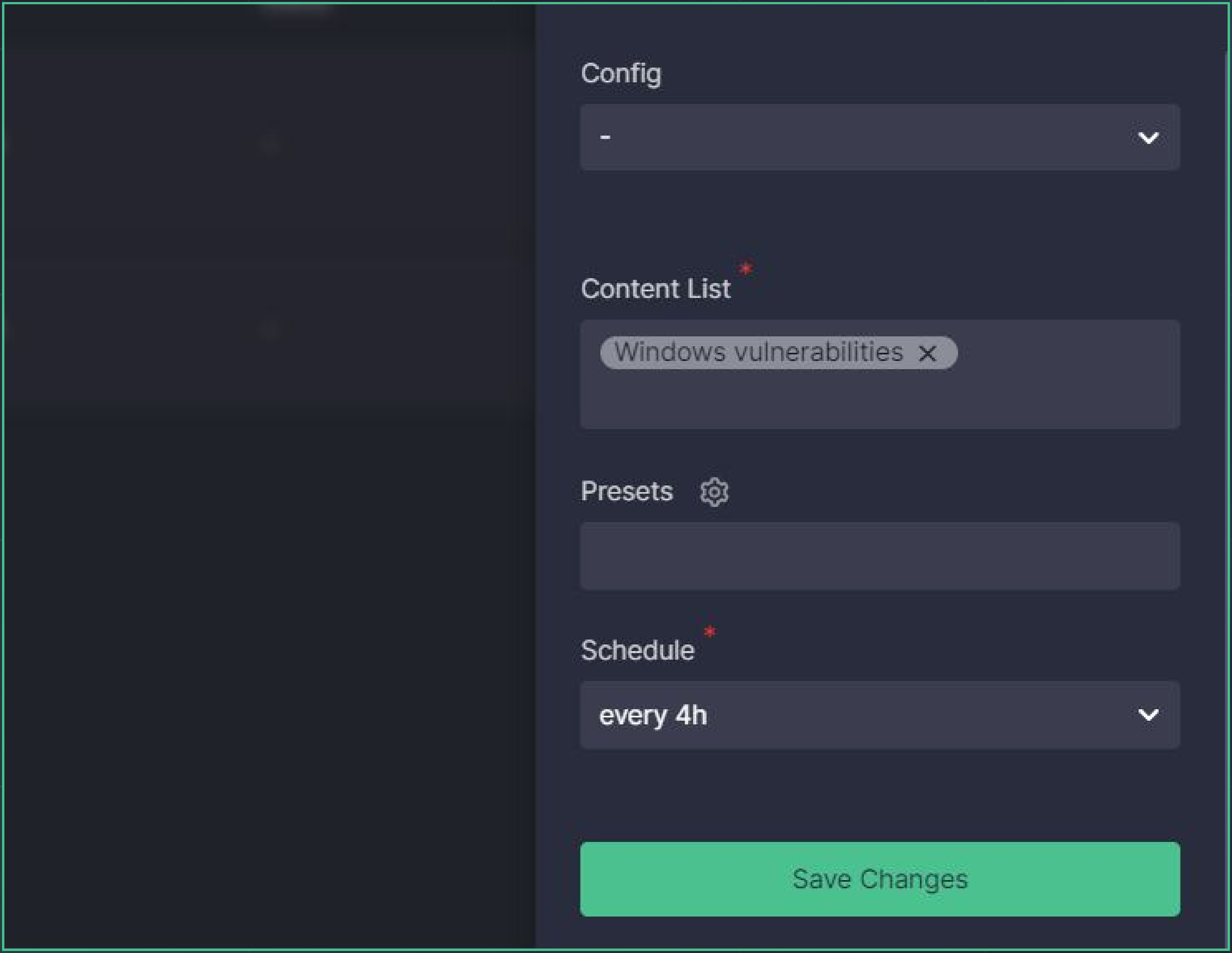
Content Type *: Query ✕ Rule ✕

Tenants

Data Plane *: SB GitHub test (shared) ✕

☑ Use Default Custom Field Mapping based on Log Source

4. Select the Dynamic Content List you've configured.



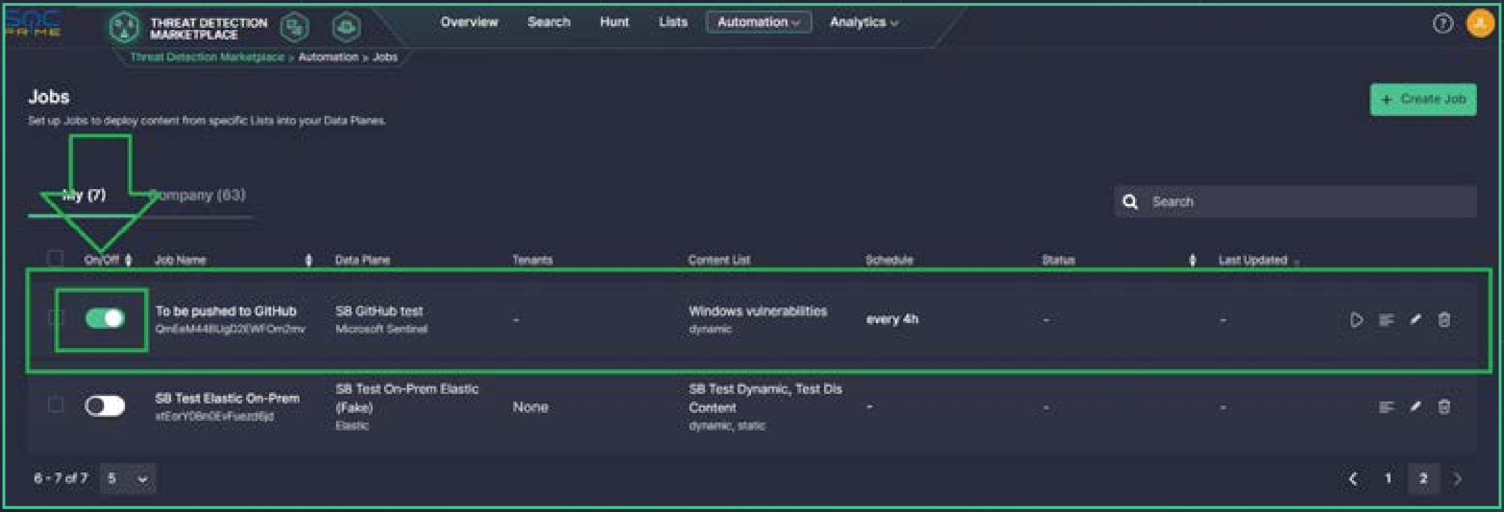
Config: -

Content List *: Windows vulnerabilities ×

Presets

Schedule *: every 4h

5. Optionally, you can select a **Config** for alternative translations and a **Preset** to modify the detection content before it is pushed.
6. Select the **Schedule** of the Job.
7. Click **Save Changes**.
8. The configured Job should be displayed on the **Jobs** page. Enable it using the **On/Off** switch. Once enabled, the Job runs according to the selected schedule and pushes the detection content.



Jobs

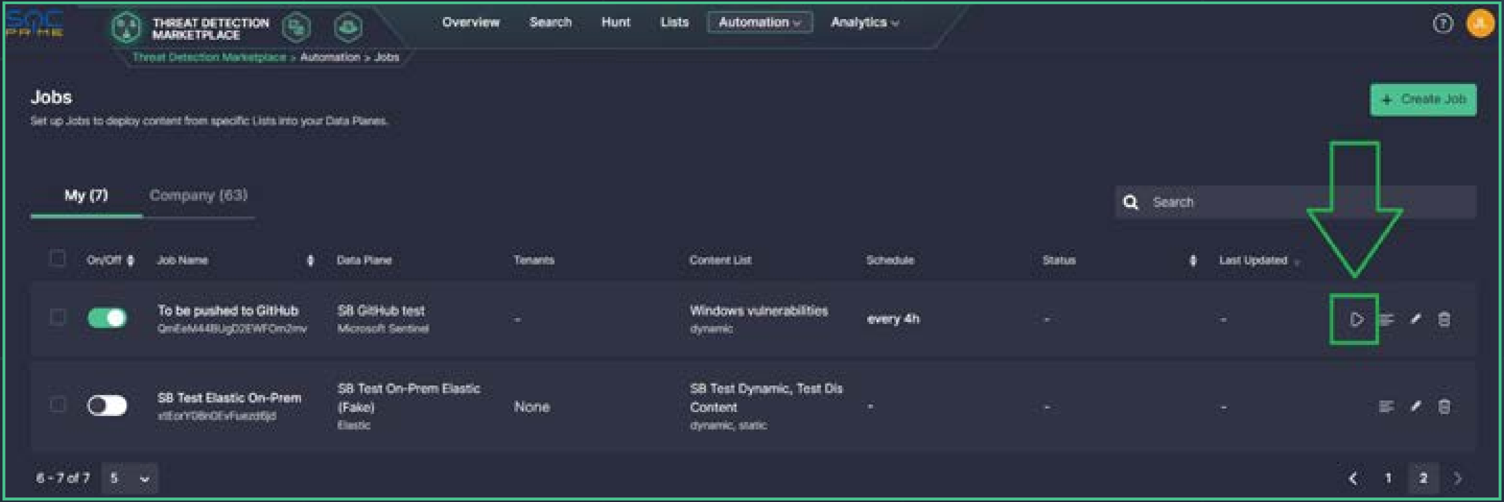
Set up Jobs to deploy content from specific Lists into your Data Planes.

	On/Off	Job Name	Data Plane	Tenants	Content List	Schedule	Status	Last Updated
□	●	To be pushed to GitHub QmEeM448UgD2EWFOm2mv	SB GitHub test Microsoft Sentinel	-	Windows vulnerabilities dynamic	every 4h	-	-
□	○	SB Test Elastic On-Prem xtEorY0BnOEvFuezd6jd	SB Test On-Prem Elastic (Fake) Elastic	None	SB Test Dynamic, Test Dis Content dynamic, static	-	-	-

6 - 7 of 7 5

< 1 2 >

You can also run the Job at any time using the **Run Now** button.



Jobs

Set up Jobs to deploy content from specific Lists into your Data Planes.

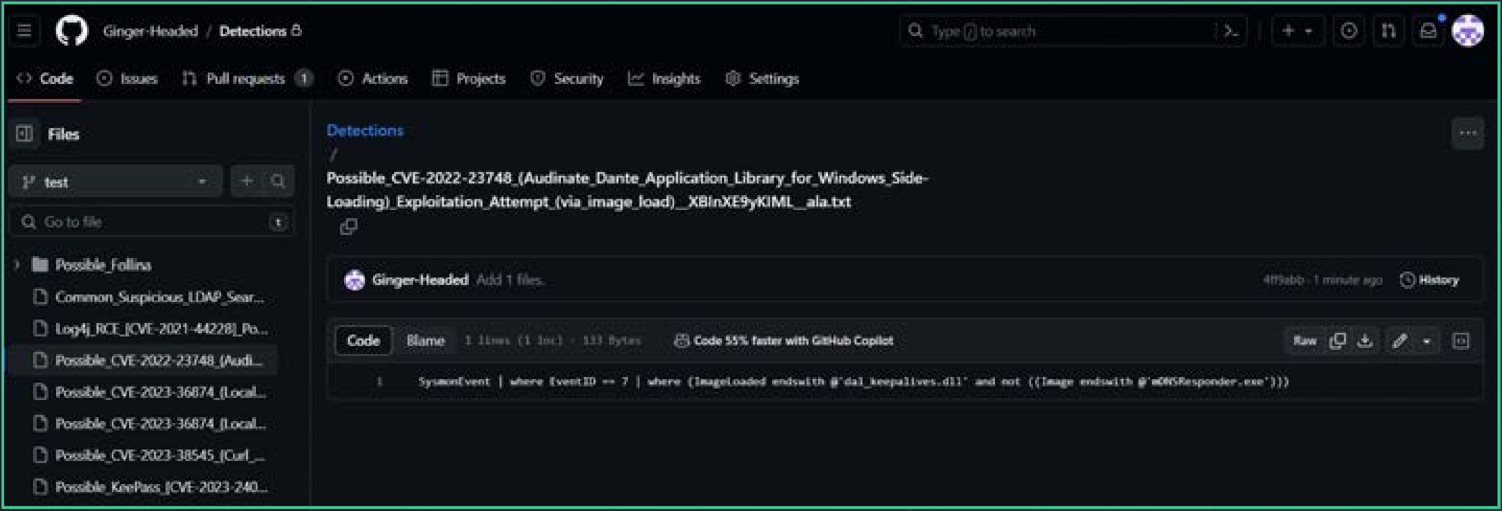
On/Off	Job Name	Data Plane	Tenants	Content List	Schedule	Status	Last Updated
●	To be pushed to GitHub QmEeM44BUgD2EWFOm2mv	SB GitHub test Microsoft Sentinel	-	Windows vulnerabilities dynamic	every 4h	-	-
○	SB Test Elastic On-Prem xtEorY0BnOEvFuezd6jd	SB Test On-Prem Elastic (Fake) Elastic	None	SB Test Dynamic, Test Dis Content dynamic, static	-	-	-

Once the Job is finished, the content from the List is pushed to the GitHub repository configured in the Data Plane.

Detection Content in GitHub

In GitHub, the detection content pushed from the SOC Prime Platform looks like this:

- Microsoft Sentinel Query (as TXT)



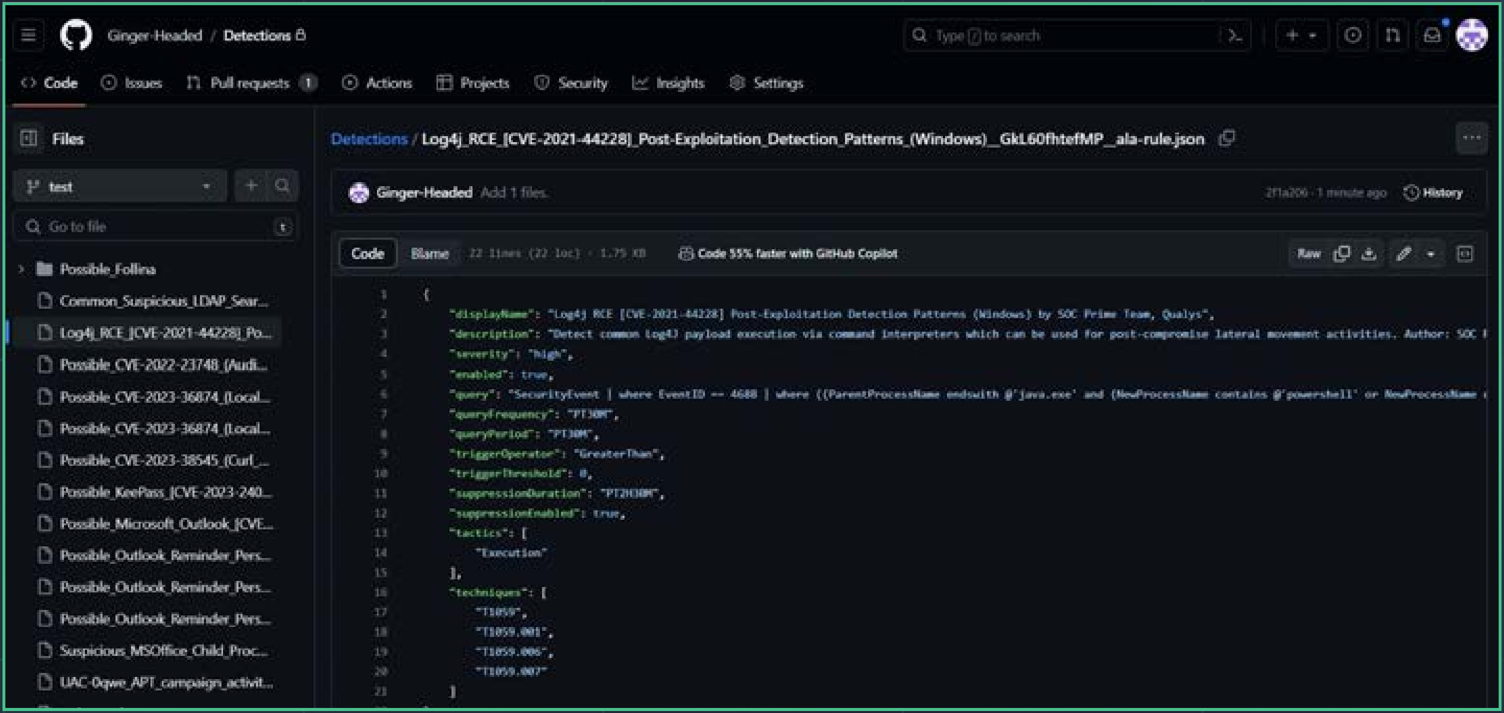
Possible_Follina
Common_Suspicious_LDAP_Sear...
Log4j_RCE_[CVE-2021-44228]_Po...
Possible_CVE-2022-23748_(Audi...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-38545_(Curl_...
Possible_KeePass_[CVE-2023-240...

Detections / Possible_CVE-2022-23748_(Audinate_Dante_Application_Library_for_Windows_Side-Loading)_Exploitation_Attempt_(via_image_load)__XBInXE9yKIML__ala.txt

Ginger-Headed Add 1 files. 4ff3abb · 1 minute ago

```
SysmonEvent | where EventID == 7 | where (ImageLoaded endswith @'dal_keepalives.dll' and not ((Image endswith @'mDNSResponder.exe')))
```

- Microsoft Sentinel Rule (as JSON):

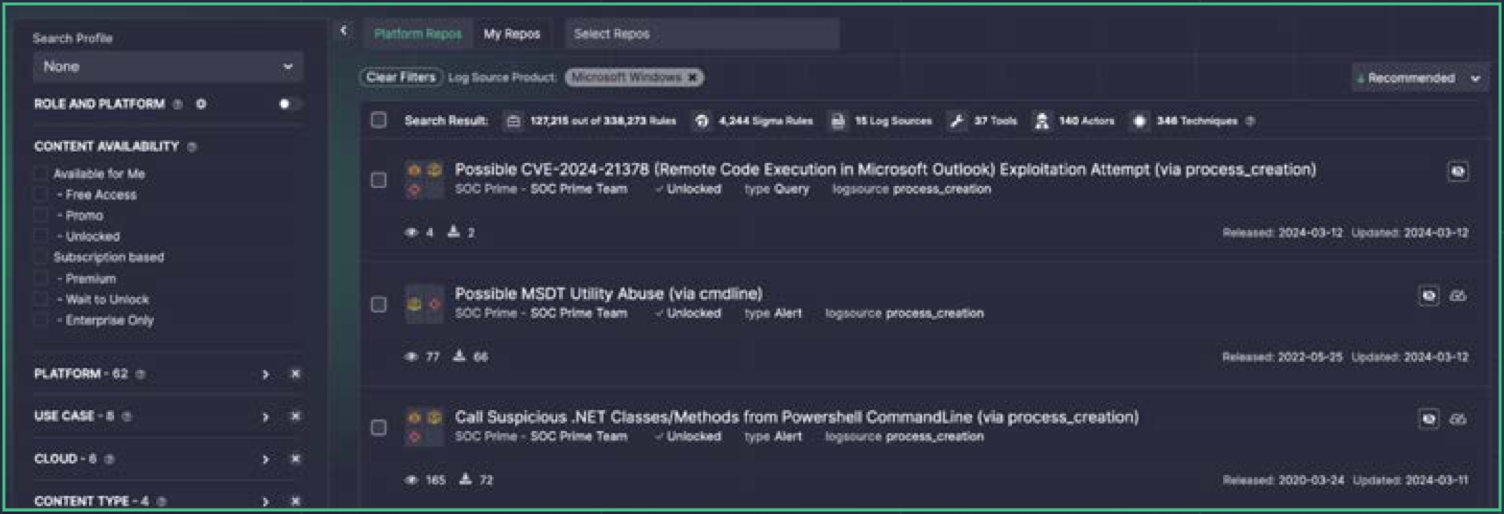

Ginger-Headed / Detections
Type / to search
Code
Issues
Pull requests 1
Actions
Projects
Security
Insights
Settings
Files
test
Go to file
Possible_Follina
Common_Suspicious_LDAP_Sear...
Log4j_RCE_[CVE-2021-44228]_Po...
Possible_CVE-2022-23748_(Audi...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-38545_(Curl_...
Possible_KeePass_[CVE-2023-240...
Possible_Microsoft_Outlook_[CVE...
Possible_Outlook_Reminder_Pers...
Possible_Outlook_Reminder_Pers...
Possible_Outlook_Reminder_Pers...
Suspicious_MSOffice_Child_Proc...
UAC-0qwe_APT_campaign_activit...
Detections / Log4j_RCE_[CVE-2021-44228]_Post-Exploitation_Detection_Patterns_(Windows)__GkL60fhtefMP__ala-rule.json
Ginger-Headed Add 1 files.
2f1a206 · 1 minute ago
History
Code
Blame
22 lines (22 loc) · 1.75 KB
Code 55% faster with GitHub Copilot
Raw

```json
{
    "displayName": "Log4j RCE [CVE-2021-44228] Post-Exploitation Detection Patterns (Windows) by SOC Prime Team, Qualys",
    "description": "Detect common Log4J payload execution via command interpreters which can be used for post-compromise lateral movement activities. Author: SOC
    "severity": "high",
    "enabled": true,
    "query": "SecurityEvent | where EventID == 4688 | where ((ParentProcessName endswith @'java.exe' and (NewProcessName contains @'powershell' or NewProcessName
    "queryFrequency": "PT30M",
    "queryPeriod": "PT30M",
    "triggerOperator": "GreaterThan",
    "triggerThreshold": 0,
    "suppressionDuration": "PT2H30M",
    "suppressionEnabled": true,
    "tactics": [
        "Execution"
    ],
    "techniques": [
        "T1059",
        "T1059.001",
        "T1059.006",
        "T1059.007"
    ]
```

Notes

You can also push selected rules to GitHub from a rule's page one by one:

a. Go to Search > Filter out content you need > Select a rule.



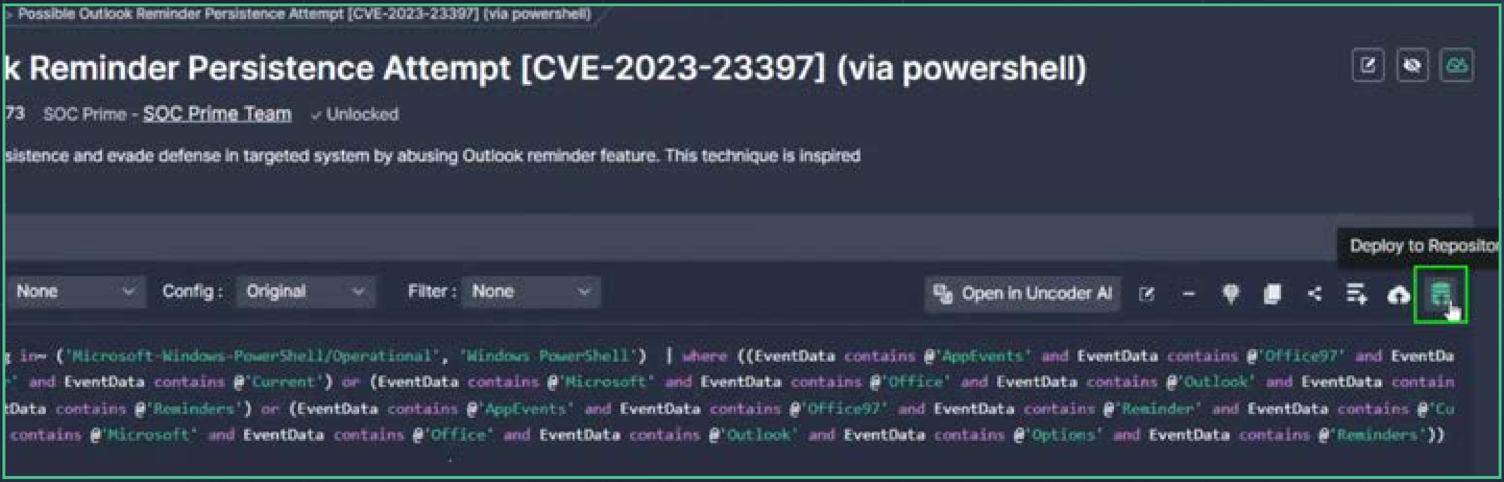
□ Search Result: 127,215 out of 338,273 Rules | 4,244 Sigma Rules | 15 Log Sources | 37 Tools | 140 Actors | 346 Techniques

□ Possible CVE-2024-21378 (Remote Code Execution in Microsoft Outlook) Exploitation Attempt (via process_creation)
SOC Prime - SOC Prime Team ✓ Unlocked type Query logsource process_creation
4 2 Released: 2024-03-12 Updated: 2024-03-12

□ Possible MSDT Utility Abuse (via cmdline)
SOC Prime - SOC Prime Team ✓ Unlocked type Alert logsource process_creation
77 66 Released: 2022-05-25 Updated: 2024-03-12

□ Call Suspicious .NET Classes/Methods from Powershell CommandLine (via process_creation)
SOC Prime - SOC Prime Team ✓ Unlocked type Alert logsource process_creation
165 72 Released: 2020-03-24 Updated: 2024-03-11

b. Open the **Code** tab > click the **Deploy to GitHub** icon > Select created integration (Data Plane).



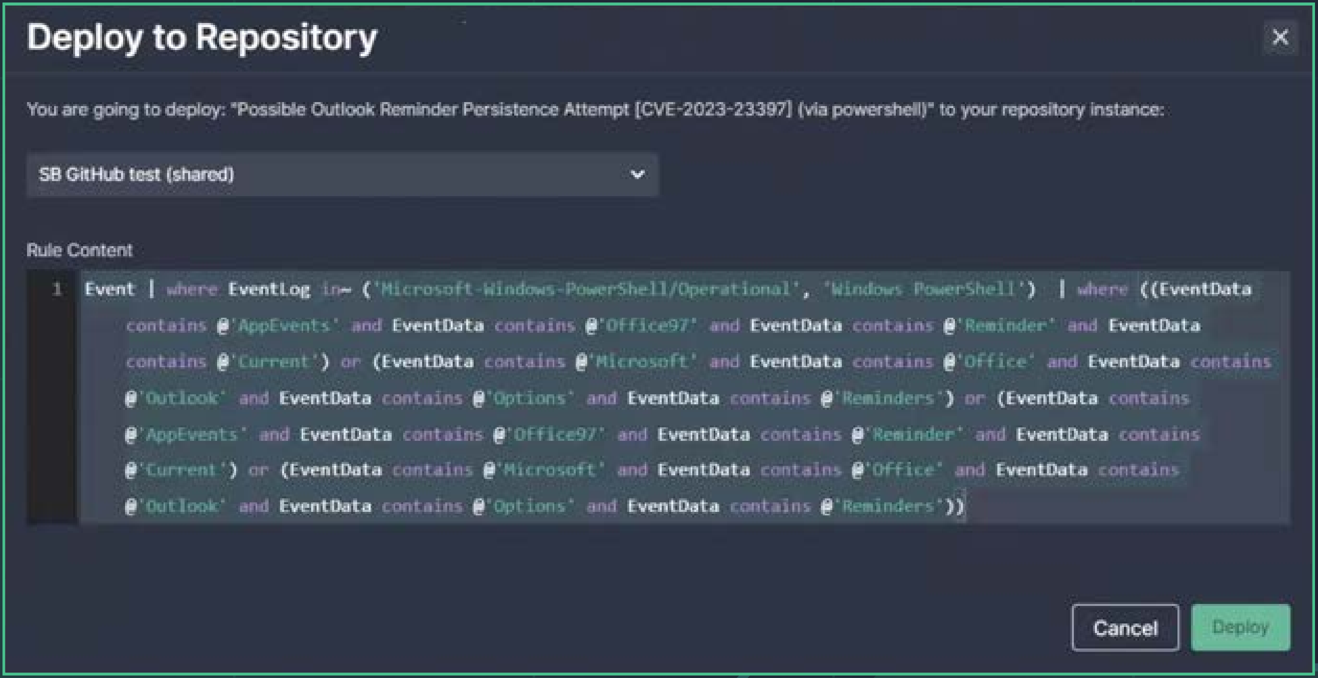
› Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via powershell)

k Reminder Persistence Attempt [CVE-2023-23397] (via powershell)

73 SOC Prime - SOC Prime Team ✓ Unlocked

sistence and evade defense in targeted system by abusing Outlook reminder feature. This technique is inspired

```
g in~ ('Microsoft-Windows-PowerShell/Operational', 'Windows PowerShell')  | where ((EventData contains @'AppEvents' and EventData contains @'Office97' and EventDa
r' and EventData contains @'Current') or (EventData contains @'Microsoft' and EventData contains @'Office' and EventData contains @'Outlook' and EventData contain
tData contains @'Reminders') or (EventData contains @'AppEvents' and EventData contains @'Office97' and EventData contains @'Reminder' and EventData contains @'Cu
 contains @'Microsoft' and EventData contains @'Office' and EventData contains @'Outlook' and EventData contains @'Options' and EventData contains @'Reminders'))
```



Deploy to Repository

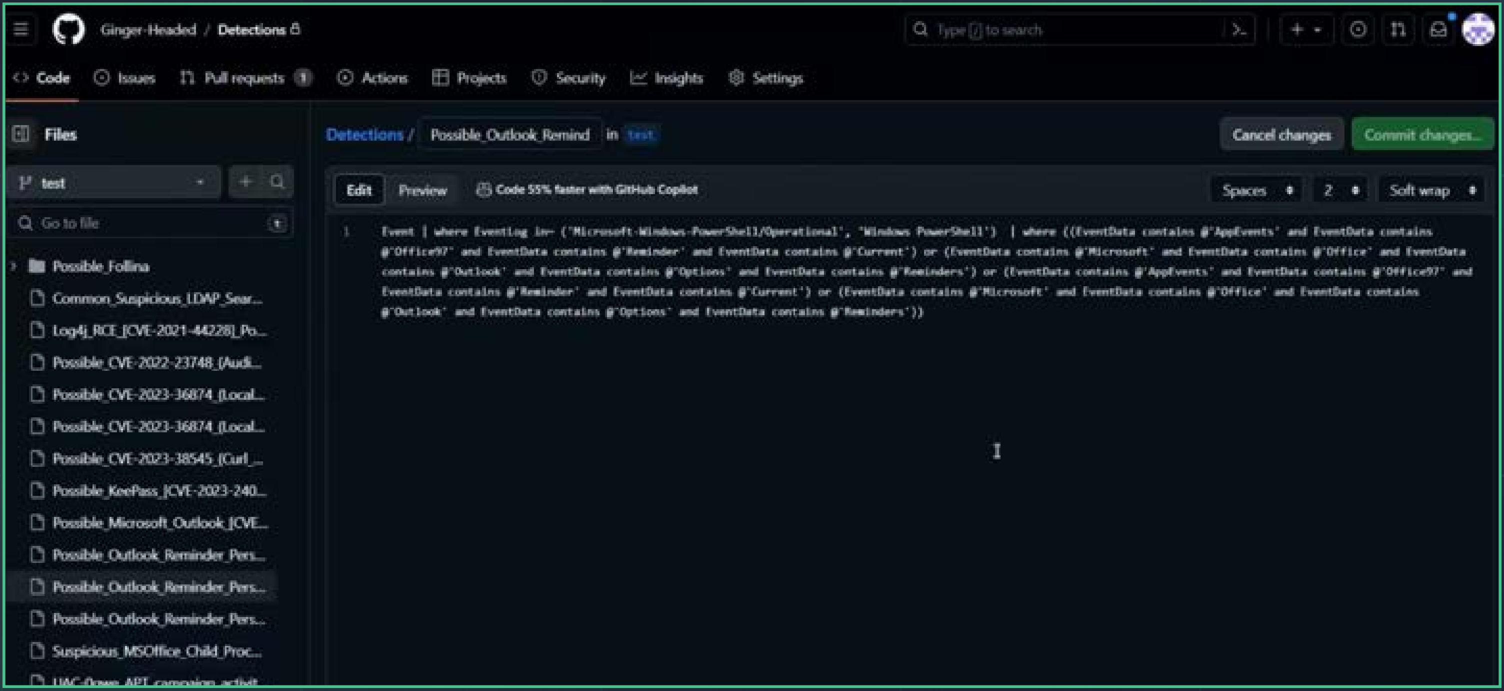
You are going to deploy: "Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via powershell)" to your repository instance:

SB GitHub test (shared)

Rule Content

```
Event | where EventLog in~ ('Microsoft-Windows-PowerShell/Operational', 'Windows PowerShell')  | where ((EventData
    contains @'AppEvents' and EventData contains @'Office97' and EventData contains @'Reminder' and EventData
    contains @'Current') or (EventData contains @'Microsoft' and EventData contains @'Office' and EventData contains
    @'Outlook' and EventData contains @'Options' and EventData contains @'Reminders') or (EventData contains
    @'AppEvents' and EventData contains @'Office97' and EventData contains @'Reminder' and EventData contains
    @'Current') or (EventData contains @'Microsoft' and EventData contains @'Office' and EventData contains
    @'Outlook' and EventData contains @'Options' and EventData contains @'Reminders'))
```

c. As a result, text documents with respective code will appear in your GitHub repo.


Ginger-Headed / Detections
Type / to search
Code
Issues
Pull requests 1
Actions
Projects
Security
Insights
Settings
Files
test
Go to file
Possible_Follina
Common_Suspicious_LDAP_Sear...
Log4j_RCE_[CVE-2021-44228]_Po...
Possible_CVE-2022-23748_(Audi...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-36874_(Local...
Possible_CVE-2023-38545_(Curl_...
Possible_KeePass_[CVE-2023-240...
Possible_Microsoft_Outlook_[CVE...
Possible_Outlook_Reminder_Pers...
Possible_Outlook_Reminder_Pers...
Possible_Outlook_Reminder_Pers...
Suspicious_MSOffice_Child_Proc...
Detections / Possible_Outlook_Remind in test
Cancel changes
Commit changes...
Edit
Preview
Code 55% faster with GitHub Copilot
Spaces
2
Soft wrap

```
Event | where EventLog in~ ('Microsoft-Windows-PowerShell/Operational', 'Windows PowerShell')  | where ((EventData contains @'AppEvents' and EventData contains
@'Office97' and EventData contains @'Reminder' and EventData contains @'Current') or (EventData contains @'Microsoft' and EventData contains @'Office' and EventData
contains @'Outlook' and EventData contains @'Options' and EventData contains @'Reminders') or (EventData contains @'AppEvents' and EventData contains @'Office97' and
EventData contains @'Reminder' and EventData contains @'Current') or (EventData contains @'Microsoft' and EventData contains @'Office' and EventData contains
@'Outlook' and EventData contains @'Options' and EventData contains @'Reminders'))
```