15. Some other tips and best practices when creating custom rules:
    a. **Tip:** The autocomplete feature can help you write the logic. For example, typing "ip" will bring up a dropdown showing all available fields related to IP addresses.
    b. **Tip:** Syntax coloring can help you write the logic. Using single or double quotes will color the text to show which characters are included inside. Sets of opening and closing parenthesis will be colored individually to give you a guide to matching them correctly.
    c. **Best practice:** Insights are named based on the tactics and techniques tagged in the signals. Consider which tactic or technique from the MITRE ATT&CK framework your rule is looking for when selecting tags.

©2025 Sumo Logic, All Rights Reserved.

Lab 9b: Write a threshold rule

There are six different rule types in Cloud SIEM -- lab exercises 9a through 9f will give you opportunities to create examples of all six types. However, they are optional for the completion of later labs, so you can decide which if any or all of the rule types you want to practice. When you are finished doing rule lab exercises, you can skip ahead to Lab 10 to continue the course.

A **threshold rule** fires when its rule expression is matched at least a certain number of times during a specified length of time. For example, if there are five or more failed login attempts for the same IP address within one hour.

Let's create a threshold rule in Cloud SIEM:

1. Click **Cloud SIEM > Rules** in the left navigation menu if you are not already there.
2. Click **Create** in the upper right.
3. Select **Threshold** rule.
4. **Name** your rule "Training Threshold Rule XXX" with your initials in place of the XXX.
5. Use the following expression (checking for a large number of failed logins):

```
objectType = 'Authentication'
AND normalizedAction = 'logon'
AND success = false
```

6. Set the match criteria to be "at least 10 Records within 1 day".
7. Click the "Show Advanced" link in the top left. Check the box marked "Group by one or more fields".
8. Add "user_username" to **with matches grouped by** along with (default) Entity Field
9. On the right side, set the Entity to "user_username".
10. Set the summary to be "Multiple failed login attempts for user: [User Username]". (Use the '+' button to add a variable token marked with [ ]).
11. Add a description "Test Rule" or a description of your choice.
12. Set the Severity to 4
13. Add a "Brute Force" and/or "Credential Access" tag
14. Select the **Save this rule as a prototype** checkbox.
15. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.

©2025 Sumo Logic, All Rights Reserved.

16. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 9c: Write a chain rule

There are six different rule types in Cloud SIEM -- lab exercises 9a through 9f will give you opportunities to create examples of all six types. However, they are optional for the completion of later labs, so you can decide which if any or all of the rule types you want to practice. When you are finished doing rule lab exercises, you can skip ahead to Lab 10 to continue the course.

A **chain rule** is similar to a threshold rule. A threshold rule fires when one rule expression is matched at least a certain number times during a specified length of time. In a chain rule you configure two more rule expressions, and for each expression, the number of matches that are required for the rule to fire a signal. The interval you define within which the matches must occur applies to all of the rule expressions in the rule.

Let's create a chain rule in Cloud SIEM:

1. Click **Cloud SIEM > Rules** in the left navigation menu if you are not already there.
2. Click **Create** in the upper right.
3. Select **Chain** rule.
4. **Name** your rule "Training Chain Rule XXX" with your initials in place of the XXX.
5. Set the first parameter to "When at least 10 Records match expression"
6. Enter "bro_rfb_authenticationSuccessful=False" as the first expression
7. Leave the second expression threshold at 1
8. Enter "bro_rfb_authenticationSuccessful=True" as the second expression.
9. Add "device_ip" to the **grouped by** value in addition to the (default) Entity Field.
10. Set the remaining values to "in any order within 5 minutes".
11. On the right side, set the **Entity** to "device_ip".
12. Add "Successful login after 10 failed logins" as the summary.
13. Add a description "Test Rule" or a description of your choice.
14. Set the **Severity** to 3.
15. Add an "Initial Access" tag.
16. Select the **Save this rule as a prototype** checkbox.
17. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.
18. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 9d: Write an aggregation rule

There are six different rule types in Cloud SIEM -- lab exercises 9a through 9f will give you opportunities to create examples of all six types. However, they are optional for the completion of later labs, so you can decide which if any or all of the rule types you want to practice. When you are finished doing rule lab exercises, you can skip ahead to Lab 10 to continue the course.

An **aggregation rule** is useful when you want to fire a signal based on multiple conditions—up to six—being met over a period of time.

As an example, suppose you want to fire a signal when the ratio of failed to successful HTTP requests is too high—75% or more. You can use an aggregation rule to calculate the percentage of failed requests, and configure the rule to fire a signal when the request failure rate is 75% or higher.

Let's create an aggregation rule in Cloud SIEM:

1. Click **Cloud SIEM > Rules** in the left navigation menu if you are not already there.
2. Click **Create** in the upper right.
3. Select **Aggregation** rule.
4. **Name** your rule "Training Aggregation Rule XXX" with your initials in place of the XXX.
5. Enter the following under the "When Records matching the expression" field:
   `metadata_vendor="Microsoft"`
   a. `AND objectType = "Authentication"`
   b. `AND !isNull(success)`
6. Add "device_hostname" to the **grouped by** field in addition to the (default) "Entity Field".
7. Set the aggregation interval as "within 1 hour".
8. Create an aggregation called "success_logon" with "count" as the function.
9. Put "success = true" as the aggregation expression.
10. Create a second aggregation with the **Add** Aggregation button on the bottom. Call this one "failed_logon" with "count" as the function.
11. Put "success = false" as the expression for the second aggregation.
12. Put the following under the **that match the following condition** field:
    a. `((false_logon/(success_logon+false_logon))*100 > 80)`
13. On the right side, set the Entity to be "device_hostname".
14. Set the name and summary to be "High Percentage of Failed Logins".

©2025 Sumo Logic, All Rights Reserved.

15. Add a description of "Test Rule" or a description of your choice.
16. Set the next set of fields to "a dynamic severity of 3 for record field: device_hostname".
17. Click the "Add More Mappings" button to add another conditional mapping.
18. Set this mapping to be "if the value is greater than 20, then 9".
19. Click the "Add More Mappings" button again to add another mapping.
20. Set this mapping to be "if the value is greater than 10, then 6".
21. Add a "Custom Rule" tag
22. Select the **Save this rule as a prototype** checkbox.
23. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.
24. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 9e: Write an outlier rule

There are six different rule types in Cloud SIEM -- lab exercises 9a through 9f will give you opportunities to create examples of all six types. However, they are optional for the completion of later labs, so you can decide which if any or all of the rule types you want to practice. When you are finished doing rule lab exercises, you can skip ahead to Lab 10 to continue the course.

An **Outlier rule** allows you to generate a signal when behavior by an entity (such as a user) is encountered that deviates from its baseline activity.

For each outlier rule, you create a filter condition to look for out-of-the-ordinary behavior that could indicate risk. For example, an outlier rule might look for the events like the following:

- Spike in login failures from a user
- Abnormal number of high severity endpoint alerts
- Spike in EC2 instance creation
- Abnormal volume of data sent to third-party storage

Let's create an outlier rule in Cloud SIEM:

1. Click **Cloud SIEM > Rules** in the left navigation menu if you are not already there.
2. Click **Create** in the upper right.
3. Select **Outlier** rule.
4. **Name** your rule "Training Outlier Rule XXX" with your initials in place of the XXX.
5. Use the following expression:

```
metadata_vendor = 'Amazon AWS'
AND metadata_product = 'CloudTrail'
AND user_username_role != "cloudhealthreadonly"
AND NOT isEmpty(user_username)
AND fields["userIdentity.type"] = "IAMUser" AND NOT
array_contains(listMatches, 'AWS_admin_users')
```

6. Use "daily" as the baseline.
7. Select "user_username" as the entity
8. Set 5 days as the retention period, and 3 days as the baseline learning period.
9. Set "count" for the **Detect an outlier...** field
10. Set the **Model Sensitivity Threshold** to 1

©2025 Sumo Logic, All Rights Reserved.

11. Set the **Minimum Count Value** to 5
12. On the right side, set **On Entity** to "user_username"
13. The name of the signal will be "Spike in API Calls"
14. Set **using the summary** to "Excessive count of AWS API Calls from user [User Username] based on daily historic activity". (Use the '+' button to add a variable token marked with [ ]).
15. Add a description of "Test Rule" or a description of your choice.
16. Set the constant severity to 2.
17. Select the "UEBA" tag.
18. Select the **Save this rule as a prototype** checkbox.
19. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.
20. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 9f: Write a first seen rule

There are six different rule types in Cloud SIEM -- lab exercises 9a through 9f will give you opportunities to create examples of all six types. However, they are optional for the completion of later labs, so you can decide which if any or all of the rule types you want to practice. When you are finished doing rule lab exercises, you can skip ahead to Lab 10 to continue the course.

First seen rules allow you to generate a signal when behavior by an entity (such as a user) is encountered that hasn't been seen before. For example, a first seen rule might look for the events like the following:

- First time a user logged in from a new geographic location (geolocation)
- Newly created or added admin accounts
- High severity EDR alert seen for the first time
- MFA acceptance from first seen device

Let's create a first seen rule in Cloud SIEM:

1. Click **Cloud SIEM > Rules** in the left navigation menu if you are not already there.
2. Click **Create** in the upper right.
3. Select **First Seen** rule.
4. **Name** your rule "Training First Seen Rule XXX" with your initials in place of the XXX.
5. Use the following expression:

```
metadata_vendor = 'Proofpoint'
AND metadata_product = 'Targeted Attack Protection'
AND metadata_deviceEventId in ('MESSAGE_BLOCKED', 'MESSAGE_PERMITTED',
      'MESSAGE_DELIVERED')
AND threat_name = 'phish'
```

6. Select "http_url" for **has a new value for the field(s)**
7. Select "global" for the baseline
8. Set the baseline retention period to 2 days
9. Set the baseline learning period to 1 day.
10. On the right side, set the **On Entity** field to be "user_username".
11. Set the name to be "Proofpoint Global First Seen Domain"
12. Set the summary to be "HTTP URL seen for the first time".
13. Set a description of "Test Rule" or a description of your choice.

©2025 Sumo Logic, All Rights Reserved.

14. Set the constant severity to 1
15. Select a Technique > Phishing or Spearphishing tag
16. Select the **Save this rule as a prototype** checkbox.
17. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.
18. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 10: Create a rule tuning expression

To tweak existing rules we can create a rule tuning expression to add to one or more rules. In this lab exercise we'll create an exception to the rules we created earlier that ignores them if the record contains a specific email address.

1. Click **Cloud SIEM > Rule Tuning** in the left navigation menu (under the **Security Detection** header).
2. Click **Add Rule Tuning Expression** in the upper right.
3. **Name** your rule tuning expression "XXX Tuning Expression" with your initials in place of the XXX. You can optionally add a description.
4. Select **Tune selected Rules**.
5. Use the search bar with your initials to find one or more of the rules you created in the earlier exercises. Select them using the dropdown.
6. Select "exclude" for the **Records that also match the expression** field.
7. Add the following expression to the text field at the bottom (with your chosen login number in place of the XXX):
   a. `user_email='training+analystXXX@sumologic.com'`
8. Some tips when writing rule tuning expressions
   a. **Best practice:** When a rule tuning expression is added to a rule, it's appended with an `AND` statement. Rule tuning expressions are usually exceptions to the rule. Keep this in mind when writing the logic.
   b. **Tip:** The autocomplete feature can help you write the logic. For example, typing "ip" will bring up a dropdown showing all available fields related to IP addresses.
   c. **Tip:** Syntax coloring can help you write the logic. Try using single quotes (`'...'`) instead of double quotes (`"..."`). Notice that the syntax coloring lights up correctly when you use single quotes, which is the best practice.
   d. **Tip:** If you are adding an exception, you can use "include" instead of "exclude" as long as you switch to the `is not` (`!=`) operator instead of is (=). For example, you can also allow yourself as an exception by using "include" and typing this: `user_email!=<your email>`. Either way, the rule will trigger as long as the email address is not yours!
9. Click **Submit** to save your rule tuning expression.
   a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.

©2025 Sumo Logic, All Rights Reserved.

10. Verify your tuning expression exists by going to **Cloud SIEM > Rule Tuning.** You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 11: Create a custom Insight

You want to be alerted right away when one of your custom rules is triggered. Create a custom Insight that looks for only this rule.

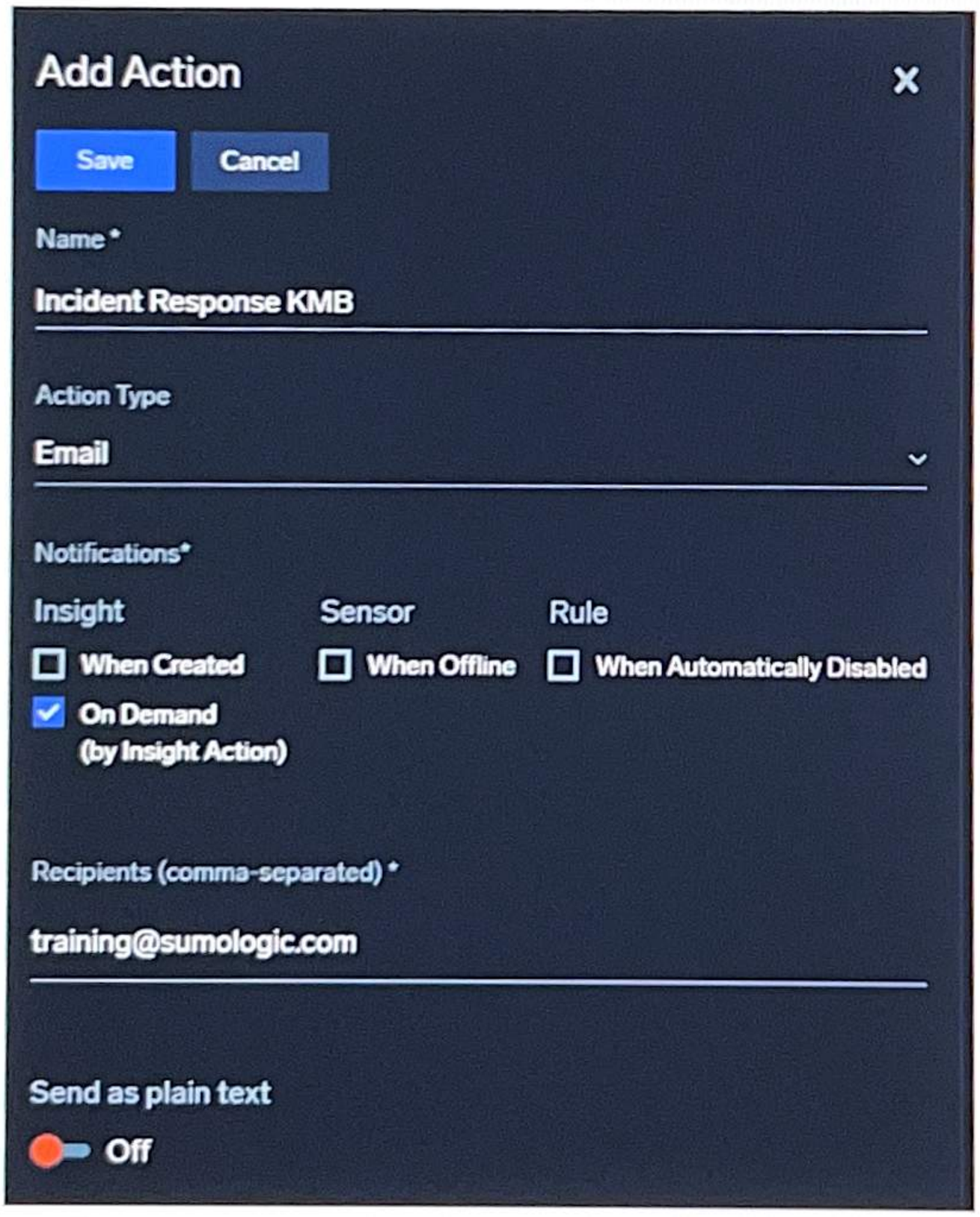
1. Click **Cloud SIEM > Custom Insights** in the left navigation menu (under the **Security Detection** header).
2. Click **Add Custom Insight** in the upper right.
3. **Name** your Insight "Custom Insight XXX" with your initials in place of XXX.
4. Select "Rules" from the **When Signals are created with the following...** field.
5. Select one or more of the rules you created earlier (use your initials to search).
6. Choose **in any order.**
7. On the right side, configure the **Insight** that will be created once the rule is triggered. The name will be automatically filled from your Insight name on top. Fill in "Test Insight" as the description (or one of your choice).
8. Keep the defaults "constant" and "low".
9. Add one or more tags from the drop-down menu
    a. **Best practice:** Insights are named based on the tactics and techniques tagged in the signals. Consider which tactic or technique from the MITRE ATT&CK framework your rule(s) are looking for when selecting tags.
10. Click **Submit** to save your Insight.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings.
11. Verify your Insight exists by going to **Cloud SIEM > Custom Insights.** You should see it there.

©2025 Sumo Logic, All Rights Reserved.

Lab 12: Customize the actions button

The Actions button is available in all Insights in Cloud SIEM and can help you collaborate with teammates. In this lab, we'll create a custom Actions button to alert your incident response team.

1. Click **Cloud SIEM > Actions** in the left nav menu (under **Cloud SIEM Integrations**).
2. Click **Add Action**.
3. **Name** your action "Incident Response XXX" with your initials in place of XXX.
4. For **Action Type**, select **Email**
5. Under **Notifications** select **On Demand**.
6. In the **Recipients** field, enter your email (if you want to receive the email notification for inspection) or a fake email such as **incidentresponse@sumologic.com**.



7. Click **Save** when finished.

©2025 Sumo Logic, All Rights Reserved.

Now, we'll test our new actions button.

1. In the left navigation menu, click **Cloud SIEM > Insights**.
2. Click the name of any **Insight**.
3. In the left pane, click **Actions**. You should see your new **Incident Response** action available.
4. Click **Execute** to use the new action.

©2025 Sumo Logic, All Rights Reserved.