Chronicle SOAR user's

TIPS AND TRICKS

#1

Create requests that can be ingested as cases later on!
Start by configuring a request template for other users and end customers to fill out on the homepage.
Those requests will then be ingested into Chronicle SOAR as "request cases" and can either be handled manually by an analyst or automatically through a playbook.

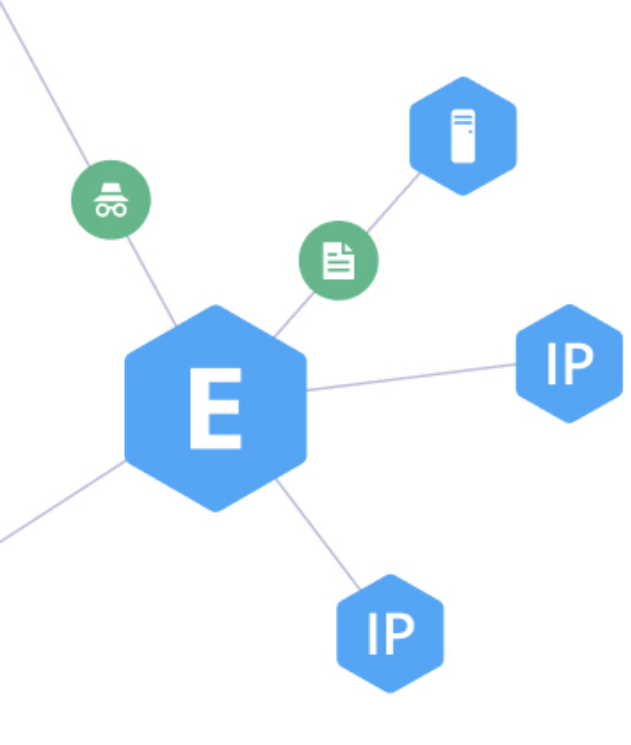
For example
Users can fill out a request to hunt an IOC or block a malicious URL within the organization

#2

Do you have an enrichment playbook/block that runs on alerts before your Tier 1 triages it?

Start by creating a placeholder role and assigning the case to it until the enrichment is complete. Once the alert is actionable you can assign the case back to Tier 1 for a clear view.

#3



Using the 'tools' power-up (marketplace > power ups > tools) you can use the action 'create entity relationships' to create a new entity and define its relationship to other entities in a single playbook action.

#4

Blocks are your friend! Make blocks for all environments and even reuse them. Blocks can and should contain enrichment, OSINT, CSINT and actions that differ on endpoints and servers (remember to isolate endpoints but not servers).

If you are a MSSP and are using a MSSP-specific version of a MDR product, you can make an all environment playbook to run on all environments for that product. Deviation is only needed when a client needs something special or out of the norm.

#5

- This tip can be used in conjunction with other tips such as assigning the case to a placeholder role (tip 2) during enrichment.
- Do you have a playbook or block that needs to run on only the FIRST alert in a case? For example, let's say that you want to assign a playbook to run in parallel to your enrichment or noise reduction playbooks which assigns the case to a placeholder role if the case is currently assigned to "Tier 1".
- You may not want to attach that playbook if it's not the first alert of the case because it may delay it being triaged when it is actually actionable. So, how do you make sure you only run that playbook on the first alert of the case (when it's possible that the first alert of the case may change due to automation/noise reduction)?
- An alert comes in and a new case is opened. Towards the beginning of your playbooks attach a GETFirstAlertContextValueBlock.

GETFirstAlertContextValueBlock

1. Siemplify: Get Context Value Action
   Scope: Case
   Key: [Case.Id]-FirstAlert

2. Condition Action:
   IF: The result is: "Not found value for key: [Case.Id]-FirstAlert in scope Case"*
   *This implies that the "first alert" context value hasn't been set yet.
   THEN: attach SETFirstAlertContextValueBlock and then attach any other blocks/playbooks for when a case is first opened .
   ELSE: proceed with enrichment/other blocks.

SETFirstAlertContextValueBlock

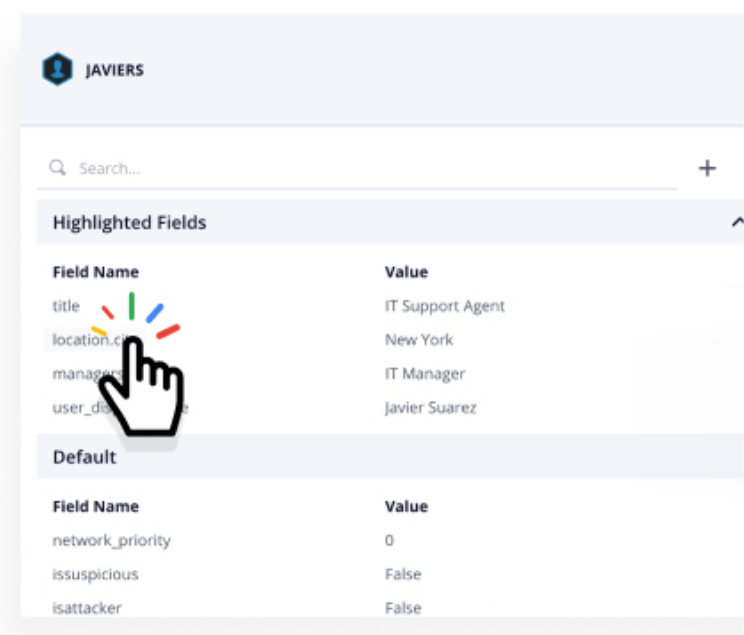
1. Siemplify: Get Scope Context Value Action

2. Set Context Value
   Value: [Find First Alert.ScriptResult]
   Key: [Case.Id]-FirstAlert
   Scope: Case

Any time you close an alert (including via noise reduction/ automation) in the playbook, run the SETFirstAlertContextValueBlock afterwards. This way, if the alert being closed is currently the first alert of the case, the NEW "first" alert of the case is assigned to the First Alert Context Value. If the alert being closed is NOT currently the first alert of the case, then the First Alert Context Value doesn't actually change by running this block

#6

You can change the enrichment value of an entity by double clicking on the field



#7

Internal entities are compared to the configured domains located in Settings → Environments > Domains!
The following three options are available for using internal entities:

1. SourceUsername/DesintationUsername
contains the domain When the SourceUsername or DestinationUsername contains a domain which is configured undersettings - the entity will be marked as internal.

Example
chronicle.security configured under settings > Environments > domains
toms@siemplify.co is mapped as SourceUsername
The entity will be marked as internal

2. Using NTDomain field
When the domain is not part of the SourceUsername/ DestinationUsername entity but is part of the event fields, you can map it to the System > NTDomain field.
When the System > NTDomain field is mapped and its value is contained in the Settings > Environments > Domains list, the entity will be marked as internal.

Example
- chronicle.security configured under settings > Environments > domains
- toms is mapped as SourceUsername
- chronicle.security is mapped as NTDomain
- The entity will be marked as internal

3. Using DNSDomain field

A. You can also link the username and the domain in case they are ingested as two different event fields
(e.g. username: toms, domain: siemplify.co.
Then they will be link as toms@siemplify.co)

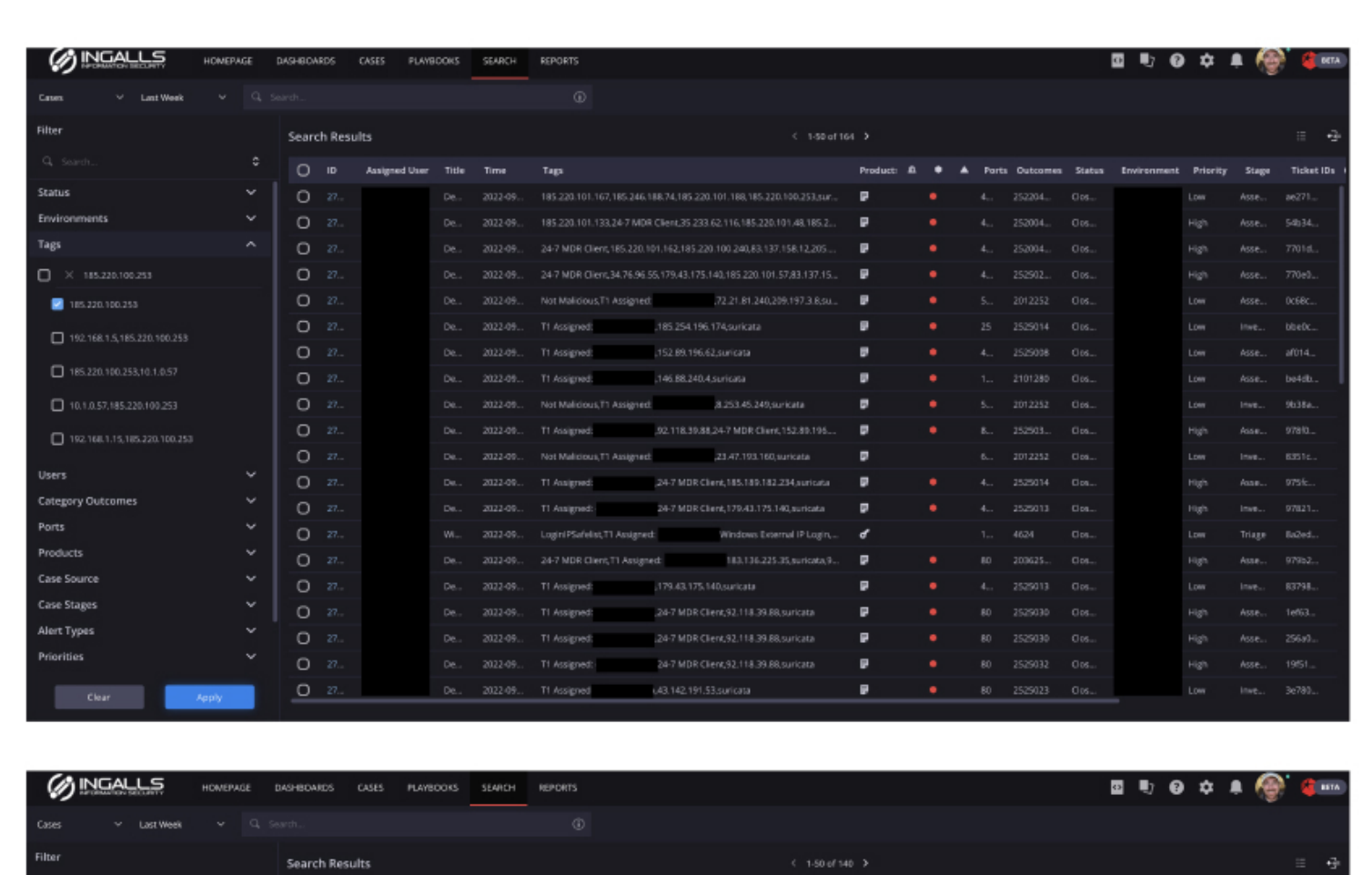
B. When the System > DNSDomain is mapped, the value will be added to any SourceUsername/DestinationUsername that will be created in the alert.

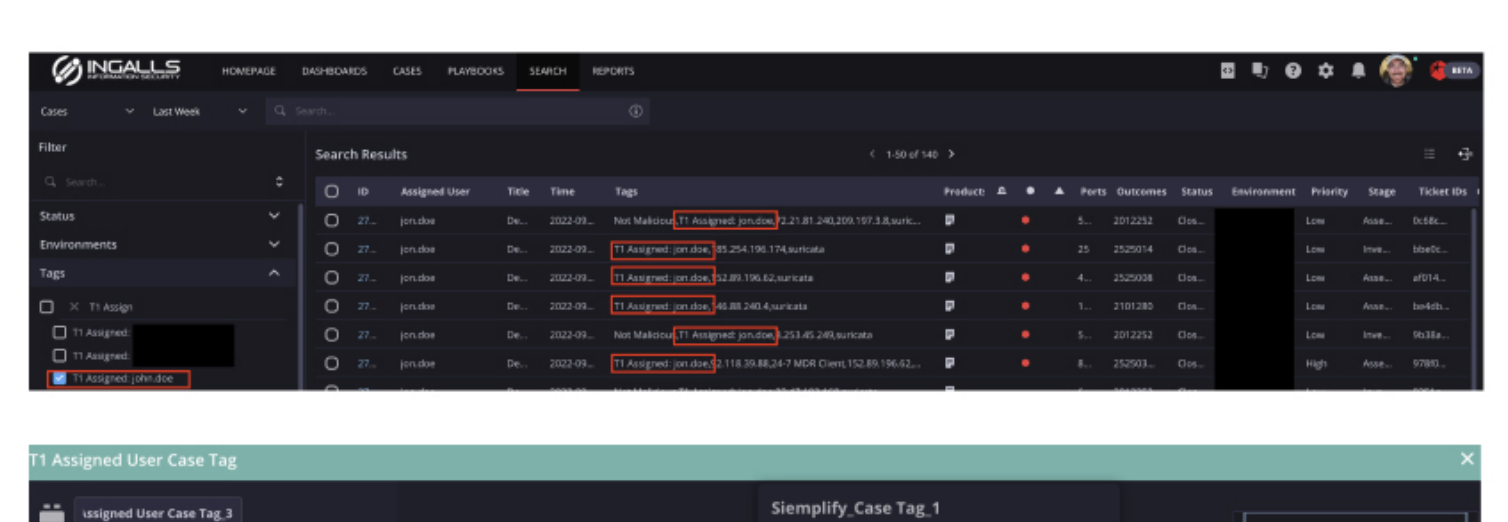
#8

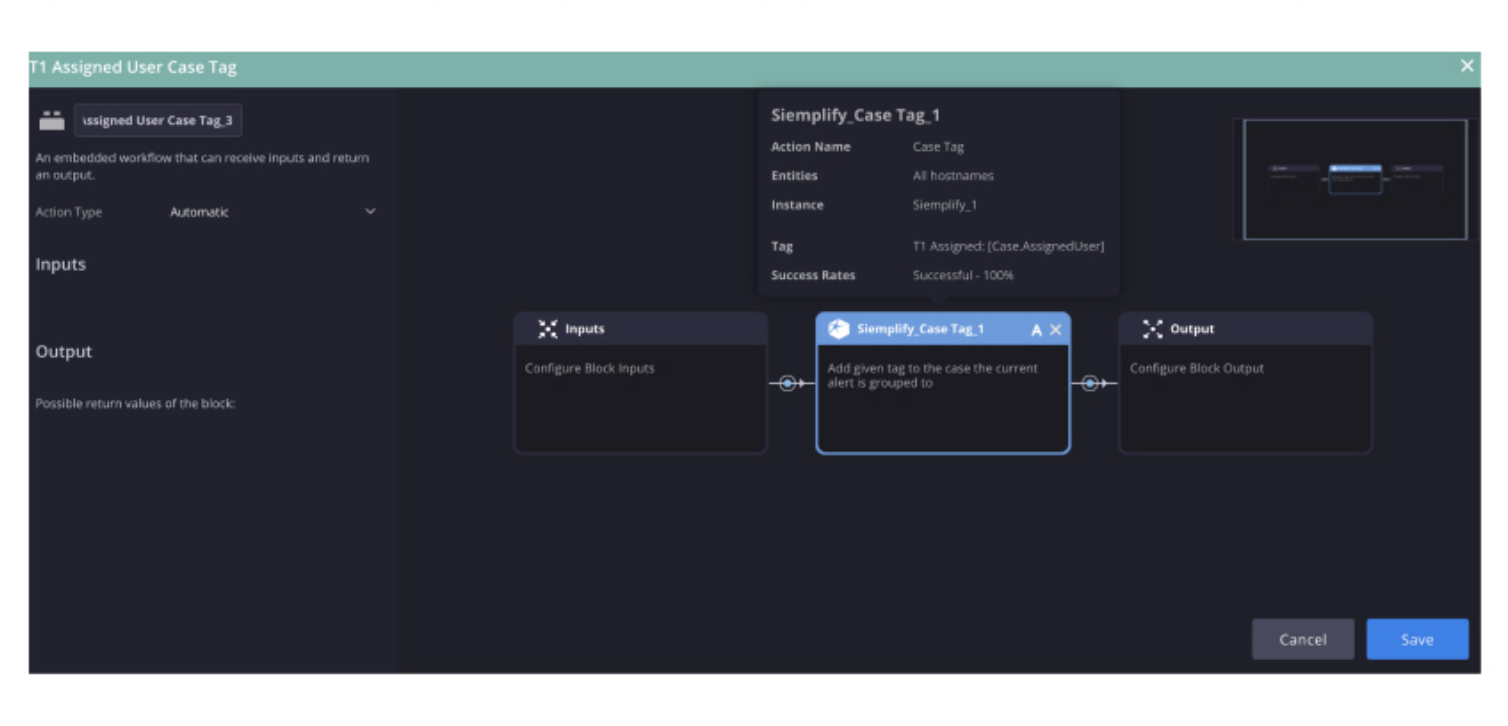
You can tag a case with the name of the analyst working the alert (create a tag with the value `T1 Assigned: [Case.AssignedUser]`)

to easily search for cases triaged by that user (the "Assigned User" at the end of the playbooks may not be the same person as the T1 Analyst who triaged the alert, so searching by "Assigned User" isn't always helpful) and to fine tune reports and dashboards.

We have a simple block that we use right after the first T1 triage interaction in a playbook for that purpose. You can also tag cases with specific entities (external IP address for example) for reporting or to bulk search for/close cases involving that entity.

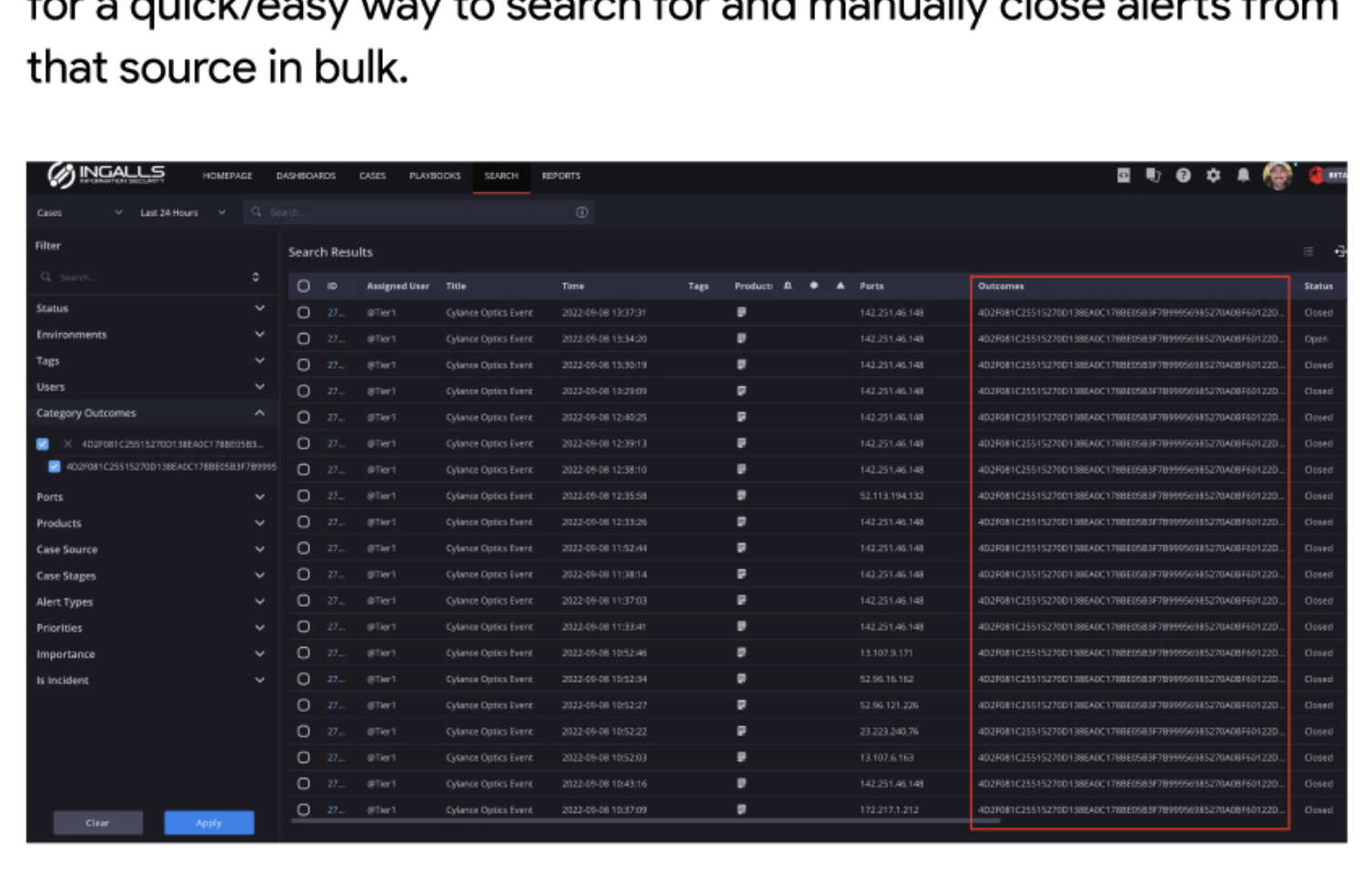




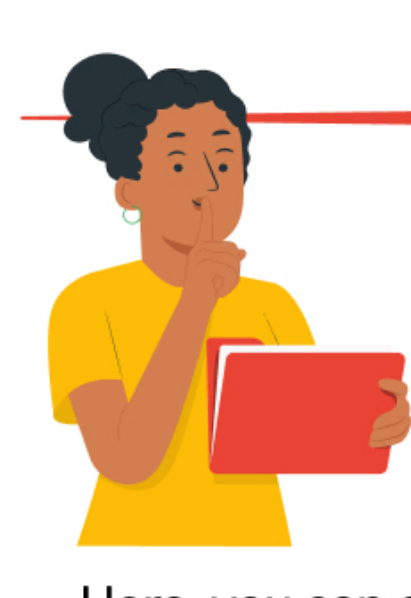


#9

You can map an event field (such as a hash value on an EDR alert or AV quarantine) to Ports or Outcomes in your Alert Ontology for a quick/easy way to search for and manually close alerts from that source in bulk.

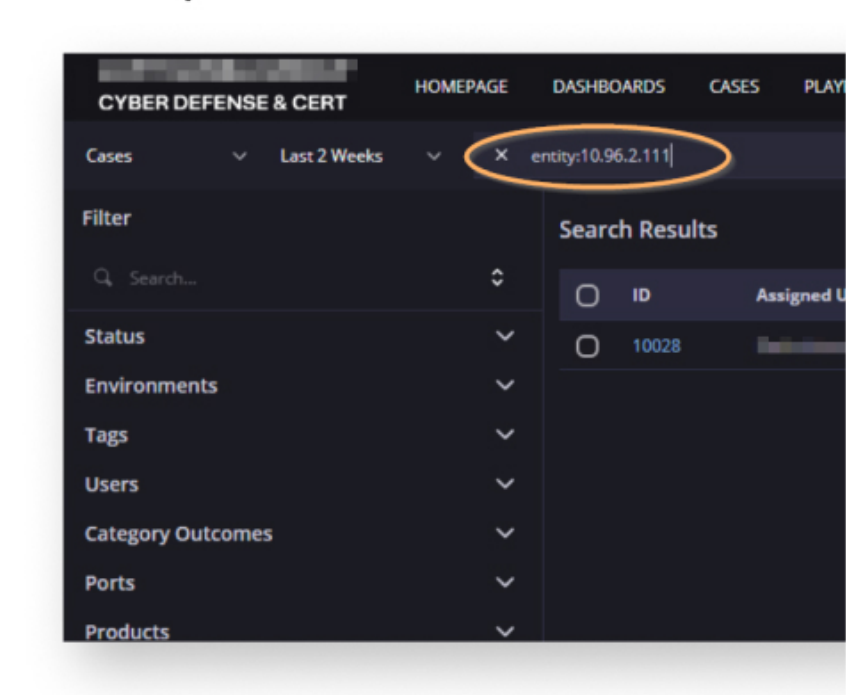


#10



The "Case Search" screen accepts a "secret" input keyword which is not described in the little (i)nfo dialogue, at least up until version 5.6.x.

Here, you can enter "entity:xyz", where xyz can be a substring of an entity you're looking for.
The search will then return all cases with at lease one entity matching this string in the given timeframe.



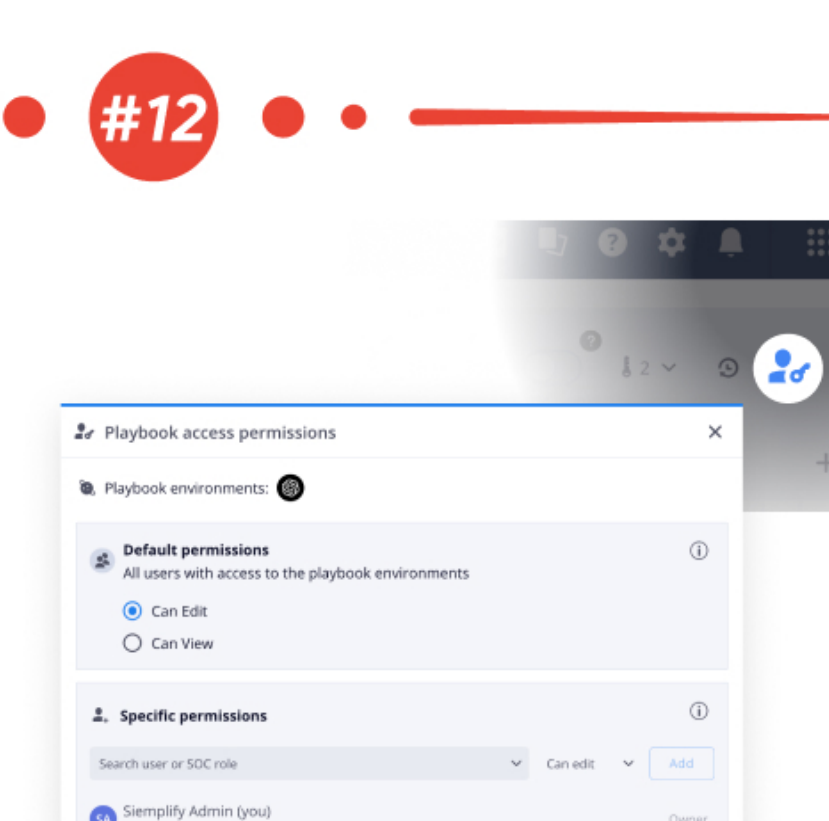
#11

Connectors can be complex. To make your life easier and the connector execution more straightforward, you can always:

- Reduce the "Run Every"
- Reduce the "Max number of alerts/events per iteration"
- make sure the configured "time backwards" is really needed and you don't query for too long

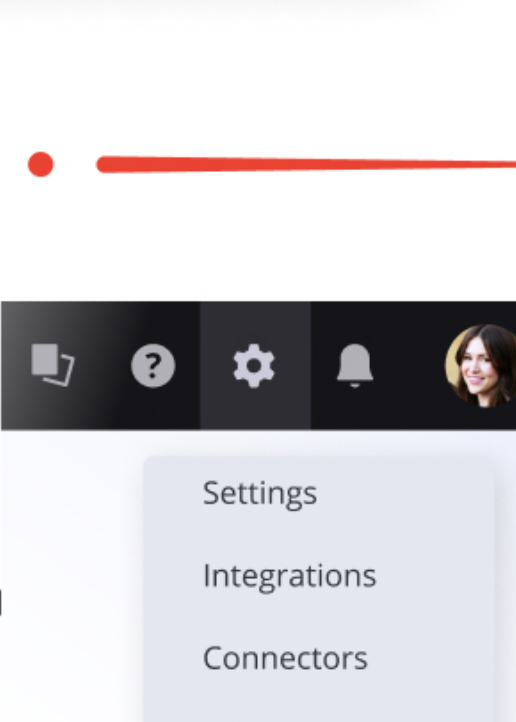
#12

You can restrict edit permissions for a specific playbook by using the Playbook permissions screen



#13

Here's a quick tip for customization! You can change how an alert will look in the views module.



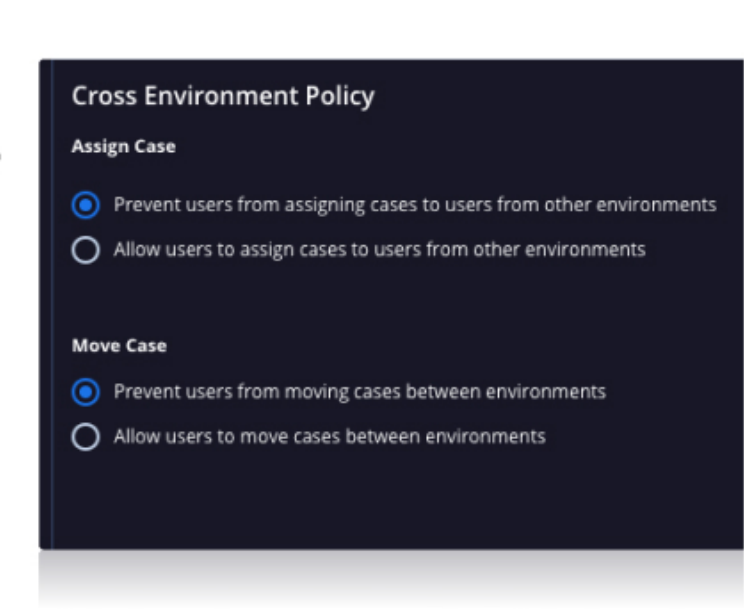
#14

Chronicle SOAR integrations offer many useful actions.
Two of the most useful actions that were recently released are the "Get/Set Context Values". These allow you to save content you care about, update it with different scopes (General, alert, case etc..) and get it whenever and wherever you want!

Click Get and Set to check it out

#15

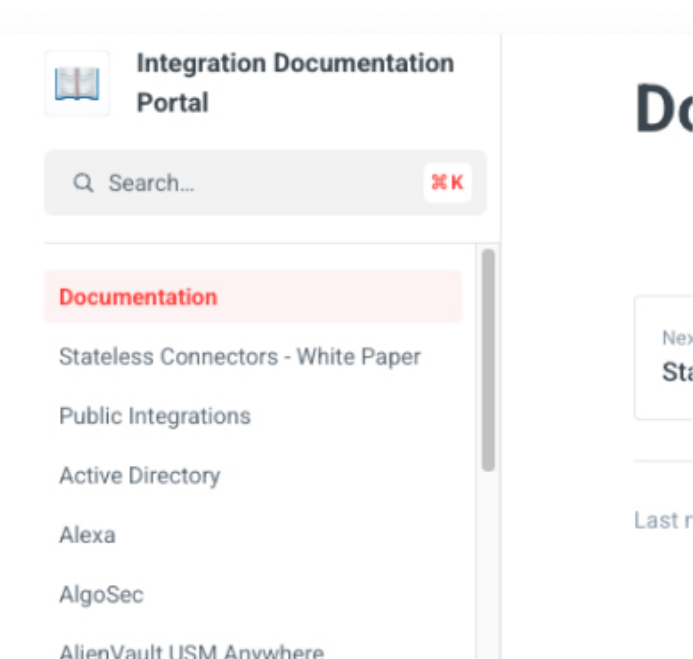
You can enable users to move case to a new environment by enabling this functionality from the Settings menu (Settings → Advanced → General)



#16

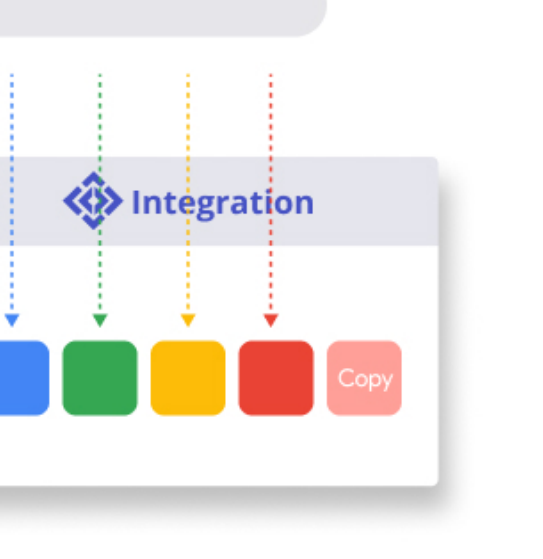
Check out the integration portal for useful information about configuring integrations and how to work with actions.

Visit the Integration Portal



#17

Duplicating specific components in integrations doesn't mean the entire integration is now customized - you will still get updates and fixes on the commercial components.



#18

Importing a custom integration with the same commercial integration identifier will update/replace the existing one