

# QRadar SOAR Bootcamp Training

IBM QRadar SOAR



**IBM**<sup>®</sup>

# Labs plan

---

Lab 1 : Prepare the environment

Lab 2 : Incident Creation & Editing

Lab 3 : Working with the Privacy Module  
and Breach

Lab 4 : Reports & Dashboards

Lab 5 : Field & Tab Customization

Lab 6 : Incident Types, Phases, and Tasks

Lab 7 : Scripts

Lab 8 : Rules

Lab 9 : Additional script and rule

Lab 10 : Inbound Email

Lab 11 : Playbooks

Lab 12 : Install the Integration Server

Lab 13 : Installing QRadar SOAR Circuits as a Service

Lab 14 : install the apphost package

Lab 15 : install your first app

Lab 16 : Install fn\_utilities app

Lab 17 : Create new Custom Playbook that uses our  
Shell Command Function

Lab 18 : Install nmap in AppHost and remote control to VM

Lab 19 : Install the Components File for App Host

Specific last half day for Partners & IBMers: Link your QRadar to SOAR

Lab 20 : Reserve a QRadar for demo on TechZone – Must Have a Partner IBMID or be IBMers for the Labs

Lab 21 : Configure your QRadar to send Alerts to SOAR

Lab 22 : Configure your SOAR to Query QRadar with 2 apps

Lab 23 : Create offense and see them in SOAR

# CEST Agenda

EMEA & APAC

## Day 1:

8h30 – 10:00 SOAR presentation and positioning – Demo of a successful automated playbook

10:00 – 10:15 Break

10:15 – 12:00 Labs 1-2-3-4 + Q&A

## Day 2:

8h30 – 10:00 Labs 5-6-7-8

10:00 – 10:15 Break

10:15 – 12:00 Labs 9-10 + Q&A

## Day 3:

8h30 – 10:00 Playbook Design – Lab 11

10:00 – 10:15 Break

10:15 – 12:00 Labs 12-13-14-15 + Q&A

## Day 4:

8h30 – 10:00 Labs 16-17

10:00 – 10:15 Break

10:15 – 12:00 18-19 + Q&A

## Day 5:

8h30 – 10:00 Labs 20-21

10:00 – 10:15 Break

10:15 – 12:00 22-23 + Q&A

QRADAR SOAR TRAINING

# EST Agenda

US & CANADA

## Day 1:

9h30 – 11:00 SOAR presentation and positioning – Demo of a successful automated playbook

11:00 – 11:15 Break

11:15 – 13:00 Labs 1-2-3-4 + Q&A

## Day 2:

9h30 – 11:00 Labs 5-6-7-8

11:00 – 11:15 Break

11:15 – 13:00 Labs 9-10 + Q&A

## Day 3:

9h30 – 11:00 Playbook Design – Lab 11

11:00 – 11:15 Break

11:15 – 13:00 Labs 12-13-14-15 + Q&A

## Day 4:

9h30 – 11:00 Labs 16-17

11:00 – 11:15 Break

11:15 – 13:00 Labs 18-19 + Q&A

## Day 5:

9h30 – 11:00 Labs 20-21

11:00 – 11:15 Break

11:15 – 13:00 Labs 22-23 + Q&A

# QRADAR SOAR TRAINING

# Lab 1

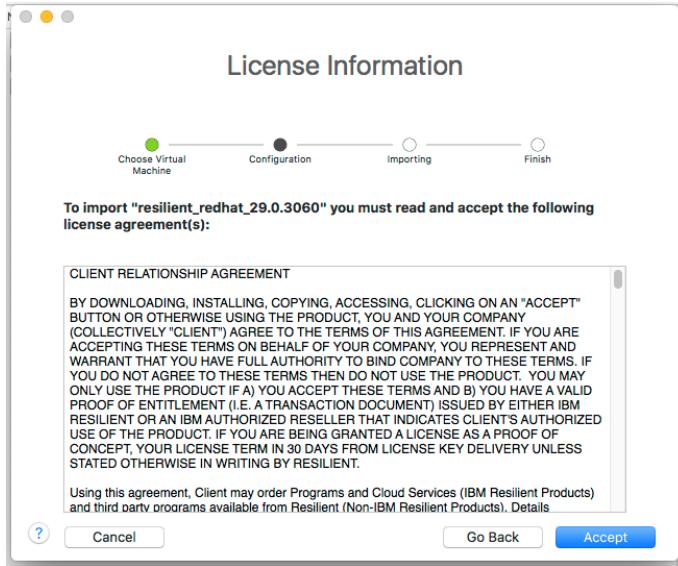
If you are working under a remote Saas Lab like ***emea-training***, most of this lab has been done to setup the remote saas environement. Please check each page if some action need to be done

Goal :

- Initialize a working environment
- Initialize a prepared Virtual Machine

# Import the OVA To VMware

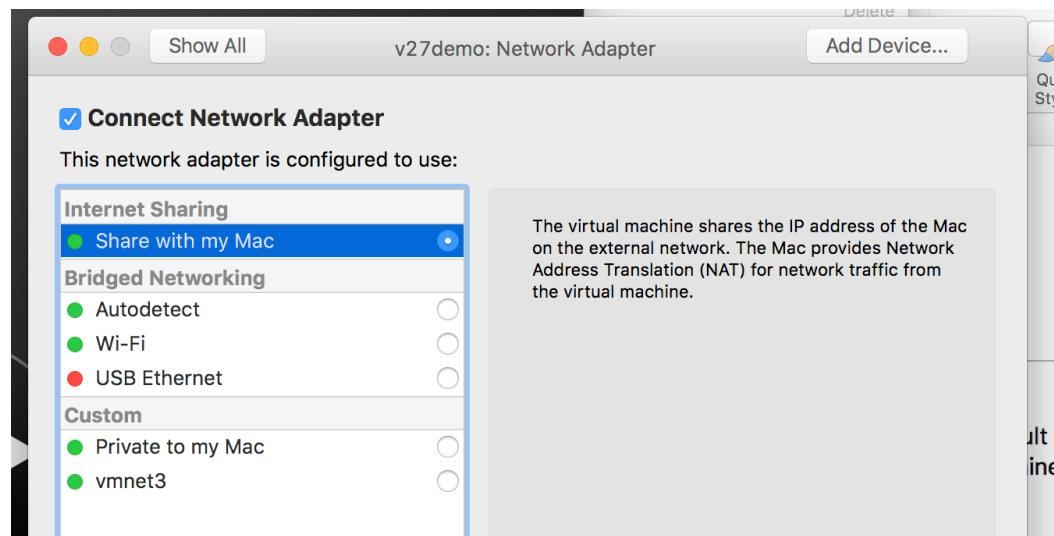
Not Able on Remote Saas **emea-training** Lab



We have found that at different locations, we have had to change the network settings from Bridge to NAT.

Start with NAT and if you have problems later on, please try changing to Bridge.

## Import to VMware or VirtualBox



# Create your passwords

Not Applicable on Remote Saas **emea-training** Lab

```
Changing password for user root.  
New password:  
BAD PASSWORD: The password contains less than 4 character classes  
Retype new password:  
passwd: all authentication tokens updated successfully.  
  
Changing password for user appadmin.  
New password:  
BAD PASSWORD: The password contains less than 4 character classes  
Retype new password:  
passwd: all authentication tokens updated successfully.  
  
Please note, SSH is disabled for root.  
In the future, please use appadmin for SSH to this system.
```

Create a password for the “**root**” and “**appadmin**” account

*Tips: the password “**resilient**” works well for demo on any keyboards*

# Get the IP for QRadar SOAR

Not Applicable on Remote Saas *emea-training* Lab

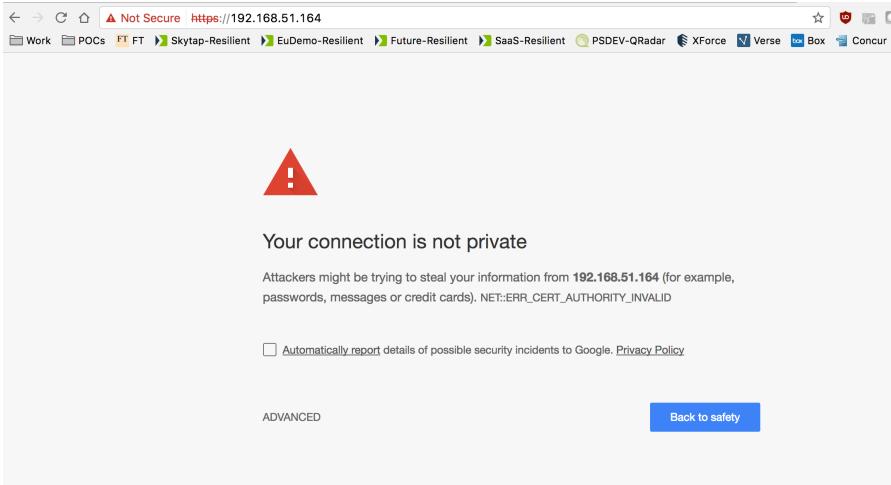
Choose dhcp and check that QRadar SOAR found an IP.

If it has not, please try changing your network card for the virtual machine, then restart.  
As a last resort, or if required, you can set a static IP.

```
Please review the network settings:  
BOOTPROTO    :  dhcp  
IP ADDRESS   :  10.10.10.154  
Does this look correct? Y/[N] y_
```

The system will then reboot.

# Access QRadar SOAR GUI



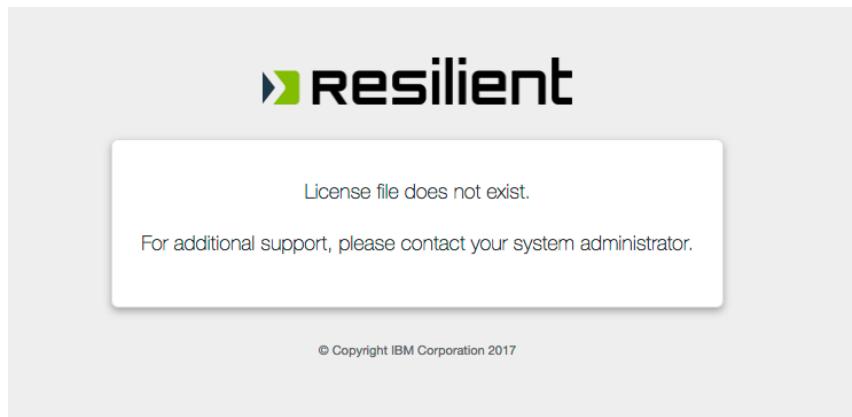
You will see a warning screen that you have no license installed.

Not Applicable on Remote Saas **emea-training** Lab  
Please use:  
<https://emea-training.poc.resilientsystems.com/>  
Go to [https://<resilient\\_ip>](https://<resilient_ip>)

You need to replace <resilient\_ip> with the ip of your machine.  
If you did not get an ip in the dhcp settings section, you can use this command to find it:

ifconfig

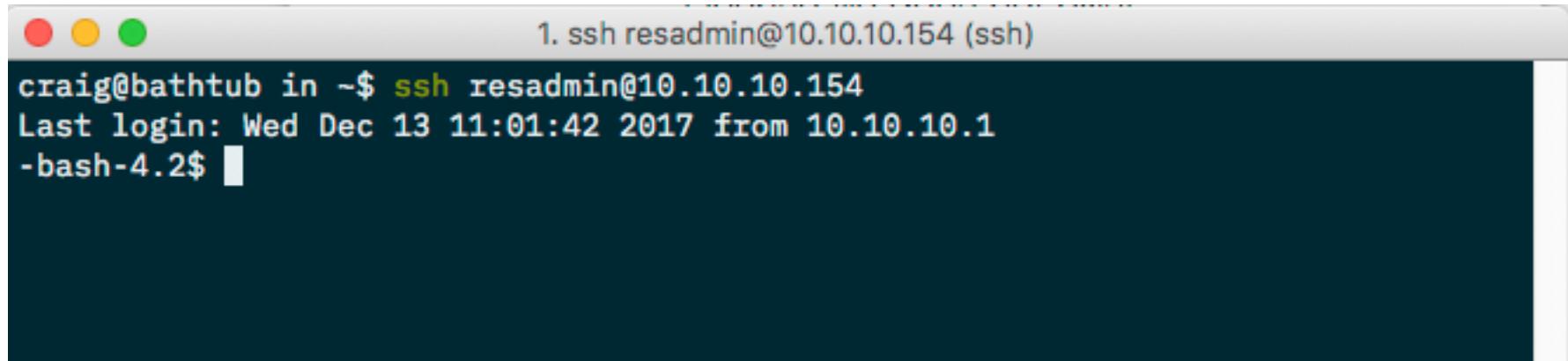
You will get a self-signed certificate warning, click through this.



# Login to QRadar SOAR CLI

Not Applicable on Remote Saas *emea-training* Lab

Login with appadmin via SSH using terminal (Mac) or putty (Windows).



The screenshot shows a Mac OS X terminal window with three colored window control buttons (red, yellow, green) at the top left. The title bar reads "1. ssh resadmin@10.10.10.154 (ssh)". The main pane of the terminal displays the following text:

```
craig@bathtub in ~$ ssh resadmin@10.10.10.154
Last login: Wed Dec 13 11:01:42 2017 from 10.10.10.1
-bash-4.2$
```

You can use 'sudo su –' to gain root or use sudo for root requiring commands

# Import license

```
-bash-4.2$ sudo license-import  
[Please enter or paste in the license:  
-----BEGIN LICENSE-----  
AB+LCAAAAAAAACFkMtqwzAQRX8lzMqtH7IcWxBooS6F0i5aAt205DE1sS2jB00o/fe0yS  
rZRAIN3EHzp1fcDh3dgIFXfpfyfPo4VF9Nu4METPTBTuTecSLufrabu83+lZ/2rX3kvicT  
3RB07Yx6pA5UcJESo0My0AyDnUHlslxvna0ngejJzWeaoR5NJfJaYiH6Sme1kSLXhegyWU  
udM39B73+sYzDkjSh1gZq2ZdNtRa+17mWhC90YiSQRzmwPao7jmICjxe7dyD+/Q1i8StNb  
fuqWxcPKvDdW+JPnMqmyFOmqrZtAZ0seR8/50azz/bPjoDz+4Xo9kS4FHvxSMHg14ILmQv  
r7B4Zs/3u1AQAA:MCwCFCjzDQLi8Sw4kggESwcWWG6ux3UpAhRBx5+kRHCIG+xS/qevUMd  
l+Kzefg==  
-----END LICENSE-----  
Successfully imported license  
Customer name: SE - UK - EMEA  
Expiration: 22-Dec-2018  
US regulators enabled: true  
CA regulators enabled: true  
EU regulators enabled: true  
APAC regulators enabled: true  
Security module enabled: true  
Actions framework enabled: true  
Users: Unlimited  
  
-bash-4.2$ █
```

Run:  
sudo license-import

Paste in the license from the file provided by your instructor. Don't forgot to include the top and bottom dashed lines.

Press Enter

# Create first Administrator User

Run the resutil newuser command to create a User account.

**You can use the commands text file in the Bootcamp folder so you do not have to write the commands out.**

```
-bash-4.2$ sudo resutil newuser -createorg -email YourEmail@Company.com -first "FirstName" -last "LastName" -org "YourOrg"
```

This should be an actual email address, you will use it to log into the platform.

Your first name      Your surname

```
-bash-4.2$ sudo resutil newuser -createorg -email YourEmail@Company.com -first "FirstName" -last "LastName" -org "YourOrg"
```

This can be the name of your company, or you can set it to IBM if you like.

**Example** (Please do not use the values from the example) :

```
-bash-4.2$ sudo resutil newuser -createorg -email jessica.c@uk.ibm.com -first "Jessica" -last "Cholerton" -org "IBM"
[Enter the password for the user:
[Confirm the password for the user:
Creating a new user Jessica Cholerton <jessica.c@uk.ibm.com>
Creating a new organization IBM
Adding the user Jessica Cholerton <jessica.c@uk.ibm.com> to the organization IBM
Assigning the following roles to user jessica.c@uk.ibm.com: Master Administrator
-bash-4.2$
```

Do not use “ “ unless you are using more than one word and using a space to separate them.

Not Applicable on Remote Saas **emea-training** Lab

you already have been invited as Masteradmin to the Saas location

# Setup Email Technical Account used by QRadar SOAR

You will have been asked to have an email account ready to use for QRadar SOAR. You can use any SMTP account.

(We have a mail-in-a-box account you can use if required.)

Run:

```
sudo resutil smtpeedit -email resilientaccount@gmail.com -name "Resilient Platform" -host smtp.gmail.com -user resilientaccount@gmail.com -port 587
```

y@mail.poc.resilientsystems.com

Technical Account email address

Example (Please do not use the values from the example) :

```
[-bash-4.2$ sudo resutil smtpeedit -email resilient.jess@gmail.com -name "Resilient Platform" -host smtp.gmail.com -user resilient.jess@gmail.com -port 587  
[Enter the password for the user:  
[Confirm the password for the user:  
Successfully edited the SMTP configuration  
SMTP Host: smtp.gmail.com  
SMTP Port: 587  
SMTP User: resilient.jess@gmail.com  
SMTP Password: hidden  
SMTP From Email: resilient.jess@gmail.com  
SMTP From Name: Resilient Platform  
SMTP StartTLS Enabled: true  
SMTP Whitelist Hostnames:  
-bash-4.2$ ]
```

This password  
needs to be the  
password you log  
in to the email with

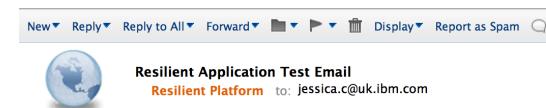
Not Applicable on Saas **emea-training** Lab  
you will receive emails from  
**donotreply@mail.poc.resilientsystems.com**

Now we need to test that it is working.

Use any email address that you can  
check, e.g. your work email

```
[-bash-4.2$ sudo resutil smtptest -email jessica.c@uk.ibm.com  
Successfully sent the test email to jessica.c@uk.ibm.com  
-bash-4.2$ ]
```

```
sudo resutil smtptest -email <your_work_email>
```



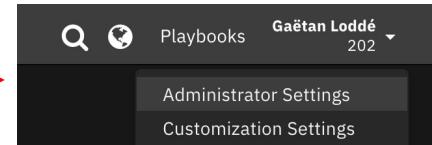
# Setup Email Technical Account Help

- If you are using gmail, you will need to enable low security for apps, otherwise the email will not work, access the settings using this link:  
**(<https://myaccount.google.com/lesssecureapps>)**
- If you get the following error message, it means that you haven't put your email address password in correctly. It needs to be the password that you log into your emails with.

```
-bash-4.2$ sudo resutil smpttest -email jessica.c@uk.ibm.com
[sudo] password for resadmin:
An error occurred while running the command line utility: Sending the email to the following server failed : smtp.gmail.com:25
Sending the email to the following server failed : smtp.gmail.com:25
[ 534-5.7.9 Please log in with your web browser and then try again. Learn more at
534 5.7.9 https://support.google.com/mail/?p=WebLoginRequired i66sm22589636wmd.0 - gsmtp
```

# Add more users and team

To reach Administrator Settings click on your user name at the top right corner of the screen



Go to Administrator Settings > Users > Invite Users > and invite the following users by their emails (replace YOURNAME by your Real Name ! – You may use another free email platform)

First Name	Last Name	Email	Permissions
Tier1	Analyst	Tier1Analyst.YOURNAME@yopmail.com	None
Tier2	Analyst	Tier2Analyst.YOURNAME@yopmail.com	None
Legal	Counsel	LegalCounsel.YOURNAME@yopmail.com	None

Go to <https://yopmail.com> and validate each user

Note: If Yopmail doesn't work, you can use any temporary mailbox service  
Just be sure to use the mail generated by the temporary mailbox service you will be using

The screenshot shows an inbox with one unread email. The email is from 'IBMResilientPOC <donotreply@mail.poc.resilientsystems.com>' dated '2020-03-20 10:29'. The subject is 'Benoit ROSTAGNI invites you to join an organization ...'. The body of the email reads:

Benoit ROSTAGNI has invited you to join one or more organizations within the Resilient Security, Orchestration and Response (SOAR) platform: 202.

If you already have a Resilient account, you can log in to the Resilient platform then click on the system menu next to your user name to view the additional organizations you can access.

The Resilient platform enables teams to orchestrate and automate the people, processes, and technology that are associated with incident response. If you are unfamiliar with the Resilient platform, you can access the Getting Started guide from: <https://www.ibm.com/support/knowledgecenter/SSBRUQ>.

To accept this invitation, click on the following link to log in to the Resilient platform. If this is your first time logging in, you will be asked to create a password.

[https://warbler.poc.resilientsystems.com/invite/index.jsp?authkey=-Eq9pfxiDfcKwiP7r-PtqHoSXRxW9c7Qg\\_uWP3oHd8mxIMIqdGf7mv/Hzb99/fgpWkSiCDM4mAV3a\\_Ekgxg](https://warbler.poc.resilientsystems.com/invite/index.jsp?authkey=-Eq9pfxiDfcKwiP7r-PtqHoSXRxW9c7Qg_uWP3oHd8mxIMIqdGf7mv/Hzb99/fgpWkSiCDM4mAV3a_Ekgxg)

Create your IBM Resilient account.

tier1analyst.rostagni@yopmail.com

First Name: Tier1

Last Name: Analyst

Email: T1A

Office Phone:

Cell:

\*\*\*\*\*

\*\*\*\*\*

I have read and agree to the [Terms of Use](#).

Create your account.

# Create groups and add users

To access the User Settings in platform:

Click on Username (upper right) → Administrator Settings → Users

Click on each of the 3 Users you just created and edit permissions to match the roles in the following table



Display Name	Email	Last Login	Roles
Gaëtan Loddé	gaetan.lodde@ibm.com	09/30/2021 15:11	Master Administrator Administrator
Legal Counsel	legalcounsel.lodde@yopmail.com	07/27/2021 14:51	Observer
Tier1 Analyst	tier1analyst.lodde@yopmail.com	07/27/2021 14:44	Incident Creator Observer
Tier2 Analyst	tier2analyst.lodde@yopmail.com	07/27/2021 14:48	Incident Creator Observer Administrator

Now, click on the “Groups” tab and create the following Groups:

Group Name	Members	Permission
CSIRT	Your User Account, Tier2 Analyst	Administrator
Analysts	Tier1 Analyst, Tier2 Analyst	Incident Creator
Legal Team	Legal Counsel	Observer

# Enable Threat Intelligence

Click on Username (upper right)→ Administrator Settings→ Threat Sources

The screenshot shows the 'Administrator Settings' page in the IBM Security QRadar SOAR interface. The top navigation bar includes links for 'IBMSecurity QRadar SOAR', 'Dashboards', 'Inbox', 'Artifacts', 'Incidents', 'Create incident', and a search icon. On the far right, it shows the user 'Gaëtan Loddé' and '200'. Below the navigation is a secondary navigation bar with tabs: 'Users', 'Groups', 'Roles', 'Workspaces', 'Timeframes', 'Network', 'Organization', 'Threat Sources' (which is highlighted in blue), 'Notifications', and 'Apps'. The main content area is titled 'Threat Sources' and contains a list of threat sources, each with a status switch (Off or On). The listed threat sources are:

- AlienVault IP Reputation Feed: A list of suspicious IP addresses from AlienVault Labs. Status: Off.
- Mandiant Threat Intelligence: Threat intelligence service provided by Mandiant. (Former: iSIGHT Partners). Status: Off.
- SANS Internet Storm Center: SANS Internet Storm Center (ISC) database. Status: Off.
- VirusTotal: Scan artifacts using VirusTotal. Status: Off.
- Geolocation with MaxMind: Gather additional artifact data using MaxMind GeoIP2 services. Status: Off.
- IBM X-Force Exchange: Search for threat intelligence using the IBM X-Force Exchange platform. Status: On.

Below the threat source list, there is a note: 'Threat sources are feeds that the IBM Security QRadar SOAR platform searches when artifacts are added to an incident.' and 'Enable and disable the threat sources as you see fit for your company.'

You *should* register for API keys for free for X-Force.

- Get your IBM Xforce API Key @ <https://exchange.xforce.ibmcloud.com/settings/api>



## QRADAR SOAR TRAINING

# Lab 2

### Goal:

- Understand the notion of incident and case
- Understand the notion of user, be part of a group, associated rights and roles, visibility of incident's tasks
- Understand the notion of artifact, IOC, and enrichment by Threat Intelligence
- Understand the notion of teamwork on a task and group communication (war room) on this task

# Lab 2: The Basics – Incident Creation & Editing

- Create a series of incidents using the New Incident creation wizard. This wizard will walk you through a new incident creation. Use the following table to populate your incidents:
  - NOTE: Artifacts can only be added to the incident after it has already been created.

Incident Type	Members	Owner	Artifacts
Malware	CSIRT	(will auto assign to you)	DNS: atmape.ru IP: 8.8.8.8
Phishing	CSIRT	(will auto assign to you)	URL: http://fatwallet.com/res?25242
Denial Of Service	CSIRT	(will auto assign to you)	DNS: poneytelecom.eu IP: 8.8.8.8

- Self Discovery: Have a play with:
  - Members Tab - add new members to an incident
  - Tasks Tab - Assign Tasks (individually and/or in bulk), note how users who are not members cannot be assigned tasks
  - Artifacts Tab - Look at the Graph view within Artifacts. Do this for each of the newly created incident, note how the different relationships are shown based on their common artifacts
  - Details Tab - Add additional Incident Types to an incident along with other field entries, observe new tasks being added to the incident
  - Notes Tab – Try sending a note to another user, using the @ functionality

# Lab 2 Review: The Basics – Incident Creation & Editing Part

- The QRadar SOAR IRP, unlike a typical ITSM/Ticketing solution is purpose built for Incident Response.
- Task playbooks based on Incident Types ensure repetitive and consistent responses.
- Task individualization and ownership can be managed under the context of a single Incident, moreover the task ownership allows for accountability as well.
- Users must be added as members in order to see information. This maintains Op Sec sensitivity.
- Artifacts are automatically enriched via activated Threat Intelligence (where enabled and applicable).
- Artifact visualization allows for a quick understanding of the pervasiveness of the managed IOC, while the related incidents allow users to leverage lessons learned from previous similar incidents.
- Incident Details can be customized to include/exclude fields as necessary minimizing confusion of what information needs to be provided.
- Directing notes allows for better collaboration between multi-faceted teams that may be involved with an incident.



## QRADAR SOAR TRAINING

# Lab 3

### Goal:

- Define threats linked to personal data depending on incidents
  - Understand the different issues during a security breach depending on the geographic area
- 

# Lab 3: Working with the Privacy Module and Breach

- What QRadar SOAR provides is information surrounding Breach Notification and does not focus on privacy generalities.
- Go to the homepage by clicking on **QRadar SOAR in the top task bar**
  - **Click on Resource Library on the right**
  - NOTE: This is used from a purely research perspective.
- Demoing Breach
  - Choose the Incident typed “Phishing”
  - Click on the Breach tab → Edit
  - We will choose a scenario. For example, select:
    - Was personal information or personal data involved? : Yes
    - Data Encrypted: No
    - Data Format: Electronic
    - Data Types: Choose all the main headers (Contact Information, Personal Information, Credit Card, etc)
    - Applicable US Federal and/or Trade Org options
    - Pertinent localities/countries
    - Save
  - Note that one task is added to ‘Assess the Risk’. You will now see the GDPR Assessment form in the Breach Tab. If you fill in that form, depending on your answers, you will see additional tasks being added.
- Self Discovery: Enable other countries for breach they may be applicable to you. Click on some of the links to understand what researchers have to work through in order to find relevant information.

You may get an error 'Unable to find Object ID 14'.

This happens when you select certain regulations for the first time.

Simply refresh the page and start again.

# Lab 3 Review: Working with the Privacy Module and Breach

- What QRadar SOAR provides is information surrounding Breach Notification and does not focus on privacy generalities.
- The Privacy Library allows for research to be conducted quickly and effectively. QRadar SOAR provides an overview of the topic pertinent to the Legislative and/or Regulatory statutes available globally. While also providing links to the source of the information should additional research be warranted.
- When a Breach happens: A quicker understanding of notification obligations can be obtained simply by identifying the nature of the breach, data types, and applicable legislative territory and/or trade organization during an ongoing incident.
- Summary:
  - Who you need to notify – Which Regulator/Authority
  - What you need to send to notify – What information is required, some notification templates
  - How you need to notify - Provides email/physical addresses of who to send the notification to
  - Why you need to notify – The Regulation/Legislation behind the need to notify



## QRADAR SOAR TRAINING

# Lab 4



Goal:

- Understand the notion of report on an incident containing different targets
- Understand the notion of dashboard, KPI, and data segregation from users accessing to those dashboards

# Lab 4: Reports & Dashboards

- Incident specific reporting:
  - Select an incident with the checkbox
  - Select the Export option
  - Click on Generate Report
  - Select any of the templates provided or “Customize”
    - Explore the output provided by each selection
    - Hint: Deselecting--> Reselecting puts the item back to the top. This can be rearranged via drag/drop
- List Incidents:
  - Click on Incidents (Grey Bar)
  - Select Fields to display as columns in the result set
  - Rearrange the order of the columns
  - Add filters based on field data (Click Filters)
  - Select All or a sub-set of Incidents
  - Click on Export to export or print
- Analytics Dashboard
  - Click Dashboard→ Analytics Dashboard
  - + Add Widget
    - Add widgets Open Incident by Type / Owner
    - Name and Save
  - Drag/Drop on screen and Save As
- Self Discovery: Create your own reports. Test the two different export options of List Incidents.

Incidents											Actions	Export	Assign to	Manage	Cancel
	ID	Name	Description	Date Discovered	Date Determined	Next Due Date	Date Created	Export all	Export selected	Generate report	Phase	Severity	Status		
<input checked="" type="checkbox"/>	3865	Manual test internal	-	09/06/2022 11:45:31	09/06/2022 11:45:31	-	09/06/2022 11:46:34				Engage	Low	Active		

<input type="checkbox"/>	ID	Name	Description	Date Discovered	Date Determined	Next Due Date	Date Created	Owner	Phase	Severity	Status
<input type="checkbox"/>	2509	Malware	-	07/27/2021...	07/27/2021...	-	07/27/2021...	Gaëtan Loddé	Respond	Low	Active
<input type="checkbox"/>	2510	Phishing	-	07/27/2021...	07/27/2021...	07/27/2021...	07/27/2021...	Gaëtan Loddé	Respond	Low	Active
<input type="checkbox"/>	2511	Denial...	Gaetan Mo...	07/27/2021...	07/27/2021...	-	07/27/2021...	Gaëtan Loddé	Respond	Low	Active

# Lab 4 Review: Reports & Dashboards

- Reporting is simple
- Options:
  - Incident Specific Reporting (via Incident case – right side)
  - Reporting in Mass (via List Incidents)
  - Analytics Dashboards (via Dashboards )
- Exporting and/or Printing



## QRADAR SOAR TRAINING

# Lab 5

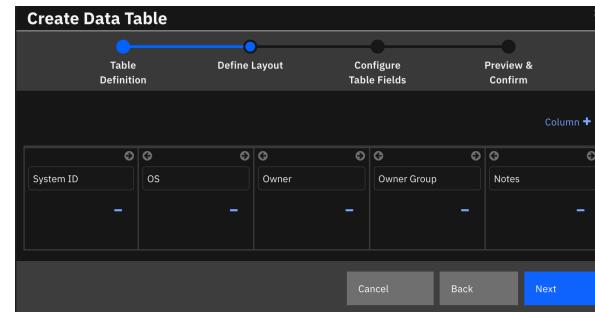
Goal:

- Know how to enrich the interface to gather interesting data
  - Master the different data gathering fields
- 

# Lab 5: Field & Tab Customization – Part 1/3

- Click on your username (upper right) → Customization Settings
- Click on Incident Tabs → Details
- Add new fields:
  - Label: “Executive Involved”, Type: Boolean
  - Label: “Systems Infected”, Type: Boolean
  - Explore other field creation
- Create a Data Table using the following matrix for columns and data types per column
  - Data Table Name: “Infected Systems”

Be careful to make sure you copy the table values exactly. If you miss capital letters or add accidental spaces, this will cause problems in later labs.



Column Name (API Access Name)	System ID (system_id)	OS (os)	Owner (owner)	Owner Group (owner_group)	Notes (notes)	Remediation State (remediation_state)
Field Type	Text	Select	Text	Select	Text Area	Select
Values		Android		Development		Pending
		Linux		Exec		Confirmed
		Mac		Finance		Escalated
		IOS		GA		Remediated
		Windows		HR		
				Marketing		
				Sales		

- Self Discovery: Create new fields and Data Tables of your own

# Lab 5: Field & Tab Customization (Placement) – Part 2/3

- While still in the Details tab:  
NOTE: Save each time you place fields where you want them
    - Drag Drop the “Executive Involved” field from the list of fields and place just below Severity
    - Drag Drop the “Systems Infected” field just below “Executive Involved”
    - Drag Drop the “Infected Systems” data table just above the “Basic Details” header.
      - NOTE: You can see how easy it is to keep adding fields and place them onto the form. But what about fields that are not immediately relevant?
  - On the right-hand side of the screen, scroll down to Blocks
  - Drag a Section over to below the recently placed “Infected Systems” data table
  - Drag the existing “Infected Systems” data table on form into the new section
  - Click on the section spanner icon  and add a condition to the section that allows it to appear only when the “Systems Infected” field is “Yes”
  - Save
- Explore your incidents, and edit within the Details Tab by toggling Yes/No for “Systems Infected” What happens a bit below this?
  - Self Discovery: Try adding fields to another tab. Are they useful there?



The screenshot shows the 'Incident: Details' form editor. A red box highlights a 'Section' block. Inside the section, there is a 'Basic Details' header and an 'Infected Systems' data table. The 'Save' button is located in the top right corner of the editor.

# Lab 5 - cont: Field & Tab Customization (Custom Tabs) – Part 3/3

- Navigate back to Incident Tabs → Manage Tabs:
  - Click the “+” at the end of the listed tabs.
  - Tab Text = “Infected Systems”
    - Add a condition to the section that allows it to appear only when the “Systems Infected” field is “Yes”.
- Now navigate to Incident Tabs → Infected Systems.
  - Drag Drop the “Infected Systems” data table into the tab space.
  - Save
- Explore your incidents, and edit within the Details Tab by toggling Yes/No for “Systems Infected”. What happens to available tabs?
- Is this a better option than adding to the Details Tab? Remove the one of the options.
- Self Discovery:
  - Add the “Executive Involved” field to the Summary Tab.
  - Have a play with fields and Tab/Section conditions. You’ll find that multiple conditions imply an AND operator.

# Lab 5 Review: Field & Tab Customization

- QRadar SOAR allows users to configure the system to include all their field entries
- Fields can be of various types:
  - Text, Text Area, Date, Date/Time, Number, Boolean, Select, Multi-Select
- The API Access Names are automatically generated, but can be edited
- Fields can be mandatory, mandatory on close, or optional (default)
- Users can also create mini spreadsheets/data tables within the solution
  - This is especially useful for incidents that may involve several systems
- Placement of the fields is as easy as drag drop once created
- Fields in the IRP can appear/disappear based on need
  - This is based on the condition(s) provided to sections or tabs



## QRADAR SOAR TRAINING

# Lab 6

Goal:

- Understand the notion of phases in the solving steps of an incident
- Understand the customization of descriptive to do tasks elements, elements to produce to accomplish it, and expected elements to produce a report

# Lab 6: Incident Types, Phases, and Tasks

- Navigate to Incident Types
  - Add a Type: "Manual Incident"
  - Parent: [Blank], Hidden: [No]
    - NOTE: Adding a parent allows for inheritance of the parent incident's tasks
- Navigate to Phases & Tasks
  - Create Phase:
    - Phase Name: Final Phase
  - Create Task:
    - Task Name: Legal Standing
    - Phase: Final Phase
    - Instructions: Confirm that all legal obligations have been fulfilled.
    - Incident Fields, drag and drop from the list:
      - Criminal Activity
      - Data Encrypted
- Self discovery:
  - Create additional Incident Types and Tasks
  - Drag Drop tasks within a phase to reset the order

# Lab 6 Review: Incident Types, Phases, and Tasks

- Creating Incident Types is quite easy. They are simply identifiers.
- Phases are also easy. They are just gatherings of tasks.
- Task creation is also easy. This flexibility allows for a gathering of tasks, much like you would gather ingredients for a recipe.
  - You'll also find that these tasks can be reused. That's coming up.
- The order of tasks within a phase dictates the order they will appear in an active incident
- Hyperlinks within task instructions are useful for providing quick access to external resources
- Why hide an incident type ?
  - Its ruleset is still under construction.
  - Hiding a parent forces the initiator to be more specific, and not generalize to a parent that may be vague.



## QRADAR SOAR TRAINING

# Lab 7

Goal:

- Create/Use a Python script



# Lab 7: Scripts – Part 1/2 , Part 2 is the lab 8

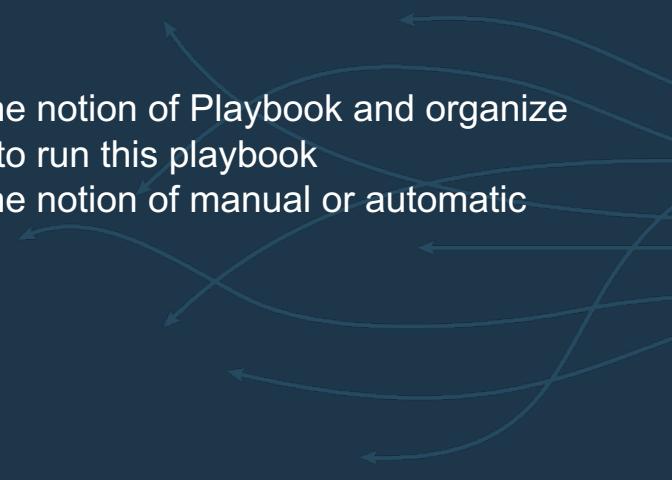
- We're not here to learn Python scripting!
- However... Python scripts can be used for advanced function within QRadar SOAR
- For now, simply copy the contents of the “CBHuntIOCs.txt” file into a new script
- Here are the parameters for the script to be created:
  - Name: "CB Hunt IOCs"
  - Object Type: Artifact
  - Script: [paste the contents into the script space]
    - It should start with: “incident = artifact.getParentObject()”
    - And end on row 42 with: “row[‘remediation\_state’] = ‘Pending’”
- NOTES: When using a script to populate fields, be sure that the entry corresponds with the available options if the Field/DT Column is of type: Select, Multi-Select, Boolean, etc.



## QRADAR SOAR TRAINING

# Lab 8

Goal:

- Understand the notion of Playbook and organize a set of rules to run this playbook
  - Understand the notion of manual or automatic actions
- 

# Lab 8: And now... Rules – Part 1/3

- The rules allow for massive flexibility when dealing with incidents, and the creation of dynamic playbooks.
- Go to the Rules tab in Customization Settings
- Let's create our first rule. Use the following matrix to create it.

Rule Type	Display Name	Object Type	Condition(s)	Activities
Automatic	Manual Incident	Incident	Incident Type: Is equal to: Manual Incident	Add Tasks: [Select 5-10 tasks]

# Lab 8: Rules – Part 2/3

- Create a series of rules using the settings below: Use the AND operator for the last.

Rule Type	Display Name	Object Type	Condition(s)	Activities
Menu Item	CB Hunt IOC	Artifact	Value: Has a value	Run Script: CB Hunt IOCs
Automatic	Set Executive Involved	Data Table Infected Systems	Owner Group: Is equal to: Exec	Set Field: “Incident: Executive Involved”: Yes
Automatic	Executive Involved	Incident	Executive Involved: Is equal to: Yes	Set Field: “Incident: Severity”: High Set Field: “Incident-Owner”: Tier 2 Analysts Set Field: “Incident: Members”: CSIRT, Legal Team, Tier2 Analysts Add Tasks: Determine if illegal activity is involved
Automatic	Assign to Legal	Task	Name: Contains: Legal  Executive Involved: Is equal to: Yes	Set Field: “Task-Owner”: Legal Counsel

# Lab 8: Rules Demonstration – Part 3/3

- Take note of the following fields:
  - Severity
  - Executive Involved
  - Incident Owner
  - Members
  - Infected Systems (Data Table)
- Take note of your tasks.
- In an incident that has an artifact, click on the ellipse [...] next to an artifact.
  - Mimic the “demonstration” of running an integrated Carbon Black scan for the identified IOC.
- What happened to the fields & tasks?

# Lab 8 Review: Rules

- Rules allow for dynamic playbooks to be created.
- This allows for not only playbook creation based on incident type(s), but also the dynamic capability to adapt to any incident based on business rules and new data.
- The drivers of these rules can be multi-conditional.
- Automatic rules are automatically enacted given the right conditions.
- Automatic rules are processed top down. However unlike a firewall rule that may stop at the first hit, all rules are processed. As such, any clashes are subject to the effects of the last applicable rule run.

QRADAR SOAR TRAINING

# Lab 9: Additional script and rule

Goal:

- Understand the notion of “click” simplification asked by automatisms
- Understand the notion of Milestone

## Lab 9: Additional script and rule work 1 of 2

Please, create script & rule that will auto assign task to user connected when the task owner is empty, and the task status is changed to close.

Hint: the python code to assign user connected to the task ownership is below.

**task.owner\_id = principal.id**

Test it with a user owner or member of an incident.

Test it also with a user that has an Administration permission, but who is NOT owner or member of the incident.

What happen ?

# Auto-assign task to user connected

Scripts / Assign task to connected user

Name \* Assign task to connected user

Description Optional

Object Type \* Incident

Language Python 3 Theme dark Mode Default Tab Size 2 - Font + Font

```
1 task.owner_id = principal.id
```

Rules / Auto Assign Tasks

Display Name \* Auto Assign Tasks

Object Type Task

Conditions Add conditions in which to invoke the rule. Clear All

All  Any  Advanced

example: 1 OR (2 AND 3)

Owner does not have a value

Status is changed to Closed

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field. Clear All

Run Script Assign task to connected user

SOLUTION Slide !!!

Please do it by yourself before looking at the solution

*Note : There is a error in this slide, for you to find !!!*

# Yes but, what if it does not work? (Auto-assign task to user connected)

When the user is not listed in the incident membership, The script is a little bit more complex :

```
# Check if the connected user that maybe viewer or full admin is a member of this incident
inside = False
log.debug("Inside: {}".format(inside))
log.info("Principal Name: {}".format(principal.name))
log.info("Owner ID: {}".format(incident.owner_id))
log.info("Members: {}".format(incident.members))

# Check Incident Owner Level
if incident.owner_id == principal.name:
    inside = True
# Check Incident Owner if Group
elif groups.findByName(incident.owner_id):
    log.debug("In incident owner group")
    inside = True
else:
    log.debug("Not in incident owner group")

# Check Members Level
for member in incident.members:
    log.debug("Looking at Member: {}".format(member))
    if member == principal.name:
        inside = True
    elif groups.findByName(member):
        log.debug("Inside group Member: {}".format(member))
        inside = True

# if 1, the connected user is a member
log.debug("Last Inside Value (0= False/1= True): {}".format(inside))

# Add current connected user as a member
if principal.type == "apikey":
    donothing = "If you have no Orchestration user or add it below as member"
    incident.members = list(incident.members) + ["resilient.action@rostagni.com"]
    task.owner_id = "resilient.action@rostagni.com"
else:
    if not inside:
        incident.members = list(incident.members) + [principal.id]
# Add current connected user as Task Owner, as this full script was made to add connected user as task owner.
task.owner_id = principal.id
```

```
1 # Check if the connected user that maybe viewer or full admin is in a member of this incident
2 inside = False
3 log.debug("Inside: {}".format(inside))
4 log.info("Principal Name: {}".format(principal.name))
5 log.info("Owner ID: {}".format(incident.owner_id))
6 log.info("Members: {}".format(incident.members))
7
8 # Check Incident Owner Level
9 if incident.owner_id == principal.name:
10     inside = True
11 # Check Incident Owner if Group
12 elif groups.findByName(incident.owner_id):
13     log.debug("In incident owner group")
14     inside = True
15 else:
16     log.debug("Not in incident owner group")
17
18 # Check Members Level
19 for member in incident.members:
20     log.debug("Looking at Member: {}".format(member))
21     if member == principal.name:
22         inside = True
23     elif groups.findByName(member):
24         log.debug("Inside group Member: {}".format(member))
25         inside = True
26
27 # if 1, the connected user is a member
28 log.debug("Last Inside Value (0= False/1= True): {}".format(inside))
29
30 # Add current connected user as a members
31 if principal.type == "apikey":
32     donothing = "If you have no Orchestration user or add it below as member"
33     incident.members = list(incident.members) + ["resilient.action@rostagni.com"]
34     task.owner_id = "resilient.action@rostagni.com"
35 else:
36     if not inside:
37         incident.members = list(incident.members) + [principal.id]
38     # Add current connected user as Task Owner, as this full script was made to add connected user as task owner.
39     task.owner_id = principal.id
```

## SOLUTION Slide !!!

Beware of Cut & Paste  
quote errors or  
indentation errors from  
PDF, use the txt file on  
Lab 9 folder

# Lab 9: Additional script and rule work 2 of 3

Please, create scripts & rules that will add a milestone when Legal Team is added to the incident, and will assign all privacy tasks to a legal user of this team.

Hint: the python code to ADD a user to the members list is below.

```
from datetime import datetime
```

```
if "Legal Team" not in incident.members:
```

```
    incident.members = list(incident.members) + ["Legal Team"]
```

```
    incident.addMilestone('Add Legal Group', 'Legal Group is added  
to incident as Privacy Analysis is needed', datetime.now())
```

The screenshot shows the configuration of a rule in the IBM Security Scripting interface. The rule is set to trigger on 'Task is created' and 'Category has one of' 'Data Breach - Organizational'. The rule is ordered and includes an activity to 'Add Task' named 'Data Breach - Organizational'.

Object Type: Task

Conditions:

- Add conditions in which to invoke the rule. Clear All
- All
- Any
- Advanced

example: 1 OR (2 AND 3)

1 Task is created

2 Category has one of

Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, an

Data Breach - Authority Notifications  
Data Breach - General  
Data Breach - Individual Notifications  
Data Breach - Organizational

Data Breach - Organizational

# Milestone when a task is assigned to Legal

## 1/2 Creation of the script

Please do it by yourself  
before looking at the solution

```
from datetime import datetime
```

```
if "Legal Team" not in incident.members:
```

```
    incident.members = list(incident.members) + ["Legal Team"]
```

```
    incident.addMilestone('Add Legal Group', 'Legal Group is added to incident as Privacy Analysis is needed', datetime.now())
```

The screenshot shows the IBM Security X-Force interface with the 'Scripts' tab selected. A new script named 'Who: Legal' is being created. The script's purpose is described as 'Add Legal Group in the Incident'. It is set to run on 'Incident' objects. The script code is as follows:

```
1 # Import current date
2 from datetime import datetime
3 # Check if Legal Group is member, if not assign to member, and set a milestone
4 if "Legal Team" not in incident.members:
5     # incident.members is a python dictionary
6     incident.members = list(incident.members) + ["Legal Team"]
7     incident.addMilestone('Add Legal Group', 'Legal Group is added to incident as Privacy Analysis is needed', datetime.now())
```

The 'Save & Close' button is highlighted in blue, indicating the action to take next.

# Milestone when a task is assigned to Legal

## 2/2 Creation of the rule (automatic)

Please do it by yourself  
before looking at the  
solution

The screenshot shows the 'Rules' tab selected in the top navigation bar. The current rule is titled 'Who: Assign all privacy tasks to Legal'. The 'Conditions' section is configured with 'All' selected. The 'Actions' section contains two categories: 'Data Breach' and 'Respond'. The 'Activities' section lists two ordered activities: 'Run Script' (Who: Legal) and 'Set Field' (Task: Owner, value: Legal Counsel). The 'Save & Close' button is highlighted in blue.

Display Name \* Who: Assign all privacy tasks to L

Object Type Task

Conditions Add conditions in which to invoke the rule. [Clear All](#)

All  Any  Advanced

example: 1 OR (2 AND 3)

Category has one of Data Breach - Authority Notifications Data Breach - General  
Data Breach - Individual Notifications Data Breach - Organizational

Phase is equal to Respond

Task is created

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field*. [Clear All](#)

1 Run Script Who: Legal

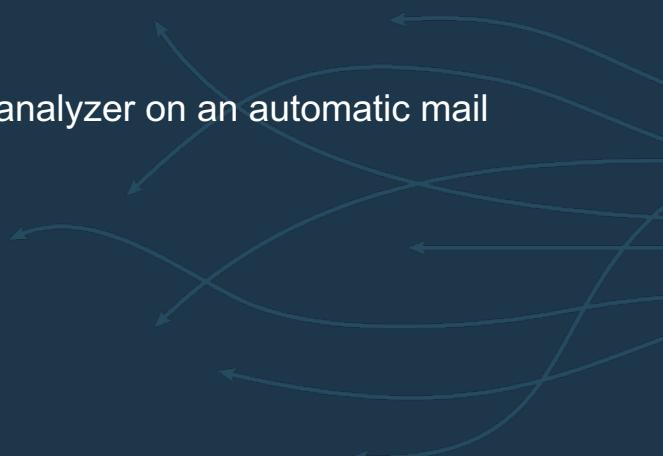
2 Set Field Task: Owner Legal Counsel (legalcounsel.lodde@yopmail.com)

QRADAR SOAR TRAINING

# Lab 10: Inbound Email

Goal:

- Create a mail analyzer on an automatic mail collect



# Setup Email Technical Account used by QRadar SOAR

You will have been asked to have an email account ready to use for QRadar SOAR. You can use any SMTP account.

(We have a mail-in-a-box account you can use if required.)

Run:

```
sudo resutil smtpeedit -email resilientaccount@gmail.com -name "Resilient Platform" -host smtp.gmail.com -user resilientaccount@gmail.com -port 587
```

y@mail.poc.resilientsystems.com

Technical Account email address

Example (Please do not use the values from the example) :

```
[-bash-4.2$ sudo resutil smtpeedit -email resilient.jess@gmail.com -name "Resilient Platform" -host smtp.gmail.com -user resilient.jess@gmail.com -port 587  
[Enter the password for the user:  
[Confirm the password for the user:  
Successfully edited the SMTP configuration  
SMTP Host: smtp.gmail.com  
SMTP Port: 587  
SMTP User: resilient.jess@gmail.com  
SMTP Password: hidden  
SMTP From Email: resilient.jess@gmail.com  
SMTP From Name: Resilient Platform  
SMTP StartTLS Enabled: true  
SMTP Whitelist Hostnames:  
-bash-4.2$ ]
```

This password  
needs to be the  
password you log  
in to the email with

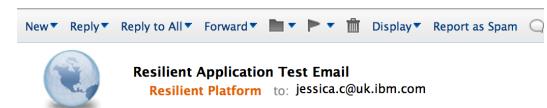
Not Applicable on Saas Lab  
you will receive emails from  
[donotreply@mail.poc.resilientsystems.com](mailto:donotreply@mail.poc.resilientsystems.com)

Now we need to test that it is working.

Use any email address that you can  
check, e.g. your work email

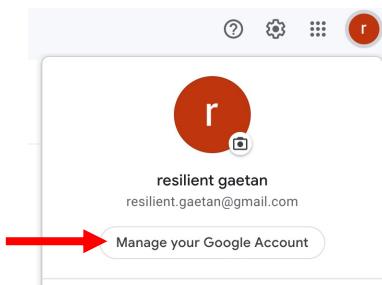
```
[-bash-4.2$ sudo resutil smtptest -email jessica.c@uk.ibm.com  
Successfully sent the test email to jessica.c@uk.ibm.com  
-bash-4.2$ ]
```

```
sudo resutil smtptest -email <your_work_email>
```



# Setup Email Technical Account used by QRadar SOAR

- Create GMAIL account named resilient.YOURNAME@gmail.com  
Do NOT USE your regular Gmail account  
QRadar SOAR will monitor all email send to this box to analyze them.
- For gmail account, you will need to create an app password to connect your mail account to the SOAR platform, otherwise the email will not work
- To do so, first go to the “Manage your Google Account” setting from your google profile:

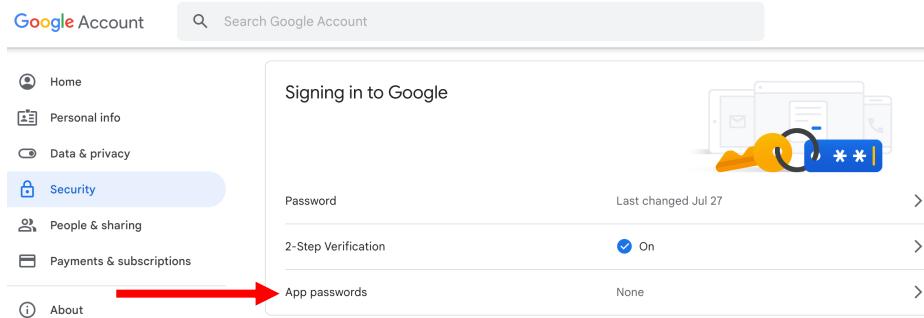


- Then select « Security » and enable the 2-step Verification with your phone number and the option « App passwords » will appear when going back to the 2-step Verification option at the bottom of the web page

A screenshot of the Google Account Security settings page. The top navigation bar says 'Google Account' and has a search bar. Below it, there are several tabs: Home, Personal info, Data & privacy, **Security** (which is highlighted in blue), People & sharing, Payments & subscriptions, and About. The 'Security' tab is currently selected. On the right, there's a large section titled 'Signing in to Google' with an illustration of a smartphone, laptop, and key. It shows the current status of 'Password' (Last changed Jul 27) and 'Use your phone to sign in' (Off). At the bottom of this section, there's a red arrow pointing to a '2-Step Verification' link. This link leads to another page where the '2-Step Verification' option is shown as being off.

# Setup Email Technical Account used by QRadar SOAR

- After the 2-Step Verification is enabled the « App passwords » option will be enabled in your security tab



- Click on the “App passwords” option and in the “select app” field select “other (custom name)” and fill with “Gmail on SOAR” and click on “Generate”
- An app password will be created, copy and paste it in a text file to use it later
- In the gmail settings, go to the POP/IMAP tab and enable IMAP access.
- If you get the following error message, it means that you haven’t put your email address password in correctly. It needs to be the password that you log into your emails with.
- When the Gmail account is ready, invite [resilient.YOURNAME@gmail.com](#) into QRadar SOAR as Master Admin, go to GMAIL and validate the invitation.

# Lab 10: Inbound Email

- Connect your email server and technical account that will receive all emails, to create automatically new incidents.
- Add a rule that will run the script « Sample script: process inbound email (v49) » when a new email is received
- Change in the « Sample script: process inbound email » the value of the owner of the incident when the incident is created (line 8)

```
7 # Change this value to reflect who will be the owner of the incident
8 newIncidentOwner = "resilient.YOURNAME@gmail.com"
9
10 # Whitelist for IP V4 addresses
```

- Note: the script can be modified to add new pattern matching, or other fields assignments please look at the script documentation and the latest version of this script at App Exchange “**Generic Email Parsing Script**” app:  
<https://exchange.xforce.ibmcloud.com/hub/extension/4ba70106b6f2dfa77cb1e3c921db7ff5>
- You can also look at the "**QRadar SOAR IRP Playbook Designer Guide.pdf**" for all objects to use in a script.

# Define the connection to the email server

## Administrator Settings

Users

Groups

Roles

Workspaces

Timeframes

Network

Organization

Threat Sources

Notifications

Apps

## General

Details	>
Settings	>

## Email Connections

Inbound	▼
✓ New Connection	>
resilient.LODDE@gm...	>
+ Add Connection	

## Migrate Settings

Import	>
Import History	>
Export	>
Export History	>

## Mailbox

Name *	i	resilientaccount@gmail.com
API Name *	i	resilientaccountgmailcom
Description		resilientaccount@gmail.com

## Connection Details

Protocol	i	IMAP
Host Name *	i	imap.gmail.com
Port *	i	993
Email Address *		resilientaccount@gmail.com
Password *		.....
Source Folder	i	
Encryption	i	<input checked="" type="radio"/> SSL/TLS <input type="radio"/> STARTTLS <input type="radio"/> None

Test Connection

Fill this field with the app password you created earlier

Save,  
then test connection

# Create the rule

The screenshot shows the IBM Security QRadar SOAR interface with the following details:

- Header:** IBM Security QRadar SOAR, Dashboards, Inbox, Artifacts, Incidents, Create incident, Search icon, Global icon, Playbooks, Gaëtan Lodde (202).
- Section:** Customization Settings
- Sub-section:** Rules / New Automatic Rule
- Form Fields:**
  - Display Name: Parse Email from Mailbox
  - Status: Enabled
  - Object Type: Email Message
  - Conditions: Add conditions in which to invoke the rule. (Clear All)
    - Email Message is created
- Buttons:** Cancel, Save & Close (highlighted in blue), Save
- Activities:** Activities will be invoked in the order specified below.
  - Ordered Activities:
    - Run Script: Sample script: process inbound email (v49)
- Footer:** © Copyright IBM Corporation 2023

The Condition has to be: **Email Message is created**

# Change in the « Sample script: process inbound email (v49) » the value of the owner of the incident when the incident is created (line 9)

The screenshot shows the IBM Security QRadar SOAR interface. At the top, there is a navigation bar with links for 'IBM Security QRadar SOAR', 'Dashboards', 'Inbox', 'Artifacts', 'Incidents', 'Create incident', and user information 'Gaëtan Lodde 202'. Below the navigation bar, the title 'Customization Settings' is displayed. A horizontal menu bar includes 'Layouts', 'Rules', 'Scripts' (which is highlighted in blue), 'Workflows', 'Functions', 'Destinations', 'Phases & Tasks', 'Incident Types', 'Breach', and 'Artifact Types'. Under the 'Scripts' section, the path 'Scripts / Sample script: process inbound email (v49)' is shown. On the right side of the screen, there are buttons for 'Delete', 'Cancel', 'Save & Close' (which is highlighted in blue), and 'Save'. The main form contains fields for 'Name' (set to 'Sample script: process inbound email (v49)'), 'Description' (containing a detailed text about the script's purpose), 'Object Type' (set to 'Email Message'), and metadata like 'Creator' (System User), 'Last Modified' (06/02/2023 19:22), 'Last Modified By' (System User), and 'Associated Rules' (with a 'Parse Email from Mailbox' button). Below the form is a code editor with Python 3 selected as the language. The code is as follows:

```
1 # Copyright IBM Corporation 2023.
2 import re
3
4 # A script to create an incident from an email message, add artifacts to the incident based on information
5 # present in the body of the message, and add any email attachments to the incident.
6
7 # The new incident owner - the email address of a user or the name of a group and cannot be blank.
8 # Change the value below to whatever will be the owner of the incident before running the script.
9
10 newIncidentOwner = "email@example.com"
```

The line 'newIncidentOwner = "email@example.com"' is circled in red at the bottom of the code editor.

Test the automatic creation of the incident by sending an email to the technical account (resilientaccount@gmail.com)

QRADAR SOAR TRAINING

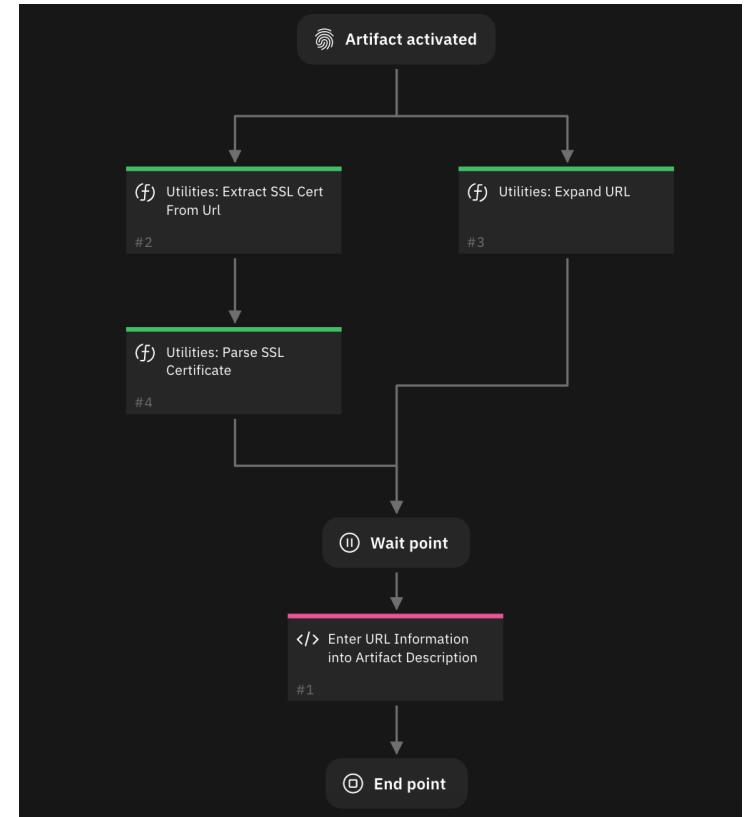
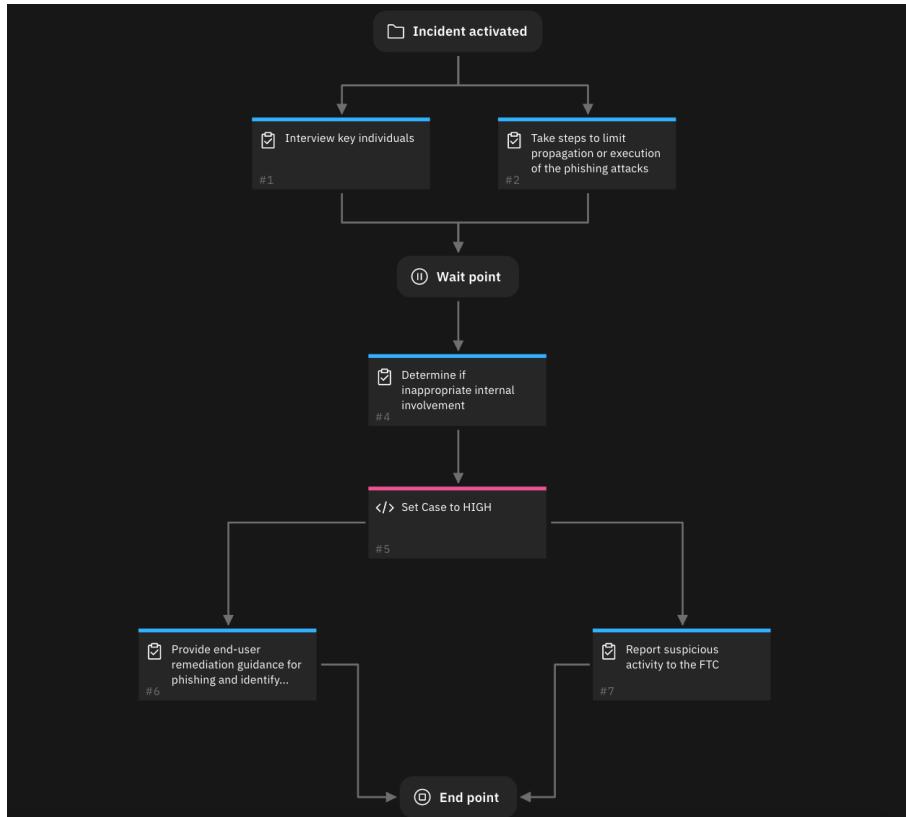
# Lab 11: Playbook

Goal:

- Know how to design a workflow to answer an issue
- Design Thinking, virtual team whiteboarding
- BPMN practice, test and validation

# Lab 11: Playbook Training

- Example of Final Work:



# Workflow Training

Use the BPMN symbol and select and click « add to canvas » to build your playbook :

Start by selecting an object type

End point



Condition point (First true)

test task

Utilities: Call REST API

</> test script

Wait point

- **Start Event.** Denotes the start point for the Playbook. It define the type of object on which the playbook will work and if it is triggered manually or automatically.
- **End Point.** Denotes an end point. If you have multiple End Events, all active paths are traversed even when one path reaches the end point.
- **Connector.** Logically connects components within the workflow to each other. You can add conditions to the connector when it is the output of a condition point.
- **Condition Point.** You assign conditions to the output paths (the Connector/arrow link to the next object). You can designate one output path as a “Else”, which is used when none of the conditional paths are true.
- **User Task.** Allows you to create a new task or select an existing task to be inserted in the corresponding incident's task list. This is comparable to adding a task from a rule. **Script.** Allows you to select an existing script to invoke. The workflow object type affects which scripts are available to the workflow.
- **Function.** Allows you to select an existing function. It also allows you to create pre-process scripts for that function.
- **Script.** Allows you to create and add a new script or add an existing script in your playbook to perform action automatically.
- **Wait Point.** At this point of the playbook, it won't progress until the previous actions are done.

## Best Practice:

Always start with ONE **Start Event**

Always finish with ONE **End Event**

# Lab Playbook: Ransomware Lab

Organize new tasks and fields with current phase to create a Ransomware workflow using the following possibilities, to be ordered:

1. Identify ransomware
2. Disconnect infected endpoint
3. Disconnect backup
4. Look ransomware IOC on other endpoints
5. Verify backup
6. Restore backup
7. Analyze encrypted data values
8. Decide to pay or not
9. Re-image endpoint
10. Patch SMB Vuln globally

## BPMN Symbols



Person in the corner = Add Task  
“When the workflow gets here, add this task”  
Mnemonic: Tasks need people to do them



Gear in the corner = Append Message Destination  
“When the workflow gets here, automatically carry out this action”  
Mnemonic: Gears represent automation



X in a diamond = Exclusive Gate  
Process Fork: “Only execute one of these paths”  
Process Join: “Advance when prior path to this is executed”  
Mnemonic: X for Xclusive



O in a diamond = Inclusive Gate  
Process Fork: “Optionally execute whichever of these paths apply”  
Process Join: “Advance when all applicable paths are executed”  
Mnemonic: O is for Optional



Plus in a diamond = Parallel Gate  
Process Fork: “Execute all of these things in parallel”  
Process Join: “Advance when all connecting paths are executed”  
Mnemonic: Plus for Parallel

## Hints

- Design on a paper all process using boxes and the ID number of the task
- Add below the task, all fields that will be asked to the analyst
- When using a question (exclusive gate), write on each arrow line the condition to follow
- The next page is wrong ! Do not take it as the solution, but only as hint. They are process errors inside.

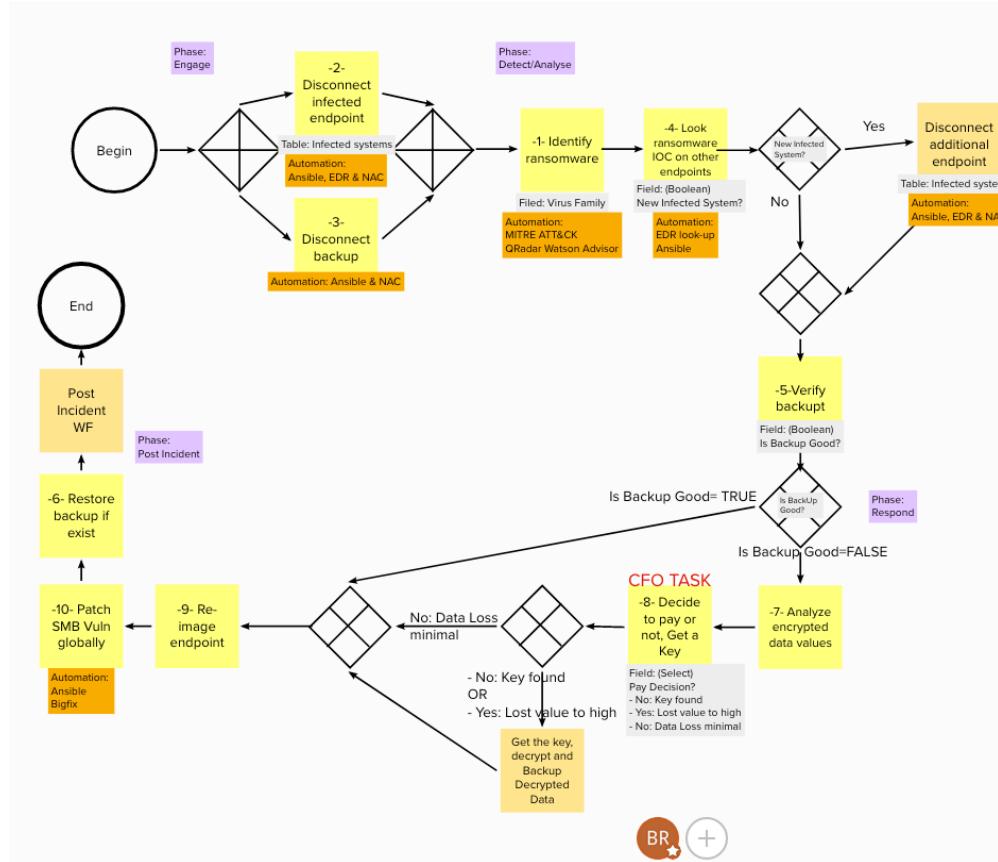
It is possible to use Mural to design the Playbook:

<https://app.mural.co/>

# Mural Design

[HTTPS://APP.MURAL.CO/INVITATION/MURAL/DIGITALCOVERAGEA\\_ndcommerce3006/1595540190673?SENDER=BENOITROSTAGNI4490&KEY=EA82155D-A6B8-48F0-8B0A-562860D312D4](https://app.mural.co/invitation/mural/digitalcoveragea_ndcommerce3006/1595540190673?sender=benoitrostagni4490&key=ea82155d-a6b8-48f0-8b0a-562860d312d4)

Please do it by yourself  
before looking at the solution



QRADAR SOAR TRAINING

# Lab 12:

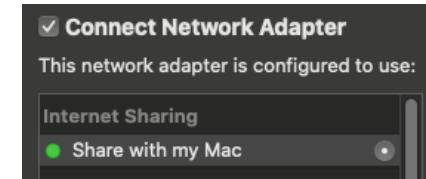
# Install the Integration Server

Goal:

- Install and Initialize an integration Virtual Machine
- Understand the notion of Message Bus, and communication flows direction
- Understand the notion of API Key

# Lab 12: Install the Integration Virtual Machine

- Official documentation:  
<https://www.ibm.com/docs/en/sqsp/44?topic=isg-introduction>
  - Download the Virtual Image of the integration server from Box :  
<https://ibm.box.com/v/TrainingAppHostOVA>
  - Install it in your Virtual Box or VMWare Fusion / Player software
  - The machine should be put in a Shared Internet network with your system.
  - You can connect to the console using **root** or **appadmin** users, with the unique password : **resilient**
  - In the console run ifconfig to get the IP given by the DHCP:



```
Red Hat Enterprise Linux Server 7.7 (Maipo)
Kernel 3.10.0-1062.12.1.el7.x86_64 on an x86_64

resilient login: root
Password:
Last login: Thu Mar 19 15:18:55 on pts/1
[root@resilient ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.113.147  netmask 255.255.255.0  broadcast 192.168.113.255
```

- For the rest of the lab, we will use **appadmin / resilient** to connect in SSH using putty in windows  
Please **DO NO USE ROOT or sudo su** in ALL LABS, except when explicitly written

# Lab 12: Integrations Setup

- We will use our own QRadar SOAR server but in production you should do this on a different server.
- First, we will use nano to simplify the edition of files. Of course, if you prefer vi, you can stay with vi!

# Get NANO on board

```
wget https://vault.centos.org/centos/8/BaseOS/x86\_64/os/Packages/nano-2.9.8-1.el8.x86\_64.rpm
sudo rpm -Uvh nano-2.9.8-1.el8.x86_64.rpm
nano .nanorc
include /usr/share/nano/python.nanorc
include /usr/share/nano/sh.nanorc
```

- We will use a specific CLI user, for the **integration server: integration**

– sudo useradd integration

You should be root for the next commands :

– sudo su

– echo "integration ALL=(ALL) ALL" >> /etc/sudoers

– passwd integration

– su integration

– cd

```
[root@apphost ~]# su integration
[integration@apphost root]$ cd
[integration@apphost ~]$ pwd
/home/integration
[integration@apphost ~]$ █
```

# Setting up QRadar SOAR Circuits

*Beware not to mess up between both 2.7 & 3.6 environments in using other users.*

Install the Python components:

- The utility functions package contains Python components that will be called by the QRadar SOAR platform to execute the functions during your workflows. These components run in the ‘resilient-circuits’ integration framework.
- The package also includes QRadar SOAR customizations that will be imported into the platform later.

Ensure that the environment is up to date:

```
sudo pip3 install --upgrade pip3
sudo pip3 install --upgrade setuptools
sudo pip3 install --upgrade resilient-circuits
sudo pip3 install --upgrade resilient-sdk
```

Note: If you encounter any error launching those commands try adding:  
**--ignore-installed**

Note 2: pip3 upgrade might not be necessary anymore, if you have an  
error just ignore the update (first sudo line)

Note: For all other « pip » installation, we will stay « integration », **no sudo !**

```
[integration@apphost ~]$ resilient-circuits help
/usr/lib/python2.7/site-packages/urllib3/contrib/pyopenssl.py:51: CryptographyDeprecationWarning: Python 2 is no longer supported
by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography import x509
usage: resilient-circuits [-h] [-v]

                                         {run,list,test,service,config,codegen,extract,customize,selftest,clone}
...
resilient-circuits: error: argument cmd: invalid choice: 'help' (choose from 'run', 'list', 'test', 'service', 'config', 'codegen',
, 'extract', 'customize', '_selftest', 'clone')
```

**QRadar SOAR Circuits configurations are maintained in the app.config file**

Auto generate the **app.config** file:

```
$ su integration  
$ cd /home/integration  
$ /usr/local/bin/resilient-circuits config -c
```

This creates /home/integration/.resilient/app.config

Open this file in **NANO**:

```
$ nano /home/integration/.resilient/app.config
```

Change the various values with these configuration settings:

```
host=emea-training.poc.resilientsystems.com  
port=443  
org=YourOrg - like 202  
componentsdir=/home/integration/.resilient/components  
logdir=/home/integration/.resilient/logs  
cafie=false
```

For cafie and componentsdir make sure you have removed the # at the start of the line too

Save by pressing **CTRL+X**

And Create directories:

```
$ mkdir /home/integration/.resilient/logs  
$ mkdir /home/integration/.resilient/components
```

# Setup the API key

We now need to get an API Key - Open QRadar SOAR in your browser and login with your credentials.

Go to the **username** at the top right and click **Administration Settings**.

The screenshot shows the 'Administrator Settings' page in the QRadar SOAR interface. The top navigation bar includes links for Dashboards, Inbox, Artifacts, Incidents, Create, and a user profile for 'Gaëtan Loddé'. Below the navigation is a search bar and a language selection for 'Gaëtan Loddé' (305). The main section is titled 'Administrator Settings' and contains a 'Users' tab selected, along with tabs for Groups, Roles, Workspaces, Timeframes, Network, Organization, Threat Sources, Notifications, and Apps. A search bar at the top allows filtering by 'Display Name' (Contains text), 'Email: All', 'Roles: All', 'Groups: 0 selected', 'Status: All', and a 'More...' dropdown. A 'Show' button is set to 100 results. On the right, a blue 'Invite User' button is visible. The user list table has columns for Display Name, Email, Last Login, Roles, Groups, and Status. It lists three users: Benoit ROSTAGNI, Gaëtan Loddé, and Samira Bataouche, all of whom are active. Each user row includes a red trash can icon for deletion. At the bottom left, it says 'Displaying 1 - 3 of 3'. The footer contains the copyright notice '© Copyright IBM Corporation 2020'.

Display Name	Email	Last Login	Roles	Groups	Status
Benoit ROSTAGNI	benoit.rostagni@ibm.com	12/17/2020 20:15	Master Administrator		Active
Gaëtan Loddé	gaetan.lodde@ibm.com	12/18/2020 09:59	Master Administrator		Active
Samira Bataouche	sbataouche@fr.ibm.com	11/26/2020 13:58	Master Administrator		Active

# Setup the API key

Click **API Keys** on the **Users** tab you are on, then **Create API Key** on the right.

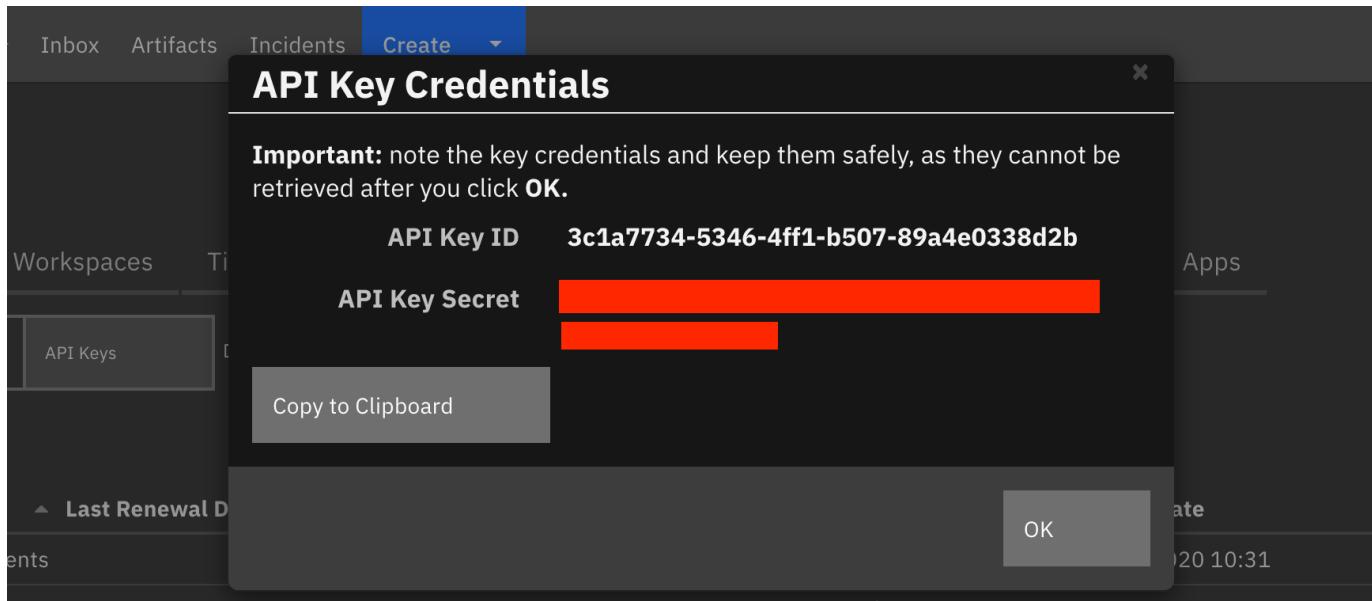
Click **All Permissions** for now and name your key

The screenshot shows the Resilient platform interface with a dark theme. At the top, there is a navigation bar with links for Dashboards, Inbox, Artifacts, Incidents, Create (dropdown), and a user profile for Gaëtan Loddé (302). Below the navigation bar, a sidebar on the left lists various administrative sections: Admin, User (selected), Show, Display, app\_1, app\_2, Integ, Integ, and Display. The main area is titled "Create API Key".  
**Summary:**  
Display Name: Integration Server  
Description: API Key for Int Server  
**Permissions:**  
 All permissions  
If checked, all of the permissions below are granted:  
**Incident Permissions:**  
 Incidents:  Read,  Create,  Delete,  Download Email  
 Edit Incidents:  Fields,  Owner,  Members,  Status,  Notes,  Workspace  
**Simulation Permissions:**  
 Create Simulations  
**Task Permissions:**  
 Edit Task Header  
 Read Tasks  
 Edit Tasks:  Fields,  Members,  Notes  
 Read Private Tasks  
 Edit Private Tasks:  Fields,  Members,  Notes

# Setup the API key

Scroll down and click Create, a new window will pop up, click Copy to Clipboard.

Reopen the `app.config` file using nano and paste the values. Then put the `Key ID` value against the `api_key_id` and `Key Secret` as the value for `api_key_secret`



- Note: sometimes the `api_key_id` can paste with a slash at the end, this should be removed.

# Run QRadar SOAR Circuits

## Open Terminal

Run resilient-circuits:

```
$ /usr/local/bin/resilient-circuits run
```

You should get this output if resilient-circuits is running successfully:

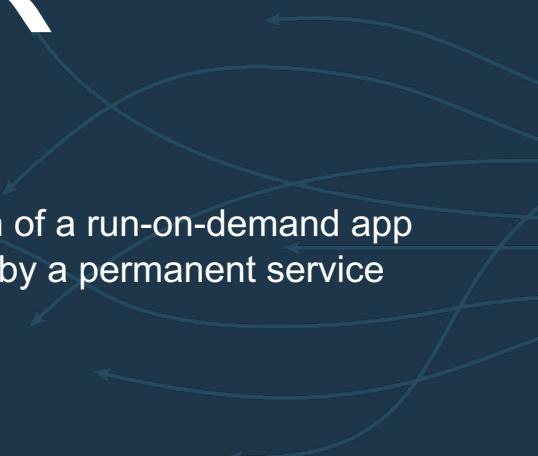
```
[integration@apphost ~]$ resilient-circuits config -c
/usr/lib/python2.7/site-packages/urllib3/contrib/pyopenssl.py:51: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team.
Support for it is now deprecated in cryptography, and will be removed in the next release.
[ integration@apphost ~]$ from cryptography import x509
CREATING config file /home/integration/.resilient/app.config
Configuration file generated: /home/integration/.resilient/app.config
Please manually edit with your specific configuration values.
[integration@apphost ~]$ nano /home/integration/.resilient/app.config
[integration@apphost ~]$ mkdir /home/integration/.resilient/logs
[integration@apphost ~]$ mkdir /home/integration/.resilient/components
[integration@apphost ~]$ 
[integration@apphost ~]$ resilient-circuits run
/usr/lib/python2.7/site-packages/urllib3/contrib/pyopenssl.py:51: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team.
Support for it is now deprecated in cryptography, and will be removed in the next release.
from cryptography import x509
2021-01-15 09:27:07,935 INFO [app] Configuration file: /home/integration/.resilient/app.config
2021-01-15 09:27:07,937 INFO [app] Resilient server: warbler.poc.resilientsystems.com
2021-01-15 09:27:07,938 INFO [app] Resilient api key id: 4a2ec0b4-2fb4-4403-8aaf-dbe3b2f94a20
2021-01-15 09:27:07,938 INFO [app] Resilient org: 302
2021-01-15 09:27:07,938 INFO [app] Logging Level: INFO
2021-01-15 09:27:07,939 WARNING [co3] Unverified HTTPS requests (cafile=false).
2021-01-15 09:27:10,803 INFO [app] Components auto-load directory: /home/integration/.resilient/components
2021-01-15 09:27:10,812 WARNING [actions_component] Unverified STOMP TLS certificate (cafile=false)
2021-01-15 09:27:10,818 INFO [stomp_component] Connect to warbler.poc.resilientsystems.com:65001
2021-01-15 09:27:10,819 INFO [app] Components loaded
2021-01-15 09:27:10,821 INFO [app] App Started
2021-01-15 09:27:10,923 INFO [actions_component] STOMP attempting to connect
2021-01-15 09:27:10,925 INFO [stomp_component] Connect to Stomp...
2021-01-15 09:27:10,926 INFO [client] Connecting to warbler.poc.resilientsystems.com:65001 ...
2021-01-15 09:27:11,249 INFO [client] Connection established
2021-01-15 09:27:11,426 INFO [client] Connected to stomp broker [session=ID:warbler.poc.resilientsystems.com-38674-1607530978199-4:494, version=1.2]
2021-01-15 09:27:11,427 INFO [stomp_component] Connected to failover:(ssl://warbler.poc.resilientsystems.com:65001)?startupMaxReconnectAttempts=3,maxReconnectAttempts=3
2021-01-15 09:27:11,428 INFO [stomp_component] Client HB: 0 Server HB: 15000
2021-01-15 09:27:11,429 INFO [stomp_component] No Client heartbeats will be sent
2021-01-15 09:27:11,430 INFO [stomp_component] Requested heartbeat from server.
2021-01-15 09:27:11,433 INFO [actions_component] STOMP connected.
2021-01-15 09:27:11,537 INFO [actions_component] resilient-circuits has started successfully and is now running...
```

QRADAR SOAR TRAINING

# Lab 13: (optional) Installing QRadar SOAR Circuits as a Service

Goal:

- Understand the notion of a run-on-demand app and an app initialized by a permanent service



# Install QRadar SOAR Circuits as a service

- When developing or customizing integrations, it is best to manually run resilient-circuits to quickly iterate and re-run. However in production we want to be able to restart as needed and on reboot etc.
- Resilient-Circuit can be installed as a service on linux or windows (see docs for windows).
- Create a file with `sudo touch /etc/systemd/system/resilient_circuits.service`
- Give the proper permissions with `sudo chmod 664 /etc/systemd/system/resilient_circuits.service`
- Put the contents below in the file: `sudo nano /etc/systemd/system/resilient_circuits.service`

```
[Unit]
Description=Resilient-Circuits Service
# If the Integration Server is added on the same machine than QRadar SOAR (do not do that on Prod),
# uncomment the 2 following lines
# After=resilient.service
# Requires=resilient.service

[Service]
Type=simple
User=integration
WorkingDirectory=/home/integration
ExecStart=/usr/local/bin/resilient-circuits run
Restart=always
TimeoutSec=10
Environment=APP_CONFIG_FILE=/home/integration/.resilient/app.config
Environment=APP_LOCK_FILE=/home/integration/.resilient/resilient_circuits.lock

[Install]
WantedBy=multi-user.target
```

Warning : This line is different from the official doc, in our case the path is different :  
`ExecStart=/usr/bin/resilient-circuits run`

# Installing QRadar SOAR Circuits as a service

```
sudo systemctl daemon-reload  
  
sudo systemctl enable resilient_circuits.service  
  
sudo systemctl start resilient_circuits.service  
  
sudo systemctl status resilient_circuits.service
```

- Circuits will reboot if there is any errors, it will also start on boot.

```
[integrations@resilient ~]$ sudo systemctl status resilient_circuits.service  
● resilient_circuits.service - Resilient-Circuits Service  
   Loaded: loaded (/etc/systemd/system/resilient_circuits.service; enabled; vendor preset: disabled)  
   Active: active (running) since Wed 2017-12-13 13:34:24 UTC; 6s ago  
     Main PID: 2094 (resilient-circu)  
        CGroup: /system.slice/resilient_circuits.service  
           └─2094 /usr/local/bin/python2.7 /usr/local/bin/resilient-circuits run  
  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,454 INFO [client] Connecting to resilient.localdomain:65001 ...  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,529 INFO [client] Connection established  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,631 INFO [client] Connected to stomp broker [session=ID:resilient.localdomain-46049-1513168481358-5...ersion=1.2]  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,631 INFO [stomp_component] Connected to failover:(ssl://resilient.localdomain:65001)?maxReconnectAttempts=1  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,631 INFO [stomp_component] Client HB: 0 Server HB: 15000  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,632 INFO [stomp_component] No Client heartbeats will be sent  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,632 INFO [stomp_component] Requested heartbeats from server.  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,633 INFO [actions_component] STOMP connected.  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,735 INFO [actions_component] Subscribe to message destination 'shell'  
Dec 13 13:34:25 resilient.localdomain resilient-circuits[2094]: 2017-12-13 13:34:25,736 INFO [stomp_component] Subscribe to message destination actions.201.shell  
Hint: Some lines were ellipsized, use -l to show in full.  
[integrations@resilient ~]$
```

QRADAR SOAR TRAINING

# Lab 14:

# Install the apphost package

Goal:

- Install an AppHost Package on a GUI
- Understand the notion of app pairing

# App Host creation

Not Applicable on Remote Saas **emea-training** Lab  
OVA already prepared for AppHost

- Official documentation to install the run file on your BYORH:  
[https://www.ibm.com/support/knowledgecenter/SSBRUQ\\_39.0.0/doc/apps/deploy\\_run\\_file.html](https://www.ibm.com/support/knowledgecenter/SSBRUQ_39.0.0/doc/apps/deploy_run_file.html)
- If you are installing the AppHost on your own Red Hat, please do

```
sudo yum install -y createrepo
sudo subscription-manager repos --enable=rhel-7-server-extras-rpms
sudo yum install container-selinux
sudo firewall-cmd --permanent --zone=trusted --add-interface=cni0
sudo firewall-cmd --permanent --zone=trusted --add-interface=flannel.1
sudo firewall-cmd --permanent --zone=trusted --add-port=443/tcp
sudo firewall-cmd --permanent --zone=trusted --add-port=6443/tcp
sudo firewall-cmd --permanent --zone=trusted --add-port=10250/tcp
sudo firewall-cmd --permanent --zone=public --add-port=22/tcp
sudo firewall-cmd --reload
sudo systemctl restart firewalld
```

And install the program from <https://ibm.ent.box.com/file/817940292554?v=ResilientAppHostRun> :

```
sudo bash apphost-1.5.218.run
```

```
Creating log directory /usr/share/apphost/logs
Performing post-installation setup...
Installation complete
```

- The OVA for the training has been prepared for App Host**
- Just use the appadmin user and enter the pairing key on the commands:**

```
su appadmin
cd
sudo manageAppHost install
```

# App Host Pairing

- And go to QRadar SOAR GUI, Administrator Settings > Apps > App Host > [Add +]
- Create the pairing key
- Copy the pairing key to clipboard
- Paste it in the SSH window:

```
-bash-4.2$ sudo manageAppHost install
Enter pairing info: {
  "manager_url": "https://warbler.poc.resilientsystems.com/services_proxy/manager",
  "controller": {
    "id": "922b48ba-a3fc-490c-9da0-11ad2547db0c",
    "tenant_id": "d0e7fb53-ac63-4815-a81e-3eb15fc70520",
    "name": "IS and AppHost on v37 OVA",
    "description": {
      "format": "text",
      "content": "Local BR MAC"
    },
    "app_ids": [],
    "keypair": {
      "private": "-----BEGIN PRIVATE KEY-----\nMIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwgg\n9En7jPTKHHp2ESJa0teN8Sr0n1ffL703cKGJ5CEQplrn4f7s8pmhMC86F7wnbAr3kjubU-U6eD2LY9D\nL861DGRRXb0tgyxq74XcBe7h8+j8HJE6qPMPydhFzufU-Nw0Zs5CB1uphnBGUFcvE9M0hozJsimyaFrZdaTb\nnxidMKuKwzpJ20yrbkzSbzefb6/ZgwdwabAUdpfjnSmixQXWAQKBgDwxbtqogWlxMOIYB1puh1YKbBC3aw6-\nhh2yaszdj9DTx08upSV4nVr7k1RZXCFE4iLjeTGn1gPH/1CIVVvCQhpw7FqIm7prj0z5Pnd8MMhnkOYQkH\n0jnrfi+a3zb0gr+y1VcZ4EA2hGax6a+N6J/SscTaAHlfzP0nzPZan0Qf+sBl0Vt/FVG1hPtKXdqphzAdGAN8\n0nGXUcgYAuGeIEnUBUV8JX/CzeoZBH2jb8AfWwCjac63pcEu1MJF45VW6syDEaJ+dBqck+9C3vfTzedK32g\n  },
  "created": 1596477483063,
  "modified": 1596477483063
}
```

## Create App Host Pairing

Before performing this procedure, you should have the App Host software installed as described in the documentation.

An App Host is created on a different system; however, you generate the information to pair the App Host with the Resilient organization here. Enter a unique name and description for the App Host, click Create then click Copy to Clipboard. You are prompted to paste this information when creating the App Host.

Name  
IS and AppHost on v37 OVA

Description  
Local BR MAC

Copy the following code to use when installing the App Host.

```
{
  "manager_url": "https://warbler.poc.resilientsystems.com/services_proxy/manager",
  "controller": {
    "id": "922b48ba-a3fc-490c-9da0-11ad2547db0c",
    "tenant_id": "d0e7fb53-ac63-4815-a81e-3eb15fc70520",
    ...
  }
}
```

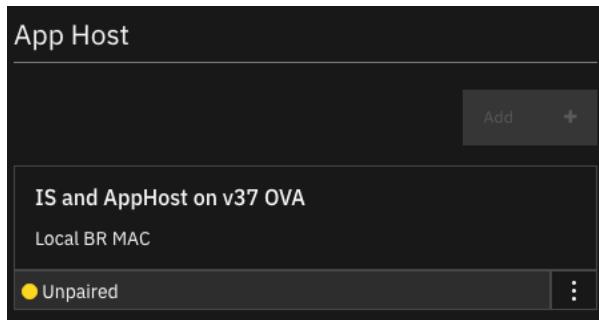
Show more

Close

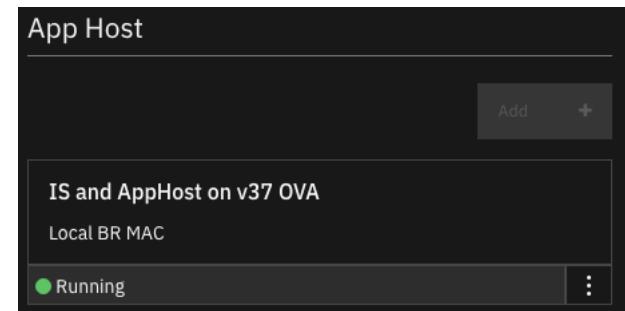
Copy to Clipboard

# App Host Paired

```
INFO: Installing
INFO: Registering custom resource
INFO: Creating/Updating controller namespace: 922b48ba-a3fc-490c-9da0-11ad2547db0c
INFO: Creating shared secret
INFO: Creating synchronizer secret
INFO: Creating controller-registry-secret secret
INFO: Creating/updating role: operator-role
INFO: Creating/updating role: synchronizer-role
INFO: Creating/updating service account: apphost-synchronizer-service-acct
INFO: Creating/updating service account: apphost-operator-service-acct
INFO: Creating role binding: synchronizer-role-binding
INFO: Creating role binding: operator-role-binding
INFO: Creating/updating synchronizer deployment
INFO: Creating/updating operator deployment
INFO: Sending heartbeat for app host
INFO: Installation succeeded
```



Wait some minutes (5)  
or  
Reboot the server



QRADAR SOAR TRAINING

# Lab 15:

# Install your first app

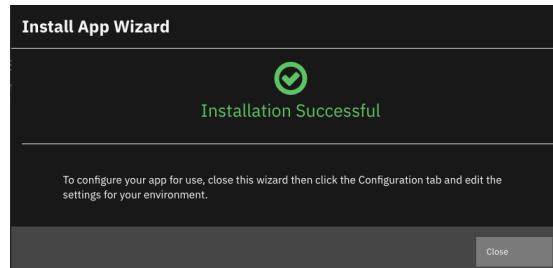
Goal:

- Install and initialize an app in a GUI
- Understand the notion of vulnerability and its significance in a SOC for remediation

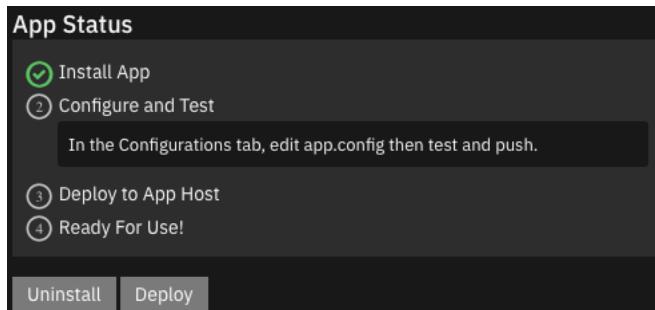


# Install your first App

- In QRadar SOAR GUI, Administrator Settings > Apps > App > [Install]
- Select the package `app-fn_cve_search-1.0.1.zip` and upload the file
- You get the result of the package and version, and all customizations
- Press [Install App]



- You get the status:



The following information was found in the package:

Name	fn_cve_search
API Name	fn_cve_search
Author	Resilient Labs
Description	The CVE search API is a RESTful web service allowing to search for vulnerabilities. by using this api vulnerabilities can be searched based on vendor name, product name, specific CVE Id's, the searched results will be updated in CVE Data Table and Incidents Notes section.
Version	1.0.1
Compatibility	35.2.32
Executables	fn_cve_search

**API Key Assigned:**  
app\_fn\_cve\_search\_exe\_fn\_cve\_search

**Package Contents: 17 Customizations**

Name	Type
CVE ID	Activity Field
CVE Vendor	Activity Field
CVE Searched Data	Data Table
CVE Browse	Function
CVE Search	Function
cve_browse_criteria	Function Input
cve_id	Function Input
cve_product	Function Input
cve_published_date_from	Function Input
cve_published_date_to	Function Input

Cancel      Install App

# Configure the first App

- Go to Configuration, double clic on the file app.config
- If needed, update if necessary the file with the integration specific ApiKey and configuration fields

Adjust if needed the certificate control (cafile = false)

changes and restart the app.

File Name  
app.config

File Path  
/etc/rescircuits

File Annotations  
Display any configuration comments and variables to be defined.  
[fn\_cve\_search]  
# Flag display maximum CVE Entries on the resilient table

File Content  
Text or code as appropriate.

Theme light File Type Initialization

```
1 - [fn_cve_search]
2 # Flag display maximum CVE Entries on the resilient table
3 max_results_display = 50
4 # Base URL of Common Vulnerability Exposures Data Base.
5 cve_base_url = https://cve.circl.lu/api
6
7 - [resilient]
8 api_key_id = 944dbb12-a06a-4fbb-b87f-8e1035a3876a
9 api_key_secret = hDK-4oIE3AFhjGS2LndMfZrzL-Xynp8MfyKZFz9Lo18
10 cafile = /etc/rescircuits/cert.cer
11 host = warbler.poc.resilientsystems.com
12 port = 443
13 org = 202
14
15
```

← Apps List

## fn\_cve\_search

Status: Waiting for Configure and Test

Details Customizations Configuration

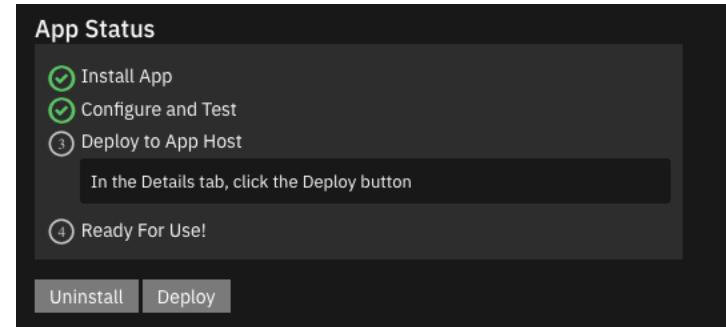
New File

App Settings

An app can consist of software code and configuration settings. The app.config file contains the settings that allow communication with the Resilient platform. You can add and edit files. You can delete files except app.config.

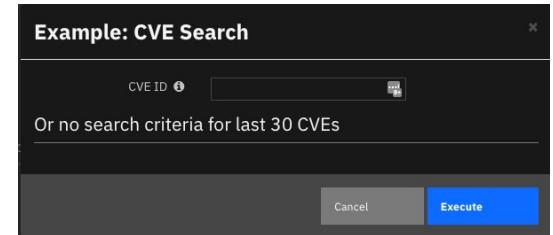
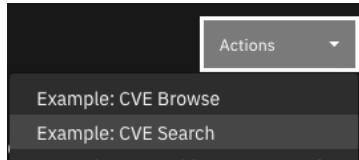
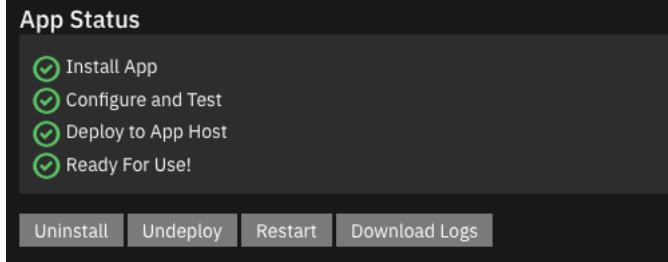
File Name	File Location	File Type	Created At	Last Modified
app.config	/etc/rescircuits	Initialization	08/03/2020 20:20	08/03/2020 20:20
cert.cer	/etc/rescircuits	Plain Text	08/03/2020 20:20	08/03/2020 20:20

- You can save and push the changes.  
If the configuration is complex, you may test before.  
Note : testing may last for several minutes
- You can deploy to App Host:



# Test your first App

- When done, the apps look like that:
- Create a Table layout tab, and add the CVE Searched Data table in. Save.
- Open an incident, select the action CVE Search
- And execute to get directly the last 30 CVEs and wait for the result.



Tasks	Details	Breach	Notes	Members	News Feed	Attachments	Stats	Timeline	Artifacts	Email	Tables	Edit
CVE Searched Data												
Search... <input type="text"/> Print Export												
CVE ID	Published Date	Summary	References	Vulnerability Config	Vulnerable Config Cpe 2							
CVE-2020-8575	08/03/2020	Active IQ Unified Manager for VMware vSphere and Windows versions prior to 9.5 are susceptible to a vulnerability which allows administrative users to cause Denial of Service (DoS).	<a href="https://security.netapp.com/advisory/ntap-20200803-0002/">https://security.netapp.com/advisory/ntap-20200803-0002/</a>	No Data	No Data	⋮	⋮	⋮	⋮	⋮	⋮	⋮
CVE-2020-8574	08/03/2020	Active IQ Unified Manager for Linux versions prior to 9.6 ship with the Java Management Extension Remote Method Invocation (RMI) service enabled allowing unauthorized code execution to local users.	<a href="https://security.netapp.com/advisory/ntap-20200803-0002/">https://security.netapp.com/advisory/ntap-20200803-0002/</a> <a href="https://security.netapp.com/advisory/ntap-20200803-0001/">https://security.netapp.com/advisory/ntap-20200803-0001/</a>	No Data	No Data	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Action Status						
Status	Type	User	Rule/Workflow Name	Information	Date	Complete
Completed	Workflow: Function	Benoit ROSTAGNI	Example: CVE Search - CVE Search	Completed	08/03/2020 21:34:15	
Information				Successfully searched the CVE Database.	08/03/2020 21:34:15	
Information				Searching the CVE Database. ID:None, Vendor:None, Product:None	08/03/2020 21:34:15	
Information						

```
-bash-4.2$ sudo kubectl logs -n 922b48ba-a3fc-498c-9da8-11ad2547dbdc deployments/4326b5d9-8554-4c43-a49a-59a5ef65b5b9
/rsrcircuits/app:entrypoint: OK
2020-08-03 19:28:29,526 INFO [app] Configuration file: /etc/rsrcircuits/app.config
2020-08-03 19:28:29,526 INFO [app] Resilient server: warbler.poc.resilientsystems.com
2020-08-03 19:28:29,526 INFO [app] Resilient user: None
2020-08-03 19:28:29,526 INFO [app] Resilient org: 293
2020-08-03 19:28:29,526 INFO [app] Logging Level: INFO
2020-08-03 19:28:31,588 INFO [app] Components auto-load directory: (none)
2020-08-03 19:28:31,740 INFO [component_loader] Loading 2 components
2020-08-03 19:28:31,740 INFO [component_loader] 'fn_cve_search.components.function_cve_browse.FunctionComponent' loading
2020-08-03 19:28:31,740 INFO [component_loader] 'fn_cve_search.components.function_cve_search.FunctionComponent' loading
2020-08-03 19:28:31,740 INFO [app] Components loaded
2020-08-03 19:28:31,740 INFO [app] App Started
2020-08-03 19:28:31,884 INFO [client] Connection to Stomp attempting to connect
2020-08-03 19:28:31,884 INFO [stomp_component] Connect to Stomp...
2020-08-03 19:28:31,884 INFO [client] Connecting to warbler.poc.resilientsystems.com:65801 ...
2020-08-03 19:28:31,884 INFO [client] Connection established
2020-08-03 19:28:32,437 INFO [stomp_component] Connected to stomp broker [session=10@warbler.poc.resilientsystems.com-49648-1595259348123-4;48, version=1.2]
2020-08-03 19:28:32,437 INFO [stomp_component] Connected to failover[ssl://warbler.poc.resilientsystems.com:65801?maxReconnectAttempts=1,startupMaxReconnectAttempts=1]
2020-08-03 19:28:32,438 INFO [stomp_component] Client HB: 0 Server HB: 15000
2020-08-03 19:28:32,438 INFO [stomp_component] No Client heartbeats will be sent
2020-08-03 19:28:32,438 INFO [stomp_component] Requested heartbeats from server.
2020-08-03 19:28:32,541 INFO [actions_component] resilient-circuits has started successfully and is now running...
2020-08-03 19:28:32,542 INFO [actions_component] Subscribe to message destination 'fn_cve'
2020-08-03 19:28:32,542 INFO [stomp_component] Subscribe to message destination actions.202_fn_cve
2020-08-03 19:28:33,550 INFO [actions_component] [EventFunction:cve_search] (id:466, workflow=example_cve_search, user=benoit.rostagni@ibm.com) 2020-08-03 19:26:32.772000
2020-08-03 19:28:33,552 INFO [function_cve_search] cve vendor: None
2020-08-03 19:28:33,553 INFO [function_cve_search] cve_product: None
2020-08-03 19:28:33,553 INFO [function_cve_search] cve_published_date_from: None
2020-08-03 19:28:33,553 INFO [function_cve_search] cve_published_date_to: None
2020-08-03 19:28:33,553 INFO [decorators] [function_cve_search] StatusMessage: Searching the CVE Database. ID:None, Vendor:None, Product:None
2020-08-03 19:28:33,759 INFO [decorators] [function_cve_search] StatusMessage: Successfully searched the CVE Database.
/etc/rsrcircuits/app.config: OK
```

QRADAR SOAR TRAINING

# Lab 16: Install fn\_utilities app

Goal:

- Install and initialize a complex app on a GUI



# Install your App

- Go to IBM App Exchange and download Utility Functions for QRadar SOAR



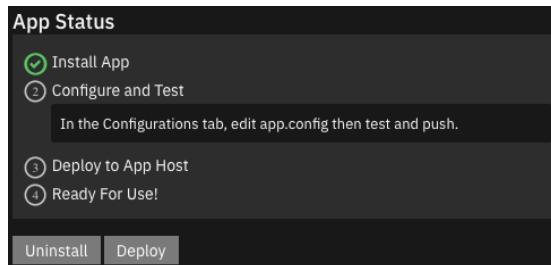
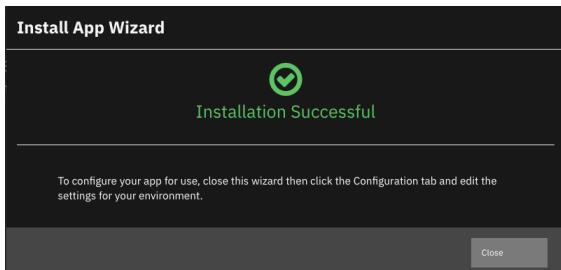
## Utility Functions for Resilient

Resilient, by IBM Resilient

IBM Validated

★★★★★ (3)

- Like in the previous lab, install the app in your QRadar SOAR GUI
- Select the package app-fn\_utilities-x.x.x.zip



**Install App Wizard**

**Package Information**

The following information was found in the package:

Name	fn_utilities
API Name	fn_utilities
Author	IBM Resilient
Description	Resilient functions simplify development of integrations by wrapping each external activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.
Version	2.0.1
Compatibility	35.2.32
Executables	fn_utilities

**API Key Assigned:**  
app\_fn\_utilities\_exe\_fn\_utilities

**Package Contents: 115 Customizations**

**Cancel** **Install App**

# Configure the App

- Go to Configuration, double clic on the file app.config
- If needed, update if necessary the file with the integration specific ApiKey and configuration fields

Adjust if nedeed the certificate control (cafile = false)

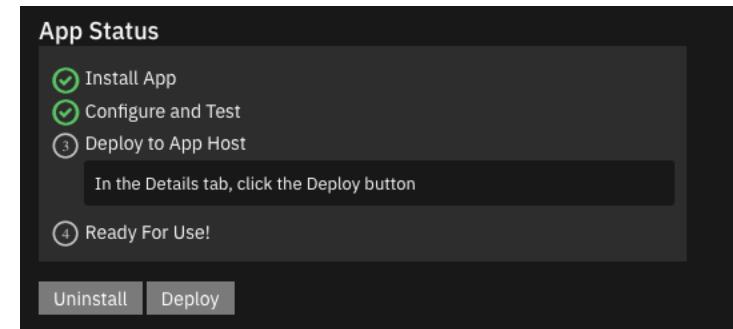
The screenshot shows the configuration interface for the app.config file. It includes sections for File Name (app.config), File Path (/etc/rescircuits), and File Annotations ([fn\_utilities]). The File Content section displays the configuration code, with the line 'cafile = false' highlighted in red.

```
17 #WIOS = WIOS ${!SHELL_PARAMETER}
18 # Max Timer sleep timeThe input string is of format "time value" concat
19 # "time unit" character, where character is: 's' for seconds, 'm' for
20 # 'd' for days. For example: '30s' = 30 seconds; '40m' = 40 minutes;
21 max_timer = 30d
22
23 # uncomment to add proxies
24 #https_proxy=https://<your_proxy>:<port>
25 #http_proxy=http://<your_proxy>:<port>
26 [resilient]
27 api_key_id = 00f82bc1-c1a4-4eca-b53f-66f8f5cbd7ba
28 api_key_secret = $API_KEY_SECRET
29 cafile = false
30 host = warbler.poc.resilientsystems.com
31 port = 443
32 org = 302
```

The screenshot shows the fn\_utilities app settings page. It lists two files: app.config and cert.cer. The app.config file is described as an Initialization file created on 12/23/2020 at 11:44. The status is "Waiting for Configure and Test". The Configuration tab is selected. A note states: "An app can consist of software code and configuration settings. The app.config file contains the settings that allow communication with the Resilient platform. You can add and edit files. You can delete files except app.config." A table shows the file details with columns: File Name, File Location, File Type, Created At, and Last Modified.

File Name	File Location	File Type	Created At	Last Modified
app.config	/etc/rescircuits	Initialization	12/23/2020 11:44	12/23/2020 11:44
cert.cer	/etc/rescircuits	Plain Text	12/23/2020 11:44	12/23/2020 11:44

- You can save and push the changes.  
If the configuration is complex, you may test before.  
Note : testing may last for several minutes
- You can deploy to App Host:



QRADAR SOAR TRAINING

# Lab 17:

# Create new Custom Playbook that uses the Shell Command Function

Goal:

- Understand the needs to modify an out-of-the-box solution to match the local production needs
- Apply creating a playbook using functions from another installed app

# Create new Custom Playbook that uses our Shell Command Function

Click the **Playbook** Tab

Create a New Playbook:

Name: **nslookup**

For the first object:

Activation Type: **Manual**

Object Type: **Artifact**

Add the Function:

**Utilities: ShellCommand**

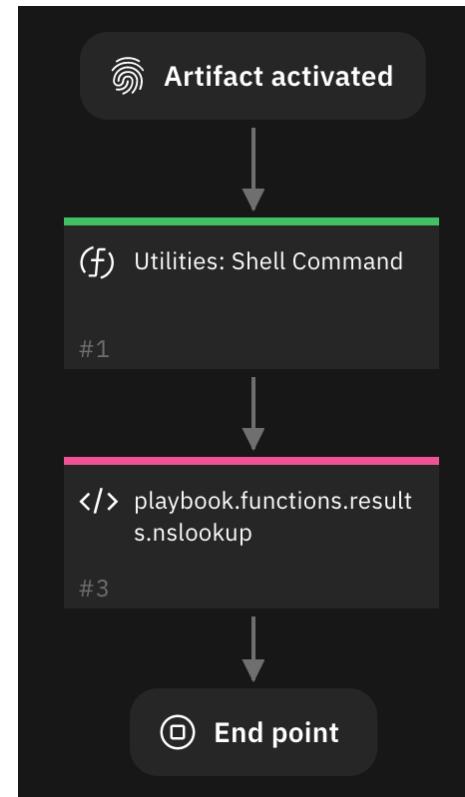
Add a new script:

Name: **playbook.functions.results.nslookup**

*(as you can't leave it empty just add any character in it and save, you can change the content later)*

Add an **End Point** to the canvas

Finally, link everything like in this screenshot



# Edit Function script and Post-Process Scripts

## Edit the Function:

Function input: **script**

Output name: **nslookup**

### Edit script

Node details  
Utilities: Shell Command #1

Use "inputs.<field\_name>" to set function inputs. Example: inputs.foo = 1200.

Language Python 3 Mode Default Tab Size 2 - Font + Font

```
1 inputs.shell_command = "nslookup"
2 inputs.shell_remote = False
3 inputs.shell_param1 = artifact.value
```

## Edit the Function Script:

```
inputs.shell_command = "nslookup"
inputs.shell_remote = False
inputs.shell_param1 = artifact.value
```

## Edit the **playbook.functions.results.nslookup** Script:

```
results = playbook.functions.results.nslookup
note_text = u"Command succeeded: {}\\n{}".format(results.commandline, results.stdout)
incident.addNote(helper.createPlainText(note_text))
```

### Edit script

Script details  
Script scope  Global  Local Script name: playbook.functions.results.nslookup

Code

Language Python 3 Mode Default Tab Size 2 - Font + Font

```
1 results = playbook.functions.results.nslookup
2 note_text = u"Command succeeded: {}\\n{}".format(results.commandline, results.stdout)
3 incident.addNote(helper.createPlainText(note_text))
```

# Run our Custom Workflow

to your **Incident**

Click the **Artifacts** Tab

Run *Nslookup* playbook on the *resilientsystems.com* Artifact

Hits	Related I...	Type	Value	Created	↓	Last Modified	Relate?	Actions
0		DNS Name	resilientsystems.com	12/11/2020 16:13		12/11/2020 16:13	As specified	
Items per page 25 ▾ 1-1 of 1 item							CB Hunt IOCs	

CB Hunt IOCs  
Example: Call REST API  
Example: Domain Distance  
Example: Extract SSL Certificate  
Example: JSON2HTML  
Example: Shell Command  
Example: String to Attachment  
**Nslookup**

See the logs in the terminal and results in the **Notes** Tab

```
app_fn_utilities_exe_fn_utilities added a note to the Incident 12/23/2020 12:34
Command Succeeded: nslookup "resilientsystems.com"
Server: 10.43.0.10
Address: 10.43.0.10#53

Non-authoritative answer:
Name: resilientsystems.com
Address: 169.46.89.149
Name: resilientsystems.com
Address: 2620:12a:8001::3
Name: resilientsystems.com
Address: 2620:12a:8000::3
```

QRADAR SOAR TRAINING

# Lab 18: (optional) Install nmap in AppHost and remote control to VM

Goal:

- Understand the notion of Kubernetes, Docker and constraints linked to those environments
- Overtake those constraints configuring remote commands from an app to answer a need

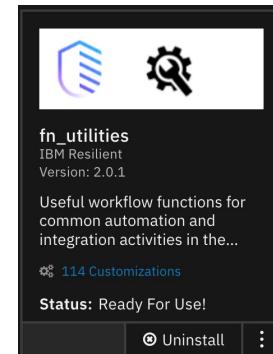
## Install nmap in AppHost in ssh

```
wget https://www.rpmfind.net/linux/centos/7.9.2009/os/x86\_64/Packages/libpcap-1.5.3-12.el7.x86\_64.rpm
wget http://mirror.ghettoforge.org/distributions/gf/el/7/plus/x86\_64/nmap-ncat-7.10-1.gf.el7.x86\_64.rpm
wget http://mirror.ghettoforge.org/distributions/gf/el/7/plus/x86\_64/nmap-7.10-1.gf.el7.x86\_64.rpm
```

```
sudo rpm -Uvh libpcap-1.5.3-12.el7.x86_64.rpm
sudo rpm -Uvh nmap-ncat-7.10-1.gf.el7.x86\_64.rpm
sudo rpm -Uvh nmap-7.10-1.gf.el7.x86\_64.rpm
```

# Configure remote command

- Go to QRadar SOAR GUI, administrator settings > app
- Click on fn\_utilities > configuration > app.config



**fn\_utilities**

Status: Ready For Use!

App Settings / app.config

Edit the settings below. You cannot change the name or location. When done, click Test Configuration to verify the settings then click Save and Push Changes to implement your changes and restart the app.

File Name: app.config

File Path: /etc/rescircuits

File Annotations:

Display any configuration comments and variables to be defined.  
[fn\_utilities]

Cancel Save and Push Changes

Created Date: 12/23/2020 11:44  
Last Modified Date: 02/22/2021 11:57

Show more

# Configure remote command

- In the « file content » section,

File Content  
Text or code as appropriate.

Theme dark File Type Initialization

```
1 [fn_utilities]
2 # For safety, shell_command parameter values are escaped - set to 'sh'
3 shell_escaping = sh
4 # accepted remote powershell extensions in a comma separated list, exa
5 remote_powershell_extensions = ps1
6 # remote auth transport one of [ntlm, basic]
7 remote_auth_transport = ntlm
8 # remote computers
9 # remote_computer = (username:password@server)
10 remote_computer = (integration: [REDACTED]@10.42.0.1) ←
11 # remote shell commands
12 remote_command_powershell = [remote path to script]
13 remote_command_linux = (remote path to script)
14 nmap = (nmap "{{shell_param1}}") ←
15 # local shell_command default commands (unix)
16 nslookup = nslookup "{{shell_param1}}"
17 dig = dig "{{shell_param1}}"
18 traceroute = traceroute -m 15 "{{shell_param1}}"
19 whois = whois "{{shell_param1}}"
20 # Max Timer sleep timeThe input string is of format "time value" conca
21 # "time unit" character, where character is: 's' for seconds, 'm' for
22 # 'd' for days. For example: '30s' = 30 seconds; '40m' = 40 minutes;
23 max_timer = 30d
24
25 # uncomment to add proxies
26 #https_proxy=https://<your_proxy>:<port>
27 #http_proxy=http://<your_proxy>:<port>
28 #resilient
```

Note: the 10.42 network is the network used by the Apphost micro kubernetes inside the App Host system. We will use the gateway to run the command on the App Host system.

You can check the gateway using the traceroute default example shell command action

Copy this line with your apphost password

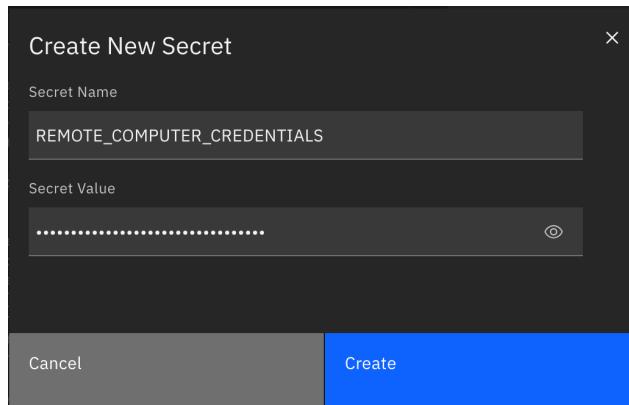
Configure the remote command by writing it in parentheses, the parameter will be added by the workflow

# Configure remote command

- For security purposes, you can also add the remote computer as a secret

```
9 # remote_computer = (username:password@server)
10 remote_computer = (integration: [REDACTED]@10.42.0.1) ←
11 # remote shell commands
```

Copy this line with your apphost password



Create a new secret and paste your remote computer credentials (**including the parentheses**) in the Secret Value field

```
8 # remote computers
9 remote_computer = $REMOTE_COMPUTER_CREDENTIALS|
10 # remote shell commands
```

Then replace the remote computer credentials in the file content script with the name of the secret

# Configure the Playbook

Create a new playbook :  
Name: **Example: Remote Command**

First Object:  
Activation Type: **Manual**  
Object Type: **Artifact**

Create new playbook

Add a name and description to create a playbook.

Name  
Example: Remote Command

API name  
example\_remote\_command

Activation details

Activation type  
Manual

Object type  
Artifact

Add a condition to the first object:

Condition builder

IF      Type      has one of      DNS Name X      IP Address X      URL X

Add the function « Utilities: Shell Command »:  
Select Function Input : **Script**  
Output name: **nmap**

Function's script:

Note : Find the python code in the directory lab file in text for a better copy and paste

### Edit script

Node details  
Utilities: Shell Command #1

Use "inputs.<field\_name>" to set function inputs. Example: inputs.foo = 1200.

Language Python 3 Mode Default Tab Size 2 - Font + Font

```
1 import re
2
3 inputs.shell_command = 'nmap'
4 inputs.shell_remote = True
5 # the conditional is used so you can add other remote commands
6 if inputs.shell_command == 'nmap':
7     inputs.shell_command = 'nmap:remote_computer'
8
9 if artifact.type.lower() in ['url']:
10    p = re.compile("(?:https?://)?(\\w+\\.(\\w+\\.(\\w+\\.\\w+)))?(\\w+\\.(\\w+\\.\\w+))?")
11    match = p.match(artifact.value)
12    inputs.shell_param1 = match.group(1) if match else artifact.value
13 else:
14     inputs.shell_param1 = artifact.value
```

Add a new script:  
Name: **playbook.functions.results.nmap**

Note : Also find this python code in the directory lab file in text for a better copy and paste

### Edit script

Script details

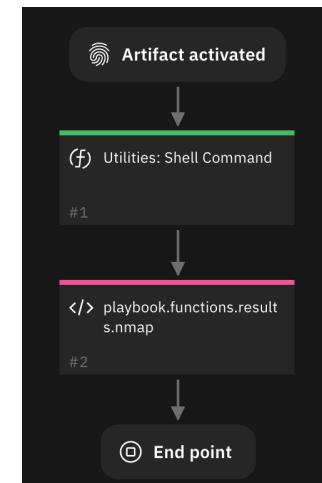
Script scope: Global Script name: playbook.functions.results.nmap Description (optional): Enter a short description

Code

Language Python 3 Mode Default Tab Size 2 - Font + Font

```
1 results = playbook.functions.results.nmap
2 if results.exitcode == 0:
3     note_text = "Command succeeded: {}\nStandard Out: {}\nStandard Error: {}".format(results.commandline, results.stdout, results.stderr)
4 else:
5     note_text = "Command failed: {}\nStandard Out: {}\nStandard Error: {}".format(results.commandline, results.stdout, results.stderr)
6
7 incident.addNoteHelper.createPlainText(note_text)
```

Add an End Point, link every object, Save and enable the playbook



# Configure the remote command

Hits	Related ...	Type	Value	Created	↓	Last Modified	Relate?	Actions
▲ 1		IP Address	9.9.9.9	02/19/2021 10:46		02/22/2021 16:26	As specified in	
0		Email Recipient	gaetan.lodde@testmail.com	12/30/2020 12:28		12/30/2020 12:28	CB Hunt IOCs	
0		DNS Name	resilientsystems.com	12/11/2020 16:13		12/11/2020 16:13	Example: Call REST API	

Items per page 25 ▾

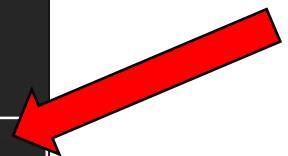
1-3 of 3 items

- Go to an incident and add an artifact (here the ip address 9.9.9.9)
- Launch the action « Example: Remote Command »
- A note is added with the result :

```
app_fn_utilities_exe_fn_utilities added a note to the Incident 02/22/2021 16:26
Command failed: nmap "9.9.9.9"
Standard Out:
Starting Nmap 7.10 ( https://nmap.org ) at 2021-02-22 15:23 UTC
Nmap scan report for dns9.quad9.net (9.9.9.9)
Host is up (0.075s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

As specified in  
CB Hunt IOCs  
Example: Call REST API  
Example: JSON2HTML  
Example: Shell Command  
Example: String to Attachment  
Nslookup  
Enrichment: Extreme IP Lookup  
Example: Virus Total  
wiki look  
Delete Data Table Row  
Delete Data Table Rows  
Get Data Table Row  
Get Data Table Rows  
Update Data Table Row  
Example: Remote Command



QRADAR SOAR TRAINING

# Lab 19: (optional) Install the Components File for App Host

Goal:

- Use an existing app to overcome specific app creation to solve an issue (here collect JSON data from a third-party website and show usable results for the Analyst)

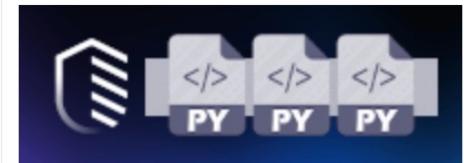
# Install fn\_components

- Install fn\_components in your Lab 21 folder
- In QRadar SOAR GUI, Administrator Settings > Apps > App > [Install +]
- Select the package app-fn\_components-x.x.x.zip and upload the file

The screenshot shows the 'fn\_components' app details page in the QRadar SOAR GUI. The page has a dark theme with white text. At the top, it says 'Status: Ready For Use!'. Below that is a large icon of a gear with horizontal lines. To the right of the icon, the app name 'fn\_components' is displayed. Underneath the name, there are sections for 'Details', 'Customizations', and 'Configuration'. The 'Details' tab is selected. It contains the following information:

- Name:** fn\_components
- API Name:** fn\_components
- Author:** Resilient Labs
- Compatibility:** 35.2.32

The 'Installation' section shows 'Installed 12/15/2020 by Gaëtan Loddé'. The 'Description' section states: 'This is a shell container for running single-file integrations which are added to the components/ directory'. The 'Version' is listed as 1.0.0. The 'App Host' section has a yellow warning icon and a placeholder 'AppHost pairing key V2'. The 'App Status' section shows five green checkmarks: 'Install App', 'Configure and Test', 'Deploy to App Host', 'Ready For Use!', and 'Ready For Use!' again. At the bottom of the page are buttons for 'Uninstall', 'Undeploy', 'Restart', 'Download Logs', and 'Upgrade'.



Resilient

## App Host Components for Resilient

Allow single-file python integrations to run in App Host

By Resilient Labs  
Community Provided

Install and deploy the app as seen in the previous labs

Add the line:

componentsdir = /var/rescircuits/components  
in the app.config

# Use Case : Create a new integration

- We are going to create a completely new integration that will collect the json of <https://extreme-ip-lookup.com/>

## eXTReme-IP-LOOKUP.COM

Login

### Free IP Lookup Geolocation API

Lookup IP

IP Address:	<b>108.20.43.77</b>	City:	<b>Winchester</b>
IP Type:	<b>Business / Education / Residential</b>	Country:	<b>United States</b>
Business:	-	Region:	<b>Massachusetts</b>
Website:	-	Continent:	<b>North America</b>
IP Name:	<b>pool-108-20-43-77.bstnma.fios.verizon.net</b>	Latitude:	<b>42.45232</b>
ISP:	<b>Verizon Business</b>	Longitude:	<b>-71.137</b>
Organisation:	<b>Verizon Business</b>		

[Click for sample Business IP](#) [Click for sample Education IP](#)  
**\*\* [How to get Service Provider back in Google Analytics \\*\\*](#)**



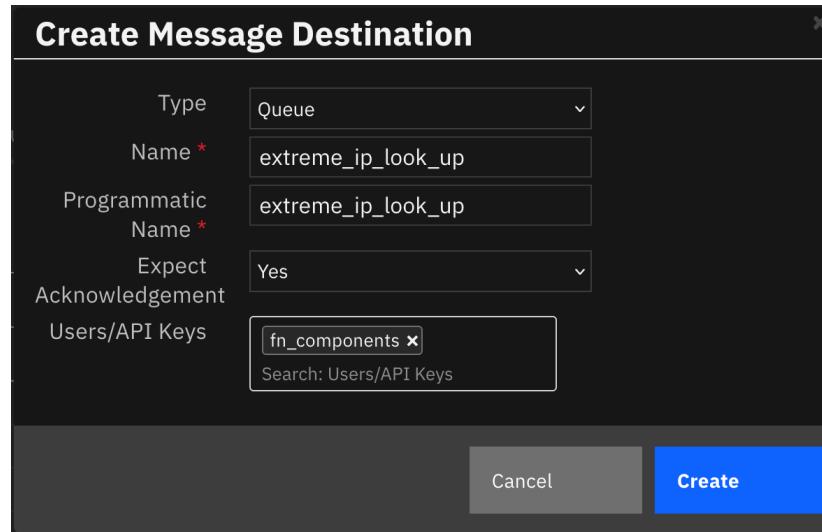
# Create a Message Destination

- Create a new message using the app\_fn\_components app key:

**Create Message Destination**

Type	Queue
Name *	extreme_ip_look_up
Programmatic Name *	extreme_ip_look_up
Expect Acknowledgement	Yes
Users/API Keys	<input type="text" value="fn_components"/> <span>x</span> Search: Users/API Keys

**Cancel** **Create**



- Remember the Programmatic Name for later `extreme_ip_look_up`

# Create the function

- Create the function that will use an IP as source text field

The screenshot shows the 'Customization Settings' page in IBM Security SOAR. The top navigation bar includes links for 'IBM Security SOAR', 'Dashboards', 'Inbox', 'Artifacts', 'Incidents', 'Create incident', 'Search', 'Playbooks', and a user profile for 'Gaetan Lodde'.

The main navigation bar has tabs for 'Layouts', 'Rules', 'Scripts', 'Workflows', 'Functions', 'Destinations', 'Phases & Tasks', 'Incident Types', 'Breach', and 'Artifact Types'. The 'Functions' tab is currently selected.

The left sidebar shows the current path: 'Functions / New'. On the right, there are three buttons: 'Cancel', 'Save & Close' (which is highlighted in blue), and 'Save'.

The form fields for creating a new function are as follows:

- Name \***: Extreme ip look up
- API Name \* ⓘ**: extreme\_ip\_look\_up
- Message Destination \***: extreme\_ip\_look\_up
- Description**: From an IP use [https://extreme-ip-lookup.com/json/\(place ip here\)](https://extreme-ip-lookup.com/json/(place ip here)) and present the output

On the right side of the form, there are status fields:

- Creator: -
- Last Modified: -
- Last Modified By: -
- Associated Workflows: Function is not currently referenced by any workflow.

The 'Inputs' section contains a single input field with the value 'ip'.

The 'Input Fields' section lists several fields with edit icons:

- incident\_id
- ip
- json2html\_data
- json2html\_keys
- relations\_child\_incident\_id
- relations\_note\_id

An 'Add Field' button is located at the top right of the 'Input Fields' section.

# Create the playbook that will run the function from an IP artifact

Create a new Playbook:

Name: **Enrichment: Extreme IP Look Up**

First Object:

Activation Type: **Manual**

Object Type: **Artifact**

Add the function you created:

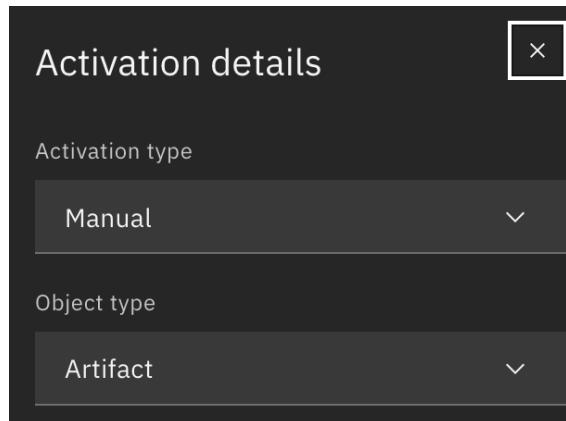
Name: **Extreme ip look up**

Function Input: **Script**

Function Output: **ip\_lookup**

Function's script:

inputs.ip = artifact.value



The screenshot shows a configuration panel for a function named 'Extreme ip look up'. It includes sections for 'Function inputs' (set to 'Script'), 'Language' (Python 3), 'Input fields' (ip (optional)), 'Description' (From an IP use https://extreme-ip-lookup.com/json/(place ip here) and present the output), and 'Function output' (Output name ip\_lookup). The 'Script' tab is selected in the 'Function inputs' section. The script code area contains the Python code: 

```
1 inputs.ip = artifact.value
```

.

The dialog box has a dark background with white text. It displays the function code under 'Node details': 

```
1 inputs.ip = artifact.value
```

. Below the code, there is a note: 'Use "inputs.<field\_name>" to set function inputs. Example: inputs.foo = 1200.' At the bottom, there are settings for 'Language' (Python 3), 'Mode' (Default), 'Tab Size' (2), and font controls.

# Create a new script to present the data the way you want

Script name: **playbook.functions.results.ip\_lookup**

The script is available to copy and paste in your Lab 21 folder, name: **ip\_lookup script**

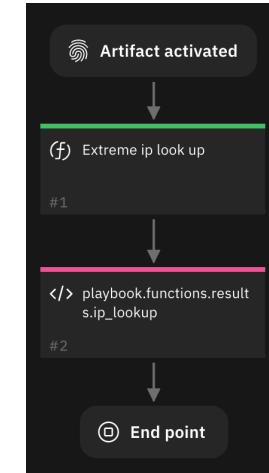
```
"""
Example output from extreme-ip-lookup.com
with numbered my usage in rich text
{
u'status': u'success',
9   u'city': u'Berkeley',
3   u'businessWebsite': u'www.quad9.net',
1   u'ipType': u'Business',
u'countryCode': u'US',
7   u'country': u'United States',
8   u'region': u'California',
10  u'isp': u'Quad9',
11  u'lbn': u'122.27275',
12  u'lat': u'37.87159',
0   u'query': u'9.9.9.9',
2   u'businessName': u'Quad9.net',
4   u'ipName': u'dns9.quad9.net',
5   u'org': u'Quad9',
6   u'continent': u'North America'
}
https://maps.google.com/?q=<lat>,<lng>
"""

if results.status == 'success':
    rich_text = '<h4><u><b>Extreme IP Lookup on {0}</h4></u></b><br>IP Type: <b>{1}</b><br>Business Name: <b>{2}</b><br>Business Website: <b>{3}</b><br>ipName: <b>{4}</b><br>Org: <b>{5}</b><br>ISP: <b>{10}</b><br>Continent: <b>{6}</b><br>Country: <b>{7}</b><br>Region: <b>{8}</b><br>City: <b>{9}</b><br>GeoLocation: <b>{11}</b><a href="https://maps.google.com/?q={11},{12}">Google Maps link on {11},{12}</a></b>'.format(results['query'], results['ipType'], results['businessName'], results['businessWebsite'], results['ipName'], results['org'], results['continent'], results['country'], results['region'], results['city'], results['isp'], results['lat'], results['lon'])
    low_text = ">>Extreme IP Lookup\IP Type: {0}\Business Name: {1}\nCountry: {2}"".format(results['ipType'], results['businessName'], results['country'])

    incident.addNote(helper.createRichText(rich_text))

# write artifact description
if artifact.description is None:
    artifact.description = "{}".format(low_text)
else:
    artifact.description = "{} \n {}".format(artifact.description["content"], low_text)
```

Add an End Point  
Link every object and save the playbook



# Create a new file in the fn\_components App Setting

- Use the Programmatic Name `extreme_ip_look_up.py`  
Enter the File Path: `/var/rescircuits/components`

The following script can be found in your Lab 21 folder name "extreme\_ip\_look\_up (final) with API Key.py"  
Paste the standard canvas, replacing `xxxxxxxxxxxxxxxxxxxx` by `extreme_ip_look_up`:

```
# -*- coding: utf-8 -*-
# pragma pylint: disable=unused-argument, no-self-use
"""Function implementation"""
import logging
from resilient_circuits import ResilientComponent, function, handler, StatusMessage,
FunctionResult, FunctionError

PACKAGE_NAME = "xxxxxxxxxxxxxxxxxxxx"

class FunctionComponent(ResilientComponent):
    """Component that implements Resilient function 'xxxxxxxxxxxxxxxxxxxx'"""
    def __init__(self, opts):
        """constructor provides access to the configuration options"""
        super(FunctionComponent, self).__init__(opts)
        self.options = opts.get(PACKAGE_NAME, {})

    @handler("reload")
    def _reload(self, event, opts):
        """Configuration options have changed, save new values"""
        self.options = opts.get(PACKAGE_NAME, {})
```

# Canvas page 2

- Continue adding the core, again replacing **xxxxxxxxxxxxxxxxxxxx** by **extreme\_ip\_look\_up**
- Duplicate the red line and adjust the name of the fields used in the function definition **zzzzzzzzzzz**

```
@function ("xxxxxxxxxxxxxxxxxxxx")
def _xxxxxxxxxxxxxxxxxx_function(self, event, *args, **kwargs):
    """Place here the program description"""
    try:
        # Get the wf_instance_id of the workflow this Function was called in
        wf_instance_id = event.message["workflow_instance"]["workflow_instance_id"]
        yield StatusMessage("Starting 'xxxxxxxxxxxxxxxxxxxx' running in workflow
'{0}'".format(wf_instance_id))
        # Get the function parameters:
        zzzzzzzzzz = kwargs.get("zzzzzzzzzz")  # text

        log = logging.getLogger(__name__)
        log.info("zzzzzzzzzz : %s", zzzzzzzzzz)
```

# Canvas Page 3

- Continue adding the core, again replacing **xxxxxxxxxxxxxxxxxxxx** by **extreme\_ip\_look\_up**
- Prepare to replace in RED the core of your working Python code, and the output in Json

```
#####
# PUT YOUR FUNCTION IMPLEMENTATION CODE HERE #
#####

yield StatusMessage("Finished 'xxxxxxxxxxxxxxxxxxxx' that was running in
workflow '{0}'.format(wf_instance_id))
results = {
    "content": "xyz"
}

# Produce a FunctionResult with the results
yield FunctionResult(results)
except Exception:
    yield FunctionError()
```

# Analyse the working Python Code

*This part will go along  
the other import*

*This part will go in the  
middle of the hash  
part,  
Except the ip = that  
already exist from the  
kwargs.get*

*This part will go in the  
result, of course  
without the print*

```
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning

session = requests.session()
session.verify = False
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
ip='9.9.9.9'

try:
    response = session.get("https://extreme-ip-lookup.com/json/%s" % ip)
    response.raise_for_status()
    ip_data = response.json()

    ipName = ip_data["ipName"]
except:
    ipName = ""

print(ip_data)
```

# # PUT YOUR FUNCTION IMPLEMENTATION CODE HERE #

- Replace in RED the core of your working Python code, and the output in Json

```
#####
# PUT YOUR FUNCTION IMPLEMENTATION CODE HERE #
#####

yield StatusMessage("Finished 'xxxxxxxxxxxxxxxxxxxx' that was running in
workflow '{0}'.format(wf_instance_id))
results = {
    "content": "xyz"
}

# Produce a FunctionResult with the results
yield FunctionResult(results)
except Exception:
    yield FunctionError()
```

# New in November 2021: we need an API KEY !

- Go to Xtreme-IP web site, register your email and get a FREE api Key
- In the dans le app.config of the fn\_components, add the section, and the api key in the secret:

```
[extreme_ip_look_up]
api_key_secret_extremeip = $API_eXtreMe_IP
```

```
1 [extreme_ip_look_up]
2 api_key_secret_extremeip = $API_eXtreMe_IP
```

API\_eXtreMe\_IP

- In the Source code off extreme\_ip\_look\_up.py, in the part Get the function parameters, add the api key secret lookup:

```
# Get the function parameters:
ip = kwargs.get("ip") # text
api = self.options.get("api_key_secret_extremeip", None)
```

who works well only if the package name match the section:

```
PACKAGE_NAME = "extreme_ip_look_up"
```

- The session.get command became:

```
try:
    response = session.get("https://extreme-ip-lookup.com/json/%s?key=%s" % (ip,api))
```

# Final Check:

```
1 # -*- coding: utf-8 -*-
2 # pragma pylint: disable=unused-argument, no-self-use
3 """Function implementation"""
4
5 import logging
6 from resilient_circuits import ResilientComponent, function, handler, StatusMessage, FunctionError
7 # Additional Import for this integration
8 import requests
9 from requests.packages.urllib3.exceptions import InsecureRequestWarning
10
11 PACKAGE_NAME = "extreme_ip_lookup"
12
13 class FunctionComponent(ResilientComponent):
14     """Component that implements Resilient function 'extreme_ip_lookup'"""
15
16     def __init__(self, opts):
17         """constructor provides access to the configuration options"""
18         super(FunctionComponent, self).__init__(opts)
19         self.options = opts.get(PACKAGE_NAME, {})
20
21     @handler("reload")
22     def _reload(self, event, opts):
23         """Configuration options have changed, save new values"""
24         self.options = opts.get(PACKAGE_NAME, {})
25
26     @function("extreme_ip_lookup")
27     def _extreme_ip_lookup_function(self, event, *args, **kwargs):
28         """Function: from an IP use https://extreme-ip-lookup.com/json/(place ip here) and
29         try:
30             # Get the wf_instance_id of the workflow this Function was called in
31             wf_instance_id = event.message["workflow_instance"]["workflow_instance_id"]
32
33             yield StatusMessage("Starting 'extreme_ip_lookup' running in workflow '{0}'".format(wf_instance_id))
34
35             # Get the function parameters:
36             ip = kwargs.get("ip") # text
37
38             log = logging.getLogger(__name__)
39             log.info("ip: %s", ip)
40
41     ##### PUT YOUR FUNCTION IMPLEMENTATION CODE HERE #####
42     session = requests.session()
43     session.verify = False
44     requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
45
46     try:
47         response = session.get("https://extreme-ip-lookup.com/json/%s" % ip)
48         response.raise_for_status()
49         ip_data = response.json()
50
51         ipName = ip_data['ipName']
52     except:
53         ipName = ''
54
55     ##### Put the JSON output in results #####
56     results = ip_data
57
58     # Produce a FunctionResult with the results
59     yield FunctionResult(results)
60     except Exception:
61         yield FunctionError()
```

# Run & Get the results

Resilient Dashboards

speed again / Artifacts / 9.9.9.9

Created 09/11/2020 22:29

Type IP Address

Description  
>>Extreme IP Lookup  
IP Type: Business  
Business Name: Quad9.net  
Country: United States

app\_fn\_components\_exe\_fn\_components added a note to the *Incident* 09/12/2020 19:23

**Extreme IP Lookup on 9.9.9.9**

IP Type: **Business**  
Business Name: **Quad9.net**  
Business Website: [www.quad9.net](http://www.quad9.net)  
ipName: **dns9.quad9.net**  
Org: **Quad9**  
ISP: **Quad9**  
Continent: **North America**  
Country: **United States**  
Region: **California**  
City: **Berkeley**  
GeoLocation: [Google Maps link on 37.87159,-122.27275](#)

Resilient Dashboards

speed again / Artifacts / 108.20.43.77

Created 09/11/2020 22:29

Type IP Address

Description  
>>Extreme IP Lookup  
IP Type: Residential  
Business Name:  
Country: United States

app\_fn\_components\_exe\_fn\_components added a note to the *Incident* 09/12/2020 19:23

**Extreme IP Lookup on 108.20.43.77**

IP Type: **Residential**  
Business Name:  
Business Website:  
ipName: **pool-108-20-43-77.bstnma.fios.verizon.net**  
Org: **Verizon Business**  
ISP: **Verizon Business**  
Continent: **North America**  
Country: **United States**  
Region: **Massachusetts**  
City: **Winchester**  
GeoLocation: [Google Maps link on 42.45232,-71.137](#)

QRADAR SOAR TRAINING

# Lab 20: (Requires IBMiD)

Reserve a QRadar for demo on TechZone,  
or use your own QRadar Lab (NOT PROD  
DATA ALLOWED)

Goal:

- Reserving a QRadar environment in TechZone

# Create a QRadar environment

Reserve a test QRadar environment at <https://techzone.ibm.com/collection/q-radar-nowdemo>

The screenshot shows the IBM Technology Zone interface with the following details:

**Resource Title:** QRadar Now demo

**Visibility:** IBMers, Business Partners

**Rating:** (0) Rate this resource

**Business value:** Complete set of QRadar tools.

**Authors:** Often identified as "Now" demo

**Comments:** (None)

**Authors:**

- Stephen Keim ([sekeim@us.ibm.com](mailto:sekeim@us.ibm.com))
- Julie Craft ([jcraft@us.ibm.com](mailto:jcraft@us.ibm.com)), Alex Hurtado ([Alexandra.Hurtado@ibm.com](mailto:Alexandra.Hurtado@ibm.com))

**Environments:**

Feb 7, 2022  
QRadar743

**Skytap 2: US-Central, EMEA, APAC-2**

Complete set of applications including Watson and QWorkBench designed so show how QRadar identifies current risks.

**Visibility:** IBMers, Business Partners

A large red arrow points to the blue "Reserve" button at the bottom of the page.

# Create a QRadar environment

Select your reservation type. Do you need this now or later?

## Single environment reservation options:

Select « Reserve now »

- Reserve now
- Schedule for later

Select « Test » purpose and your preferred geography

You can also select the time of availability of the platform (up to 7 days)

After that you can submit your request and press « Done » on the final page

You will receive later a mail with your connect informations to the Qradar platform

Name

Name this reservation. This will help identify it in your reservation list.

Purpose  ⓘ

Please select the purpose for this reservation request and review the [Reservation Duration Policy](#) to understand default durations allowed for specific infrastructures based on purpose.

Purpose description

What are you doing? Why do you need this? What are you trying to accomplish?

Preferred Geography

# Create a QRadar environment

You should receive an email with credentials when your environment is ready

IBM Technology Zone   
Build. Show. Share.

## Your environment is ready

Your environment is now available. Please use the following information to access the environment.

For guidance and support for your environment named **QRadar75**, please refer to these helpful links:

Collection Name: QRadar Now demo [EMEA] - [OKAY TO DELETE  
04/25/2022]  
Collection URL:  
<https://techzone.ibm.com/collection/61dc81c7959c52001f1ee25f>

- QRadar ssh:<http://services-emea.skytap.com:11071>
- QRadar https:<https://services-emea.skytap.com:11200>
- QRadar 9381:<http://services-emea.skytap.com:11220>
- Desktop URL:  
<https://cloud.skytap.com/vms/b90a028aa2564658e25a17fd0902a318/desktops>
- Desktop password: [REDACTED]
- Environment ID: [REDACTED]
- Environment name: DTE2\_2130311\_GAETA\_2022-05-03 07:43:00\_2022-05-03 11:43:00

QRADAR SOAR TRAINING

# Lab 21:

# Configure your QRadar to send Alerts to SOAR

Goal:

- Configure QRadar and SOAR to connect each other
- Integrate QRadar in SOAR environment to open, manage and enrich incident

# Configure your QRadar

From your Techzone collection page, click on the https link in your web browser

The screenshot shows a collection page for 'QRadar Now Instance' in the IBM Technology Zone. The page includes a logo with the text 'Build. Show. Share.', navigation links for 'My library' and 'Help', and a search bar. It displays the date (Jan 25, 2023 11:33 AM) and status (Ready). A red arrow points from the 'Published services' section to the URL for the QRadar Console UI.

## Published services

### Published services

Access QRadar Console UI: <https://services-eu-de-074883a762862973bdd3b817307f2ca8-0000.eu-de.containers.appdomain.cloud:30066/>  
SysLog Receiver: <https://services-eu-de-074883a762862973bdd3b817307f2ca8-0000.eu-de.containers.appdomain.cloud:31095/>

### Purpose

### Purpose

#### Purpose

Test

#### Customer(s)

{}

### Notes

### Notes

test

### Environment

### Environment

#### Reservation ID

63d105a26f13a100176292c9

#### Type

IBM Cloud

#### Reservation method

vmware-template

#### Transaction ID

d970c6ed-714f-4b92-acdb-e20f28e19f21

# Configure your QRadar

The QRadar https link will open a login page:



Enter username and password to access supported apps in the IBM QRadar Deployment:  
UN: admin/ PW: Q1d3m0.Demo

# Configure QRadar

Create a Token to authorize access from SOAR

In your QRadar environment, go to the **Admin Tab**, in **Authorized Service**, **New Authorized Service** with “**Admin**” role & profile, no expiry.

New Authorized Service X

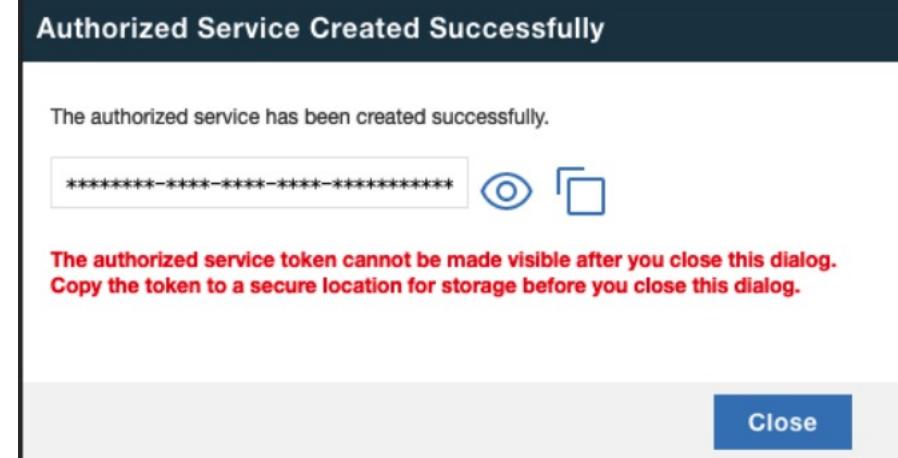
Authorized Service Label  
SOAR

**Permissions**

Security Profile	Manage Security Profiles
Admin	▼
User Role	Manage User Roles
Admin	▼

**Expiry Settings**

This Authorized Service expires



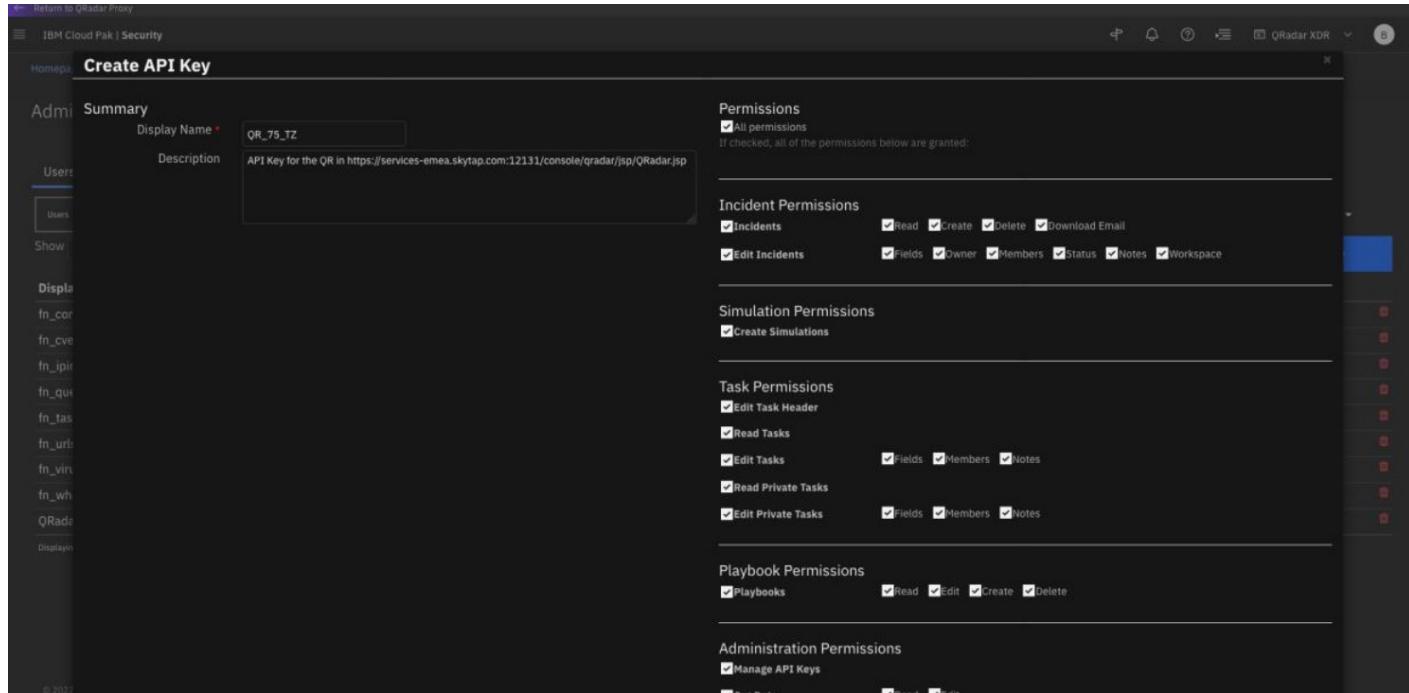
And of course save it in a Safe place

# Configure SOAR

## Create a SOAR new API key for QRadar

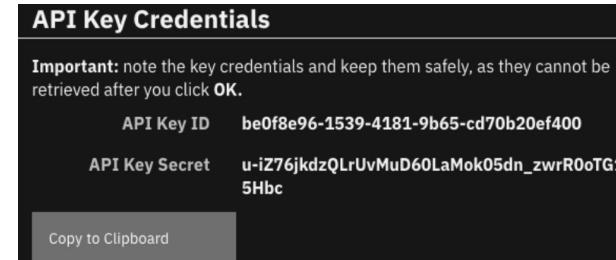
Administrator settings > Users > API keys > Create API key

Create an API key with ALL permission



# Configure SOAR

Store your credentials in a safe place



Get the organization name:  
Administrator settings > Organization

The screenshot shows the 'Administrator Settings' interface with the 'Organization' tab selected. Under the 'Organization Details' section, the 'Organization Name' field is highlighted with a red arrow pointing to it. The value 'GLO-DEV' is displayed in the field.

General	Organization Details
Inbound Email Connections	Use the <code>resutil editorg</code> command to change organization details. Enter <code>resutil editorg -help</code> for more information.
Migrate Settings	ID: 205 Organization Name: GLO-DEV Address: Address 2: City: State: Zip Code:

# Download the SOAR Plugin for QRadar

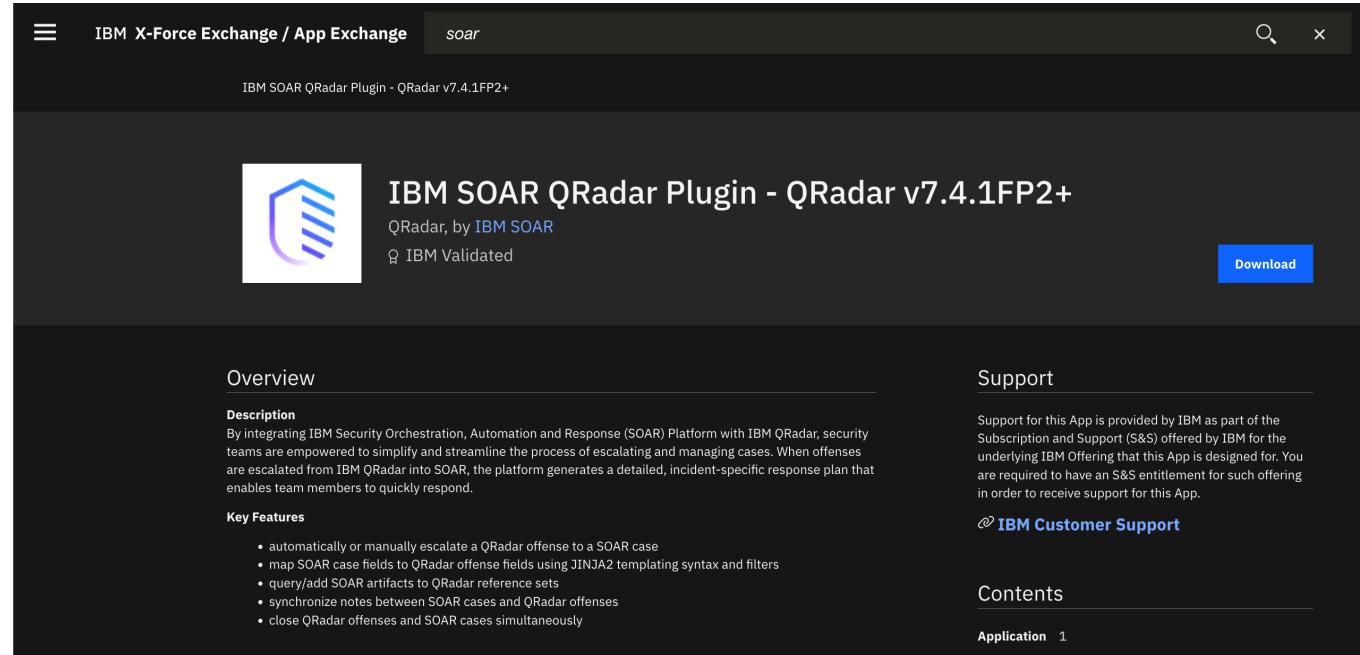
Download the app IBM SOAR Qradar Plugin from the IBM AppExchange:

<https://exchange.xforce.ibmcloud.com/hub/extension/bfa8a293489f21da69efec1c4e2c7acc>



The screenshot shows the IBM X-Force Exchange / App Exchange interface. The search bar at the top contains the text "soar". Below the search bar, the results for "IBM SOAR QRadar Plugin - QRadar v7.4.1FP2+" are displayed. The app card includes the following details:

- QRadar SOAR Plugin**
- QRadar**
- IBM SOAR QRadar Plugin - QRadar v7.4.1FP2+**
- Description:** Integrate IBM SOAR with IBM QRadar to simplify and streamline the process of escalating and managing cases.
- Key Features:**
  - automatically or manually escalate a QRadar offense to a SOAR case
  - map SOAR case fields to QRadar offense fields using JINJA2 templating syntax and filters
  - query/add SOAR artifacts to QRadar reference sets
  - synchronize notes between SOAR cases and QRadar offenses
  - close QRadar offenses and SOAR cases simultaneously
- By IBM SOAR**
- IBM Validated**



The screenshot shows the detailed view of the "IBM SOAR QRadar Plugin - QRadar v7.4.1FP2+" app page on the IBM AppExchange. The page includes the following sections:

- IBM SOAR QRadar Plugin - QRadar v7.4.1FP2+** (Title)
- QRadar, by IBM SOAR** (Developer)
- IBM Validated** (Validation status)
- Download** button (Action)
- Overview** section (Summary of the app's purpose and integration benefits)
- Description** section (Detailed description of the app's functionality and how it integrates IBM SOAR with QRadar)
- Key Features** section (List of specific features and capabilities)
- Support** section (Information about support provided by IBM)
- IBM Customer Support** link (Contact information)
- Contents** section (Table of contents for the app documentation)
- Application 1** (Link to the first application document)

# Install the SOAR Qradar Plugin

- Back in Qradar, go to the « admin » tab
- Select « Extensions Management »
- Click the « Add » button
- Select the app you just downloaded from your computer
- Check the « install immediately » checkbox and then press « Add »
- On the window that will appear next, press « install »

The screenshot shows the IBM QRadar Admin interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Admin (which is selected), Pulse, Use Case Manager, and User Analytics. The left sidebar has sections for Admin (System Configuration, Data Sources, Remote Networks and Services Configuration, Try it out), Apps (QVM Configuration, Custom Offense Close Reasons, Store and Forward, Reference Set Management), and a prominent Extensions Management section. A red arrow points to the Extensions Management icon. The main content area displays a message: "There are undeployed changes. Click 'Deploy Changes' to deploy them. View Details". Below this is a "System Configuration" section with icons for Auto Update, Backup and Recovery, Index Management, Aggregated Data Management, QVM Configuration, Custom Offense Close Reasons, Store and Forward, Reference Set Management, Email Server Management, and Resource Restrictions.

The screenshot shows the IBM Security App Exchange Extensions Management page. The top navigation bar includes a search bar, a link to the IBM Security App Exchange, and a help icon. Below the navigation is a table with columns for Name, Status, Author, and Added On. The table shows three entries: "User Behavior Analytics Exfiltration Content" (Installed, IBM QRadar, January 5, 2023), "User Behavior Analytics Endpoint Content" (Installed, IBM QRadar, January 5, 2023), and "User Behavior Analytics Domain Controller Content" (Installed, IBM QRadar, January 5, 2023). A red arrow points to the "Add" button at the top right of the table header.

Extensions Management				
Search by extension name				
IBM Security App Exchange				
ALL ITEMS	INSTALLED	NOT INSTALLED	Add	
User Behavior Analytics Exfiltration Content	⚠ Installed	IBM QRadar	January 5, 2023	
User Behavior Analytics Endpoint Content	⚠ Installed	IBM QRadar	January 5, 2023	
User Behavior Analytics Domain Controller Content	⚠ Installed	IBM QRadar	January 5, 2023	

## Add a New Extension

From local storage:

IBMSOARQRadarIntegrationV4.1.0.2436.:

Install immediately

# Create the configuration in QRadar

In QRadar Admin > Apps > IBM QRadar SOAR Plugin

Note: if the app does not appear after install, please refresh the page

The screenshot shows the IBM QRadar Admin interface. The top navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, and Admin. The Admin link is highlighted with a blue underline. On the left, a sidebar menu under the Admin heading lists System Configuration, Data Sources, Remote Networks and Services Configuration, Try it out, and Apps. The Apps section is expanded, showing a list of installed plugins: QRadar Log Source Management, QRadar Use Case Manager, Pulse - Dashboard, Pulse - Threat Globe, Threat Intelligence, and IBM QRadar SOAR Plugin. The main content area is titled "Deploy Changes" with a "Advanced ▾" button. A message states "There are no changes to deploy." Below this, there is a section titled "IBM QRadar SOAR Plugin" with a "Configuration" link, accompanied by a purple and black icon.

# Create the configuration in QRadar

IBM SOAR QRadar Plugin

Access Escalation Preferences Mapping Poller Status

### Application Access

QRadar Destination Name: qradar\_75

Authorized Service Token: 3b-300f-470e-a9c3-e40c8db9099c

SOAR Server URL: mea-dev.poc.resilientsystems.com/

CP4S mode

Authentication method: Click to select

**API key**  **Username/Password**

API Key ID: 5c8e-9419-4e0a-82f1-a596e20fff16

API Key Secret: \*\*\*\*\*

Multiple Organization Support:

Organization Name: GLO-DEV

SOAR Timeout (seconds): 30

Connect securely:  **Enable Configuring SOAR**  Need to configure a proxy?

Proxy settings

Host:   
Port:   
User:   
Password:

**Cancel** **Verify and Configure** **Save**

As we are performing a training you don't have to check this case It is optional because we won't verify certificates

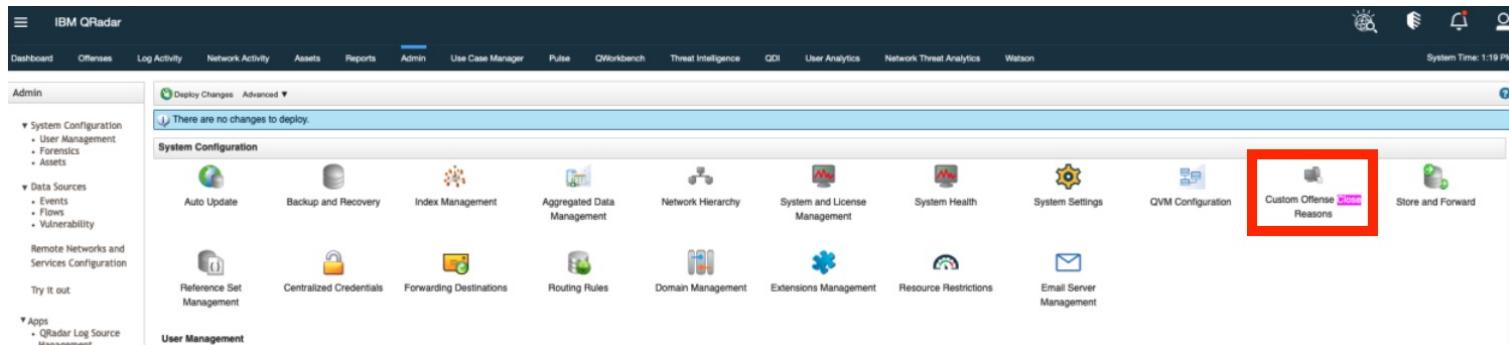
Then you can verify your configuration  
Don't forget to save !

# Create the configuration in QRadar

The following closing reasons exist in SOAR but not in QRadar.

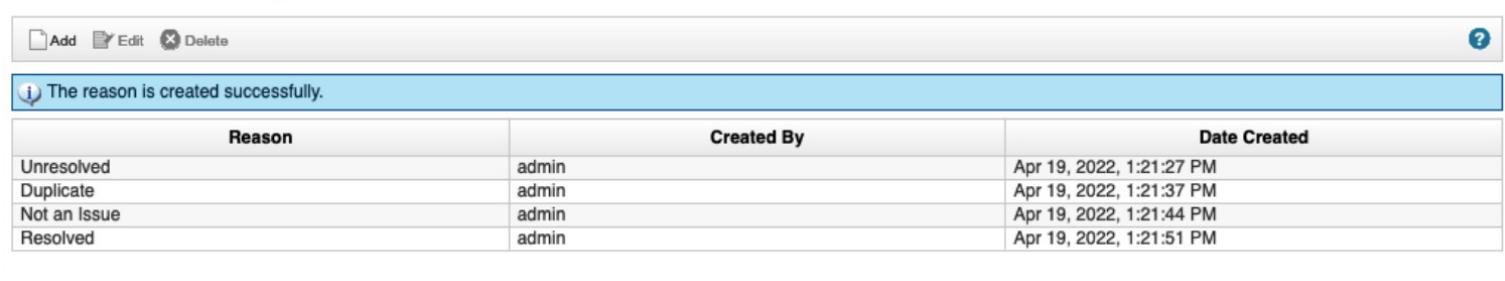
Unresolved, Duplicate, Not an Issue, Resolved

They should be added to prevent a default closing reason from being used



The screenshot shows the IBM QRadar Admin interface. On the left, there's a sidebar with 'Admin' selected. Under 'System Configuration', there are several icons: Auto Update, Backup and Recovery, Index Management, Aggregated Data Management, Network Hierarchy, System and License Management, System Health, System Settings, QVM Configuration, Reference Set Management, Centralized Credentials, Forwarding Destinations, Routing Rules, Domain Management, Extensions Management, Resource Restrictions, Email Server Management, and Custom Offense Reasons. The 'Custom Offense Reasons' icon is highlighted with a red box. At the top, a message says 'There are no changes to deploy.'

Add the 4 closing reasons



Reason	Created By	Date Created
Unresolved	admin	Apr 19, 2022, 1:21:27 PM
Duplicate	admin	Apr 19, 2022, 1:21:37 PM
Not an Issue	admin	Apr 19, 2022, 1:21:44 PM
Resolved	admin	Apr 19, 2022, 1:21:51 PM

# Create the configuration in QRadar

The screenshot shows two side-by-side configurations of the IBM SOAR QRadar Plugin interface.

**Left Configuration (Escalation Tab):**

- Template Files:** Buttons for "Build a New Template" and "Upload a Template". A "Default Template" dropdown with "Modify", "Download", and "Delete" buttons.
- Ignored Artifacts:** A list of "Source IPs" and "Local Destination IPs" with dropdown menus.
- Escalations:** An "Artifact Limit" input field set to 20.
- Automatic Escalation Conditions:** A table for defining rules based on offense fields and value match expressions, using a "Default Template".
- Manual Escalation Mode:** Radio buttons for "Create incidents immediately upon escalation" (selected) and "Review incidents prior to escalation".
- Buttons at the bottom:** "Cancel", "Verify and Configure", and "Save".

**Right Configuration (Preferences Tab):**

- Custom Actions:** A section for enabling SOAR users to search Ariel databases from a Case. It includes an "Available Queries" list and a "Query" editor with a sample query: `select * from events where domainid={{qradar_dom_id}} AND sourceip={{artifact.value}}' LAST {{properties.days_to_search}default(10)}} DAYS`.
- Enable Adding Reference Entries From SOAR:** A checkbox checked, with a list of "Reference Sets" including "Phishing IPs", "Suspicious MD5 Hashes", "Botnet C&C IPs", "Phishing URLs", "Risky User", "Malware URLs", "Malware IPs", "Botnet IPs", "Malicious URLs", "IT Admins", and "TOR IPs".
- Synchronization:** Checkboxes for "Synchronize notes between QRadar and SOAR", "Close Offense when Case closes", "Close Case when Offense closes", and a "Map SOAR Fields Required on Closing" section with dropdowns for "Resolution" (set to "Resolved") and "Resolution Summary" (set to "Resolved on QRadar").
- Buttons at the bottom:** "Cancel", "Verify and Configure", and "Save".

Don't forget  
To save !

QRADAR SOAR TRAINING

# Lab 22:

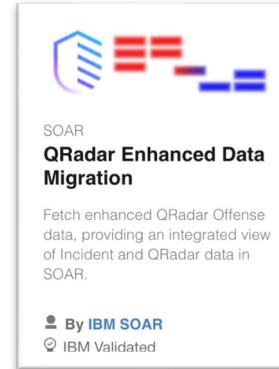
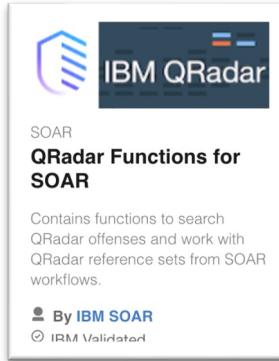
## Configure your SOAR to Query QRadar with 2 apps

Goal:

- Deploy App using Qradar to enrich an incident
- Connect SOAR to a SIEM to gather data from an external app

# Create a QRadar environment

Download and add the following two apps to your SOAR platform:



(Also available in your « lab QRadar » folder)

A screenshot of the IBM Security QRadar SOAR interface. The top navigation bar includes 'IBM Security QRadar SOAR', 'Dashboards', 'Inbox', 'Artifacts', 'Incidents', 'Create incident', and tabs for 'Users', 'Groups', 'Roles', 'Workspaces', 'Timeframes', 'Network', 'Organization', 'Threat Sources', 'Notifications', and 'Apps'. The 'Apps' tab is selected. Below this, a search bar contains 'qradar' and an 'Install' button with a '+' icon. Two app cards are listed: 'QRadar Enhanced Data Migration' (version 1.2.2) and 'IBM QRadar' (version 2.2.1). Both cards show '59 Customizations' and '64 Customizations' respectively, and both have a status of 'Waiting for Config...'. Each card has 'Uninstall' and 'Details' buttons at the bottom.

# Configure QRadar Functions App

In the app tab, select QRadar Integration app and go to the app.config file  
Change the credentials with the ones you were provided in skytap

## Administrator Settings

**File Content**  
Text or code as appropriate.

File Type Initialization

```
1 # Note: If [fn_qradar_integration] is present without a label then all
2 # be disregarded and only the server under [fn_qradar_integration] wil
3 #
4 # The QRadar instance name that you want to communicate with, must equ
5 # QRadar Destination Name that is set when configuring the SOAR Plugin
6 # Example: SOAR_Plugin_Destination_Name1
7
8 [fn_qradar_integration:SOAR_Plugin_Destination_Name1]
9 host = services-emea.skytap.com:12176
10 username = admin
11 #qradarpassword = Q1d3m0.Demo ←
12 #Note, if both qradarpassword and qradartoken are given, password will
13 qradartoken = e2d8d73b-300f-470e-a9c3-e40c8db9099c ←
14 #verify_cert = false|/path/to/cert
15 #verify_cert = /etc/rescircuits/qradar.cert
16 verify_cert = false
17
18 #search_timeout=
19 [resilient]
20 api_key_id = 1ae629f3-4c06-415f-b86b-5f34b4d4479b
21 api_key_secret = $API_KEY_SECRET
22 cafile = false
23 #cafile = /etc/rescircuits/cert.cer
24 host = emea-dev.poc.resilientsystems.com
25 port = 443
26 org = GLO-DEV
27
28
```

App Host ⚠  
AppHost EMEA-DEV GLO-DEV ↗

Test Configuration

**Secrets**

Secret Name
API_KEY_SECRET

As we just want to connect to QRadar and not access As an admin, password Isn't required, we will connect Using the token

Remember that you can place your token in a secret and the value won't be visible

When done test your Configuration, if the test is successful, save and push Then deploy the app on your AppHost

# Configure QRadar Enhanced Data Migration App

In the app tab, select QRadar Enhanced Data Migration app and go to the app.config file  
Change the credentials with the ones you were provided in skytap

## Administrator Settings

### File Content

Text or code as appropriate.

```
File Type Initialization
1 # Note: If [fn_qradar_integration] is present without a label then all
2 # be disregarded and only the server under [fn_qradar_integration] will
3 #
4 # The QRadar instance name that you want to communicate with, must equ
5 # QRadar Destination Name that is set when configuring the SOAR Plugin
6 # Example: SOAR_Plugin_Destination_Name1
7
8 [fn_qradar_integration:SOAR_Plugin_Destination_Name1]
9 host = services-emea.skytap.com:12176
10 username = admin
11 #qradarpassword = Q1d3m0.Demo
12 #Note, if both qradarpassword and qrardartoken are given, password will
13 qrardartoken = $QRADAR_TOKEN
14 verify_cert = false
15
16 #search_timeout=
17 [resilient]
18 api_key_id = 9de9904b-21a7-4fa0-99ed-9052fad2b24b
19 api_key_secret = $API_KEY_SECRET
20 cafile = false
21 host = emea-dev.poc.resilientsystems.com
22 port = 443
23 org = GLO-DEV
24
25
```

Secrets	
Secret Name	
API_KEY_SECRET	<input type="checkbox"/> <span style="color:red;">[ ]</span>
QRADAR_TOKEN	<input type="checkbox"/> <span style="color:red;">[ ]</span>



Here is the token in a secret

The config file is the same as  
The previous app

App Host ⚠

AppHost EMEA-DEV GLO-DEV lc

Test Configuration

When done test your  
Configuration, if the test is  
successful, save and push  
Then deploy the app on your  
AppHost

# Add data tables from app to incident layout

Go to your Customization Settings > Layout

Create a new tab

Customization Settings

Layouts   Rules   Scripts   Workflows   Functions

New Incident Wizard

Incident Tabs

Manage Tabs

- Summary Section
- Details
- Tasks
- Notes
- Members
- News Feed
- Attachments

Add a Tab

Tab Text \* QRadar Tables

Tab Visible  Yes  No  Conditional

Cancel Add

Artifact Types

Cancel Save

Details Tasks Notes Members News Feed Attachments Stats Timeline Artifacts Email

Tables Threat O... Breach Debug Multiselect... POT SOAR +

Tab Text \* Details

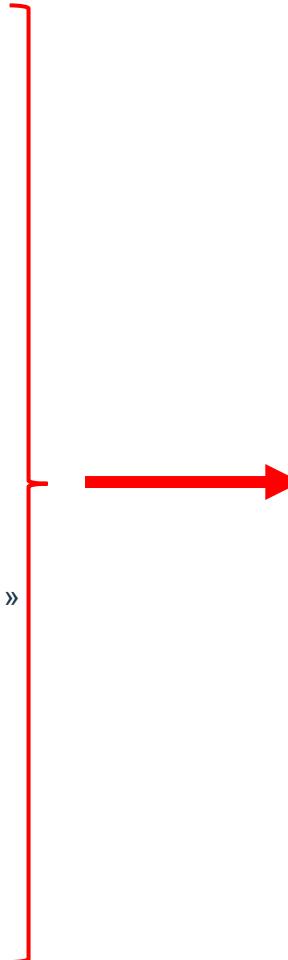
Tab Visible  Yes  No  Conditional

Add and Save !

# Add data tables from app to incident layout

Go to the Custom tab Layout you just created and add tables in it:

- Qradar\_destination
- QR Offense ID
- QR Index Type
- QR Offense Index Value
- QR Offense Source
- QR Source IP Count
- QR Destination IP Count
- QR Event Count
- QR Flow Count
- QR Assigned
- QR Magnitude
- QR Credibility
- QR Relevance
- QR Severity
- Section
  - Header « Qradar Integration Functions »
  - Datatable « QRadar Reference Tables »
  - Datatable « QRadar Reference Tables Queried Rows »
  - Datatable « QRadar Reference Sets »
  - Datatable « QRadar Offense Events »
- Section
  - Header « Qradar Integration Functions »
  - Datatable « QR Source IPs (First 10) »
  - Datatable « QR Destination IPs (First 10) »
  - Datatable « QR Assets »
  - Datatable « QR Categories »
  - Datatable « QR Flows »
  - Datatable « SR Triggered Rules »



Incident: QRadar Tables

Save

qradar_destination	x
QR Offense Id	x
QR Offense Index Type	x
QR Offense Index Value	x
QR Offense Source	x
QR Source IP Count	x
QR Destination IP Count	x
QR Event Count	x
QR Flow Count	x
QR Assigned	x
QR Magnitude	x
QR Credibility	x
QR Relevance	x
QR Severity	x
Section	✓ x
QRadar Integration Tables	✓ x
QRadar Reference Tables	x
QRadar Reference Table Queried Rows	x
QRadar Reference Sets	x
QRadar Offense Events	x
Section	✓ x
QRadar Enhanced Data	✓ x
QR Assets	x
QR Categories	x
QR Source IPs (First 10)	x
QR Destination IPs (First 10)	x
QR Flows	x
QR Triggered Rules	x

QRADAR SOAR TRAINING

# Lab 23:

## Create offense and see them in SOAR

Goal:

- Launch a use case and see how incidents are created and enriched from QRadar

# Test Connection

To test connection, go to **Qworkbench tab** and launch « **UC 10007 Log4j Vulnerability Dec 2021** »

The screenshot shows the IBM QRadar QWorkbench interface. In the top navigation bar, the 'QWorkbench' tab is selected. Below it, the 'Use Cases' section displays various entries. One entry, 'UC 10007 Log4j Vulnerability Dec 2021', is highlighted with a red border. This entry includes status indicators like 'Ready', buttons for 'Use Case Details', 'Deploy Results', 'Run Results', 'Offenses', and 'Mark as "Not Deployed"', and a timestamp '20/20/20'. To the right of the main content, there are filter panels for 'Use Case Filter', 'QRadar Features', 'Use Case Status', and 'Use Case Groups', each with checkboxes and dropdowns.

Wait a few minutes and it should appear in your QRadar Offense tab

The screenshot shows the IBM QRadar Offense tab. The top navigation bar includes the 'Offenses' tab, which is currently active. The main area displays a table of offense details. The first row of the table is highlighted with a red border. The columns include 'Id', 'Description', 'Offense Type', 'Offense Source', 'Magnitude', 'Source IPs', 'Destination IPs', 'Users', and 'Log Sources'. The 'Description' column shows a truncated message: 'Potential Log4Shell Evasion detected preceded by Potential Log4...'. The 'Offense Source' column shows '169.254.3.9'. The 'Magnitude' column shows a red bar indicating a high severity level. The 'Source IPs' column shows '169.254.3.9'. The 'Destination IPs' column shows 'Multiple (2)'. The 'Users' column shows 'N/A'. The 'Log Sources' column shows 'Multiple (3)'.

# Test Connection

An incident should have been created in SOAR few minutes later

IBM Security QRadar SOAR

Dashboards ▾

Inbox

Artifacts

Incidents

Create incident



## Incidents

All Open Incidents \* ▾

Filters ▾

✗ Incident Disposition = Confirmed ×

✗ Incident Disposition = Unconfirmed ×

✗ Status ~ Active ×

<input type="checkbox"/>	ID	Name	Description	Date Discovered	Date Determined	Next Due Date
<input type="checkbox"/>	2304	QRadar ID 67 , Potential...	36 events in 2 categorie...	05/05/2022 12:38:57	05/05/2022 12:38:57	-

# Test Connection

Short time later the tables from « QRadar Enhanced Data » should have some values

QR Source IPs (First 10)									
Source IP	Event Count	Flow Count	Category Count	Vulnerability Count	Network	Domain	MAC	Usernar	
45.83.65.162	—	1.0	1.0	0	—	Default Domain	—	—	
45.83.65.162	1.0	—	1.0	0	—	Default Domain	—	0.0	
Displaying 1 - 2 of 2									

To fill the other tables you will have to launch the actions

- Example: QRadar – Get all Reference Tables
- Search QRadar for Offense id

And refresh the page

QRadar Reference Tables					
QRadar Server	Reference Table	Collection Id	Namespace	Number Of Elements	⋮
SOAR_Plugin_Destination_Nam e1	Phishing Subjects Data	105	SHARED	0	⋮
SOAR_Plugin_Destination_Nam e1	Phishing Senders Data	113	SHARED	0	⋮
SOAR_Plugin_Destination_Nam e1	Malware URLs Data	110	SHARED	0	⋮
SOAR_Plugin_Destination_Nam e1	UBA : Rule Data	163	SHARED	4338	⋮
SOAR_Plugin_Destination_Nam e1	pulse_imports	28	SHARED	84	⋮

# Add a note to SOAR and QRadar

Try adding a note to SOAR and post it

The screenshot shows the SOAR Notes interface. At the top, it displays "QRadar ID 67 , Potential Log4Shell". Below that is a "Description" section stating "36 events in 2 categories: Potential Log4Shell Evasion detected preceded by Log4Shell Activity containing HTTP 200 - OK". A navigation bar below the description includes tabs for "Details", "Tasks", "Notes" (which is underlined), "Members", "News Feed", and "Attachments". Underneath the tabs are sub-tabs: "Breach", "Multiselect", "POT SOAR", and "QRadar Tables". The main content area contains a rich text editor toolbar with options like "Sans Serif", "Normal", "B", "I", "U", etc., followed by a text input field containing "This is a test note". At the bottom are two buttons: a blue "Post" button and a grey "Cancel" button.

Then go to the offense with the same id in QRadar and open it  
You will notice that the notes are shared between QRadar and SOAR

The screenshot shows the IBM QRadar Offenses page. The top navigation bar includes links for Dashboard, Offenses (which is selected and highlighted in blue), Log Activity, Network Activity, Assets, Reports, Admin, Use Case Manager, Pulse, QWorkbench, Threat Intelligence, QDI, User Analytics, and Network Threat Analytics. It also shows "System Time: 11:25 AM" and icons for Watson, search, notifications, and user profile. The main content area shows a table titled "All Offenses > Offense 67 (Summary)". The table has three columns: "Notes", "Username", and "Creation Date". The first row shows a note from "gaetan.lodde@ibm.com" with the content "This is a test note", "API\_token: SOAR" as the username, and "May 5, 2022, 11:19 AM" as the creation date. There are also "Notes" and "Add Note" buttons at the top of the notes column.

## Close an Offense from SOAR

The same way, notice that closing an incident in SOAR will close the Offense related in QRadar

IBM Security QRadar SOAR Dashboards ▾ Inbox Artifacts Incidents Create incident ▾

QRadar ID 67 , Potential Log4Shell Evasion detected precede...

Playbook progress | No playbooks started | Actions ▾

Description  
36 events in 2 categories: Potential Log4Shell Evasion detected preceded by Potential Log4Shell Base Pattern detected preceded by Detected Potential Log4Shell Activity containing HTTP 200 - OK

Details Tasks Notes Members News Feed Attachments Stats Timeline Artifacts Email Tables

Breach Multiselect POT SOAR QRadar Tables

Sans Serif ▾ Normal ▾ B I U S E E A A W ▾

Post Cancel

Search...  Show Task Notes  Oldest Notes First Created By: 0 selected Date Created: All ▾

Gaetan Lodde added a note to the Incident 05/05/2022 17:15

This is a test note

fn\_task\_utils added a note to the Task TOR Network Search Status on 169.254.3.9 05/05/2022 12:36

Add IOCs Assign Incident to me CVE Browse CVE Search Enrichment: Send Incident mail HTML Example: Get Incident Contact Info Example: Multiselect P2 Example: Multiselect P3 Example: QRadar - Get all Reference Tables Example: Send Incident Email HTML Example: Send Incident Email Text Example: Timer Epoch Example: Timers in Parallel Force Integration Simulation to YES Force TLP Search QRadar for offense id Update Incident Tag List Validation Step: Add a Management control Action Status Workflow Status Close Incident Delete Incident

# Close an Offense from SOAR

**Close Incident**

Please review the following fields for accuracy before continuing.

**Required for Close**

The following fields are required to have a value before you can close the incident.

Resolution \* ⓘ Not an Issue

Resolution Summary \* ⓘ Sans Serif Normal B I U S E E closing an offense from SOAR

Cancel OK

Offense with id 67 has been closed

Current Search Parameters:								
		All Offenses		View Offenses with:		Select An Option:		
Exclude Hidden Offenses <a href="#">(Clear Filter)</a>			Exclude Closed Offenses <a href="#">(Clear Filter)</a>					
#	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users
	68	Detected Potential Log4Shell Activity containing Web.Web	Source IP	45.83.65.162		45.83.65.162	192.168.56.101	N/A
	69	Flow Source/Interface Stopped Sending Flows	Rule	Flow Source Stoppe...		Multiple (3)	192.168.56.101	N/A

Showing closed offense

#	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	67	Potential Log4Shell Evasion detected preceded by Potential Log4...	Source IP	169.254.3.9		169.254.3.9	Multiple (2)	N/A	Multiple (3)

# THANK YOU

FOLLOW US ON:

-  [ibm.com/security](http://ibm.com/security)
-  [securityintelligence.com](http://securityintelligence.com)
-  [xforce.ibmcloud.com](http://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

