Universitat Oberta de Catalunya

uoc.edu

Robot Process Automation (RPA) al SOC

Sergi Majoral LLimiñana
Màster MISTIC
M1.749 - TFM-Seguretat empresarial

Jordi Guijarro Olivares
Victor Garcia Font

01/06/2021

FITXA DEL TREBALL FINAL

Títol del treball:	*Robot Process Automation (RPA) al SOC*
Nom de l'autor:	*Sergi Majoral LLimiñana*
Nom del consultor/a:	*Jordi Guijarro Olivares*
Nom del PRA:	*Victor Garcia Font*
Data de lliurament (mm/aaaa):	*06/2021*
Titulació o programa:	Màster MISTIC
Àrea del Treball Final:	M1.749 - TFM-Seguretat empresarial
Idioma del treball:	*Català*
Paraules clau	*SOAR OpenRPA CSIRT-KIT*

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

Els equips de resposta a incidents han de fer front cada cop a més incidents de seguretat i una resposta automatitzada a aquests ha passat a ser una necessitat per a aconseguir que el temps de resposta sigui el més petit possible.

L'automatització no és quelcom nou ja que s'ha automatitzat des de sempre via scripts aprofitant les APIs de les aplicacions. Les eines modernes d'automatització de fluxos i de RPA permeten que perfils no programadors puguin automatitzar tasques/processos de forma més o menys senzilla tant a partir d'APIs com aprofitant les interfícies d'usuari de les aplicacions.

L'entorn de treball utilitzat ha estat la versió actualitzada de CSIRT-KIT que ofereix un conjunt complet d'eines, de codi obert i gratuïtes, per a monitoritzar la seguretat i gestionar-ne els incidents. Les eines que formen el kit estan pre-integrades entre elles i l'objectiu d'aquest treball ha estat explorar les eines d'automatització de codi obert i gratuïtes disponibles, provar les que millor s'adapten a les eines que composen l'entorn de treball i aconseguir implementar uns casos d'ús d'automatització que aportin valor a la operativa diària que realitzen els equips de resposta a incidents.

Els resultats d'aquest treball mostren que és viable automatitzar aquesta operativa amb les eines proposades, tant de forma col·laborada amb els operadors humans com de forma autònoma per part dels robots software, i fer-ho de forma segura podent cobrir un horari 24x7.

Abstract (in English, 250 words or less):

Incident response teams must deal with more and more security incidents and an automated response to these incidents has become a necessity to keep response time as small as possible.

Automation is nothing new because it has always been done via scripts using application APIs. Modern flow automation and RPA tools allow non-programmers to automate tasks and processes in a more or less simple way both from APIs and using Applications user interfaces.

The working environment used has been the updated version of CSIRT-KIT, which offers a complete set of free and open-source tools for security monitoring, incident management and response. The tools that make up the kit are pre-integrated with each other and the objective of this work has been to explore the open source and free automation tools available, test those that best fit the tools that make up the working environment and implement automation use cases adding value to the daily operations performed by the incident response teams.

The results of this work show that it is feasible to automate this operation with the proposed tools, both in collaboration with human operators and autonomously by software robots, and to do it in a safe way being able to cover a 24x7 schedule.

Índex

Llista de figures

1. Introducció

1.1 Explicació detallada del problema a resoldre

El repte que s'afronta en aquest projecte es basa en aplicar l'automatització robòtica de processos (RPA) a les activitats que es realitzen en un Centre d'Operacions de Seguretat (SOC) o en qualsevol altre equip de gestió d'incidents de seguretat informàtica en general.

L'entorn de treball en el que es posarà en pràctica l'automatització està compost per un conjunt d'eines que permet donar resposta a incidents de seguretat anomenat CSIRT-KIT-NG, que és una evolució del CSIRT-KIT impulsat per CSUC-CSIRT, CERT-SI [INCIBE], ES-CERT UPC, i que es distribueix de forma gratuïta a partir d'una imatge (OVA) que permet desplegar una màquina virtual amb les eines que formen l'entorn de treball [1] sobre un sistema operatiu Debian 10.

	CSIRT-KIT	CSIRT-KIT-NG
Incident handling information	• IntelMQ	• IntelMQ
Investigation Ticketing system	• RTIRT	• TheHive • Cortex • Thehive4py
Network forensic	• Nfsen	• Packetbeat • Nfsen
Operational intelligence	• ElasticSearch • Kibana • Logstash	• Elasticsearch • Kibana • Logstash • Filebeat
Vulnerability Assessment	• Pakiti	• Wazuh

Figura 1: Taula comparativa entre les eines de CSIRT-KIT i CSIRT-KIT-NG [2]

És rellevant destacar que aquestes eines ja estan integrades entre elles i una vegada desplegat l'entorn està llest per a començar a treballar (plug&play). El detall s'analitzarà en el transcurs del TFM però, per a fer-se una primera idea, INTELMQ és una eina que automatitza la recol·lecció d'esdeveniments processant-los i adaptant-los als formats necessaris de sortida que requereixen les eines que els rebran. La integració entre les eines que formen el "kit" es pot veure a la figura següent:

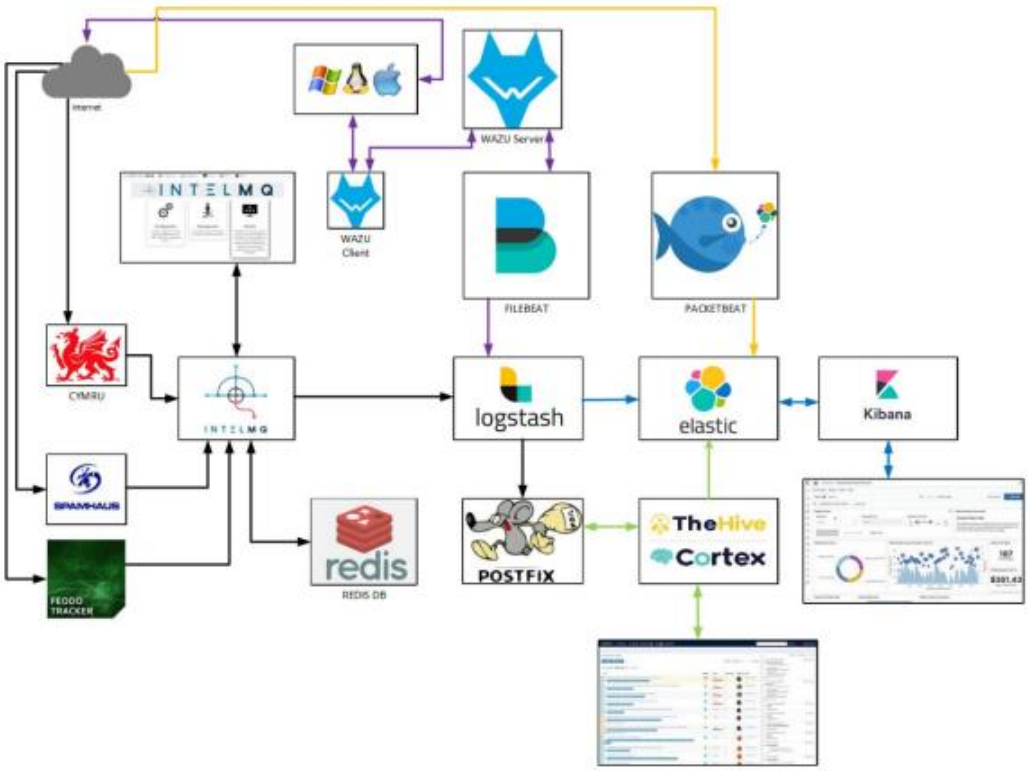


Figura 2: Diagrama integració entre les eines del CSIRT-KIT-NG [2]

Per tant ja podem avançar que les automatitzacions que s'hauran de dur a terme s'hauran de centrar en altres tasques o processos a automatitzar que aportin valor als equips que gestionen els incidents de seguretat en aquest entorn de treball.

1.2 Objectius que es volen aconseguir

Els objectius principals del treball es poden dividir en una part d'estudi i una part pràctica d'implementació.

La part d'estudi es dividirà a la seva vegada en dues parts. D'una banda s'analitzarà les aplicacions existents que permeten implementar robots software a l'entorn de treball proposat i s'escollirà les eines que millor poden encaixar i que preferentment hauran de ser de codi obert i gratuïtes seguint la filosofia que envolta a CSIRT-KIT-NG. Per altra banda serà necessari familiaritzar-se amb les eines que composen l'entorn de treball amb l'objectiu de detectar els casos d'ús en que les eines de RPA poden aportar un valor diferenciador.

La part pràctica, que es pot considerar la més rellevant, consistirà en implementar els casos d'ús identificats a la part d'estudi i testejar-ne el correcte funcionament. Sobre aquestes implementacions serà sobre les que s'analitzarà els riscos de seguretat que implica l'ús de dites eines i s'aplicaran, o es proposaran, solucions per a mitigar-los.

Finalment caldrà considerar també com a objectius la redacció dels diferents lliuraments que composen l'avaluació continua donat que tenen un pes destacable dins la planificació del treball final de màster.

1.3 Metodologia

Els passos i estratègies que es seguiran per a dur a terme els objectius anteriorment esmentats seran:

- Realitzar un estudi de les aplicacions existents que permeten implementar robots software a l'entorn de treball proposat. A partir d'una cerca per internet es realitzarà una comparativa de les principals característiques i s'escollirà les eines que millor poden encaixar.
- Documentar-se al respecte de les eines que formen part de l'entorn de treball i les possibilitats que ofereixen. És necessari conèixer en detall les seves possibilitats per a poder escollir de forma adient els casos d'ús que s'implementaran.
- S'avaluarà els recursos necessaris que ha de complir l'equip sobre el que es desplegarà dit entorn de treball i es realitzaran les millores en aquest que puguin ser necessàries.
- Es desplegarà el CSIRT-KIT-NG a l'equip comprovant el correcte funcionament de les eines i posant en pràctica les utilitats que ofereixen.
- Elecció dels casos d'ús que es voldran automatitzar amb la finalitat que esdevinguin un complement útil i que aporti valor als equips que gestionen els incidents de seguretat.
- A continuació serà necessari instal·lar les eines RPA escollides a la fase d'estudi comprovant el seu correcte funcionament i resolent els diferents errors que puguin sorgir per compatibilitat de versions i altres.
- Seguidament es desenvoluparan els casos d'ús escollits adaptant-los a les possibilitats de les eines RPA.
- El darrer pas consistirà en analitzar els riscos de seguretat que poden comportar els casos d'ús implementats i en cas de detectar-ne proposar-hi solucions.

1.4 LListat de tasques a realitzar

Per a assolir els objectius definits caldrà realitzar les tasques que es detallen a continuació:

- Lectura prèvia de la documentació proporcionada.
- Cerca d'informació relacionada.
- Definició del pla de treball que es seguirà i la redacció del mateix.
- Estudi comparatiu de les aplicacions de RPA i selecció de les escollides.
- Estudi de les aplicacions que composen l'entorn de treball.

- Revisió de les característiques que ha de complir l'equip sobre el que es desplegarà l'entorn de treball i les aplicacions escollides.
- Elecció dels casos d'ús que s'implementaran.
- Redacció de les conclusions de la fase d'estudis.
- Desplegar CSIRT-KIT-NG a l'entorn de treball.
- Instal·lació de les eines de RPA escollides resolent els errors que puguin aparèixer.
- Implementació dels casos d'ús i testejar el seu correcte funcionament.
- Redacció de les conclusions de la fase d'implementació.
- Anàlisi dels riscos de seguretat dels casos d'ús implementats i proposta de les millores que caldria aplicar per a mitigar-los.
- Redacció de la memòria final.
- Preparació de les diapositives i exemples d'implementació que s'empraran com a contingut al lliurament del vídeo.

1.5 Planificació temporal detallada

La planificació s'ha dividit en cinc fases clarament diferenciades que estan condicionades per les dates fixes dels lliuraments parcials que s'ha de realitzar durant l'avaluació continua. D'aquesta manera s'estableix una dependència natural d'acabament de la fase anterior, i les tasques que la composen, abans de començar la fase següent. També destacar que algunes tasques es preveu que es podran executar en paral·lel com és el cas de la redacció dels documents dels lliuraments.

Fase/Tasca	**Data Inici**	**Data Fi**	**Duració** (dies)
1: Pla de treball	17-febr.	2-març	14
1.1-Lectura prèvia	18-febr.	21-febr.	4
1.2-Revisió de la literatura	21-febr.	25-febr.	5
1.3-Definició i redacció del pla	25-febr.	1-març	5
1.4-Entrega PAC1	2-març	2-març	1
2: Estudis i casos d'ús	3-març	30-març	28
2.1-Estudi aplicacions RPA	3-març	10-març	8
2.2-Estudi entorn de treball	10-març	20-març	11
2.3-Recursos equip de treball	20-març	21-març	2
2.4-Escollir casos d'ús	21-març	22-març	2
2.5-Redacció de conclusions	20-març	29-març	10
2.6-Entrega PAC2	30-març	30-març	1
3: Implementació	31-març	27-abr.	28
3.1-Desplegar CSIRT-KIT-NG	31-març	1-abr.	2
3.2-Instal·lació eines RPA	1-abr.	5-abr.	5
3.3-Implementar i testejar els casos d'ús	5-abr.	26-abr.	22
3.4-Redacció de conclusions	20-abr.	26-abr.	7
3.4-Entrega PAC3	27-abr.	27-abr.	1

Fase/Tasca	Data Inici	Data Fi	Duració (dies)
4: Seguretat i Memòria Final	28-abr.	1-juny	35
4.1-Riscos de seguretat i mitigacions	28-abr.	14-maig	17
4.2-Redacció de la memòria	10-maig	31-maig	22
4.3-Entrega PAC4	1-juny	1-juny	1
5: Presentació en vídeo	2-juny	8-juny	7
5.1-Preparació i enregistrament	2-juny	7-juny	6
5.2-Entrega PAC5	8-juny	8-juny	1
Defensa TFM	14-juny	18-juny	5

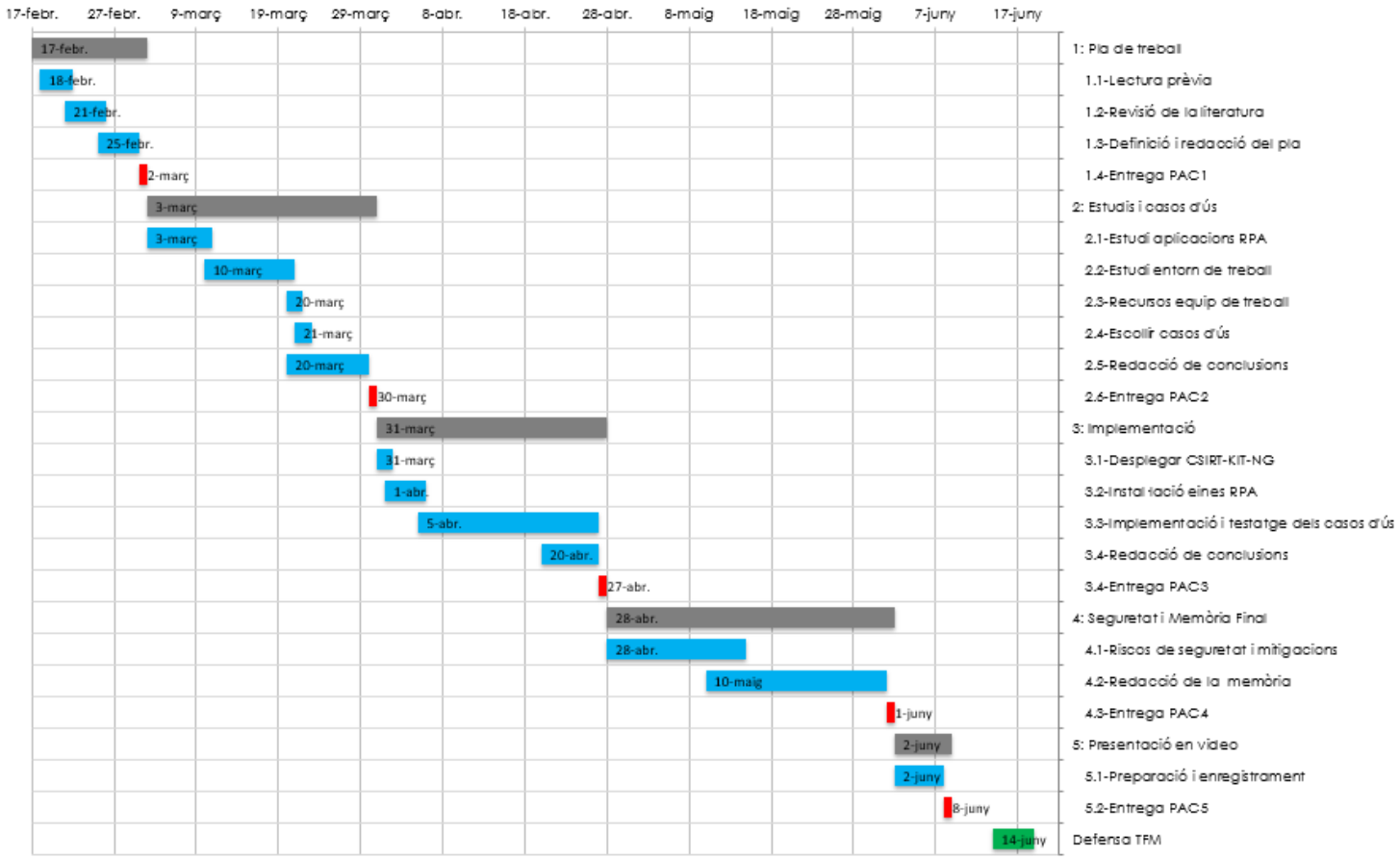


Figura 3: Planificació temporal de les fases i tasques (diagrama de Gantt)

1.6 Recursos necessaris

Respecte l'estimació dels recursos necessaris cal tenir en compte que, per una banda, la voluntat és cercar una aplicació d'automatització que sigui de codi obert i gratuïta com la resta d'eines que formen el Kit. Per altra banda l'equip de treball disponible segurament requerirà ser ampliat a nivell de memòria segons comentat al TFM [2] per tant s'estima que la inversió que serà necessària pot arribar a ser aproximadament d'uns 50€.

1.7 Estat de l'art

Segons Gartner [3][4] RPA és un dels segments de més ràpid creixement dels darrers anys dins del mercat del software. Les principals raons per les que les organitzacions adquireixen una eina de RPA són la optimització de la eficiència operativa, accelerar un procés existent i la optimització dels costos. En aquest sentit cal tenir en compte que moltes organitzacions disposen d'aplicacions existents, propietàries o de tercers, que només permeten interacció a través d'interfície d'usuari (UI), sense tenir o estar disponibles APIs, i en aquest punt és on la RPA permet donar sortida a diferents necessitats. També cal tenir en compte que si el sistema o aplicació disposa d'APIs la RPA també se'n pot aprofitar permetent accelerar molt l'automatització del procés.

Els robots software que es poden implementar es podem agrupar en:

- **Atesos**: Que es basen en col·laborar amb l'humà en diferents parts del procés per a completar/ampliar les seves capacitats i habilitats augmentat d'aquesta manera la seva productivitat.
- **Desatesos**: Destinats a la realització de tasques repetitives per les que la participació d'un humà no aporta un valor addicional o diferenciador al procés i per tant es poden dur a terme sense la seva participació reduint els errors comesos en dur a terme tasques monòtones.

Els **casos d'ús** més representatius que es destaquen [3] són:

- Integració utilitzant les interfícies gràfiques de les aplicacions permetent extreure ràpidament informació d'una aplicació per ser tractada amb una altra.
- Migracions de dades massives de diferents sistemes cap a un de nou.
- Recol·lecció i transformació de dades de documents i sistemes adaptant-les al format esperat que necessita el treballador quan interactua amb clients. Fer-ho de forma eficient ajuda a millorar l'experiència del client.

La mateixa font destaca certs aspectes a tenir en compte al respecte dels desenvolupaments amb RPA.

- Els robots software no són equivalents als humans donat que no poden interpretar i adaptar-se a les necessitats ja que en el fons no són més que scripts d'integració que s'implementen fàcilment a través de les eines de RPA.

- RPA no permet automatitzar fàcilment processos de llarga execució. Quan parlem de processos en l'àmbit de RPA cal pensar més aviat en tasques discretes de curta duració o en senzills fluxos de tasques. Per anar més enllà cal una aplicació que gestiona intel·ligentment els processos de negoci (a les que anomenen iBPMS). Les eines de RPA són una més de les múltiples eines que permeten la transformació digital.
- Moltes de les eines de RPA presenten poca resiliència als canvis que poden patir les eines de tercers. Aquest fet s'entén com un deute tècnic des del punt de vista que implica adaptar novament els robots software a la nova situació.

Considerant les setze eines comercials, dels principals proveïdors de solucions RPA, que contempla la comparativa del darrer any [4] crida l'atenció que només una d'elles és compatible amb el SO Linux. Aquest fet, juntament amb el fet que en dita comparativa s'exclou els proveïdors que ofereixen eines de codi obert sense oferir una oferta comercial basada en RPA, anticipa que en la fase d'estudi del projecte es descobriran eines de codi obert, en gran part segurament gratuïtes, que caldrà tenir molt en compte com a possibles candidates a formar part de l'entorn de treball proposat.

Respecte els desafiaments futurs del RPA hem de parlar de les habilitats cognitives [4] combinades amb l'autoaprenentatge i la intel·ligència artificial el que s'anomena CRPA (RPA cognitiva) [5]. Aquesta implica que la RPA deixa de servir només per a automatitzar tasques repetitives a partir d'unes regles definides per a passar a definir les seves pròpies regles, ajudar als humans a prendre decisions i, fins i tot, prendre les seves decisions.

Finalment al respecte de la seguretat de la informació [6] cal tenir en compte que els principals riscos de seguretat que pot implicar el desenvolupament de robots software podran estar principalment relacionats amb la gestió de les identitats (degut a que la majoria de vegades s'utilitzen usuaris amb drets privilegiats), la traçabilitat de l'activitat dels robots i el compliment (donat que en accedir a dades sensibles és necessari complir amb la GDPR).

Encara que la CRPA queda lluny dels objectius d'aquest treball final de màster queda clar que en un futur serà encara més important garantir el compliment a tots els nivells i establir clarament unes regles de joc basades en principis ètics i morals.

2. Estudis i casos d'ús

2.1 Estudi d'aplicacions RPA

Com s'avançava a l'apartat anterior, l'estudi realitzat a la recerca d'eines de RPA ha descobert moltes eines de codi obert que permeten implementar automatitzacions. Dites eines les podem arribar a agrupar en dos grans grups.

Per una banda tenim les eines enfocades a RPA pensades per automatitzar tasques o, fins i tot, conjunt de tasques definint un procés més o menys complex a través de les interfícies d'usuaris de les eines o a través d'APIs però que no duen incorporat un orquestrador. Aquestes es poden arribar a combinar amb eines que permeten programar-ne l'execució suplint d'alguna manera aquesta mancança (en aquest grup es poden incloure també les eines de testeig o de monitorització i descàrrega d'informació com un cas concret d'automatització).
Per altra banda tenim les eines enfocades en automatitzar l'execució de fluxos de tasques en general i que poden estar integrades amb un nombre més o menys gran d'aplicacions existents permetent implementar automatitzacions complexes de forma relativament senzilla. La majoria d'aquestes permeten ser ampliades via programació o executant scripts propis que podem suplir les mancances d'automatització quan les aplicacions a automatitzar no disposen d'APIs, o aquestes no estan suficientment desenvolupades, i cal emprar la interfície d'usuari per a aconseguir-ho (escenari que cobreixen per defecte les eines de RPA pures).

Tenint en compte aquesta gran varietat d'eines la classificació que es presenta a continuació està filtrada descartant directament les eines que no són de codi obert per a seguir la filosofia que envolta a CSIRT-KIT-NG. Altres aspectes rellevant serien si són gratuïtes, o tenen una versió gratuïta amb certes limitacions, i si els sistemes operatius en els quals es poden desplegar inclou Linux. També s'ha afegit un camp de comentaris amb informació addicional a tenir en compte i finalment un camp de valoració personal tenint en compte certs criteris com poden ser la bona sensació que dóna la informació consultada, si la comunitat està activa o si es van resolent els errors reportats amb certa agilitat:

Nom	Sistema Operatiu	Codi obert	Gratuïta?	Comentaris i fonts	Valoració
Actiona	Windows, Linux	Si	Si	Automatització de tasques sense codi i es pot ampliar amb JavaScript. https://actiona.tools	Mitja
Apache Airflow	Linux	Si	Si	Permet automatitzar fluxos de treball a partir de gràfics acíclics. Disposa d'una interfície d'usuari per a la monitorització dels fluxos. Pot ser una bona alternativa per a complementar amb l'eina RPA Python per exemple. https://github.com/apache/airflow#getting-started	Mitja
Autokey	Linux X11	Si	Si	Automatització d'escriptori per a entorn Linux (no funcionarà al 100% en distribucions que utilitzen Wayland en comptes de Xorg). Massa senzilla per al propòsit del TFM. https://github.com/autokey/autokey	Baixa
Beehive	Windows, Linux, MacOS	Si	Si	Similar a n8n. Disposa d'integracions fetes però no són interessants per aquest treball. Falta informació i exemples. https://github.com/muesli/beehive	Mitja
BPMN RPA	Windows, Linux	Si	Si	Automatització de fluxos de tasques a partir de diagrames de forma senzilla. Projecte no madur que requereix de més temps. https://github.com/joostvangils/BPMN_RPA	Baixa
Comunda	Windows, Linux	Si	Si (limitada)	Eina interessant per a l'automatització de processos. La part empresarial té opcions avançades no disponibles a la versió gratuïta. Disposa d'integració amb UiPath per exemple. https://camunda.com/solutions/integrate-with-rpa/	Alta
Huginn	Windows, Linux	Si	Si	Similar a n8n. Disposa d'integracions fetes però no són interessants per aquest treball. Falta informació i exemple https://github.com/huginn/huginn	Mitja
Kibitzr	Linux	Si	Si	Enfocada principalment a la automatització d'avisos de webs i descàrrega d'informació. https://github.com/kibitzr/kibitzr https://kibitzr.readthedocs.io/en/latest/scenario.html	Baixa
Luigi	Linux	Si	Si	Eina que permet encadenar i automatitzar fluxos de tasques de forma oberta en Python. Té una UI per a visualitzar els diagrames de fluxos i l'estat d'avançament. Entre altres contribucions fetes per la comunitat té integració amb Datadog (eina de seguretat). https://github.com/spotify/luigi https://github.com/spotify/luigi/tree/cf2abbdb998f9e0d72801b8c8e9b2f8cfc16b7a1/test/contrib	Mitja
n8n	Windows, Linux, MacOS	Si	Si	Eina molt versàtil (100% operativa i sense cap limitació) que permet l'automatització de tasques a través de fluxos sense escriure codi. Té integració a moltes eines. Inclou nodes creats per TheHive i Cortex. Rundeck també que està a la llista. https://n8n.io/	Alta

Nom	Sistema Operatiu	Codi obert	Gratuïta?	Comentaris i fonts	Valoració
Orchestra	Windows, Linux, MacOS	Si	Si	Gestió de fluxos de tasques col·laboratiu entre màquines (robots) i persones…. idea interessant però falta documentació i exemples. https://blog.b12.io/introducing-orchestra-23bace45d4a7 https://github.com/b12io/orchestra https://orchestra.b12.io/	Mitja
Phantomjs	Windows, Linux, MacOS	Si	Si	Principalment enfocada al testeig de pàgines web. https://phantomjs.org/	Baixa
Puppeteer	Windows, Linux, MacOS	Si	Si	API a alt nivell per automatitzar chrome i Chromium. Similar a RPA Python però sense OCR. https://pptr.dev/	Baixa
Robocorp	Windows, Linux, MacOS	Si	Si	Solució RPA de codi obert i gratuïta (excepte la part Cloud que la versió gratuïta està força limitada). Per a desenvolupadors i execució en local no està limitada i pot ser mot bona opció gracies al conjunt d'eines i llibreries (anomenat RCC) basat en Python per automatitzar processos : https://robocorp.com/developers/ https://github.com/robocorp/rcc	Alta
Robot framework	Windows	Si	Si (limitada)	Destinada al testeig de pàgines web. https://github.com/robotframework	Mitja
RPA Python	Windows, Linux, MacOS	Si	Si	Antigament anomenat TagUI-Python. Basat en TagUI. Automatitza les comanes bàsiques simplificant molt el codi que cal implementar per a automatitzar aplicacions web o d'escriptori. OCR (SikuliX). Combinada amb Airflow pot ser molt potent. https://airbnb.io/projects/airflow/	Mitja
rundeck	Linux	Si	Si (limitada)	Eina d'automatització de fluxes per a gestionar incidents, la continuïtat del negoci i operacions d'autoservei. Seria interessant disposar de la versió empresarial. https://github.com/rundeck https://www.rundeck.com/community-vs-enterprise	Mitja
Scrapy	Windows, Linux, MacOS	Si	Si	Enfocada principalment a l'automatització d'avisos de webs i descàrrega d'informació i també permet testing. https://scrapy.org/ https://josefgonzalez.me/es/post/automate-pdf-download-scrapy/	Baixa
Sikuli	Windows, Linux, MacOS	Si	Si	Permet automatitzar qualsevol cosa que es veu a la pantalla. OCR http://sikulix.com/	Baixa

Nom	Sistema Operatiu	Codi obert	Gratuïta?	Comentaris i fonts	Valoració
StackStorm	Linux	Si	Si (poc limitada)	Eina per a automatitzar fluxos de tasques que té integracions fetes amb moltes eines (TheHive, datadog, zabbix entre moltes Altares). Té una versió empresarial de pagament però la versió gratuïta està molt poc limitada podent ser una bona Alternativa per a automatitzar qualsevol cosa que es necessiti. https://stackstorm.com/ https://stackstorm.com/clone-of-stackstorm/ https://stackstorm.com/clone-of-stackstorm/#ewc	Alta
Shuffler	Windows, Linux	Si	Si (limitada)	Integració amb TheHive i Cortex però està limitada i segueix essent més interessant n8n. https://shuffler.io/pricing	Mitja
Ui.Vision	Windows, Linux, MacOS	Si	Si (limitada)	No té orchestrador i es pot utilitzar qualsevol eina de programació de tasques . La versió gratuïta té limitacions com la quantitat de lectures OCR per exemple. https://ui.vision/rpa https://ui.vision/rpa/x/pricing https://forum.ui.vision/t/itpa-tasks-orchestrator/4298/2	Mitja
Walkoff	Windows, Linux	Si	Si	Plataforma SOAR interessant per les eines de seguretat integrades. Falta Cortex i per a TheHive hi ha el llistat de funcions permeses (és més complet n8n). https://gist.github.com/frikky/7ed26bb5259eabb4eabc5854a3ba7553 https://github.com/nsacyber/walkoff-apps https://github.com/billmurrin/thehive-walkoff-app	Alta
Xdotool	Linux X11	Si	Si	Simula clics del ratolí de forma senzilla però és massa simple per al propòsit del TFM. https://github.com/jordansissel/xdotool	Baixa

Figura 4: Valoració de les eines d'automatització analitzades a l'estudi

Com es pot veure existeixen diferents eines amb valoració alta i mitja que poden ser bones candidates per a utilitzar en el transcurs d'aquest treball. Com a punt de partida apostaré per **n8n** com a eina de treball per a desenvolupar les automatitzacions dels casos d'ús degut a que està integrada amb TheHive i Cortex i permet també ser ampliada. Cal tenir en compte però que si sorgeixen dificultats que impedeixen la implementació dels casos d'ús es podrà emprar en el seu lloc alguna altra d'aquestes eines o combinar n8n amb alguna altra d'aquestes.

2.2 Estudi entorn de treball

En el transcurs de l'estudi de l'entorn de treball he tingut l'oportunitat de participar a un seminari online [7] el qual presentava les novetats que incorpora l'evolució de l'eina CSIRT-KIT a CSIRT-KIT-NG.

CSIRT-KIT-NG incorpora un conjunt d'eines bàsiques que permeten disposar d'avisos proactius, reactius i gestionar la resposta a incidents de seguretat. Aquest paquet es presenta com una solució bàsica destinada a qualsevol tipus d'equips de gestió d'incidents de seguretat. Veure figura 2.

De la recollida automatitzada d'informació de diferents fonts ("feeds" interns i externs) se n'encarrega **IntelMQ** [8] amb l'objectiu de recopilar i processar intel·ligència relacionada amb amenaces. Aquesta tasca es fa a partir del que s'anomenen "Bots" (o plugins) que permeten adaptar el format dels events a l'esperat per l'eina que els emmagatzemarà. Porta incorporat un entorn web per a fer la gestió i canvis de configuració de forma senzilla (IntelMQ-Management). En iniciar el kit s'executa la comana intelmqctl start que posa en funcionament tots els bots implementats.

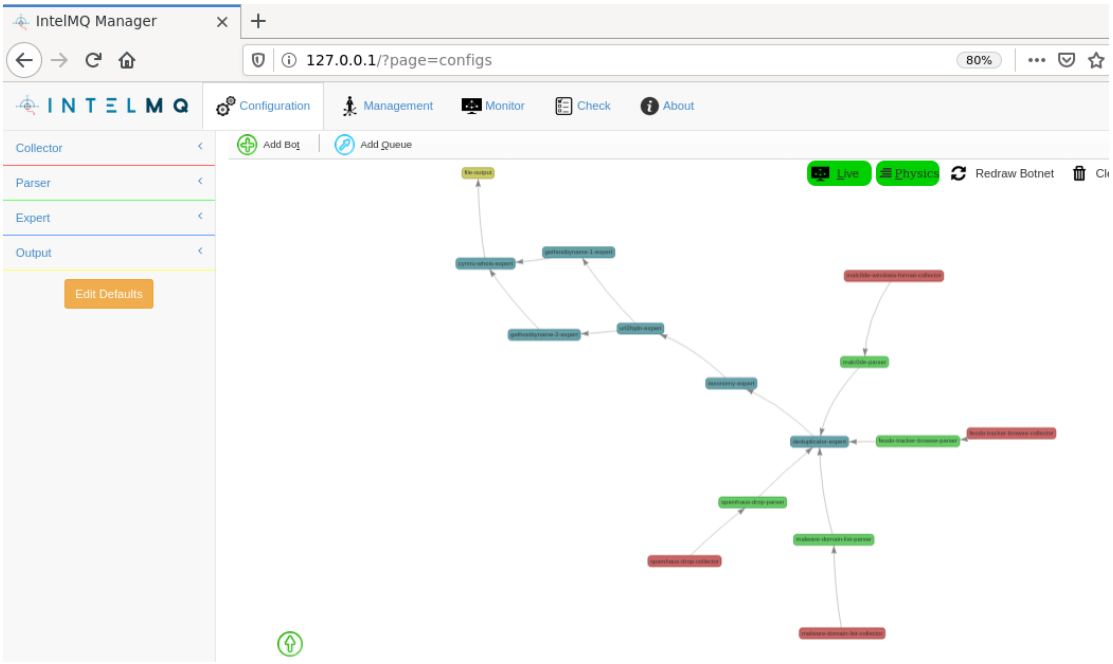


Figura 5: Verificació visual de la configuració d'un Bot.

L'anàlisi de vulnerabilitats la realitza **Wazuh** [9]. A banda de ser un sistema per a detecció d'intrusos (HIDS) inclou també la gestió de vulnerabilitats, permet monitoritzar el comportament maliciós dels equips de la xarxa i donar-hi resposta. A cada servidor que es vol monitoritzar es desplega un agent que reporta a un servidor de Wazuh que està integrat amb Elasticsearch, a través de filebeat que és un agent que recopila dades, i la informació es representa en dashboards de Kibana.

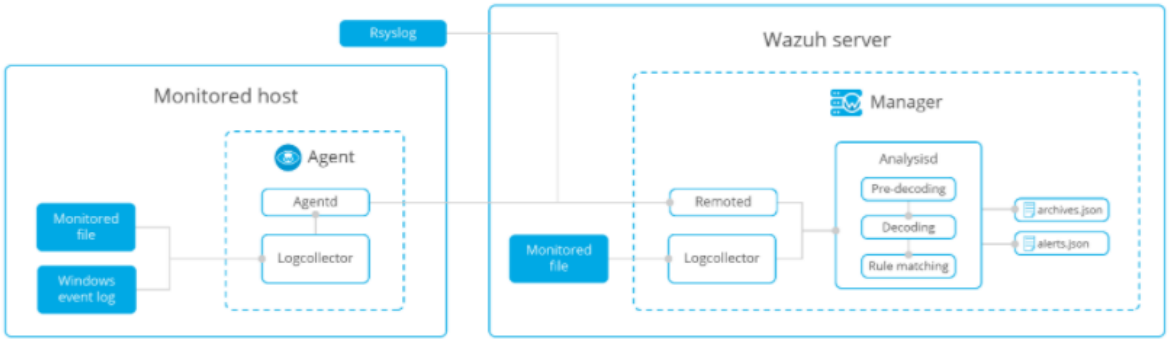


Figura 6: Esquema funcionament client servidor Wazuh

La monitorització del tràfic de la xarxa es fa amb **Packetbeat** [10]. Aquest agent de Elasticsearch recopila informació del temps de latència, temps de resposta, errors i tendències que permeten detectar comportament anòmal a la xarxa.

Elasticsearch [11] fa la funció del que seria un SIEM en emmagatzemar esdeveniments i informació de seguretat de les diferents eines permetent gestionar-los a partir de dasboards de Kibana i generar alertes.

TheHive [12] s'encarrega de la gestió de l'incident i permet rebre alertes i gestionar casos als quals es poden associar tasques i observables. Permet crear plantilles que ajuden a la gestió en funció dels escenaris definits.

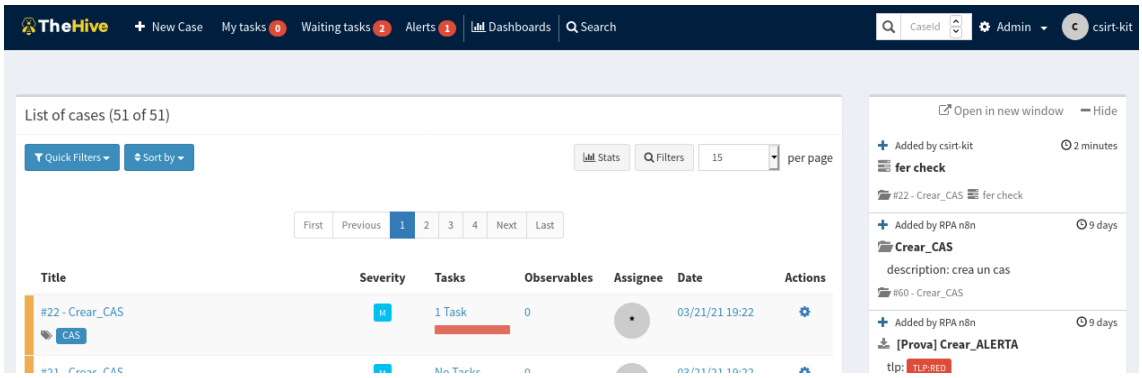


Figura 7: Vista de gestió de casos de TheHive.

Finalment **Cortex** [13] és un motor d'anàlisi per a enriquir informació respecte els observables associats als casos oberts a TheHive. També pot servir per a analitzar observables sota demanda, a través de la seva API, quan s'està gestionant incidents per exemple i també per a executar accions (a través del que s'anomenen "responders").

Aconseguir implantar amb èxit una de les eines, d'automatització robòtica de processos o d'automatització de fluxos de tasques, seleccionades que faciliti la gestió dels operadors dels equips de resposta a incidents complementarà el kit a nivell de les capacitats de SOAR.

2.3 Recursos equip de treball

L'equip de treball disponible i que s'utilitzarà per desplegar l'entorn de treball i per a la implementació dels casos d'ús d'automatització és un HP 15-fq1088ns amb un processador i5-1035G1 i 8GB de RAM.

Com s'ha avançat a l'apartat 1.6, al TFM [2] s'indica que haver afegit l'aplicació Cortex, que permet enriquir els casos de TheHive, implica que l'entorn de treball requereix 8GB de RAM pel que està clar que cal ampliar la memòria de l'equip. Tenint en compte que es disposa d'una ranura addicional per a poder fer dita ampliació i que el més

aconsellable és que les dues targetes de memòria siguin iguals, per a que l'aprofitament sigui òptim, s'afegirà una nova targeta de 8GB fent un total de 16GB.

2.4 Escollir els casos d'ús

Com s'ha pogut veure als apartats 2.1 i 2.3 les eines que composen el kit estan perfectament integrades i no s'aprecia marge de millora en aquest moment. Si en el futur es requereix integrar noves eines més modernes segurament permetran integració via APIs amb les eines existents també. És per aquesta raó que el punt on és més evident que l'automatització pot ser una ajuda, i aportar valor als equips de gestió d'incidents, és concretament a la operativa manual que han de realitzar els operadors ja sigui de forma autònoma, o desatesa, o col·laborant conjuntament (persona i robot). La intenció és posar en pràctica aquestes dues modalitats de treball.

Els casos d'ús que es defineixen a continuació es redacten de forma general degut a que la manera en com es pot arribar a implementar pot tenir diverses variants i, una vegada s'aprofundeixi amb les possibilitats durant el seu desenvolupament poden apareixen maneres diferents de fer-ho o, fins i tot, millorant el cas d'ús proposat. Dit això, els casos d'ús que es proposa implementar són els següents:

- **CAS 1 de col·laboració**:
  A través de la creació d'una alerta a TheHive el robot crearà automàticament un cas enriquint les dades associades a l'alerta amb informació addicional a tenir en compte per a que després un gestor pugui valorar quin seria el pas següent. Fins i tot el robot podria fer alguna primera acció de forma autònoma. Per exemple imaginem que un CERT rep una alerta d'SPAM provinent d'una adreça d'una institució, o una IP associada a aquesta institució està fent un escaneig, i s'ha rebut un correu d'abús el robot crearà el cas i enviarà un primer correu informatiu a la institució per a informar-los de la situació per a que puguin prendre mesures.

- **CAS2 de col·laboració:**
  A través d'un cas d'ús ja existent l'operador ha de poder assignar una tasca al robot amb la intenció que aquest faci una tasca concreta i que en altre cas s'hauria de realitzar de forma manual i repetitiva per part d'un operador.

- **CAS3 desatès**:
  Si un cas obert a TheHive té totes les tasques associades tancades aquest s'ha de poder tancar de forma automàtica pel robot afegint un comentari que així ho indiqui. D'aquesta manera el robot ajudarà a fer un seguiment dels casos.

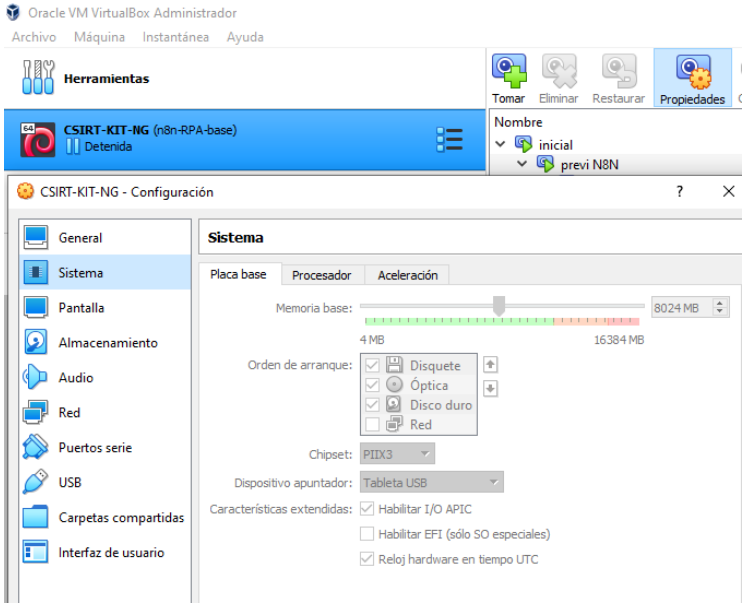
- **CAS4 desatès**:
  Pot ser necessari haver de compartir internament, o amb terceres parts, alguns indicadors de rendiment relacionats amb la operativa realitzada pel SOC. Per exemple es podria contemplar l'enviament d'un correu electrònic amb aquests indicadors.

Aquests són els possibles casos d'ús que es consideren representatius tenir en compte en aquest treball. En funció de les dificultat que puguin sorgir a l'hora d'implementar-los podria ser que algun d'aquests no es pugui implementar tal i com s'ha plantejat però segur que serà possible proposar una alternativa igual o més interessant.

3. Implementació

3.1 Desplegar CSIRT-KIT-NG

El primer pas per a poder començar a implementar els casos d'ús és instal·lar CSIRT-KIT-NG. La instal·lació és molt senzilla donat que tan sols és necessari descarregar la OVA [14], concretament per a la implementació dels casos d'ús la versió descarregada ha estat la 1.2.1, i importar-la a l'entorn de virtualització escollit que en el meu cas ha estat virtualbox.



Com s'ha mencionat a l'apartat 2.3 era necessari ampliar la memòria RAM de l'equip de treball donat que per a un funcionament òptim era necessari assignar 8GB a l'entorn de treball.

Les credencials per defecte per a accedir a l'entorn virtualitzat, i a les eines que el composen, són:

- usuari: **csirt-kit**
- contrasenya: **csirt-kit**

En el cas de voler accedir a l'entorn com a administrador l'usuari serà root i la contrasenya csirt-kit.

En accedir a l'entorn a l'escriptori veurem que es disposa d'un menú per a realitzar operacions bàsiques de manteniment i verificar l'estat de les aplicacions:

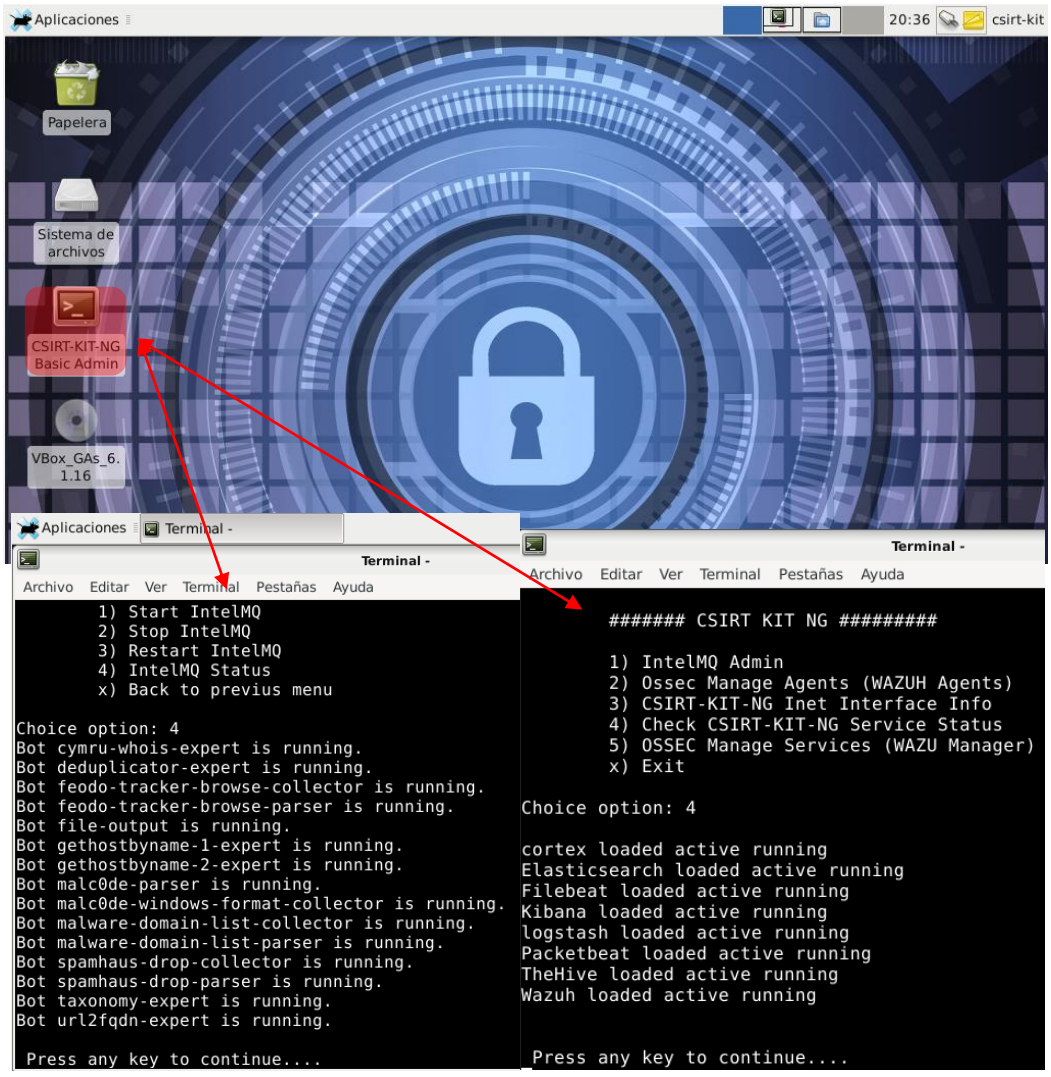


Figura 8: csirt-kit-ng menú d'administració i verificació d'estat de les aplicacions.

A Kibana podem veure l'estat de monitorització del stack de d'asticsearch:

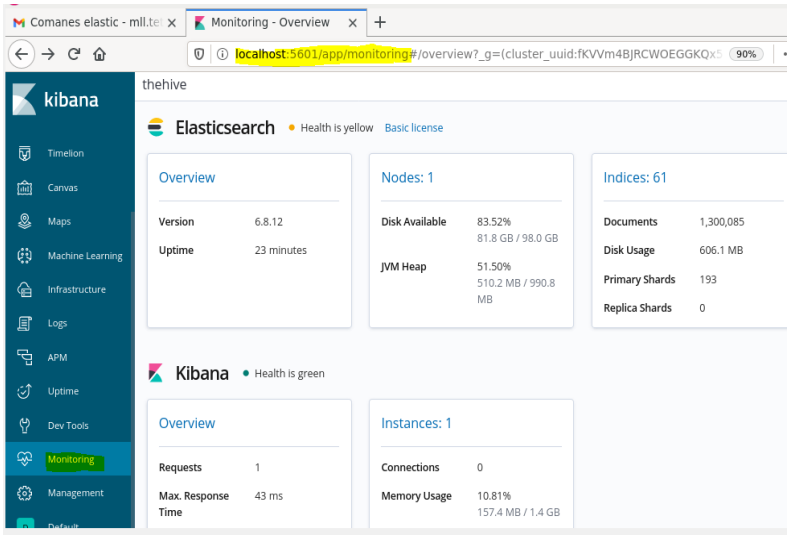


Figura 9: Monitorització de l'estat del stack d'elasticsearch

3.2 Instal·lació eines d'automatització de processos

Com s'ha comentat a l'apartat 2.1 l'eina d'automatització escollida ha estat n8n donat que permet automatitzar fluxos de treball amb TheHive i Cortex a partir dels nodes disponibles que exploten les seves APIs.

A la comunitat n8n [15] hi ha un manual detallat per a procedir amb la instal·lació a un sistema operatiu debian pel que en comptes reproduir el procediment serà millor centrar-se en els punts concrets en els quals han aparegut certes dificultats que ha estat necessari resoldre per a poder completar amb èxit la instal·lació de l'eina.

Recordar que abans de començar amb la instal·lació és necessari fer una actualització de paquets (sudo apt update). A l'hora d'instal·lar el gestor de la base de dades sqlite3 ha aparegut un error de compatibilitat amb la versió de NodeJS instal·lada:

```
root@CSIRT-KIT-NG:~# npm i sqlite3 -g --build-from-source
npm WARN deprecated har-validator@5.1.5: this library is no longer supported
npm WARN deprecated request@2.88.2: request has been deprecated, see https://github.com/request/request/issues/3142
npm WARN deprecated node-pre-gyp@0.11.0: Please upgrade to @mapbox/node-pre-gyp: the non-scoped node-pre-gyp package
is deprecated and only the @mapbox scoped package will recieve updates in the future
npm ERR! code 127
npm ERR! path /root/.nvm/versions/node/v15.12.0/lib/node_modules/sqlite3
npm ERR! command failed
npm ERR! command sh -c node-pre-gyp install --fallback-to-build
npm ERR! sh: 1: node-pre-gyp: Permission denied

npm ERR! A complete log of this run can be found in:
npm ERR!     /root/.npm/_logs/2021-03-20T15_25_09_611Z-debug.log
```

Figura 10: Error instal·lació n8n per compatibilitat amb versió NodeJS existent

requerint desactivar la versió actual, des-instal·lar-la i instal·lar la versió 14.16.0 que és la que s'indica al procediment per aconseguir instal·lar el gestor de la base de dades.

Una vegada completada la instal·lació ha estat necessari executar les comanes següents per a que es pugui executar l'eina per qualsevol usuari que no sigui root:

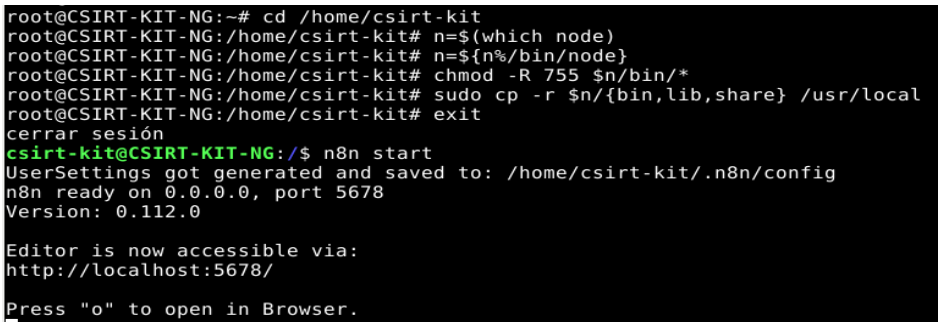


Figura 11: donar permisos a tots els usuaris i iniciar n8n

Una vegada iniciada l'aplicació per a accedir a la interfície gràfica només cal obrir un explorador i escriure http://localhost:5678/.

Com a complement a n8n, entre les diferents eines analitzades a l'apartat 2.1, s'ha decidit instal·lar RPA-Python que a partir d'uns scripts en Python permet automatitzar qualsevol acció que podria fer un usuari amb eines web i d'escriptori gràcies a una biblioteca de funcions que facilita molt l'automatització. Com es veurà al darrer cas d'ús de l'apartat 3.3 els scripts de Python es poden executar fàcilment des de n8n.

Previ a la instal·lació de l'eina cal instal·lar Python (en aquest cas s'ha instal·lat Python 3). La instal·lació de RPA-Python [16] és també força senzilla i només es considera necessari explicar:

Que en entorn Linux si es vol activar el mode d'automatització visual (reconeixement d'imatges) es requereix tenir instal·lat OpenCV i Tesseract [17] i també es requereix la instal·lació del navegador Chrome.

A l'hora d'executar un primer exemple de prova ha aparegut un error de OPEN SSL i la solució ha consistit en comentar una línia de configuració per defecte del fitxer openssl.conf [18].

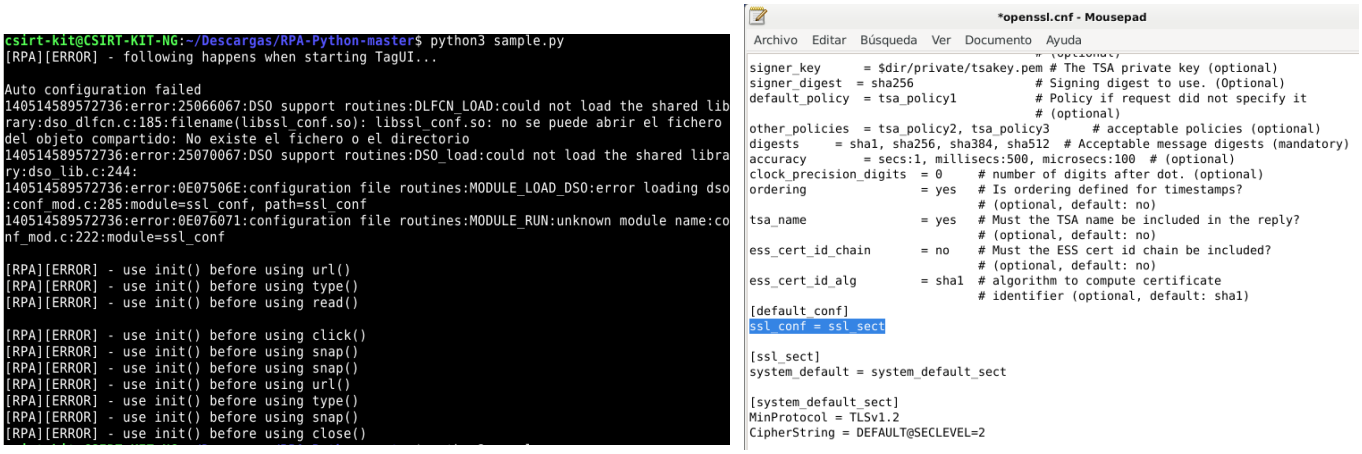


Figura 12: Error OPENSSL i solució aplicada

3.3 Implementar i testejar els casos d'ús

Abans de començar a explicar els casos d'ús implementats es considera necessari fer una breu explicació dels nodes [19] principals de n8n que permeten implementar automatitzacions amb dues eines de l'entorn de treball:

- **TheHive**

Aquest és el node que permet realitzar accions amb l'eina de gestió de tiquets TheHive. A continuació es pot veure una imatge amb els recursos que permet controlar i per cadascun d'aquests hi ha una sèrie d'operacions disponibles algunes de els quals es comenten de forma més detallada als casos d'ús implementats.

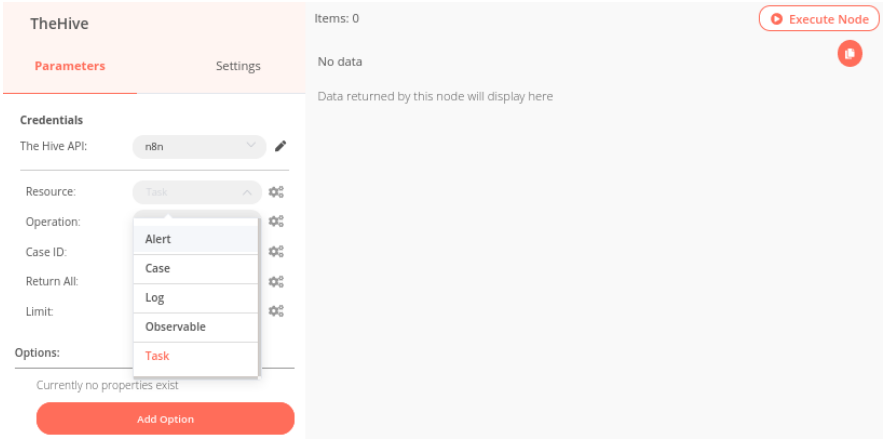


Figura 13: paràmetres node n8n TheHive

- **TheHive trigger**

Aquest node permet activar l'execució d'un flux a partir de la successió de certs esdeveniments ocorreguts a TheHive. És important tenir en compte que per a poder utilitzar-lo cal modificar el fitxer el fitxer application.conf de TheHive i sempre primer cal fer una prova amb el webhook de test [20] ja que en altre cas el de producció no funcionarà i retornarà un error. En aquesta imatge es pot veure com el webhook retorna la informació corresponent a la creació d'una nova alerta i també es mostren els esdeveniments que poden activar-lo:

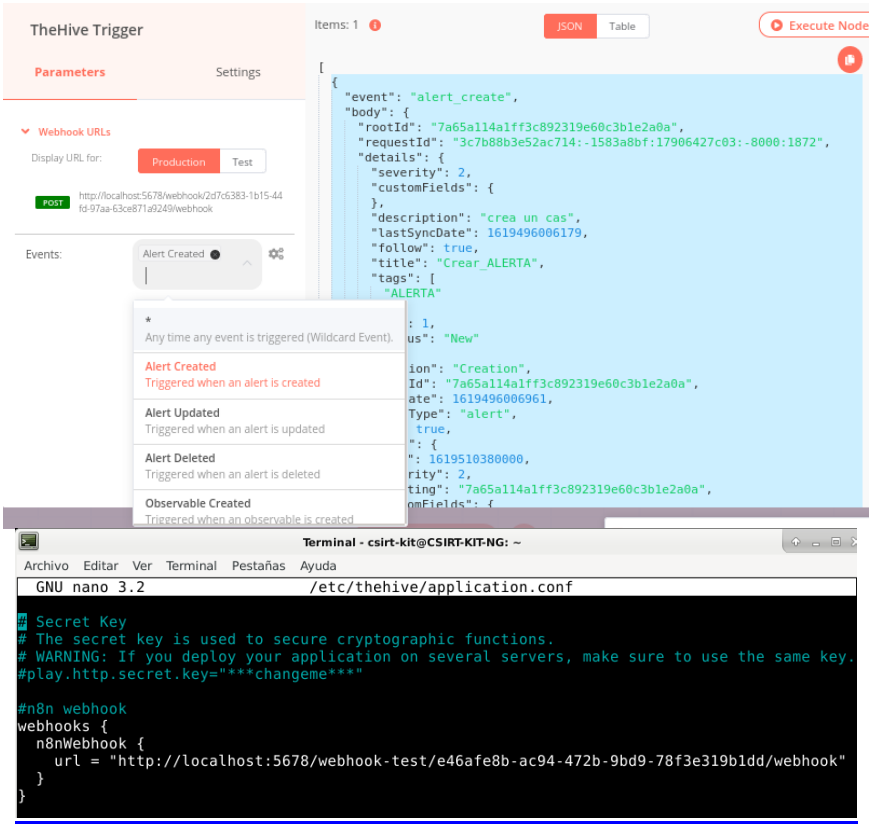
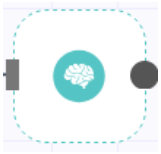


Figura 14: paràmetres del node n8n TheHive trigger i configuració del webhook

- **Cortex** 

Aquest node permet executar analitzadors, actuadors (anomenats “responders”) i recuperar detalls i reports dels treballs executats. Per a poder utilitzar-los cal prèviament haver-los instal·lat i configurat quan correspon (només alguns són gratuïts).
Evidentment per a poder utilitzar els analitzadors i actuadors cal haver-los configurat de forma adient [21]. Sense entrar en el detall si que es important recordar que cal crear a Cortex una organització addicional amb els seus usuaris per a poder assignar els permisos als analitzadors i actuadors que cal haver configurat.

A la imatge següent es pot veure com a banda de la organització “cortex” per defecte s’ha creat una nova organització anomenada CSIRT-KIT-NG:

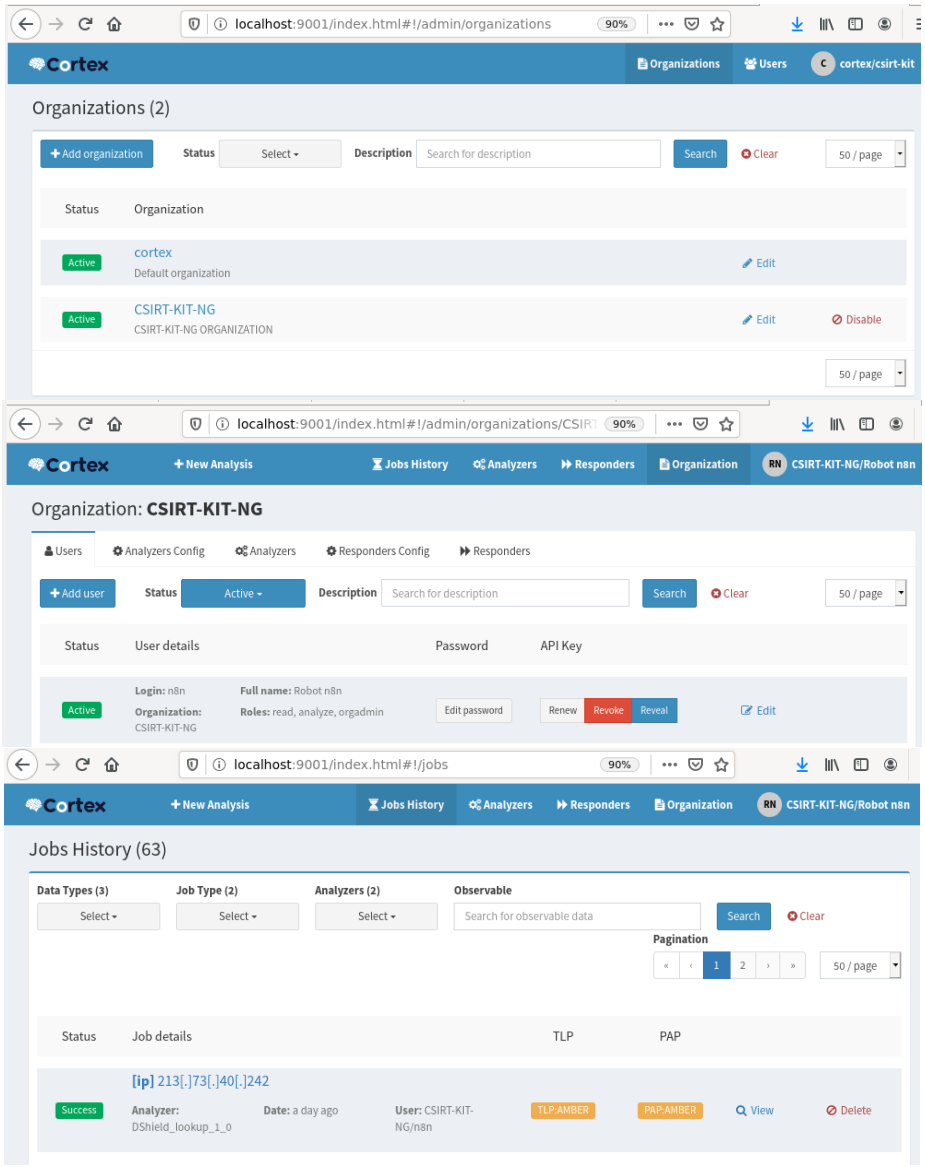


Figura 15: Cortex: organitzacions, configuració dels analitzadors-actuadors i resultat d'execució.

Als casos 1 i 2 que veurem a continuació serà necessari emprar al node Cortex les credencials de l'usuari "n8n" configurat dins d'aquesta nova organització (figura 15) donat que serà el que tindrà els permisos per a executar un analitzador i recuperar els resultats de la seva execució.

3.3.1 CAS1 - Nova alerta a TheHive com a inici automàtic d'accions

A partir de la creació d'una nova alerta amb un observable del tipus IP s'inicia l'execució del flux automatitzat de les tasques que implementen aquest cas d'ús a partir del node TheHive trigger. A la imatge següent es pot veure en diferents colors l'agrupació de la funcionalitat implementada i que s'explica a continuació:

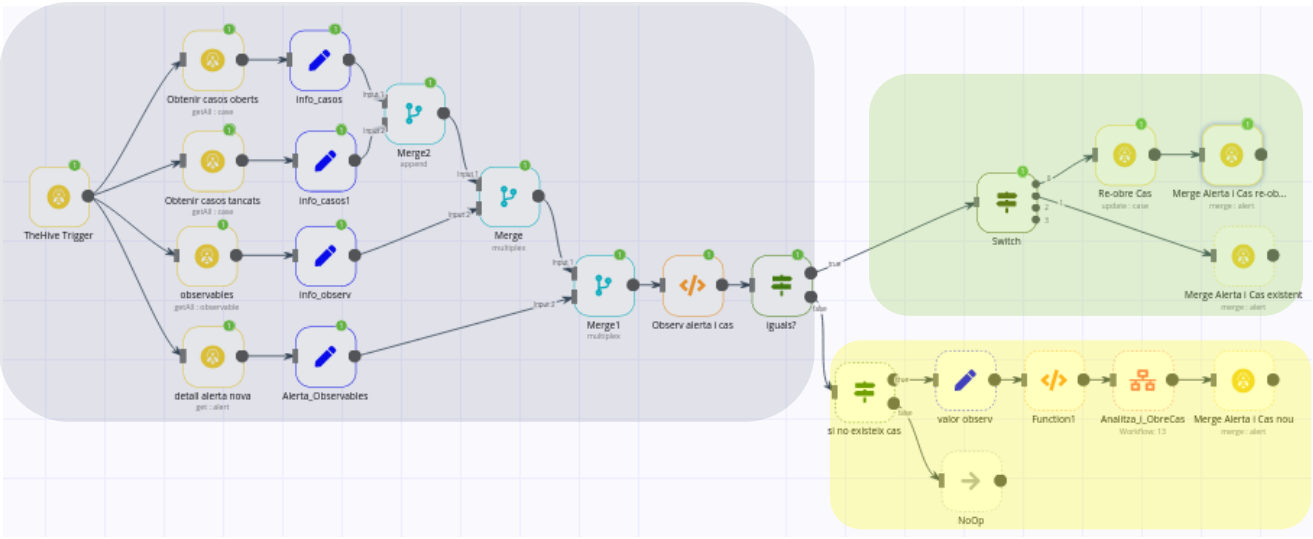


Figura 16: diagrama de flux del cas d'ús 1

- En color blau es pot veure una primera part del flux que recull informació de la nova alerta creada, es recuperen els casos existents a TheHive (tancats i oberts) i també es recuperen els observables creats amb els identificadors de cas al que estan associats. Totes aquestes dades es combinen amb varis nodes "merge" per finalment aconseguir fer una comparació amb un node "function" amb nom "observables alerta i cas" que afegeix una propietat (iguals) als objectes JSON pels quals identificadors del cas i el valor de l'observable són els mateixos. A banda també s'afegeix una nova propietat (trobats) que indica el nombre de coincidències detectades entre tots els objectes. Totes dues propietats són necessàries per a saber les accions finals que es realitzaran a les tasques agrupades en color verd i groc.

Edit JavaScript Code

JavaScript Code:

```
var trobats = 0;

for (var i = 0; i < items.length; i++) {
  if ((items[i].json.CaseID == items[i].json.ObservCaseID) && (items[i].json.DataObservable == items[i].json.DataAlerta)){
    items[i].json.iguals = "true";
    trobats++;
  }
}
for (var j = 0; j < items.length; j++) {
  items[j].json.trobats = trobats;
}

return items;
```

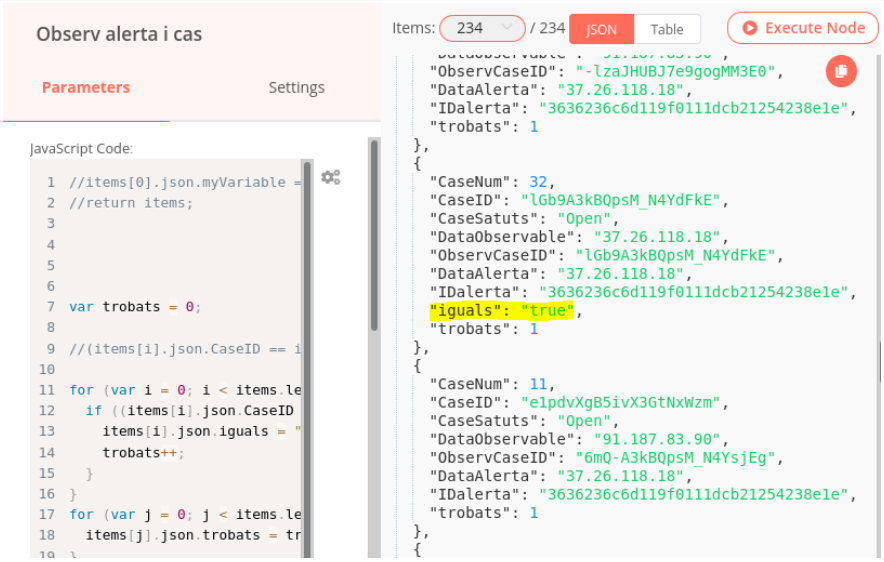


Figura 17: detall del codi javascript del node funció i visualització de la sortida

- En color verd tenim la part del flux que s'encarrega de vincular l'alerta amb un cas existent o de re-obrir el cas i vincular l'alerta si l'observable associat a l'alerta nova ja havia estat associat amb anterioritat a un cas tancat. En aquest punt el node de "TheHive" permet fer dites accions fàcilment passant-li els objectes JSON de sortida dels nodes anteriors (principalment l'identificador del cas i de l'alerta).

- Finalment en color groc el que es fa és recuperar el valor de la IP associada a la nova alerta i a continuació es fa un anàlisi de la reputació d'aquesta IP per poder obrir un nou cas afegint-hi dita informació. Aquest anàlisi es fa realitzant una crida a un flux independent, a través del node "execute workflow (13)", amb la voluntat d'explorar aquesta opció veure com cal treballar amb el pas dels paràmetres entre els fluxos donat que és molt interessant per a poder reaprofitar el codi. De fet aquest codi va ser dissenyat pel CAS2 que veurem a continuació i com podia complementar al CAS1 s'ha reaprofitat. A continuació es pot veure el detall de les tasques que composen el diagrama de flux que realitza dita acció i amb els valors retornats per aquest finalment s'acaba associant l'alerta al cas creat.

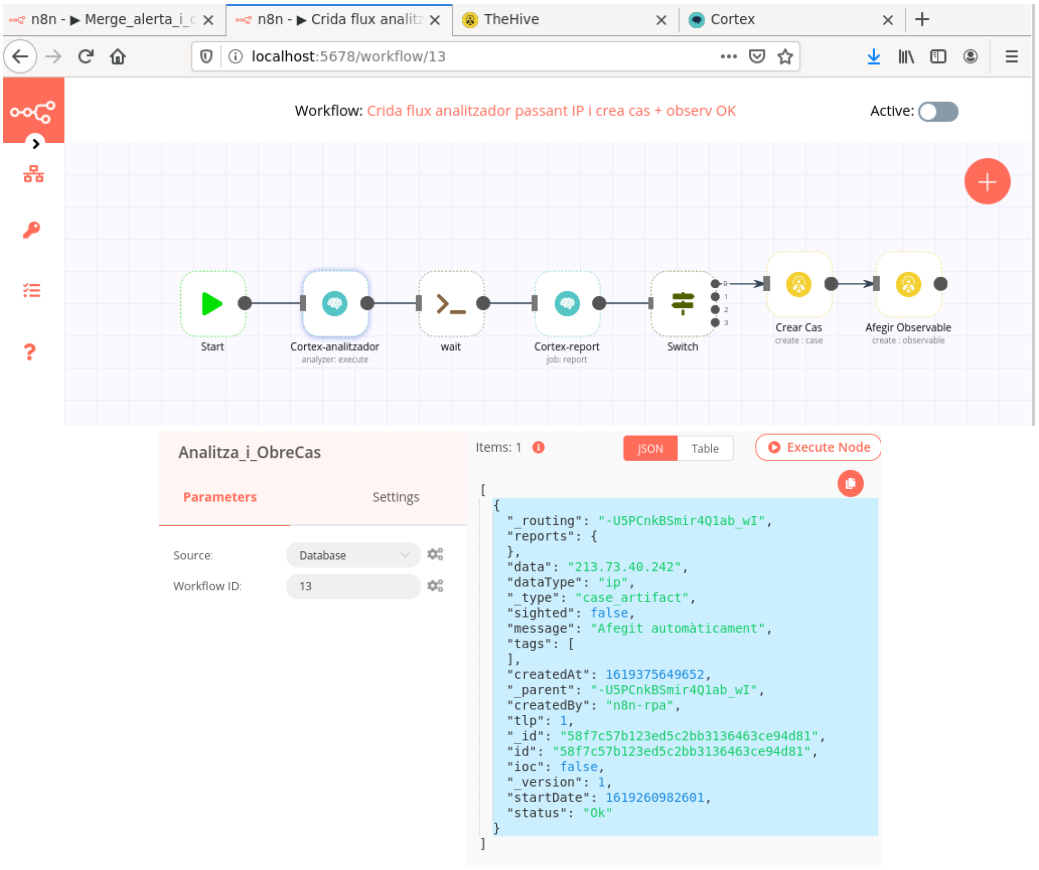


Figura 18: cas 1 flux que analitza l'observable i resultat que retorna

A mode d'evidència a les imatges següents es pot veure com, en no trobar cap coincidència, s'ha creat un cas nou amb un títol que està compost per l'observable de l'alerta i el resultat de la reputació (safe en aquest cas) de l'anàlisi realitzat i que s'ha afegit una descripció amb el correu de contacte per a notificar abús i s'ha associat un observable al cas creat:

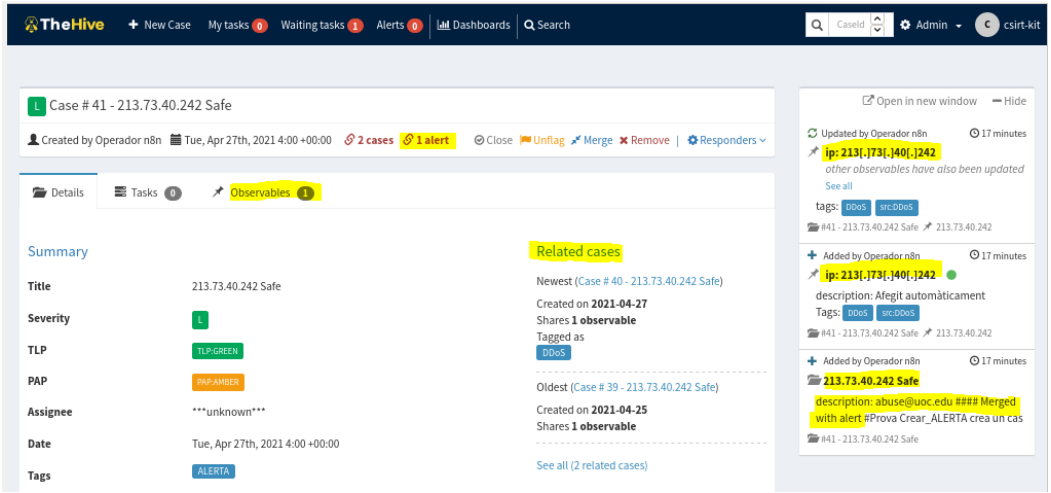


Figura 19: cas 1 evidència exemple de creació d'un cas nou

Si ara tanquem aquest mateix cas i, forcem la creació d'una nova alerta amb el mateix observable, podem veure com en aquest ocasió es re-obre el cas associant la nova alerta creada:

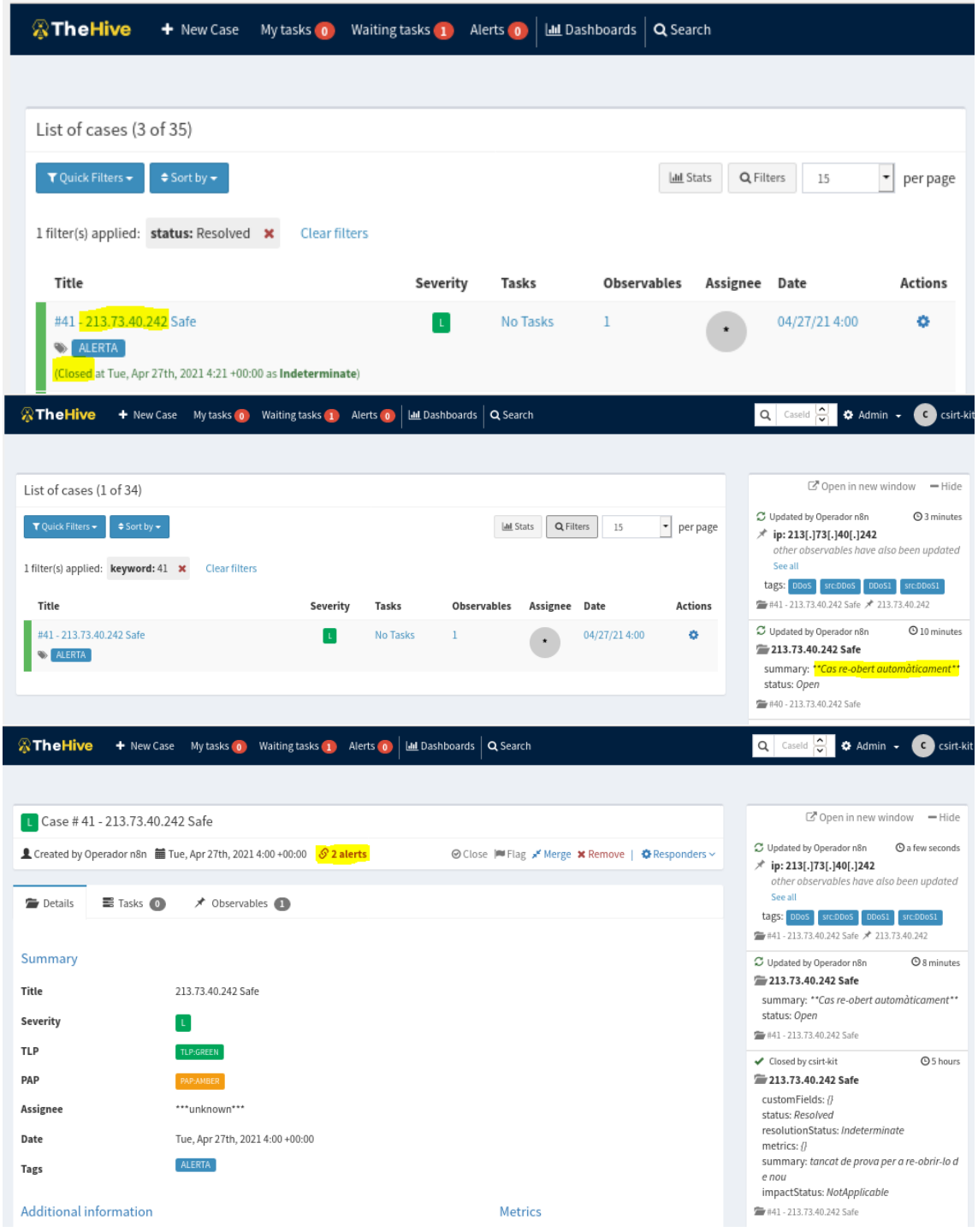


Figura 20: cas 1 evidència de re-obertura d'un cas tancat

3.3.2 CAS2 - Assignació d'una tasca a l'agent virtual n8n

Com en tot equip de treball poden existir torns en els quals hi ha menys operadors (festius, horari nocturn, etc.) i l'automatització pot ser un gran aliat per a que, en funció de la severitat de l'alerta, un gestor virtual pugui avançar certes accions si se li assigna una tasca. En aquest cas l'operador virtual analitza la reputació de l'observable associat al cas i a partir del resultat actualitza la descripció de la tasca per a que un operador pugui realitzar altres accions segons el seu criteri i operativa definida.

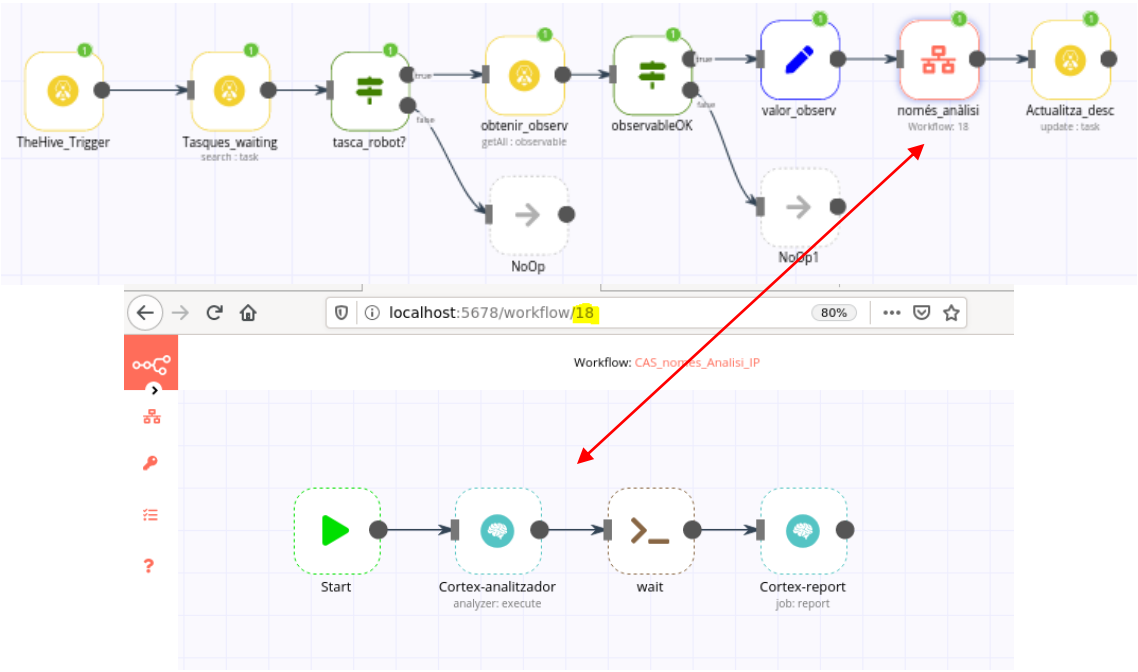


Figura 21: cas 2 diagrama de flux i sub-flux

Respecte al pas dels objectes JSON entre diagrames de flux diferents cal tenir en compte que aquest es realitza a través del node "start" que hi ha per defecte a tot nou flux creat. A la imatge següent es pot veure la expressió que cal escriure per a poder recuperar el valor de l'observable provinent del flux inicial per a que es pugui iniciar l'execució de l'anàlisi:

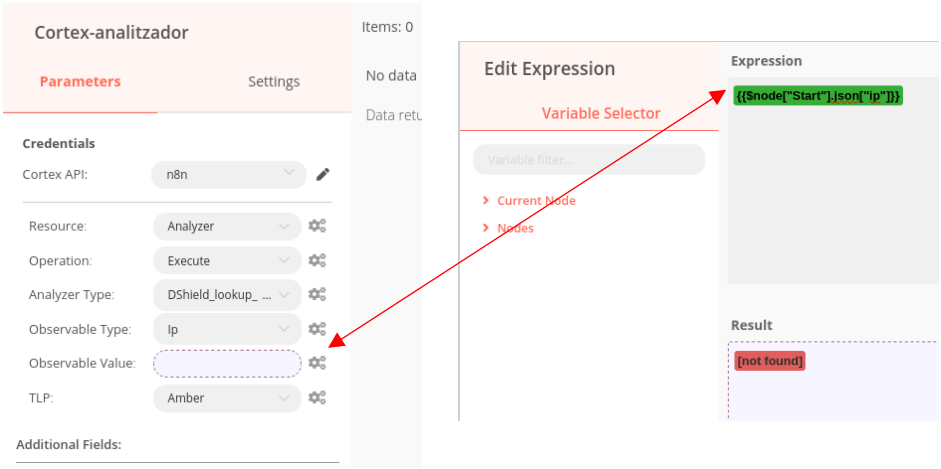


Figura 22: cas 2 expressió per a recuperar el valor de l'observable al sub-flux

A continuació es pot veure les evidències del resultat que retorna el flux al node que fa la crida, l'actualització de la descripció de la tasca que realitza el node i finalment com es veu aquesta actualització directament a TheHive:

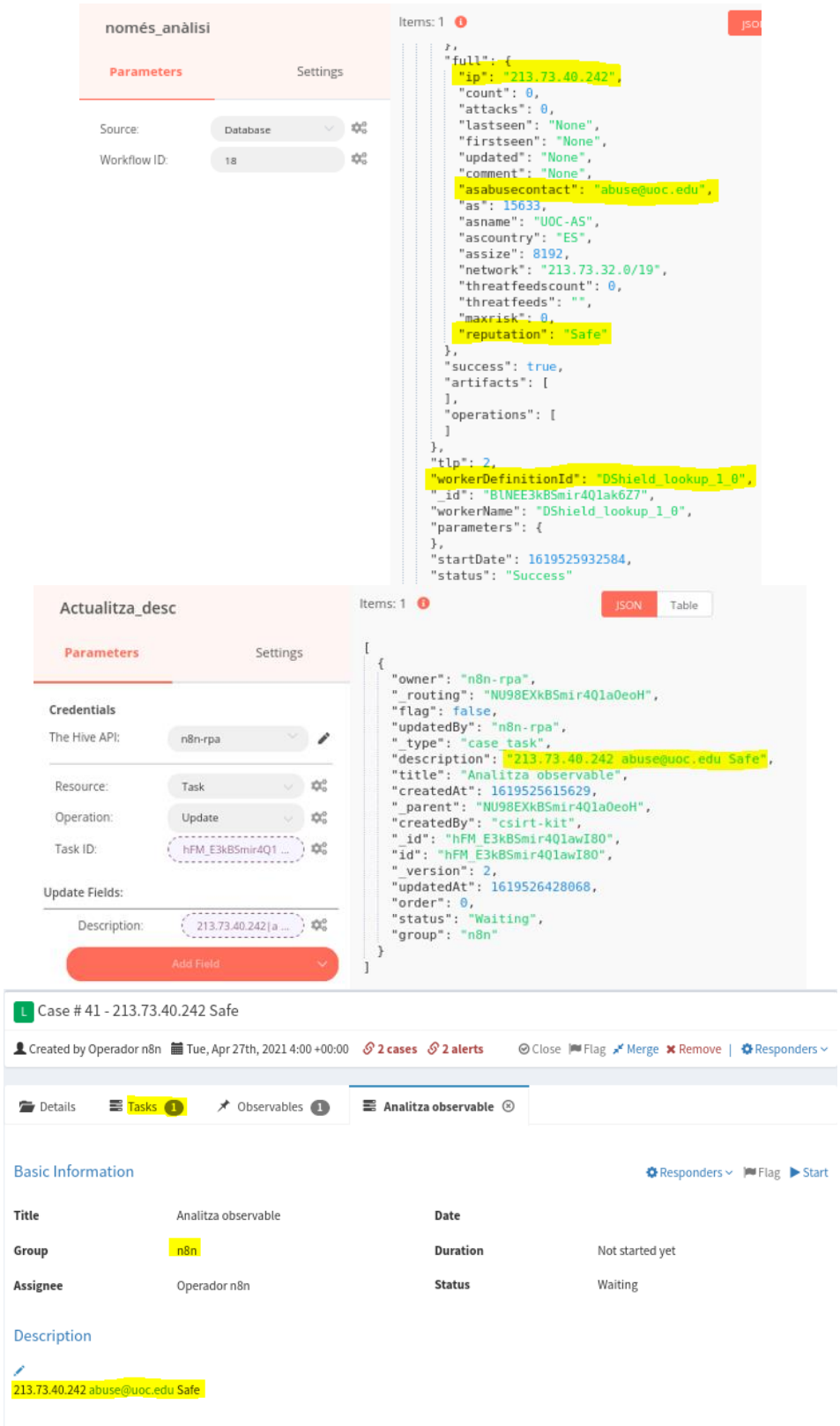


Figura 23: cas 2 valors retornats de l'anàlisi i actualització de la descripció de la tasca

3.3.3 CAS3 - Tancament automàtic de casos

En aquest cas es parteix del supòsit que si les tasques associades a un cas estan totes tancades aquest es pot tancar una vegada transcorreguts més de 3 dies del tancament de la darrera tasca.

El node TheHive com hem vist permet consultar casos, consultar tasques i també actualitzar l'estat dels casos. Com es pot veure al diagrama de flux hi ha 3 mòduls que realitzen aquestes accions. El mòdul de funció és el que en aquesta ocasió té implementat un codi javascript la funció principal del qual és saber si totes les tasques associades al cas estan tancades i calcular el temps que ha passat des de que la darrera tasca es va tancar. Per a programar una periodicitat d'execució es podria emprar el node "Cron" en comptes de fer servir el "Start".

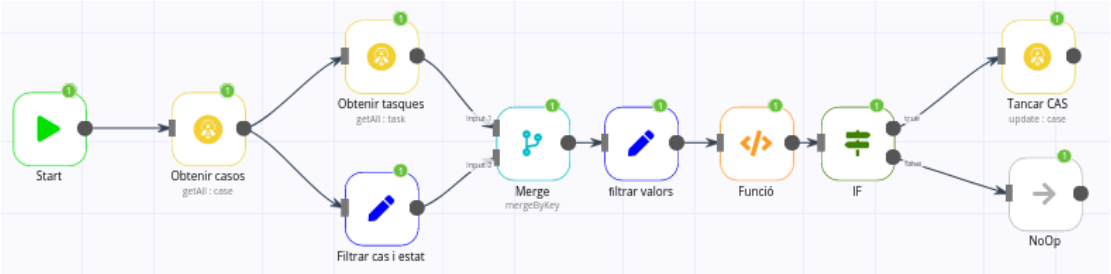


Figura 24: cas 3 diagrama de flux

A continuació es pot veure el detall del codi que realitza aquesta funció:

Edit JavaScript Code

JavaScript Code:

```
var num_tasques = 0;
var num_tasques_completades = 0;
const avui = new Date().toISOString();
var actualitzat = new Date;

for (var i = 0; i < items.length; i++) {
  for (var j = 0; j < items.length; j++) {
    if(items[i].json.case_id == items[j].json.case_id) {
      num_tasques++;//cada cas es repeteix tantes vegades com tasques té
      if (items[j].json.task_status == "Completed") num_tasques_completades++;
      if (items[i].json.update_time < items[j].json.update_time) actualitzat = items[j].json.update_time;
      else actualitzat = items[i].json.update_time; //si la data no és més actual es manté la mateixa
    }
  }
  items[i].json.num_tasques = num_tasques;
  items[i].json.num_tasques_completades = num_tasques_completades;
  if ((num_tasques - num_tasques_completades) == 0) items[i].json.es_pot_tancarcas = "true";
  else items[i].json.es_pot_tancarcas = "false";
  items[i].json.lastupdate = actualitzat;
  durada = (new Date(avui) - new Date(actualitzat))/1000/60/60/24; //conversió de ms a dies
  items[i].json.temps = durada;
  j = 0;
  num_tasques = 0;
  num_tasques_completades = 0;
  actualitzat = 0;
}
return items;
```

Figura 25: cas 3 codi del node funció

Finalment el node “IF” comprova si la duració ha estat superior als dies fixats per a procedir al tancament dels casos que compleixen amb dita condició.

3.3.4 CAS4 - Report d’indicadors del SOC

Tot equip de treball requereix presentar indicadors de rendiment de forma periòdica i per tant és una feina que té sentit automatitzar. En aquest cas d’ús es posa en pràctica la combinació de n8n amb l’eina RPA-Python[16] per a crear una presentació amb varis fulls d’indicadors. El flux de n8n que permet executar un script python implementat amb RPA-Python, veure figura 26, requereix utilitzar el node “execute” que és el que executa l’script implementat i que es pot veure a la figura 27:

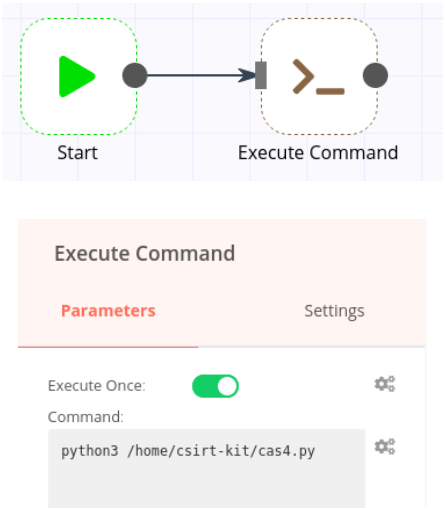


Figura 26: cas 4 diagrama de flux i comana que s’executa

```
 GNU nano 3.2                        cas4.py                          Modificado

import rpa as r
r.init(visual_automation = True)

#Kibana Wazuh
r.url('http://localhost:5601/app/kibana#/dashboard/2b2c40f0-0cb0-11eb-a069-1d5fa0ca7ee3')
r.wait(6)
r.click('Visualize1.png')
r.wait(3)
r.click('//*[@id="kibana-body"]/div/nav/div[2]/div[1]/app-switcher/div[3]/a/div[2]')
r.wait(6)
r.keyboard('[tab]')
r.keyboard('[down]')
r.keyboard('[down]')
r.snap(185, 185, 1210, 650, 'grafic.png')

#dashboard TheHive
r.click('TheHive.PNG')
r.click('dashboards.png')
r.click('case.png')
r.wait(2)
r.keyboard('[pagedown]')
r.keyboard('[pagedown]')
r.keyboard('[pagedown]')
r.click('image.png')

#Preparar presentació
r.click('aplicaciones.png')
r.click('oficina.png')
r.click('impress.png')
r.wait(3)
r.dclick('CSIRT-KIT.png')
r.wait(3)
r.keyboard('[tab]')
r.wait(3)
r.type('(246,430)','CSIRT-KIT-NG RPA al SOC')
r.wait(3)
r.keyboard('[pagedown]')
r.click('insertar.png')
r.wait(3)
r.click('imagen.png')
r.type('(340,195)','/home/csirt-kit/grafic.png[enter]')
r.type('(440,250)','INDICADORS WAZUH')
r.keyboard('[pagedown]')
r.click('insertar.png')
r.wait(3)
r.click('imagen.png')
r.type('(340,195)','/home/csirt-kit/Descargas/chart.png[enter]')
r.type('(440,250)','INDICADORS CASOS TheHive')
r.close()
```

Figura 27: cas 4 codi RPA-Python

El codi anterior és fàcilment interpretable a partir dels noms de les funcions que s'utilitzen (click, keyboard i type principalment). Aquest es basa en consultar la url d'un dashboard de kibana, concretament de vulnerabilitats detectades per Wazuh, del qual agafa una captura (grafic.png). A continuació obre la finestra de l'explorador a la que hi ha oberta l'aplicació TheHive i es desplaça fins al gràfic concret que es vol adjuntar a la presentació i el guarda. Finalment obre l'apliació d'escriptori "Impress" que permet preparar una presentació de diapositives i s'escriu el text CSIRT-KIT i RPA al SOC al primer full. Al segon full s'enganxa la imatge capturada de Wazuh acompanyada d'un títol i al tercer full es fa el mateix per a la imatge dels casos de TheHive. A partir d'aquí l'exemple es podria seguir ampliant obrint una aplicació de correu, d'escriptori o web, i enviant la presentació a certs destinataris si no es considera necessari que us humà faci una revisió visual prèvia al seu enviament.

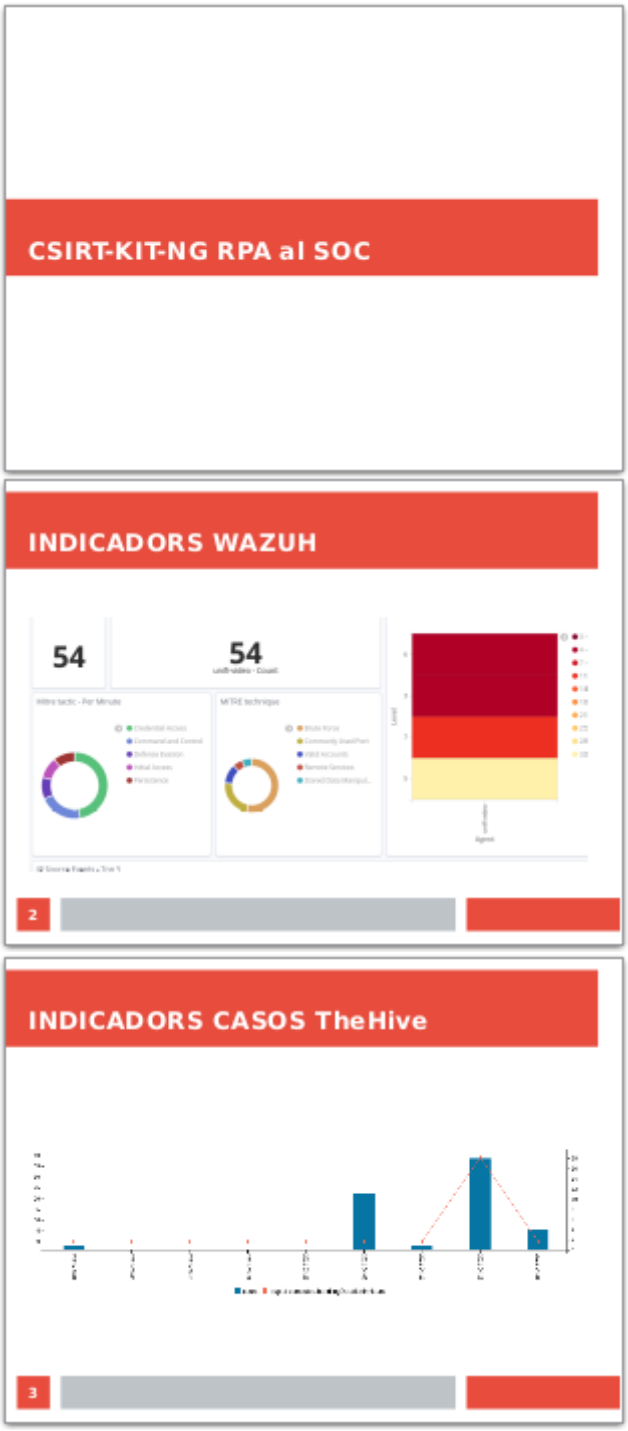


Figura 28: cas 4 presentació d'indicadors generada automàticament

Per acabar només tenir en compte unes consideracions pràctiques a l'hora d'utilitzar RPA Python. És important que no es modifiqui la mida de la pantalla ni el zoom donat que en altre cas l'aplicació no seleccionarà correctament les posicions indicades a l'script. Es poden emprar identificadors dels elements web als quals es vol accedir (per exemple selectors XPath, CSS o certs atributs web) com es pot veure a la línia 8 del codi de la figura 27) però si aquest no funciona correctament sempre es pot utilitzar una imatge per a que l'aplicació la reconegui i pugui fer-hi clic (veure línia 4 del codi).

3.4 Conclusions

El temps de resposta a un incident és vital per a minimitzar o, en el millor dels casos eliminar, les conseqüències negatives que aquest pot comportar i l'automatització de la resposta s'ha de veure com un aliat necessari per aconseguir reduir-lo al mínim possible.

Els casos d'ús exemple implementats confirmen que és possible automatitzar processos compostos per conjunt de tasques per a disposar, del que podríem anomenar, un operador virtual que pugui col·laborar amb operadors humans d'un equip de resposta a incidents realitzant certes tasques més rutinàries i per les que l'automatització aporta grans estalvis de temps amb l'avantatge de poder cobrint un horari 24x7. Les eines emprades permeten també poder donar una resposta automàtica a certs escenaris concrets i la voluntat d'implementació dependrà finalment del grau de confiança i experiència dels equips de resposta.

Encara que l'objectiu inicial no era automatitzar el bloqueig d'un incident de seguretat és important comentar que és perfectament factible fer-ho i de formes diferents. Com s'ha vist TheHive disposa de "responders" o actuadors i també permet implementar-ne de propis adaptats a l'entorn de treball [22]. Concretament un dels disponibles és un de Wazuh [23] que permet bloquejar una IP a un dels endopints que formen part de la xarxa però per a poder fer-ho és necessari haver instal·lat els agents Wazuh als equips. Per tant manualment des de TheHive un operador podria arribar a realitzar aquesta acció o també podria fer-se a través d'un flux de n8n utilitzant el node "cortex". Tot i així la resposta activa enfocada a bloquejar és una opció que ja contempla per defecte Wazuh donat que disposa de diferents scripts pre-configurats per a ser executats com a resposta activa a partir d'una alerta o regles definides [24]. Per tant si Wazuh està correctament configurat no hauria de ser necessari acabar executant aquesta acció des d'altre aplicacions. Per a demostrar que aquesta podria ser una opció viable que es podria automatitzar també amb n8n a continuació es pot veure l'script python [25] que empra el mètode d'autenticació bàsica per a fer login a la API de Wazuh. A partir d'aquí si es tenen agents desplegats seria possible executar totes les accions disponibles a Wazuh (veure figura 29).

El manteniment de les automatitzacions implementades és també un factor important a considerar. En aquest sentit n8n permet modificar els fluxos de forma àgil i poder adaptar-los als canvis que puguin ser necessaris (noves eines i actualitzacions entre altres). Tot i així la recomanació es basa en fer codis de funcionalitat concretes que puguin ser cridats des d'altres fluxos per a que si es produeix algun canvi aquest només sigui necessari implementar-lo una vegada i que la resta de codis segueixin funcionant normalment comportant un gran estalvi de temps (recomanació habitual per a qualsevol desenvolupament de codi).

Finalment cal destacar que el fet de complementar a n8n amb RPA-Python permet que, a banda de poder automatitzar fluxos amb les integracions disponibles, es pugui controlar qualsevol aplicació que no disposi d'APIs, ja sigui web o d'escriptori, a través de la interfície d'usuari. A n8n existeix l'opció de crear nodes personalitzats per a ser

integrats a l'eina però l'ús de RPA-Python pot ser una alternativa senzilla i de ràpida implementació per a aconseguir fer el mateix.

```
 GNU nano 3.2                                    logging-wazuh.py

#!/usr/bin/env python3

import json
import requests
import urllib3
from base64 import b64encode

# Disable insecure https warnings (for self-signed SSL certificates)
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

# Configuration
protocol = 'https'
host = 'localhost'
port = 55000
user = 'foo'
password = 'bar'
#login_endpoint = 'security/user/authenticate'

login_url = f"{protocol}://{host}:{port}"
#login_url = f"{protocol}://{host}:{port}/{login_endpoint}"
basic_auth = f"{user}:{password}".encode()
login_headers = {'Content-Type': 'application/json',
                 'Authorization': f'Basic {b64encode(basic_auth).decode()}'}

response = requests.get(login_url, headers=login_headers, verify=False)
resp = json.loads(response.content.decode())

print(resp)
```

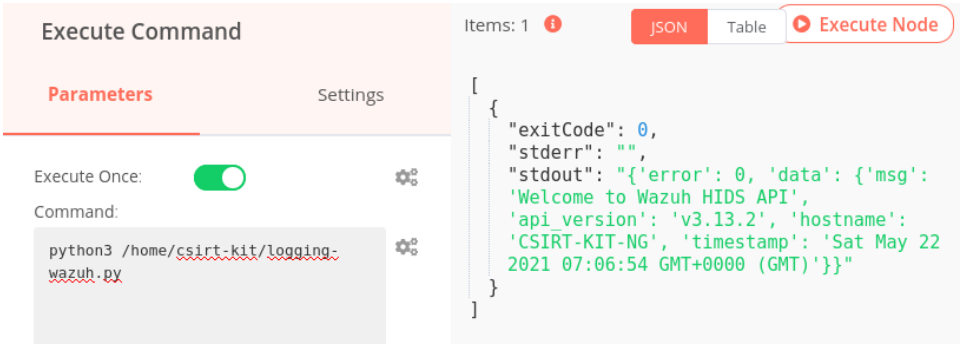


Figura 29: Script login API de Wazuh i execució des de n8n.

4 Aspectes de seguretat

4.1 Riscos sobre la seguretat de la informació

L'objectiu d'aquest apartat és analitzar els riscos de seguretat que implica l'ús d'eines d'automatització de fluxos de tasques i eines de RPA amb la intenció de tractar-los a l'apartat següent.

Abans de començar a parlar dels possibles riscos és important tenir en compte que l'automatització ben feta [26][28], aplicant les mesures de seguretat adients, en realitat ha de permetre reduir els riscos de seguretat de la informació donat que els robots software implementats faran exactament les accions definides sense cometre errors per cansament, distraccions o de forma malintencionada i no són susceptibles de ser víctimes de tècniques d'enginyeria social. Evidentment serà necessari testejar-los correctament abans de començar a treballar amb dades productives.

Per a que es materialitzi un risc cal que existeixi una vulnerabilitat que sigui explotada per una amenaça. Per a diferenciar-les cal tenir en compte que les amenaces son externes als actius considerats mentre que les vulnerabilitats són atributs dels actius que les amenaces poden explotar. A continuació es pot veure un llistat [26][27][28][29] de les principals amenaces y vulnerabilitat que poden implicar un risc sobre la disponibilitat, confidencialitat, autenticitat, Integritat o traçabilitat de la informació en utilitzar eines de RPA i d'automatització en general:

- Ús de credencials privilegiades per part dels robots software (Amenaça): Caldria emprar el principi de mínims privilegis necessaris per a dur a terme les accions corresponents.
- No definir una política de canvi de mots clau de forma periòdica (Vulnerabilitat).
- Credencials guardades en emmagatzematges no xifrats o escrites directament al codi en text pla (Vulnerabilitats).
- No disposar d'un control d'accés segur a l'eina d'automatització (Vulnerabilitat): Com a mínim una autenticació bàsica hauria de ser requerida i si es permet poder habilitar el doble factor d'autenticació seria el més recomanable.
- No actualitzar l'eina regularment (Amenaça): Impedeix corregir vulnerabilitats identificades.
- Error en l'actualització de l'eina d'automatització, error en realitzar canvis sobre les automatitzacions o la discontinuació de l'eina per part del proveïdor (Amenaces): Són situacions que podrien impactar seriosament a l'activitat d'una empresa en poder comportar l'aturada de processos o activitats crítiques per a la continuïtat del negoci. Disposar de clàusules específiques al contracte amb el proveïdor, disposar d'un procés intern de gestió de canvis que requereixi haver testejat correctament i disposar de còpies de seguretat per a poder tornar a la situació anterior serien mesures caldria contemplar. En darrera instància no s'hauria d'oblidar disposar de procediments de contingència documentats per a

poder realitzar manualment les activitats automatitzades que hagin estat interrompudes.

- Incompliment legal (Amenaça): En el cas que el robot tracti dades sensibles cal garantir el compliment de la GDPR.
- No disposar de monitorització adequada sobre els robots software (Vulnerabilitat): És important tenir tota la traçabilitat possible. En aquest sentit cal que els robots software disposin de credencials específiques i que no utilitzin les mateixes que les dels usuaris existents per a poder saber qui ha fet què.
- Falta de control d'errors i d'excepcions de l'eina d'automatització (Vulnerabilitat): Impliquen un risc per a la integritat de les dades. En aquesta situació caldria aplicar controls de validacions manuals que hauria de fer forçosament un humà.
- Segregació de responsabilitats (Vulnerabilitat): Aplicar un model de treball en el qual el desenvolupador és diferent a la persona que testeja el correcte funcionament abans de permetre aplicar un codi en un entorn productiu seguint un procediment definit de gestió de canvis. En el cas de no respectar-se es corre el risc d'aturar activitats critiques de l'empresa que podrien posar en risc la continuïtat del negoci.
- Formació insuficient dels desenvolupadors (Vulnerabilitat): Les eines actual d'automatització permeten automatitzar de forma senzilla sense implementar complexos scripts. Especialment amb les eines de RPA s'utilitza com un argument comercial indicar que es pot automatitzar sense tenir un perfil desenvolupador. Cal tenir en compte però que sense una formació adient augmenta considerablement el risc d'alteració i destrucció de la informació. A banda aquests usuaris acostumen a emprar les seves credencials als robots i ells mateixos implementen i validen els seus robots sense tenir en compte les bones pràctiques esmentades anteriorment.

4.2 Tractament dels riscos

Existeixen diferents estratègies de tractament de riscos. Una de les més àmpliament difoses es basa senzillament en quatre accions: mitigar, eliminar, acceptar o transferir el risc.

A l'apartat anterior s'ha vist que la major part dels principals riscos es corresponen amb amenaces i vulnerabilitats relacionades directa o indirectament amb la operativa i la gran majoria no es poden considerar encara com aplicables en la situació actual. Si que s'ha pogut confirmar l'existència de risc principalment sobre la confidencialitat de la informació degut a l'amenaça i a les vulnerabilitats següents:

- Ús de credencials privilegiades
- No disposar d'un control d'accés segur a l'eina
- Credencials guardades en repositoris no xifrats o escrites directament al codi.

Com veurem a continuació tractant dita amenaça i vulnerabilitats s'estarà tractant el risc associat que poden comportar.

Ús de credencials privilegiades

Revisant els usuaris específics creats inicialment amb TheHive i Cortex s'ha vist que l'usuari "n8n" s'havia creat amb credencials privilegiades i s'ha procedir a esmenar-ho traient aquest permís a l'usuari. Degut a errors de funcionament inicial entre Cortex i TheHive va ser necessari fer diferents proves fins aconseguir solucionar-ho i una de les proves va consistir en donar permisos d'administrador a l'usuari. Tot i que a posteriori es va veure que l'error no era degut als permisos no es va treure aquest permís a l'usuari situació que perfectament es podria donar en un entorn productiu sense una política de gestió de canvis adient.

Control d'accés segur a l'eina

La instal·lació per defecte de n8n no disposa de cap tipus d'autenticació al control d'accés i, com s'ha vist anteriorment a la figura 11, en obrir la url a l'explorador ja es podia començar a implementar o consultar automatitzacions existent.

A la documentació de l'eina [30] s'explica les diferents alternatives disponibles i en aquest cas en concret s'ha optat per a habilitar una autenticació bàsica a través de les variables d'entorn disponibles. Per a aconseguir-ho s'ha creat un fitxer "n8n.service" al directori /etc/systemd/System/ que permet iniciar i aturar n8n com un servei més. A la figura 30 es poden veure els valors d'aquestes variables per a aconseguir arrencar l'aplicació n8n i habilitar l'accés amb unes credencials bàsiques a partir de les variables d'entorn N8N_BASIC_AUTH_XXX (s'ha aplicat les mateixes credencials per defecte de csirt-kit).

A continuació s'ha habilitat el protocol HTTPS (podent escollir el port 443 o utilitzar el per defecte de l'eina 5678) i finalment ha estat necessari indicar el certificat que s'utilitzarà que s'ha hagut de generar prèviament optant per un certificat auto-signat per a poder validar el correcte funcionament (veure figura 31). La versió de OPENSSL disponible a l'entorn de treball es pot veure que és antiga i no s'ha actualitzat a l'hora de realitzar la prova però dita actualització si que seria necessària a un entorn productiu.

```
  GNU nano 3.2                  /etc/systemd/system/n8n.service

[Unit]
Description=n8n

[Service]
Restart=always
//ExecStart=/usr/bin/node $HOME/.npm-global/lib/node_modules/n8n/bin/n8n
ExecStart=/root/.nvm/versions/node/v14.16.0/lib/node_modules/n8n/bin/n8n
//ExecStart=/usr/bin/n8n
//ExecStart=/home/csirt-kit/n8n
//ExecStart=/usr/local/bin ../.nvm/versions/node/v14.16.0/lib/node_modules/n8n/bin/n8n
//ExecStart=/usr/local/bin/n8n
//Environment="VUE_APP_URL_BASE_API=https://n8n.rootkit.ch/"
//Environment="WEBHOOK_TUNNEL_URL=https://n8n.rootkit.ch/"
Environment="N8N_BASIC_AUTH_ACTIVE=true"
Environment="N8N_BASIC_AUTH_USER=csirt-kit"
Environment="N8N_BASIC_AUTH_PASSWORD=csirt-kit"
//Environment="N8N_PORT=443"
Environment="N8N_PORT=5678"
Environment="N8N_LISTEN_ADDRESS=127.0.0.1"
Environment="GENERIC_TIMEZONE=Europe/Andorra"
Environment="N8N_PROTOCOL=https"
Environment="N8N_SSL_KEY=/home/csirt-kit/servidor.key"
Environment="N8N_SSL_CERT=/home/csirt-kit/servidor.pem"
```

```
root@CSIRT-KIT-NG:/etc/systemd/system# nano n8n.service
root@CSIRT-KIT-NG:/etc/systemd/system# systemctl daemon-reload
root@CSIRT-KIT-NG:/etc/systemd/system# sudo systemctl enable n8n
root@CSIRT-KIT-NG:/etc/systemd/system# sudo service n8n start
root@CSIRT-KIT-NG:/etc/systemd/system# sudo service n8n status
● n8n.service - n8n
   Loaded: loaded (/etc/systemd/system/n8n.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-05-01 17:59:49 UTC; 4s ago
 Main PID: 26328 (node)
    Tasks: 11 (limit: 4915)
   Memory: 149.1M
   CGroup: /system.slice/n8n.service
           └─26328 node /root/.nvm/versions/node/v14.16.0/lib/node_modules/n8n/bin/n8n

may 01 17:59:49 CSIRT-KIT-NG systemd[1]: Started n8n.
may 01 17:59:53 CSIRT-KIT-NG n8n[26328]: UserSettings got generated and saved to: /.n8n/config
```

Figura 30: Variables d'entorn del fitxer n8n.service i arrencar el servei

```
csirt-kit@CSIRT-KIT-NG:~$ openssl version
OpenSSL 1.1.1d  10 Sep 2019
csirt-kit@CSIRT-KIT-NG:~$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650
-nodes -keyout servidor.key -out servidor.crt -subj /CN=localhost -addext subjec
tAltName=DNS:localhost,IP:127.0.0.1
Generating a RSA private key
.........................................++++
..............++++
writing new private key to 'servidor.key'
-----
csirt-kit@CSIRT-KIT-NG:~$
```

```
csirt-kit@CSIRT-KIT-NG:~$ cat servidor.key servidor.crt > servidor.pem
csirt-kit@CSIRT-KIT-NG:~$ openssl x509 -in servidor.crt -out servidor.pem
```

Figura 31: Generació de certificat auto-signat i conversió a format .pem

Després de fer els canvis esmentats anteriorment al port 443 es pot validar com l'inici de l'aplicació requereix de les credencials configurades i el servei s'aixeca correctament en HTTPS havent d'acceptar el risc de l'ús del certificat de prova que no ha estat emès per una entitat certificadora de confiança.

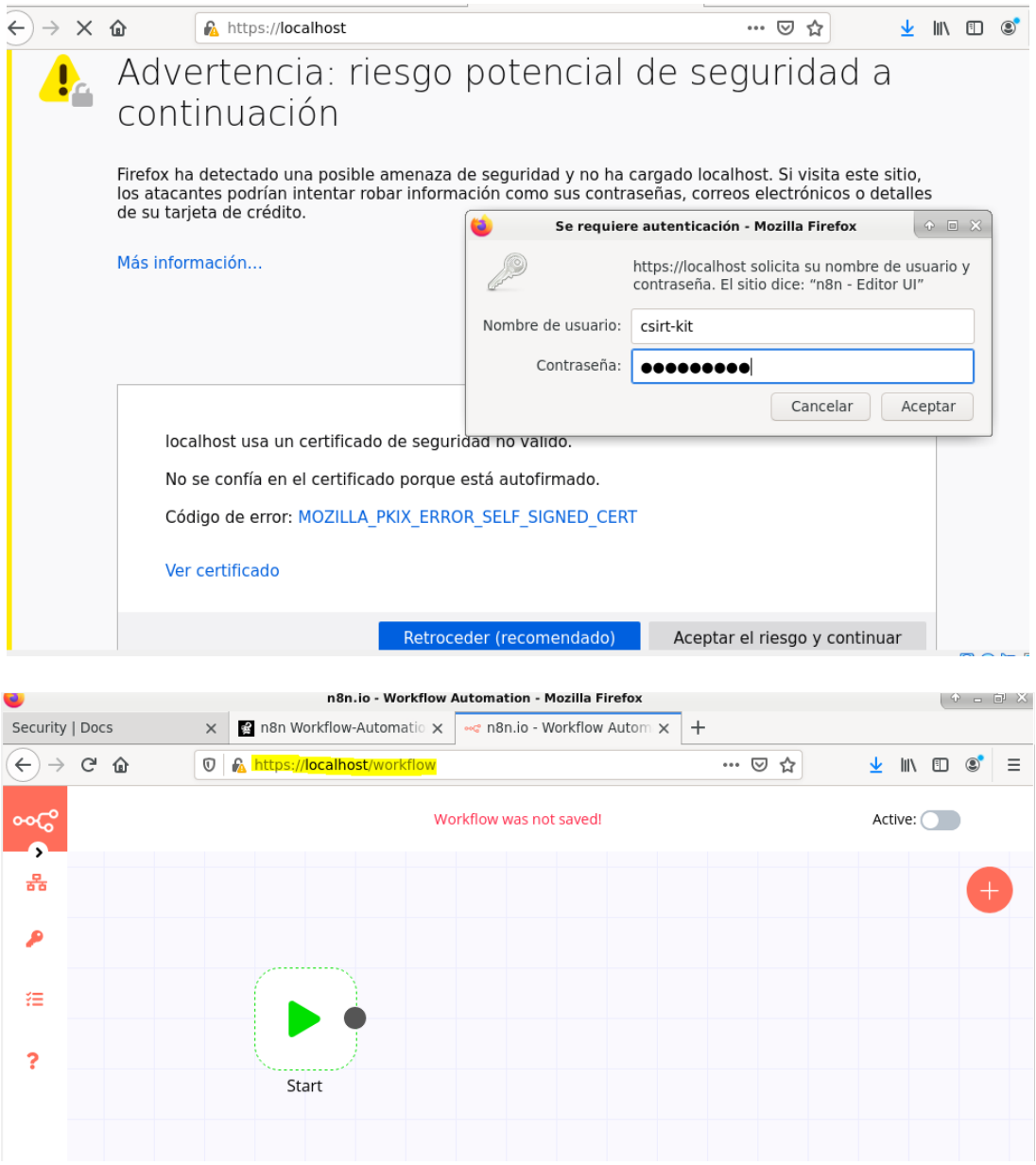


Figura 32: Evidències inici n8n amb autenticació bàsica i HTTPS habilitat

Credencials guardades en repositoris no xifrats o escrites directament al codi

Aquestes vulnerabilitats apliquen específicament a l'eina RPA Python donat que n8n encripta les credencials a partir d'una clau que es crea al moment de la instal·lació de l'eina [30] i aquesta alternativa no està disponible en RPA Python per defecte. Encara que per a la implementació del cas d'ús proposat no ha estat necessari emprar aquesta opció, donat que s'han utilitzat les eines en les que ja s'està enregistrat, en el cas de voler implementar altres robots software de forma autònoma amb aquesta eina, sense requerir que l'usuari afegeixi manualment les credencials, seria necessari cobrir aquesta necessitat. S'ha comprovat que existeixen alternatives que permeten aplicar gestió de credencials en Python [31] per a mitigar la vulnerabilitat que presenta l'eina.

4.3 Conclusions

Com s'ha pogut veure en aquest apartat fent un bon ús de les eines de codi obert i gratuïtes que s'han posat en pràctica (n8n i RPA Python) és possible mitigar o fins i tot eliminar els riscos sobre la seguretat de la informació que implica fer ús d'eines d'automatització. Tot i així cal posar de manifest que hi ha molts dels riscos que estan directament relacionats amb la seva posada en producció i el tipus d'ús que es pugui arribar a fer d'aquestes eines. És per aquesta raó que les bones pràctiques aconsellen que s'implementin controls concrets per a mitigar aquest riscos així com disposar d'una política de Govern i un procés de control de canvis que en regulin la seva activitat.

5. Glossari

API (Interfície de programació d'aplicacions): Conjunt de regles que permeten la comunicació entre dues aplicacions.
GDPR (Reglament General de Protecció de Dades): Reglament Europeu de protecció de dades (UE) 2016/679
HIDS: Sistema de detecció d'intrusos per a hosts.
IA: Intel·ligència Artificial
iBPMS (Intelligent Business Process Management System): terme emprat per Gartner per a definir les eines intel·ligents de gestió de processos.
JSON (JavaScript Object Notation): és un estàndard obert basat en text dissenyat per a l'intercanvi de dades llegible pels humans. Deriva del llenguatge JavaScript, per a representar estructures de dades simples i llistes associatives que s'anomenen objectes.
OVA (Format de virtualització obert): És un estàndard obert per a empaquetar i distribuir programes informàtiques que s'executaran en una Màquina Virtual.
RPA (Automatització robòtica de processos): És una tecnologia que permet configurar un robot software per a interpretar les aplicacions existents i poder comunicar-se amb altres sistemes digitals.
Script: és un conjunt d'ordres guardades en un arxiu que s'executa línia a línia o per blocs en temps real per un programa que interpreta les instruccions convertint-les a llenguatge màquina per a que puguin ser processades i executades per un ordinador.
SIEM: Terme creat per Gartner que sorgeix d'unir el SIM (Security Information Management) i SEM (Security Event Management) que fan referència a l'anàlisi en temps real d'alertes de seguretat.
SO (Sistema Operatiu): És el conjunt de programes d'un sistema informàtic que gestiona els recursos físics i proveeix de serveis a les aplicacions.
SOAR: terme creat per Gartner per a definir els sistemes d'orquestració, automatització i resposta d'incidents de seguretat.
SOC (Centre d'Operacions de Seguretat): Equip que gestiona incidents de seguretat.
SPAM: Terme emprat actualment per a definir qualsevol comunicació no sol·licita i enviada de forma massiva. Principalment aquesta situació es sol donar amb els correus electrònics però també pot donar-se amb els missatges de text o les xarxes socials.
UI (Interfície d'usuari): És l'element que permet la comunicació o interacció entre l'usuari i l'aplicació.
Webhook: És un sistema de comunicació en temps real entre aplicacions web. No s'ha de confondre amb una API, tot i que aquesta pot fer la mateixa funció, en general la comunicació es fa de forma periòdica i són més flexibles.

6. Bibliografia

[1] *csirt-kit*[en línia][data consulta:17/02/21].Disponible a: https://csirt-kit.org/
[2] Zamora Nelson, Rodrigo. Evolución de Appliance CSIRT-KIT. Treball final de màster: València,2020.
[3] Miers,D.;Kerremans,M.;Ray,S.; Tornbohm,C. Magic Quadrant for Robotic Process Automation Software[en línia].2019. Pàg1-40.ID G00379618.[Consulta:20/02/2021]. Disponible a:
https://b2bsalescafe.files.wordpress.com/2019/09/gartner-magic-quadrant-for-robotic-process-automation-software-july-2019.pdf
[4] Ray,S;Villa,A;Tornbohm,C;Rashid,N.Alexander,M. Magic Quadrant for Robotic Process Automation Software[en línia].2020. Pàg1-29. ID G00441474. [Consulta:23/02/2021].Disponible a:
http://www.project-consult.de/files/Gartner_MQ_RPA_2020.pdf
https://www.gartner.com/doc/reprints?id=1-1ZK435W1&ct=200728&st=sb&mkt_tok=OTk1LVhMVC04ODYAAAF7g82qaBklVX1aAa89vl4XgzRxzeuD-5dneRfvxWrgtzBUeqiONWfBUtzjI8vot7F1fVPHuO29HNqlo5Wrk9YGr7TOH_8Sjb7QXE7OCDI
[5] La RPA cognitiva eleva la inteligencia a otro nivel[en línia][data de consulta:27/02/2021].Disponible a: https://www.vectoritcgroup.com/tech-magazine/artificial-intelligence/la-rpa-cognitiva-eleva-la-inteligencia-a-otro-nivel/
[6] RPA e IA: Nuevos riesgos y oportunidades en Ciberseguridad[en línia][data de consulta:28/02/2021].Disponible a: https://www.a2secure.com/blog/rpa-e-ia-nuevos-riesgos-y-oportunidades-en-ciberseguridad/
[7] Seminari online ofert per Cloudadmins respecte l'evolució del CSIRT-KIT[en línia][data de consulta:04/03/2021]. Disponible a: https://www.csuc.cat/ca/noticia/el-csuc-participa-al-meetup-cybersecurity-operations-e-techday-barcelona)
[8] IntelMQ[en línia][data de consulta:04/03/2021]. Disponible a:
https://github.com/certtools/intelmq
[9] Wazuh [en línia][data de consulta:04/03/2021]. Disponible a:
https://wazuh.com/
https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/how-it-works.html
[10] Elasticsearch [en línia][data de consulta:04/03/2021]. Disponible a:
https://www.elastic.co/es/
[11] Packetbeat [en línia][data de consulta:05/03/2021]. Disponible a:
https://www.Elastic.co/es/beats/packetbeat
[12] TheHive [en línia][data de consulta:05/03/2021]. Disponible a:
https://thehive-project.org/
[13] Cortex [en línia][data de consulta:10/03/2021]. Disponible a:
https://github.com/TheHive-Project/CortexDocs
[14] CSIRT-KIT[en línia][data de consulta: 30/03/2021]. Disponible a:
https://csirt-kit.org/
[15] Comunitat n8n[en línia][data de consulta: 30/03/2021]. Disponible a:
https://comunidad-n8n.com/instalacion-con-npm/

[16] RPA-Python[en línia][data de consulta: 30/03/2021]. Disponible a: https://github.com/tebelorg/RPA-Python
[17] detall instal·lació OpenCV i Tesseract [en línia][data de consulta: 30/03/2021]. Disponible a: https://sikulix-2014.readthedocs.io/en/latest/newslinux.html
[18] Error OPENSSL i solució [en línia][data de consulta: 31/03/2021]. Disponible a: https://github.com/dotnet/runtime/issues/27792
[19] nodes disponibles a n8n [en línia][data de consulta: 03/04/2021]. Disponible a: https://n8n.io/integrations
[20] error webhook no regitrat solució [en línia][data de consulta: 05/04/2021]. Disponible a: https://community.n8n.io/t/webhook-the-requested-webhook-is-not-registred/184
[21] informació sobre instal·lació dels analitzadors i actuadors de Cortex [en línia][data de consulta: 10/04/2021]. Disponible a: https://github.com/TheHive-Project/CortexDocs/blob/master/installation/install-guide.md#installation
[22] Cortex creació d'actuadors personalitzats [en línia][data de consulta: 20/05/2021]. Disponible a: https://github.com/TheHive-Project/CortexDocs/blob/master/api/how-to-create-a-responder.md
[23] Cortex responder Wazuh [en línia][data de consulta: 20/05/2021]. Disponible a: (https://thehive-project.github.io/Cortex-Analyzers/responders/Wazuh/
[24] Wazuh scripts de resposta pre-configurats [en línia][data de consulta: 21/05/2021]. Disponible a: https://documentation.wazuh.com/current/user-manual/api/reference.html#operation/api.controllers.default_controller.default_info
[25] Wazuh script login a la API [en línia][data de consulta: 22/05/2021]. Disponible a: https://documentation.wazuh.com/current/user-manual/api/getting-started.html#logging-into-the-wazuh-api-via-scripts
[26] Creating a Robust Controls System for RPA Programs [en línia][data de consulta: 24/05/2021]. Disponible a: https://digital.gov/pdf/rpa-playbook-ic-addendum-v1.0.pdf
[27] RPA e IA: Nuevos riesgos y oportunidades en Ciberseguridad [en línia][data de consulta: 24/05/2021]. Disponible a: https://www.a2secure.com/blog/rpa-e-ia-nuevos-riesgos-y-oportunidades-en-ciberseguridad/
[28] Automatización Robótica de Procesos (RPA) [en línia][data de consulta: 25/05/2021]. Disponible a: https://www.cyberark.com/es/what-is/robotic-process-automation/
[29] 10 riesgos de seguridad en Robotics Process Automation (RPA) [en línia][data de consulta: 26/05/2021]. Disponible a: https://ciberseguridad.blog/10-riesgos-de-seguridad-en-robotics-process-automation-rpa/
[30] n8n security configuration [en línia][data de consulta: 26/05/2021]. Disponible a: https://docs.n8n.io/reference/configuration.html#security
[31] Vault Python password manager [en línia][data de consulta: 29/05/2021]. Disponible a: https://github.com/gabfl/vault