Market France

CACF **Incident Remediation growth**

project closure report

Radoslaw (Radek) Pawlowski
A&O PM

Purpose of document

Project : Event Automation upgrade & Incident Remediation growth on FR accounts.

Goal : Grow successful incident remediation performed by CACF from account events.

Purpose : Present the results and lessons of Incident Remediation growth actions performed on top account(s) in CACF-ANSIBLE,

involving :

- OS / DB admins,
- TAA,
- SRE when named,

coached by FR A&O experts

Conclusions, main lessons

To maximize Event / Incident Remediation outcomes, **team of senior admins and TAA shall work on actions, under SRE lead**, in agile mode.

These actions shall be defined and prioritized **according to AIOPS data** (KSI Inc. Automation insight) and **automation execution results.**

- **Event Automation role configuration, tuning, upgrade** actions shall increase successful remediations.
- **Ansible CMDB timely updates** and **maximum endpoints connectivity %** shall decrease the count of escalations / failures to execute playbook
- **Account admins** and **TAA** shall **take Global and France learnings** to become familiar with Event Automation administration and continuous improvement.

How to access AIOPS – Kyndryl Service Insights (KSI) : follow the link

Event Automation Bootcamp

Must read for all Senior admins, TAA, SRE, PM

The purpose of **Event - Incident Automation Boot Camp** is to provide practical education material / guides to help delivery teams increase their skills, knowledge and practices in this area, leveraging at best the AIOPS and CACF capabilities and information.

Available from github or in box :

https://github.kyndryl.net/firat-say/eventautomationbootcamp

Besides this, you find material such as

- Step by step **guide to test, fix and validate an Event Automation playbook** from event generated on endpoint ;

  https://kyndryl.box.com/s/ysigwdqfu5ddyjmv1cwasla18fqqapwn

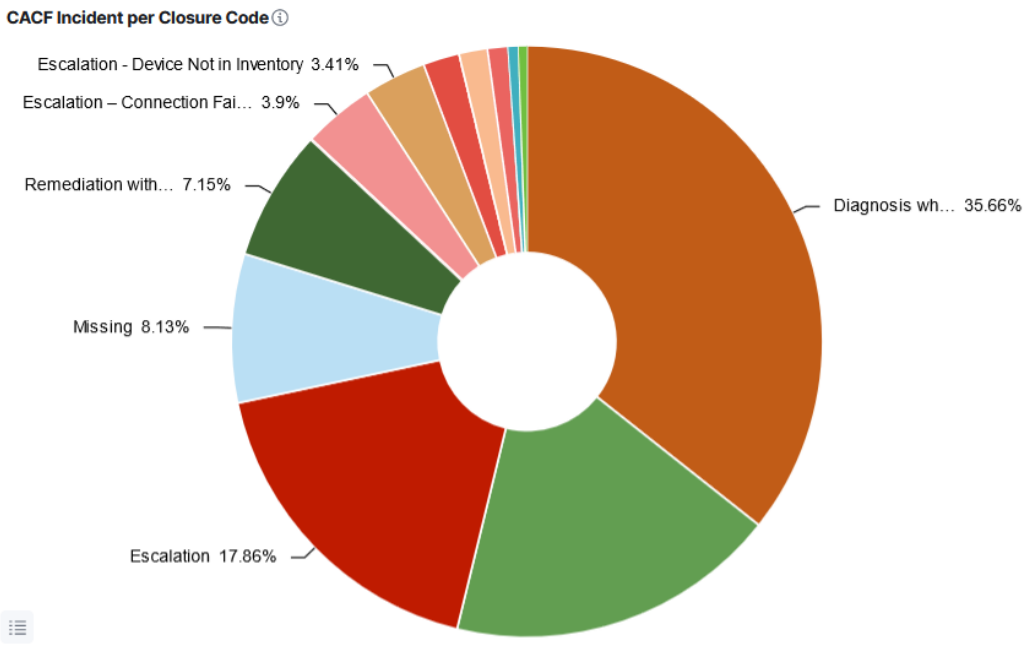
- CACF **Incident Remediation growth project closure report** providing conclusions and lessons to help teams in the Event Automation continuous improvement / BAU … (this prez ☺)

  https://kyndryl.box.com/s/0u2sczkzz417lqovmedsj49uqho0mzlq

Incident Remediation under KSI (AIOPS)

KSI Event Automation results / return-code

Running Event Automation may give various results …



Execution result	Details
Remediation with corrective closure	Incident cause remediated by playbook ; ticket resolved and closed automatically in ISM
Remediation with validation closure	Incident cause on endpoint was cleared, validated by playbook ; ticket closed automatically in ISM
Diagnosis when remediation failed	Incident cause diagnosis (data collection) was done while playbook could not run remediation on Endpoint ; ticket escalated to support group in ISM
Missing	Pending RC from Event Automation execution on EndPoint ; ticket may end up in one of above states.
Escalation	Event Automation could not be triggered for event received in NEXT ; ticket escalated to support group.
Escalation – connection failed	Event Automation could not run due to Endpoint not reachable ; ticket escalated to support group.
Escalation – device not in inventory	Event Automation could not run due to Endpoint not in Ansible CMDB ; ticket escalated to support group.
Escalation – automata execution interrupted	Event Automation playbook execution failed (could be a bug in playbook code) ; ticket escalated to support group.
Escalation – device exluded from automation	Event Automation could not run due to Endpoint blacklisted? in Ansible CMDB ; ticket escalated to support group.
Escalation – event / incident excluded from automation	Event Automation could not run due to <to be described>; ticket escalated to support group.

KSI: https://data.managed-solutions.cloud.ibm.com/dashboards/dashboard/17fc497d-18e8-4396-93de-98041c9f3291?accountId=delivery

Incident Remediation / France Market

Top contributors for failed remediation / event automation

Among the 5 biggest accounts, the most frequent event automations are :

1. **Disk usage alert**
2. **Process handler**
3. **Server unavailable**
4. **System disk cleanup and disk usage**

EA playbook / role Return Codes explanation can be found under Continuous Engineering /pages below:
https://github.kyndryl.net/orgs/Continuous-Engineering/repositories

Below is an example of a KSI report of Event Automation playbooks failing to complete remediation for some reason.
RC gives the opportunity to understand the cause and address it.
Count tells you how many times we got this unsuccessful result.

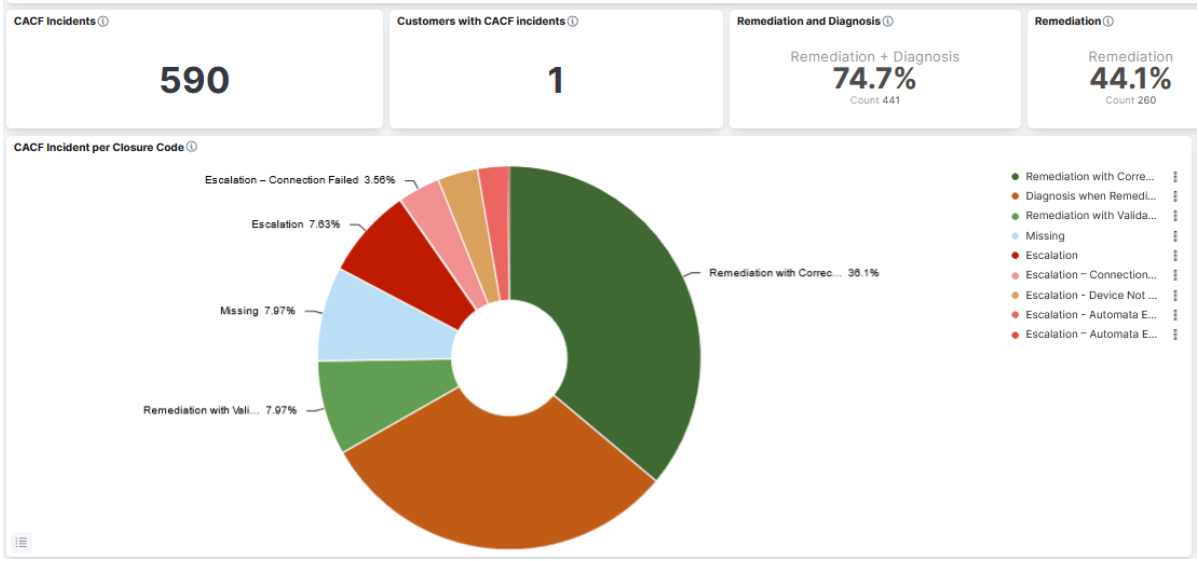
Playbook Name	Return Code	Count
disk-usage-alert	3009	471
process-handler	1000	403
disk-usage-alert	3008	256
tsm-missed-and-failed-backup	1000	180
logfile-statistics-monitor	3500	156
itm-agent-offline	3005	144
server-unavailable	3001	137
memory-consumption-checker	3000	125
tsm-missed-and-failed-backup	3501	114
system-disk-cleanup-and-disk-usage	3000	105
cpu-aggregate-high-handler	3001	77
check-errpt-alert	3001	73

Incident Remediation / France Market

Zoom on account actions outcome : **Schneider**

Global targets for Inc. remediation :
30% of remediation with corrective closure

From May 23 to 29,
CACF managed **590** incidents, automated almost **75%** of them, closed automatically **44%,** corrected & closed **36% of them**



Event type	Week 14	Week 15	Week 16	Week 17
Missing	54	32	26	40
High memory handler	8	7	3	11
Server unavaliable	8	24	0	12
Disk usage alert	11	27	19	24
Device not in the inventory	6	16	96	5

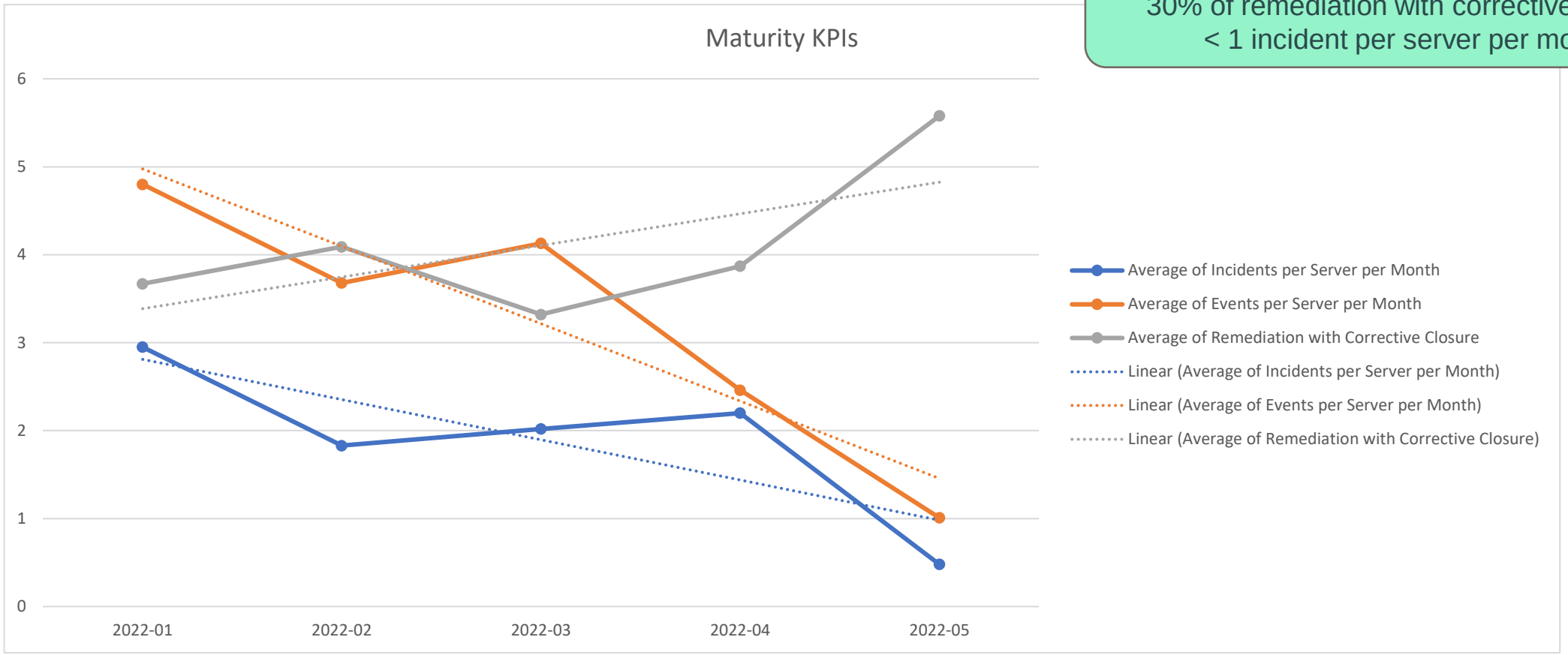
1. Missing
   - When EA playbooks are launched and not finished yet, this counter is increasing accordingly.
2. High memory handler
   - Playbook had a bug thus team used a custom version (Firat opened issue #1556 to CACF). Account enabled default version of the playbook – brought some remediation but pending a bug fix for final outcome
3. Server unavailable
   - Server up → remediation with validation ; Server down → remediation failed (no way to get a corrective closure in this case).
4. Disk usage alert
   - FS missing are for SAP instance IDs (not available currently) → to be backlisted
5. Device not in Inventory :
   - monitoring not disabled after decommission chg
   - Endpoint not loaded in Ansible CMDB yet though moved in prod.

kyndryl

Incident Remediation / France Market

Trend of outcomes / account : **Schneider**

Global targets for Inc. remediation :
30% of remediation with corrective closure
< 1 incident per server per month



Row Labels	Average of Incidents per Server per Month	Average of Events per Server per Month	Average of Remediation with Corrective Closure
2022-01	2.95	4.8	3.67
2022-02	1.83	3.68	4.09
2022-03	2.02	4.13	3.32
2022-04	2.2	2.46	3.87
2022-05	0.48	1.01	5.58
Grand Total	**1.896**	**3.216**	**4.106**

Appendix - Register of corrective actions

Disk usage alert

- RC 3009
  - SCS : FS is missing in the config.yml file in the role -> check instance IDs , instance ID can be configured in the role
  - on SAP, ORACLE there is may not be an EA playbook available yet.
    → Eventually SAP SMEs should work with FR DevOps on new playbook development (raise the request)
  - SGI : App logs belong to client application -> account to agree with the client to add additional rule to zip or remove the log
- RC 3008
  - SGI : app logs belongs to client application -> SMEs are working redirecting those logs to different FS or event reduction or to archive the logs, in the meantime log retention decreased.
- CMA : Cleanup rule to be added to the Event Automation role for the top contributing File Systems

Process handler

- CMA : some alerts cannot be remediated due to missing processes in EA playbook config.yml (taken from instance ID list out of KSI report)

Appendix - Register of corrective actions

Server unavailable

- CFR : Waiting time increase might help
- The playbook works like this: if server is up -> validation closure; if server is down -> remediation failed (not possible to move from validation closure to corrective closure)

System disk cleanup & disk usage

- CMA : Alerts pointing to SQL servers -> rule in BlueCare to be set (clear the ticket and create incident directly to resolver group); most contributing drive to have capacity added

High memory handler

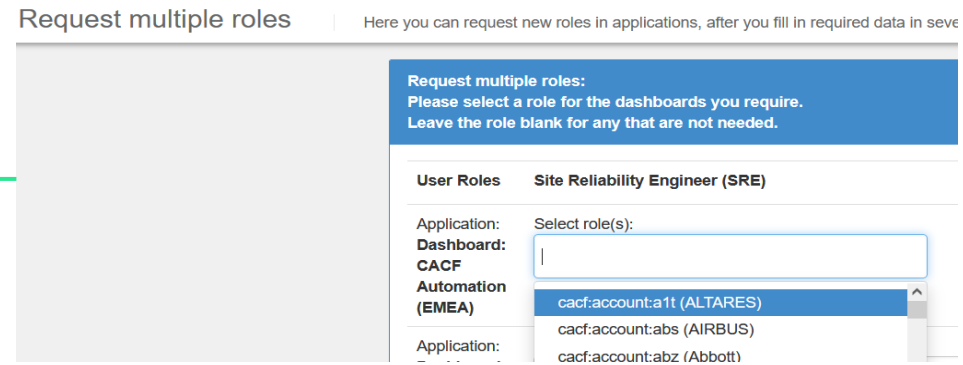
- CFR : RC 3001 points to svc process config
- SCS : Bug in the playbook (issue #1556) -> ongoing

Memory consumption checker

- SGI : RC 3000 -> account to track which application is causing this memory consumption and in which hours → talk with client if possible to increase the capacity (assuming that this is job scheduled by the client and it must stay like that) OR to get approval from the client to ignore that alert

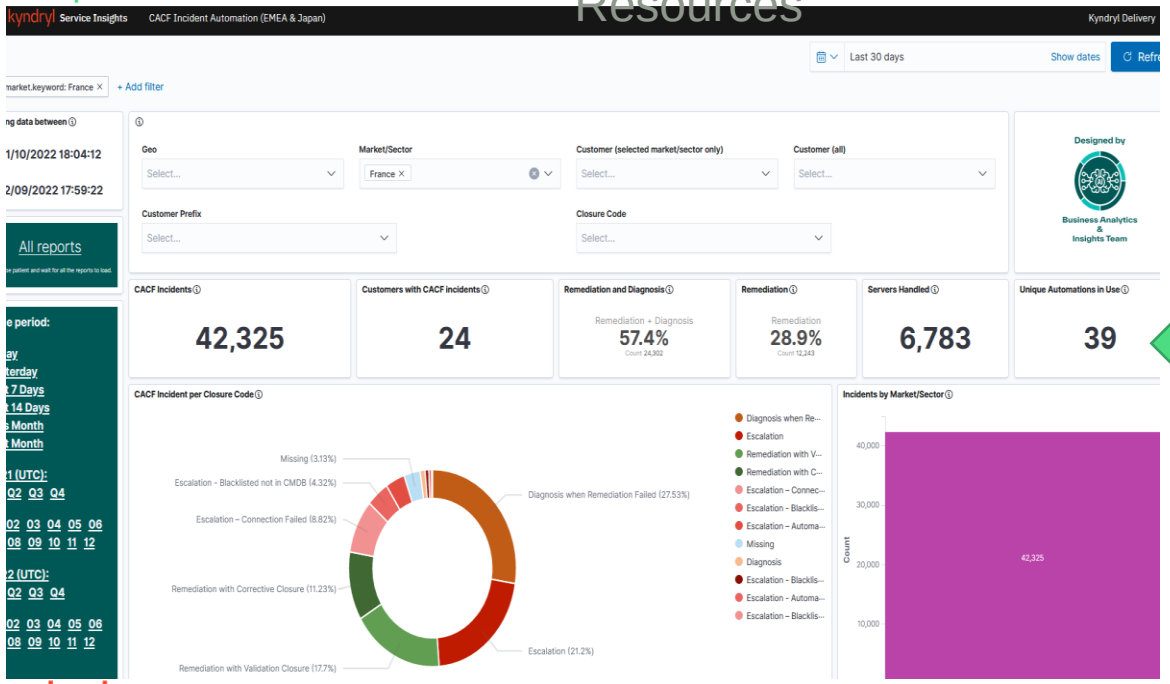
Resources
Access AIOPS – Kyndryl Service Insights (KSI)

- Procedure to get access, select needed dashboards / insights and use KSI : https://pages.github.kyndryl.net/delivery/insights/dash-access
- Link to AIOPS **KSI platform :** https://data.managed-solutions.cloud.ibm.com/dashboards?accountId=delivery
- lunch & Learn **KSI demo session :** https://ec.yourlearning.ibm.com/w3/meeting/10180103



Start with those 2 …

Snapshot to INCIDENT AUTOMATION KSI dashboard …



AIOPS – KSI dashboard & insights ‘menu’	
CACF Automation (EMEA)	1. ALL automations = HC-Compliance, Incident & Other automation execution → **Account Ansible Automation insights** 2. EVENTS / INCIDENT automations → **Incident Remediation insights** (KPI: Automated corrective closure)
Event Noise Reduction (EMEA)	3. MNE / Event Reduction insights, → **volume & type of events / top contributors, auto-ticketing status and remediation palybook opportunities** (KPI : Incidents / server / month)
…/…	MORE to come available soon !

kyndryl

Thank you
and
KEEP IT UP ☺