IBM Cloud Platform
Security & Compliance Center :

Exploring the ways in which enterprise security functions achieve GRC goals and overall perceptions on CSPM tools

Mixed Methods
Foundational study

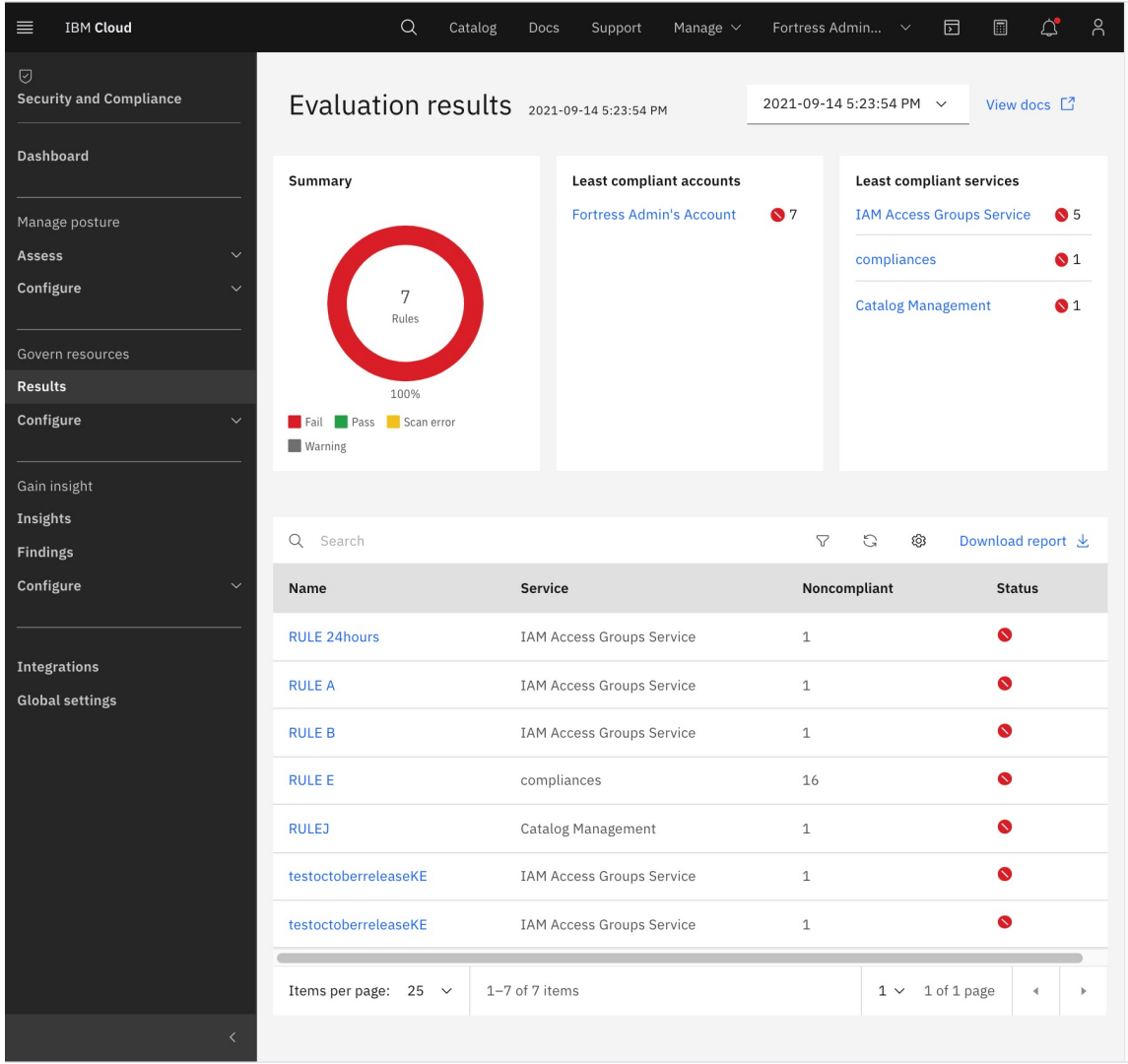
Helping product management, engineering and design stakeholders gain insight into the type of users and usecases that Security and Compliance Center needs to serve in order to determine design and architecture direction as well as product roadmap prioritization.

Background

Security and Compliance Center is positioned as IBM Cloud's Platform CSPM tool which will help organizations achieve continuous posture management.

SCC was first launched in 2020 after the acquisition of a compliance tool called Spanugo in order to accelerate the general availability of this tool as a part of a mission critical strategy to capture the financial services cloud market

Today SCC's various homegrown and acquired components are architected as 3 pillars/silos where there are many overlapping functions. Maintaining these separate architectures is no longer scalable and has caused SCC's end to end UX to be considered suboptimal.



“We know that we need to redefine the architecture and UX, our architects have some ideas, but they can’t agree on a direction. What makes sense to our users?”

Product Owner - IBM Cloud Security Services

“We need to rearchitect and redesign SCC, We have 1 chance to get this right. We need to understand who we are designing this for, and what do they expect from this tool?”

Distinguished Engineer, IBM Cloud Platform Security Architect

Research Design Overview

Research Objective:

1. Understand how our current architecture is affecting the user experience/perception
2. Gain insight into the common themes, patterns, terminology and UX that our competitors have established that future SCC users may be familiar with/expect
3. Explore the overall needs of main user profiles, and their expectations or pain points using competitor CSPM tools
4. To identify opportunities for differentiators and delightful end to end UX for each user profile

Research Design

Phase 1:

- Figure out where we are in comparison to competition

Phase 2:

- Understand who users of our competitors are and how they are using those tools and what their expectations are

Phase 3:

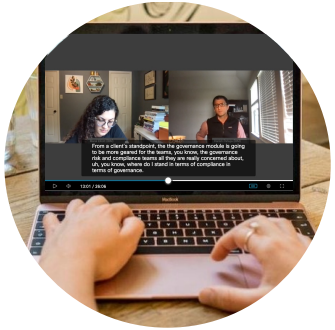
- Specific lean deep dives as needed

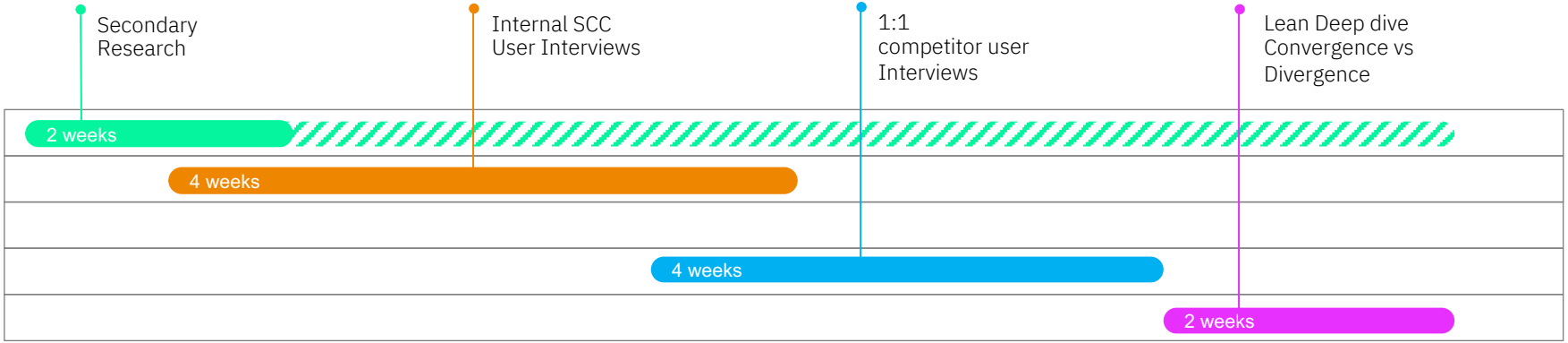
Phase 4 (WIP):

- Prioritize features and capabilities

Research Design

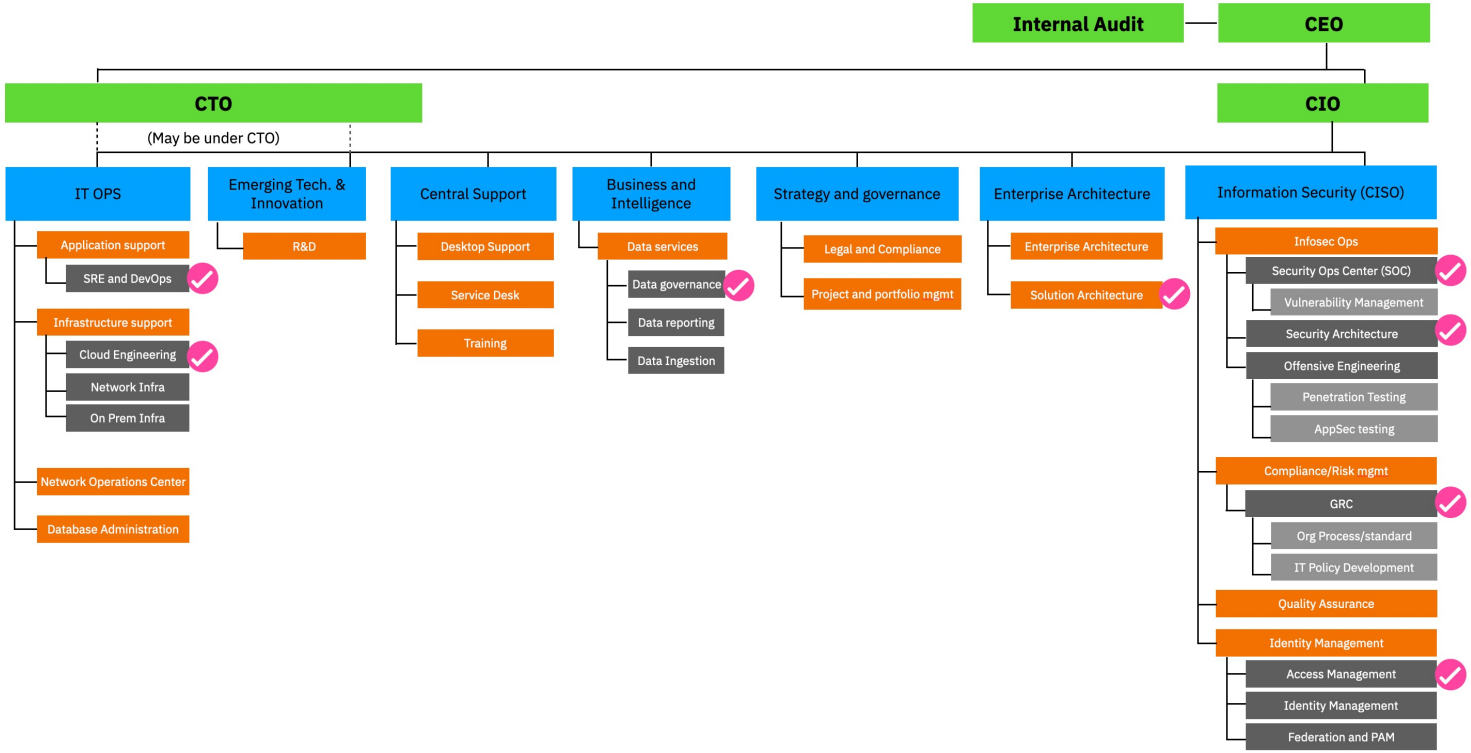
To gain a better understanding of user's expectations from a CSPM tool and uncover opportunities to provide a delightful and differentiated UX, A mixed Methods foundational research was conducted.





Top Research Findings

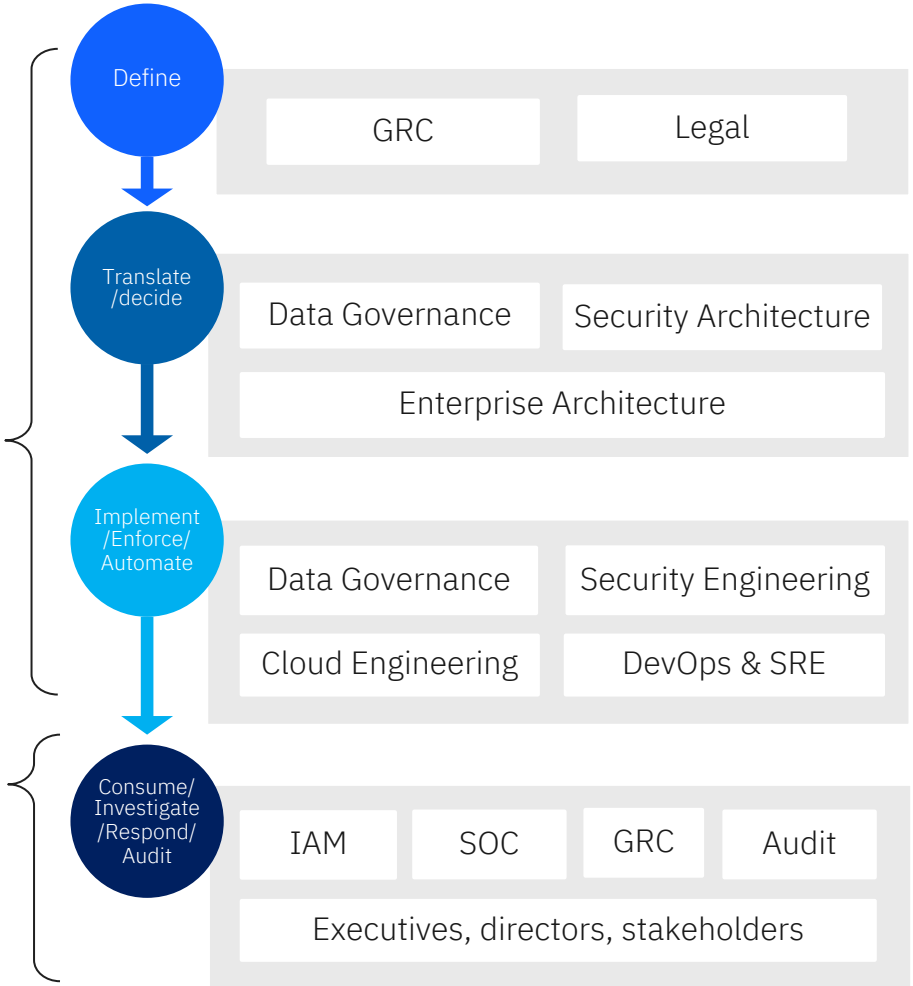
Identified all key Central IT roles involved in posture management



Identified each user profile's involvement in regulatory and security compliance posture management

Various roles within different functions work together to define, implement, and enforce policies and automate mitigation

A large array of roles are considered the consumers, investigators and auditors of findings and reports generated from a posture management tool



Examples of User Profiles/Personas

Ishan

"We do internal audit but not enough internal control testing."

We don't do a good job of managing the findings from internal audits"

Job role:
Internal Audit

Archetype:
Analyst

Team:
Internal Audit

Department:
CISO

Top responsibilities:

- Stay abreast of regulatory compliance standards, and new and emerging risks and best practices
- Develop a risk management strategy including process improvement, control design and assessments
- Develo
- Lead in
- Draft a
- Identif
- Develo
- Consul
- Ensure

Top pa

- Too m
- Difficu
- Insuffi
- Fear o
- Board
- Not pr

Top to

- Micros
- Cyber
- Certifi

Celine

"We have to go back and in investigate in multiple other tools like Splunk and Netwitness to analyze activities detected on Azure sentinel"

Job role:
Cyber Security Analyst

Archetype:
Operations

Team:
Security Operations Center - SOC

Department:
CISO

Top responsibilities:

- Detect attacks and suspicious activities. (Mitigating attacks is the goal.)
- Identify unresolved vulnerabilities, their severity, and their remediation status
- Incident response
- Monitoring logs and alerts, Investigating, and triaging
- Cyber Security Incident reporting and documenting findings

Top pain points:

- Lack of comprehensive hybrid monitoring tools. Investigating across multiple data sources is painful
- Cloud security alerts that rely on information that can only be obtained via on prem is challenging.
- Too many false positives and low quality, ambiguous alerts and lack of Machine Learning capabilities
- Dependence upon developers to remediate software security flaws which causes some friction
- Shared tools between segregated roles and lack of separate work environment
- Poor Cloud training experience.

Top tools:

- Azure Security Center
- Azure Sentinel
- Archer
- Splunk

Phase 1 and 2
Top 5 Insights & Opportunities

Onboarding environments and assets is the first and most important user experience that shapes user's expectations and perceptions of a CSPM tool

SCCs onboarding experience is considerably subpar due to requiring a labor-intensive manual step to create scopes and schedule scans. Most users are stuck at this step.

Opportunities:

- A seamless IBM onboarding UX (automatic, "One click" onboarding of IBM accounts)
- Complete and organized first view of assets inventory (Auto-classification)
- Automatic scans against best practices upon onboarding an environment

"Azure Security Center is great; It immediately gives you the inventory of all resources and shows you your secure score and if there is something that you can improve"

Cloud Solutions Architect – Ryanair

Many severe usability issues are preventing users from confidently creating scopes and moving forward with scheduling scans

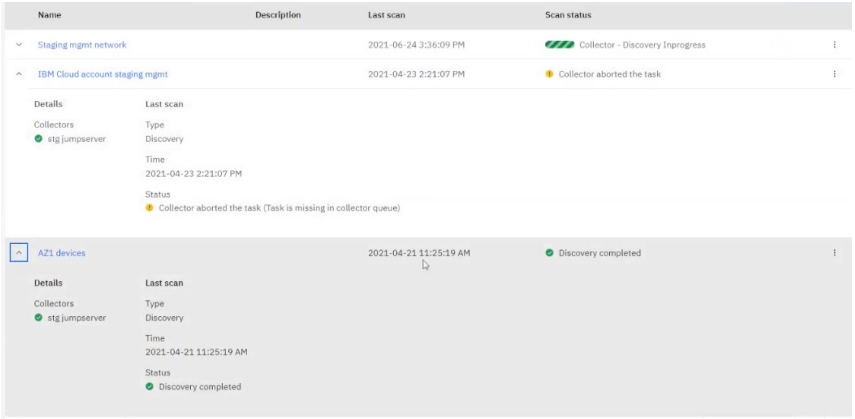
- All participants reported lack of visibility of system status and uninformative errors as some of the major hurdles when onboarding

Opportunities:

- A comprehensive heuristic evaluation to identify outstanding usability issues as well as documentation and improvement of current system status visibility handling and error messages may facilitate the onboarding process

"I was never able to make it past onboarding my environments and pulling in the inventory of resources in SCC. Too much manual stuff and too many errors that are not helpful. I'm wondering how anyone would ever be able to use this tool. It's just not a straightforward tool. And I'm not a novice person"

Software Developer - IBM Systems - IBM



Internal SCC users or Clients tend to compare SCCs capabilities with Azure, Prisma and CloudGuard and find many shortcomings that renders their perception of SCC sub par to competitors.

- Some frequently mentioned shortcomings are automatic real time scan triggers as well as predefined periodic scans (no scheduling)
- Users are more and more inclined to reduce the number of security tools and are attracted to tools that combine CSPM + CMPP capabilities

Opportunities:

- Workload protection is an attractive feature that can become a potential premium featur

Notable differentiating capabilities our competitors offer:

- Automatic discovery, categorization and initial scan of assets upon onboarding
- Workload Protection capabilities
- Powerful search and filtering
- Rule builder (Instead/in addition to JSON)
- Customizable multi dashboards
- AI + ML based Security alerts

Many existing CSPM tools do not fully address the “communication” factor between security and GRC/Audit personas

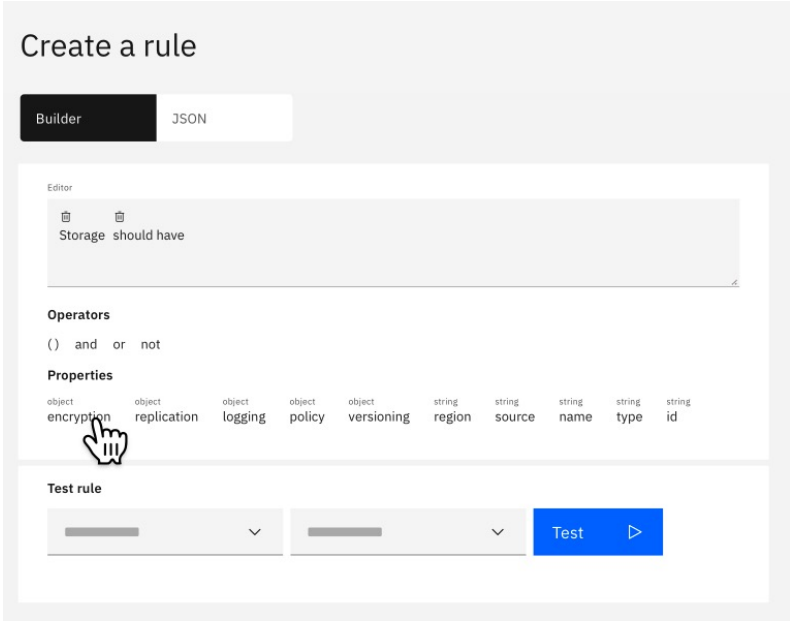
Lack of technical understanding of coded policies or lack of understanding of legal and regulatory requirements by Security SMEs is causing a communication gap

Opportunities:

- An easy to use “Rule Builder” to help internal audit and GRC in the review/audit process
- Easy to understand definitions, intent and context of each predefined individual Rule

Having the ability to have a GUI Rule builder is great for different personas but also having access to the JSON for automation purposes is as important.”

Director of cloud Security – Global Payments



A CSPM tool is expected to run periodic compliance scans on a predefined schedule once policies are assigned

Today SCC is the only CSPM tool that requires manual scheduling to start the compliance scans. This is unnecessary and time consuming.

Users do not need to schedule their own compliance scans (They preferred a predefined schedule) however, they do need a seamless on-demand scan capability for when they need an evaluation immediately.

Opportunities:

- Predefined schedules (24 hr.) rule upon assignment to an environment
- Seamless on-demand scans

"Azure Security Center runs scans on a predefined schedule, not controlled by us which is great, but we can't run on demand scans without calling the API which is a pain point. I really prefer that a CSPM tool allows for running on demand scans in the GUI. Sometimes I can't wait for the next scheduled scan, I need to see if my actions had an affect on the posture NOW"

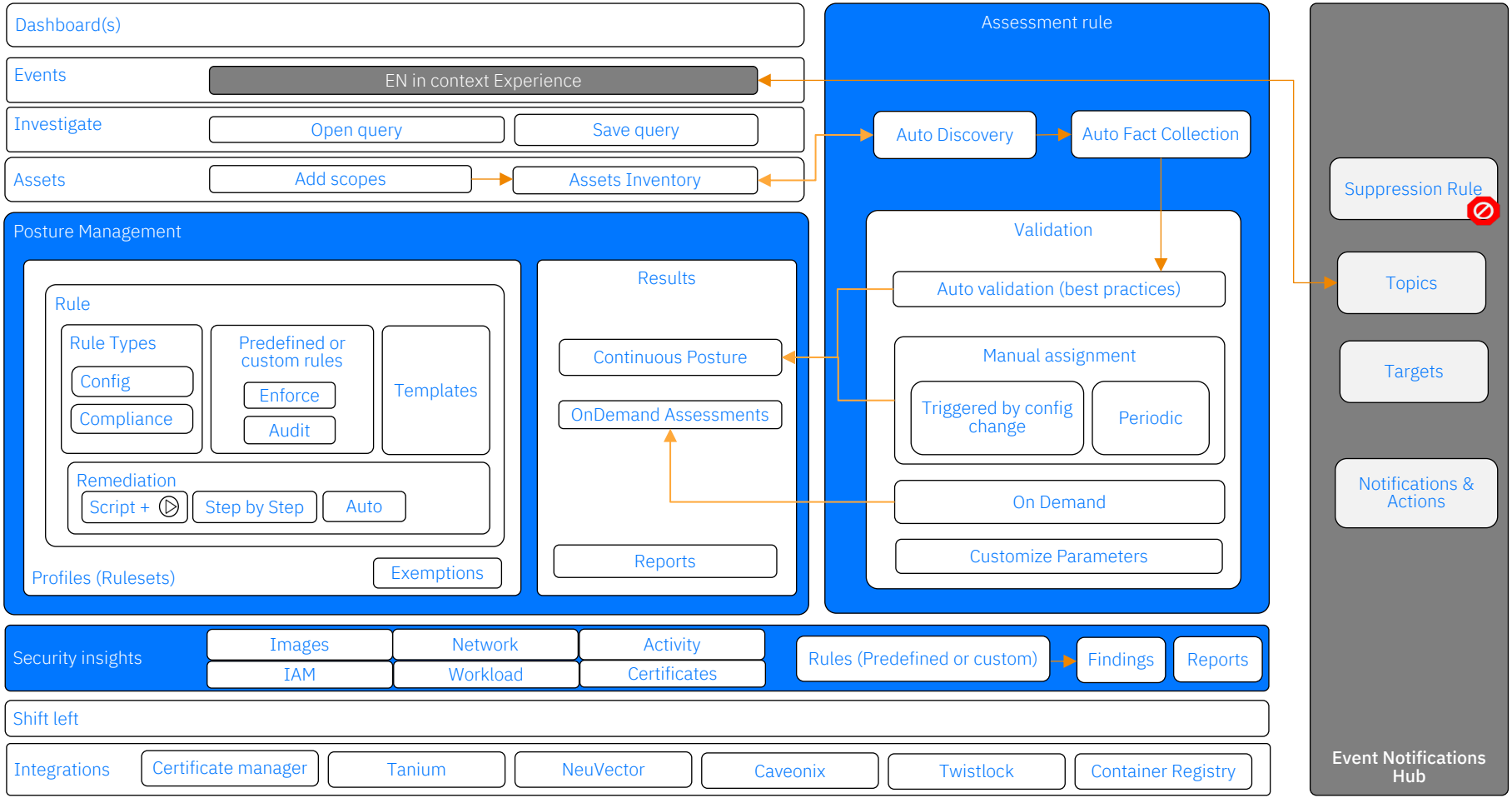
Cloud Solutions Architect – Ryanair

I summarized opportunities in order of perceived criticality:

Redefine IA | Usability | Customization | Search + Filter | Expansion

1. Communicating capabilities by rethinking terminology, and information architecture (proposal on the next page)
2. De-couple Assets from Posture management
3. Combine Config and Posture
4. Automatically create an inventory of assets for IBM accounts
   - Account onboarding process to be only for non-IBM accounts
5. Automatically run periodic fact collection, and validation against IBM best practices profile on all onboarded assets
6. Custom policy/Rule Builder + Query Language
   - Easy to use rule builder
   - Duplicating an existing goal/profile then making modifications
   - Creating “exceptions”
   - Available JSON and or Terraform script
   - save a query + turn a query into a policy or build a policy based on a saved query
7. Customized Insights Rules
8. Enhance visibility of system status and system feedback/error
9. Re-think the onboarding concepts
   - [Collectors + credentials + scopes]
10. Additional trigger types
    - Manually scheduled or predefined Periodic triggers
    - Manually defined or predefined Config Change triggers
11. Powerful and extensive search and filtering capability
12. Comprehensive categorization, tagging and description of each policy/rule for ease of consumption
13. Enhance Compliance score and add secure score:
    - Provide “value” per control/goal to help users prioritize response
14. Explore opportunities to expand capabilities:
    - Addition/emphasize on of AI and ML
    - Workload and endpoint protection
    - behavioral anomaly detection
    - CI/CD integration

I proposed a new architecture and new terminology



Once I reviewed findings with stakeholders, they asked a questions I could not confidently answer

"Why did Azure separate governance from Security center? Is there a use case for it? Should we diverge too?"

CPO/CTO Compliance Technology, IBM Cloud

Additionally, I started to question SCC's value proposition as I was synthesizing my study but was not confident enough to make an argument against it

"Do users have certain usecases for SaaS vs PaaS CSPM tools with multi cloud users? Where does SCC fit? Does positioning SCC as a comprehensive hybrid multi cloud CSPM tool make sense?"

Myself

So, I took the initiative to conduct a lean study (Phase3) to answer these outstanding questions before any major decisions were made.

No strong use case was uncovered to support a complete divergence of governance from monitoring.

AWS and Azure security centers are focused on compliance monitoring however, SCC can simply be positioned as a tool that covers a broader scope, incorporating governance, which is an acceptable concept

- Governance Policy usecases that are not related to security or regulatory compliance appear to be related to cost optimization, or company or region preferences
- Most participants didn't mind the idea of combination of governance and security compliance monitoring in one tool as long as fine grained IAM policies can be crafted to address SOD matters

" I think If IBM has a solution that covers the whole G and R and C in GRC (Governance, Risk, Compliance) that would be a differentiator"

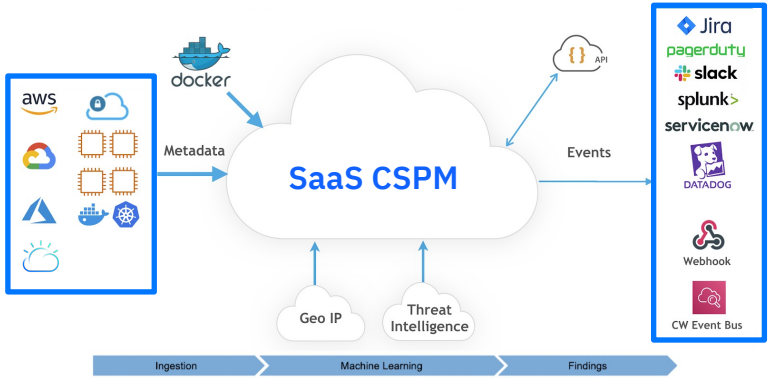
Infrastructure Architect – Security – Beca

Using a third-party SaaS CSPM tool as a single pane of glass is highly preferred amongst multi-Cloud users

- General perception is that a SaaS CSPM tools usually do a better job as a single pane of glass for multi cloud use cases
- Multi cloud users prefer to avoid getting “hooked” to one cloud provider for one specific need
- Single Cloud Azure users, tend to use Azure products for CSPM needs (due to a comprehensive free tier)
- Single Cloud AWS users, are more likely to use SaaS CSPM solutions since Security hub is paid, and is not comprehensive or customizable but offers a “nice integration” with SaaS

Implications:

- Although supporting non-IBM environments is a nice to have, a **seamless IBM experience** and supporting **integrations** may be more beneficial short-term focus.
- A pricing model with an **unlimited “free tier”(for IBM) and “premium paid features”** may encourage single cloud IBM users to utilize SCC for all their CSPM needs



“We think SaaS CSPM tools have more service capability and would do it better. We also don't know if we want to stay with one service provider. We don’t want to be hooked.

AWS feels like there are many manual tasks needed to get to a secure state. You must collect the reports, push them yourself, not good alerts, we think SaaS cuts down the manual work. The ease element!

It’s more than a matter of dollars in an enterprise. ”

Associate Director – IT Assurance - BMS

Top business outcomes

Insights Gained:

Clarified personas and usecases for SCC
This research gave us a clear understanding on who will be using SCC and for what usecases

Gained insight into preferences and perceptions for PaaS vs SaaS CSPM solutions
Stakeholders have more clarity on how to position SCC and what capabilities to focus on

Stakeholder alignment
After over a year of stakeholder misalignment and conflicts in stakeholder POV, this research was able to give the team needed evidence, clarity and alignment to be able to make more confident strategic and tactical decisions

Actions taken to date

Redefined the “to be” end to end
The SCC team has started the complete redesign and redefining of the end-to-end UX of SCC based on my research study

Short term strategy shift
The SCC product owners have dramatically shifted SCCs short term goals from heavily focusing on supporting a multi/hybrid cloud framework to focusing on delivering the best experience for IBM Cloud and Financial Services Cloud users but in the meantime support SaaS integration and agent based multi cloud onboarding

Partnerships with SaaS CSPM and CWPP tools:
IBM Security and Compliance team has accelerated partnership efforts with CloudGuard and LaceWork in order to provide integrations with SaaS CSPM and CWPP solutions for our enterprise users multi cloud framework

Feature Prioritization (WIP)
I’m currently running a Kano study to help product management prioritize my proposed capabilities