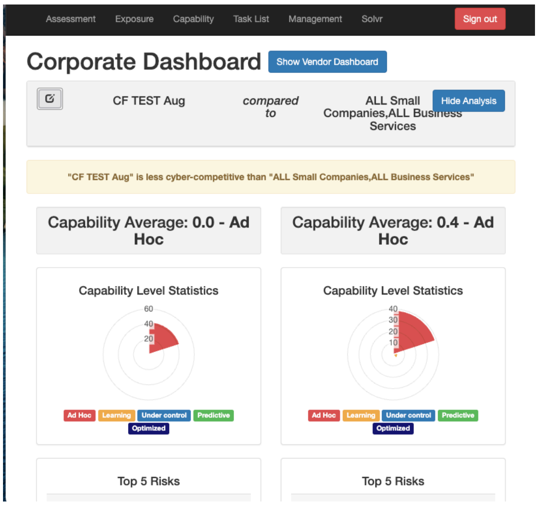
Cyberfense Overview

Two Integrated Apps for Two Different Audiences & Needs



Corporate Dashboard

CF TEST Aug *compared to* ALL Small Companies,ALL Business Services

"CF TEST Aug" is less cyber-competitive than "ALL Small Companies,ALL Business Services"

Capability Average: 0.0 - Ad Hoc

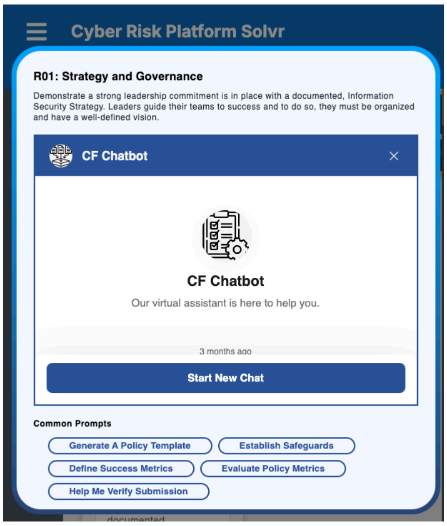
Capability Average: 0.4 - Ad Hoc

Capability Level Statistics

Capability Level Statistics

Top 5 Risks

Top 5 Risks



R01: Strategy and Governance

Demonstrate a strong leadership commitment is in place with a documented, Information Security Strategy. Leaders guide their teams to success and to do so, they must be organized and have a well-defined vision.

CF Chatbot

Our virtual assistant is here to help you.

3 months ago

Common Prompts

Risk Portal (Identifies Risk)

- Based on ISO 27001
- Organised in 43 risk domains
- Calculates risk
- Compares performance
- Restricted access to Business Leaders
- Sends & receives data via API to Solvr

Solvr (Solves Risk)

- Tracks risk resolution progress (KanBan)
- Project Card = risk domain
- Bot guides user w/ next steps
- Access by invitation for Contributors
- Sends & receives data via API to Risk Portal

Notes

A. ISO 27001 is a global standard.
B. There are 113 “Annex A” Controls that are measured.
C. We distilled & reorganized the 113 controls to make the process more manageable (doable). This is a proprietary innovation. However, all 113 controls are still covered.
D. User can compare their performance against industry peers. This is important because
    A. Incentive to create a market differentiator (win more business w/ upstream suppliers)
    B. Frames budget - spend the same or more than peers to remain safe from attacks.
    C. The idea is, don’t be the least prepared because the attacker prey on the weak.

User Journey

1) Business Leader (BL) registers & opens Risk Portal account
2) BL completes assessment (soon user won’t have to do an assessment)
3) Risk Portal pinpoints & prioritizes risk tailored to the organization.
4) BL invites Contributors to Solvr (employees, contractors, vendors).
5) Users log on to Solvr and engages Bot.
6) Bot guides user through next steps to resolve risk.
7) Risk resolution is measured by the Cyber Maturity (CM).

8) There are (4) four levels of Cyber Maturity (CM) which is a continuous lifecycle (PLAN, DO, ACT & CHECK).
    1) CM -1
    2) CM-2
    3) CM -3
    4) CM - 4
9) Each CM Level has its own objective & activities.
10) When a user achieves a new level of Cyber Maturity, the company earns points.
11) Companies can use the point system to compare (rank) themselves against peers.
12) Points = time, effort & money spent on cyber security.
13) The more safe, protected and resilient a company is the more business they can win because most attacks originate from weak 3rd party vendors (business partners) who connect or share information and critical systems with upstream suppliers.
14) So, the idea is Business Leaders spend time in the Risk Portal to monitor and manage risk for their company and supply chain while Contributors spend their time in Solvr resolving risk.
15) As risk is resolved in Solvr, these resolution efforts are reflected in the the company's Risk Portal.
16) Their risk is continually recalculated and compared to industry peers in real time.
17) Thus, the concept is to become "Cyber-Competitive".
18) The benefit is being more resilient than peers who are likely to be attacked and lose data or critical systems (which equals loss of revenue and business reputation).
19) The Bot is continuously engaged by assigned Contributors to complete activities. The Bot is the Virtual Cyber Advisor.

CM Objectives that the Bot helps the User Complete

CM -1: Generate a policy for each of the 43 Risk Domains.

CM -2: Recommend safeguards to implement in support of the policy. These can be administrative, technical or physical.

CM -3: Identify success metrics of the safeguards.

CM -4: Evaluate & Improve safeguards

High-Level Bot Requirements

1. Bot must successfully guide user to complete each CM level for each of the 43 risk domains.
2. Bot must be fully conversational via chat window.
3. Bot conversation must be low latency.
4. Bot conversation must reflect 'real-life' (syntax, cadence)

Order of Our DEV Operations

1. CM -1 Generate a Policy
    1. Fix Risk Domain R01
    2. Fix Risk Domain R02 and R03
    3. Complete full functionality R04
    4. Test
2. CM -2 Recommend Safeguards
    1. Recommend Guideline
    2. Test
3. CM-3 Identify Success Metrics
    1. Capture metrics & other data
    2. Test

4. CM -4 Evaluate & Improve
    1. Bot arranges future appointment and sends invites.
    2. Test
5. Return to CM -2 Recommend safeguards (paid)
    1. Bot recommends ‘best-fit’ products & services
    2. Bot closes the sale
    3. Bot directs for payment
    4. Bot captures success metrics for CM-3
    5. Bot arranges for evaluation at future date.

Team

Thomas (Founder, located in France) responsible for product management, marketing and sales.

Otto (Co-Founder, located in France) responsible for R&D, Testing and Technical Writing.

Frank (located in Michigan) is responsible for development of Risk Portal

Christopher (Relay Technology located in Chicago) is responsible development for Solvr.

Ambes (located in DC Metro) is responsible for configuring & managing AWS network.