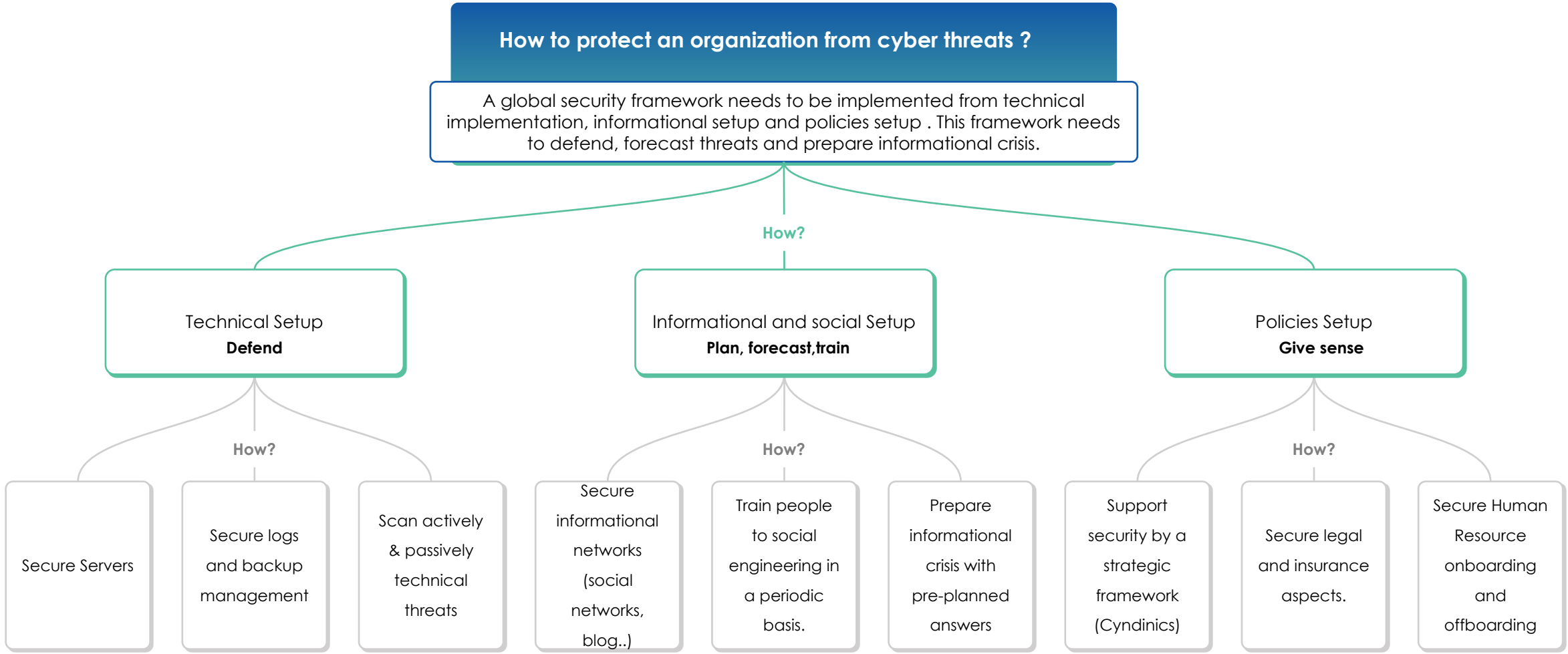
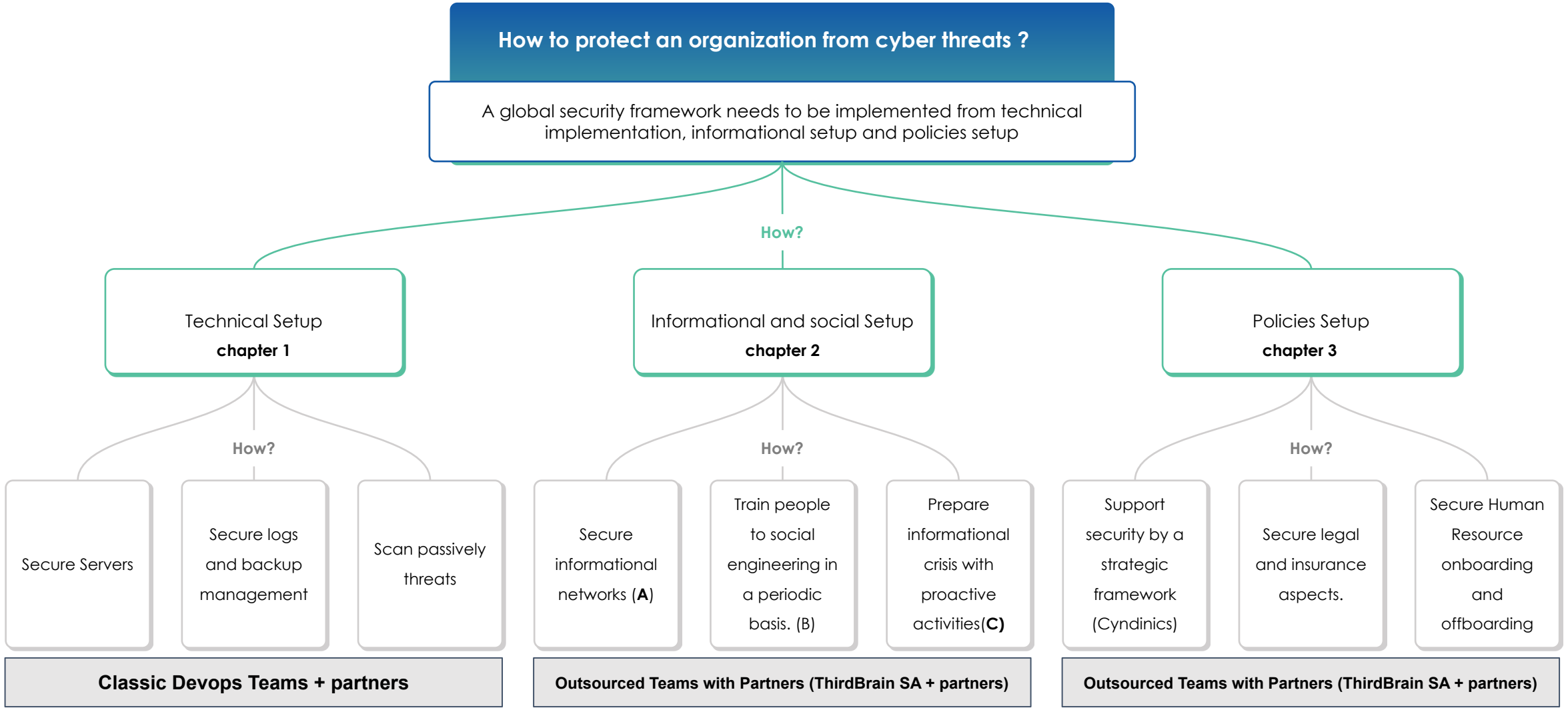
Defensive Global CyberSecurity Framework “as a product”.

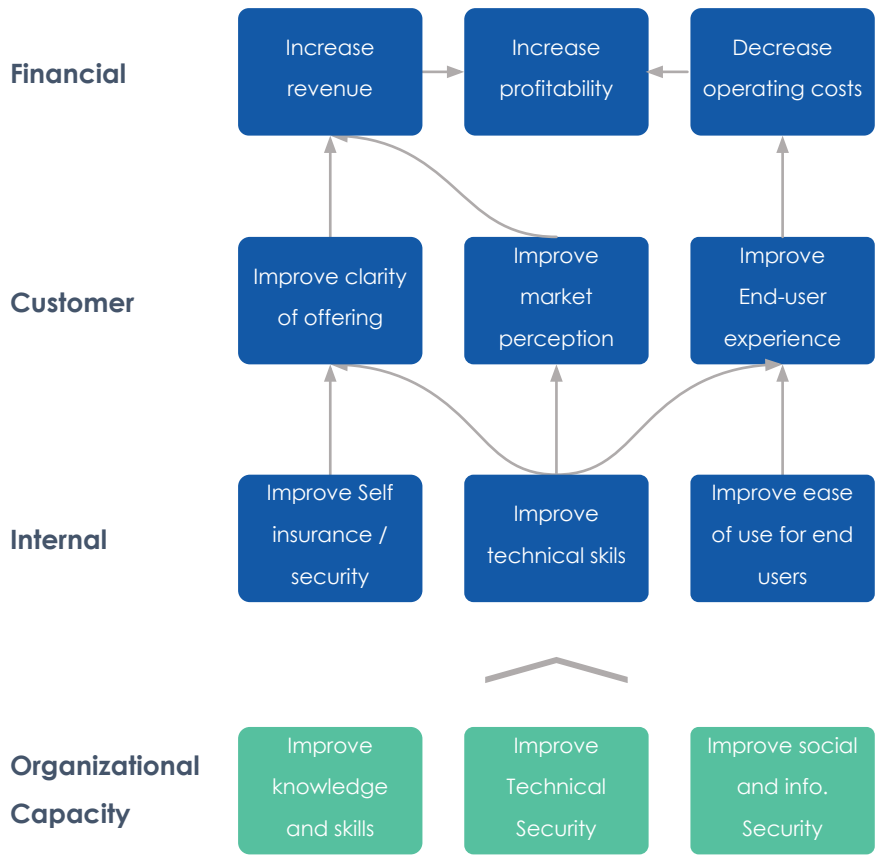


Actors of the product.



Strategic Journey for CyberSecurity product (s)

STRATEGIC OBJECTIVES & STRATEGY MAP



MEASURES

- Net profit
- Operating costs
- Revenue in target markets

- % Market share index
- % Customer satisfaction index

- New products as % of sales
- Brand awareness score
- End user experience score

- Employee development plans
- Technology training index
- Network efficiency index

TARGETS

-
-

-

-

- 95% in place
- 90% efficient
- 99.99% uptime
- few incidents.

INITIATIVES

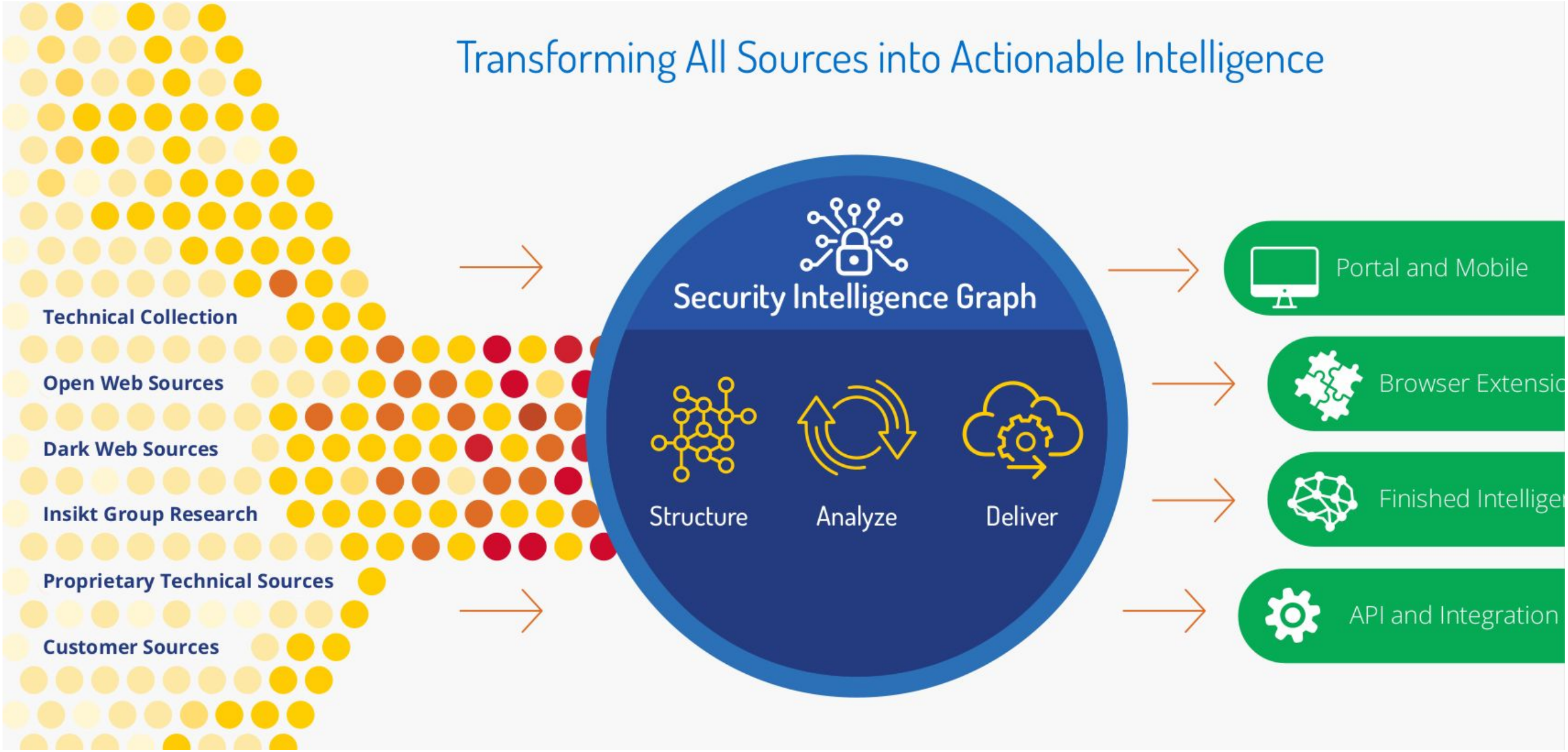
- Implement new financial accounting system
- Simplify billing operations

- Competitive end user requirements market studies for new XX regions
- “Improve the offering” two year program

- Create improved offering selection process
- Hook into “improve the offering” program
- Training program for new offerings and user interface

- Product and marketing training program
- 2 year renew the network staged plan and roll-out
- Technology improvement program

Informational setup (chapter 2 - a)



COLLECTION

Automated Analysis Powered by Machine Learning

1,500+ FORUMS

Hacker, criminal, extremist, and research

65+ THREAT FEEDS

Every high-value feed available on the web

BLOGS & SOCIAL MEDIA

Security community, public Tweets, Facebook, and more

50+ PASTE SITES

Leak posts, credential breaches, corp IP

DARK WEB COLLECTION

Dark web sourcing from top tier, invite only, forums globally, including China, Russia, Brazil

ORIGINAL RESEARCH

Industry leading research at your fingertips

CODE REPOSITORIES

Code sharing, malware, C2s, POCs, app stores, vuln DBs

INTERNAL NOTES

Customer-generated intel notes and your IOC annotations

PROPRIETARY 3rd-PARTY FEEDS

Customer-exclusive internal & proprietary feeds and data

TECHNICAL COLLECTION

Shodan RAT controllers, Google dorking, domain and certificate registrations, NetFlow, GEO IP

CERTIFIED INTELLIGENCE

High-confidence, proprietary, block-grade feeds including Weaponized Domains & URLs, Command & Control, and Exploits in the Wild

DEEP LANGUAGE EXPERTISE

Automated analysis for every language with deep analysis for 12 languages

8 MODULES TO BE ACTIVATED DEPENDING ON THE CLIENT