

Defensive Global CyberSecurity Framework “as a product”.

How to protect an organization from cyber threats ?

A global security framework needs to be implemented from technical implementation, informational setup and policies setup . This framework needs to defend, forecast threats and prepare informational crisis.

How?

Technical Setup
Defend

Informational and social Setup
Plan, forecast,train

Policies Setup
Give sense

How?

How?

How?

Secure Servers

Secure logs and backup management

Scan actively & passively technical threats

Secure informational networks (social networks, blog..)

Train people to social engineering in a periodic basis.

Prepare informational crisis with pre-planned answers

Support security by a strategic framework (Cyndinics)

Secure legal and insurance aspects.

Secure Human Resource onboarding and offboarding

Actors of the product.

How to protect an organization from cyber threats ?

A global security framework needs to be implemented from technical implementation, informational setup and policies setup

How?

Technical Setup
chapter 1

Informational and social Setup
chapter 2

Policies Setup
chapter 3

How?

How?

How?

Secure Servers

Secure logs
and backup
management

Scan passively
threats

Secure
informational
networks (A)

Train people
to social
engineering in
a periodic
basis. (B)

Prepare
informational
crisis with
proactive
activities (C)

Support
security by a
strategic
framework
(Cyndinics)

Secure legal
and insurance
aspects.

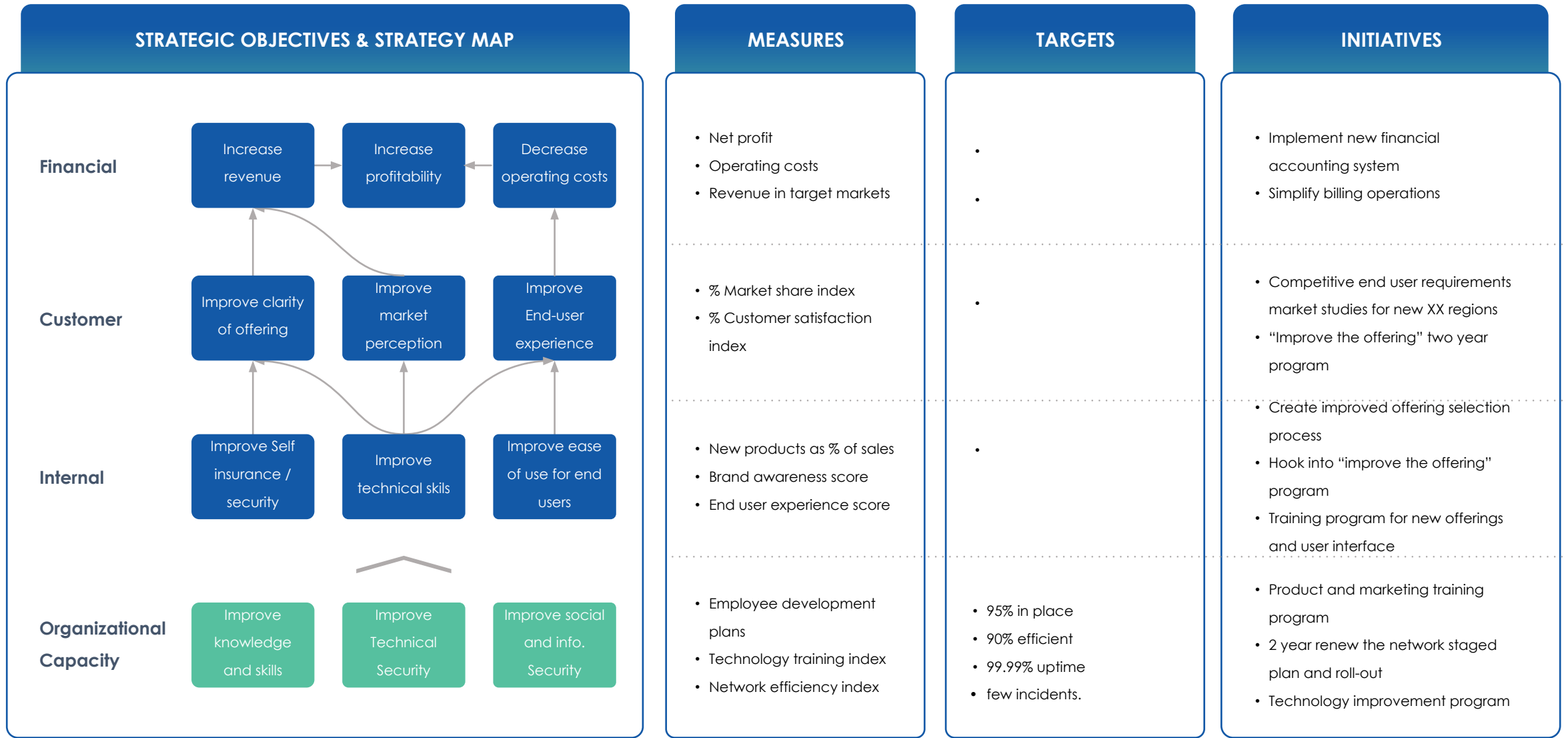
Secure Human
Resource
onboarding
and
offboarding

Classic Devops Teams + partners

Outsourced Teams with Partners (ThirdBrain SA + partners)

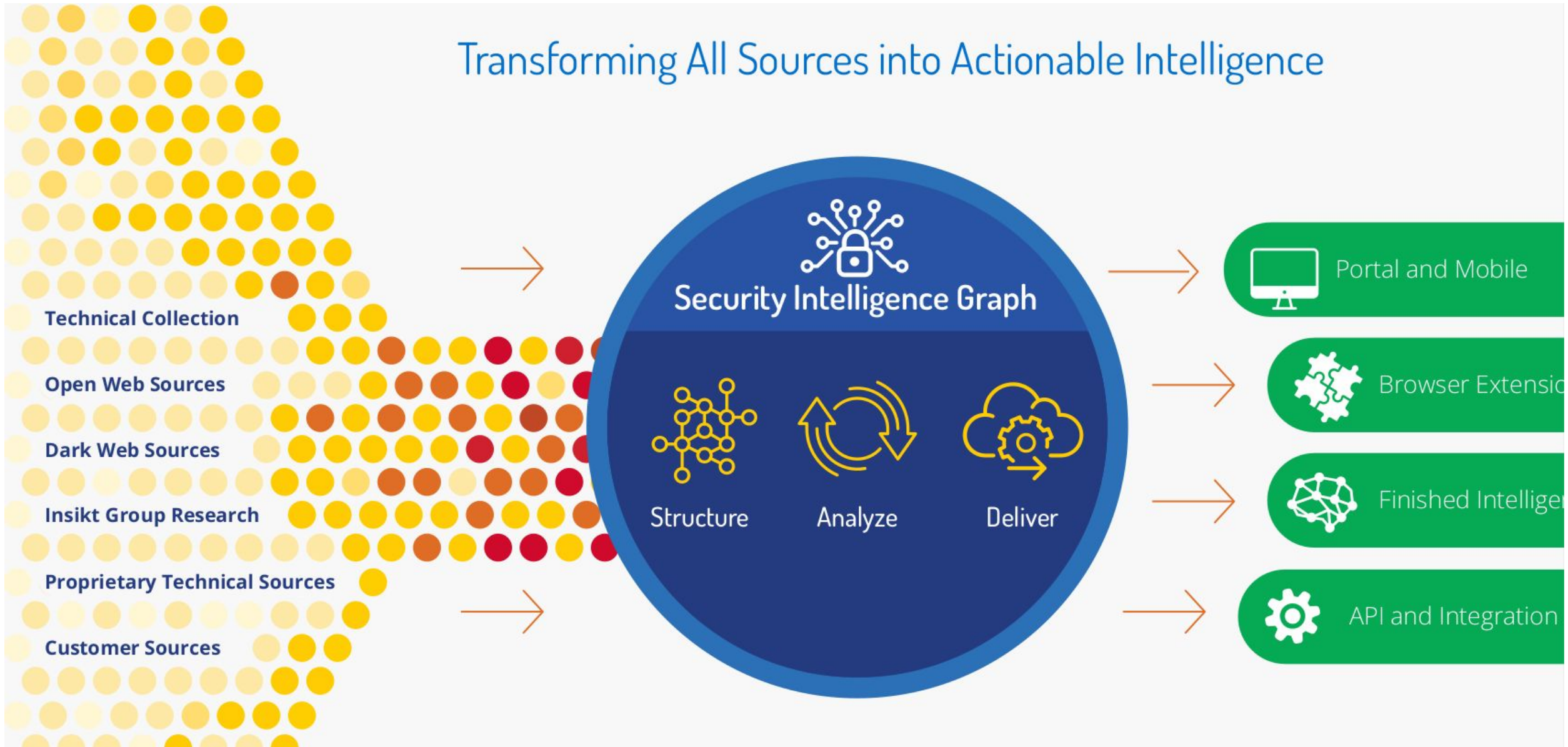
Outsourced Teams with Partners (ThirdBrain SA + partners)

Strategic Journey for CyberSecurity product (s)



Informational setup (chapter 2 - a)

Transforming All Sources into Actionable Intelligence



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



SECOPS INTELLIGENCE

Alert Triage

Threat Detection

Threat Prevention



THREAT INTELLIGENCE

Advanced Threat
Research & Reporting

Advanced Detection & Validation

Monitor Threats to Your Tech Stack

Dark Web Investigation



BRAND INTELLIGENCE

Domain Abuse

Data Leakage Monitoring

Brand Attack Mitigation

Digital Asset Monitoring

Monitoring Threats to Your Industry

Fraud Detection



IDENTITY INTELLIGENCE

Account Takeover Prevention

Personnel Identity Monitoring

Third-Party Identity Monitoring



VULNERABILITY INTELLIGENCE

Vulnerability Prioritization
Monitoring for Vulnerabilities
in Your Tech Stack



THIRD-PARTY INTELLIGENCE

Continuous Third-Party
Risk Management
Procurement Assessment



GEOPOLITICAL INTELLIGENCE

Location Risk Monitoring

Event Monitoring

Geopolitical Trend Analysis



CARD FRAUD INTELLIGENCE

Payment Card Fraud Prevention

Magecart Skimming Monitoring

Underground Cybercriminal Reporting