TLP:CLEAR

How to Develop Priority Intelligence Requirements for YOUR Organization

Ondra Rojčík

Senior CTI Analyst, Red Hat

Red Hat

TLP:CLEAR

Priority Intelligence Requirements (PIRs) for YOUR Org

- What are PIRs and what they are good for
- Deficiencies of the existing PIRs processes
- The Red Hat approach
- Internal focus
- External focus
- Adjust the process to your needs
- Process of iterations
- Integration of PIRs into the CTI lifecycle
- Challenges & Opportunities

TLP:CLEAR

Ondra Rojčík

- Senior CTI Analyst at Red Hat
- Co-founder and Head of Strategic Analysis Unit at Czech Cyber Security Agency (NÚKIB)
- Threat Intell analyst since 2006: Czech gov and NATO

@orojcik

ondrejrojcik/

TLP:CLEAR

If we collect and analyse everything, we collect and analyse nothing

PIRs will help you to improve:

Collection Plan and Detection

> identify relevant data in SIEM

> alerts on relevant information in your CTI platform

Threat Hunting

guide your threat hunting program

Analytical Deliverables

planning your analytical production and reporting

Existing approaches to PIR development

- **Not much guidance on how to develop PIRs**
- The existing approaches assume that you know what is important for your organization
- Might be difficult in geographically distributed organizations with diverse portfolio of products and services

PIRs at Red Hat

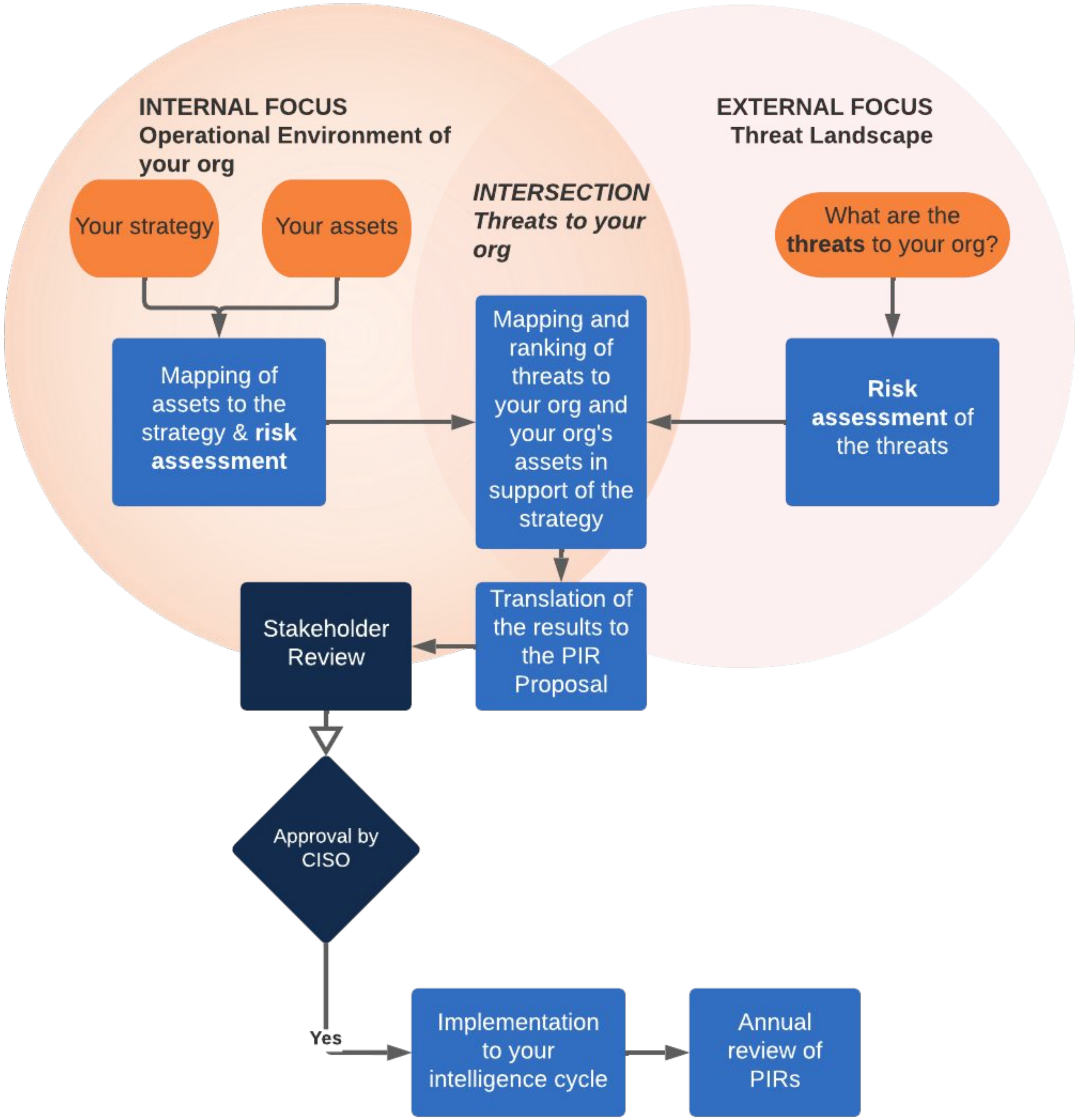
- First > understand ourselves

Basic elements of our approach:

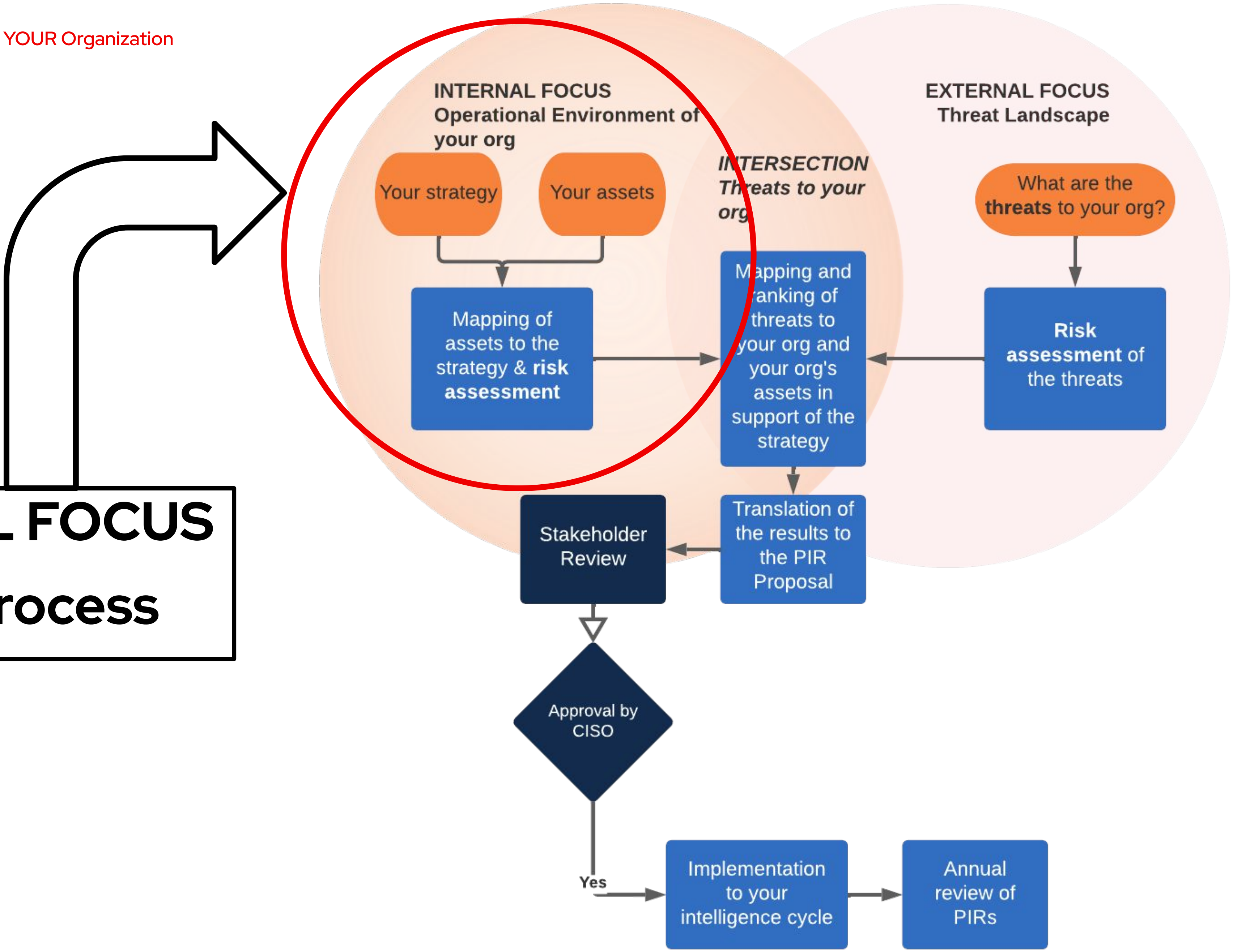
- Strategy, values, and other intangible aspects
- Supporting critical technology assets
- External threat environment and adversary
- Answering what, who and how

TLP:CLEAR

Red Hat's process of developing PIRs


INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & risk assessment
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the threats to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

TLP:CLEAR

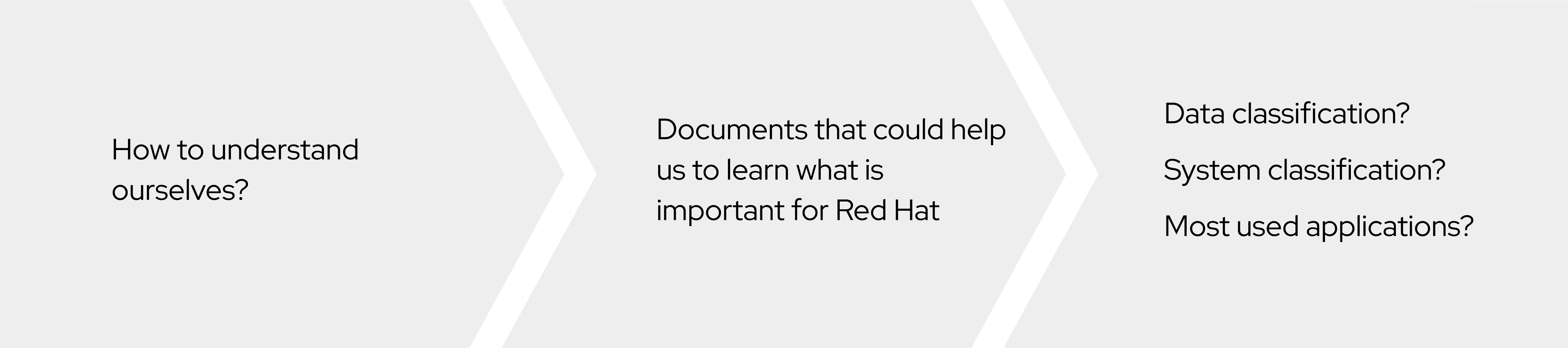

INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & **risk assessment**
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the **threats** to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

INTERNAL FOCUS of the process

Red Hat

The process of developing PIRs

INTERNAL FOCUS - Elements of Your Organization



How to understand ourselves?

Documents that could help us to learn what is important for Red Hat

Data classification?

System classification?

Most used applications?

The process of developing PIRs

INTERNAL FOCUS - Elements of Your Organization

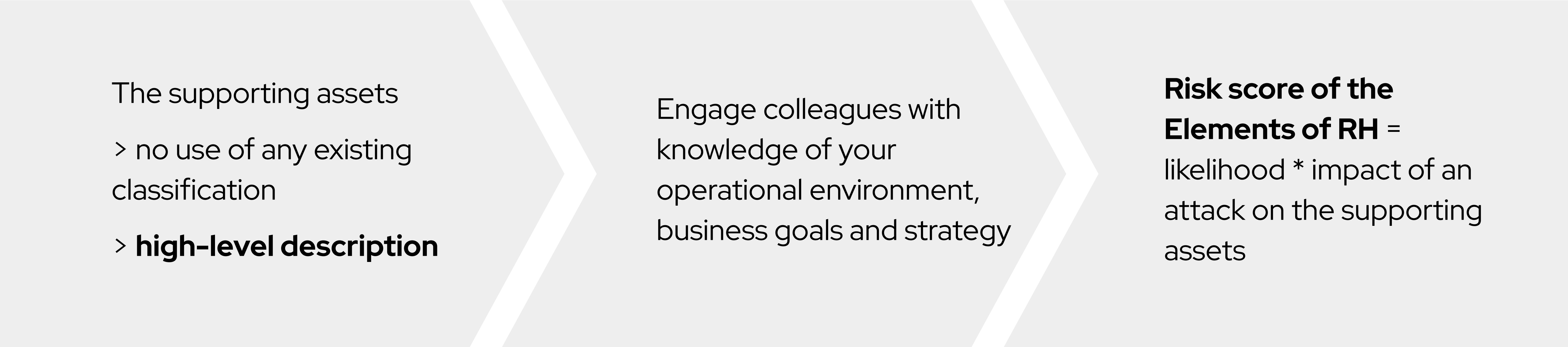
What about intangible aspects of Red Hat such as culture? Is that documented?

Extracting keywords from strategic documents describing RH and the RH strategy > **ELEMENTS of Red Hat**

Each ELEMENT of Red Hat has **supporting technical assets** that could be attacked

The process of developing PIRs

INTERNAL FOCUS - Elements of Your Organization



The supporting assets

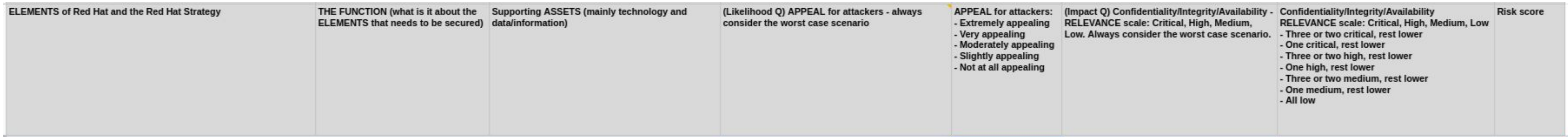
> no use of any existing classification

> **high-level description**

Engage colleagues with knowledge of your operational environment, business goals and strategy

Risk score of the Elements of RH = likelihood * impact of an attack on the supporting assets

INTERNAL FOCUS - Elements of Red Hat Sheet



ELEMENTS of Red Hat and the Red Hat Strategy	THE FUNCTION (what is it about the ELEMENTS that needs to be secured)	Supporting ASSETS (mainly technology and data/information)	(Likelihood Q) APPEAL for attackers - always consider the worst case scenario	APPEAL for attackers: - Extremely appealing - Very appealing - Moderately appealing - Slightly appealing - Not at all appealing	(Impact Q) Confidentiality/Integrity/Availability - RELEVANCE scale: Critical, High, Medium, Low. Always consider the worst case scenario.	Confidentiality/Integrity/Availability RELEVANCE scale: Critical, High, Medium, Low - Three or two critical, rest lower - One critical, rest lower - Three or two high, rest lower - One high, rest lower - Three or two medium, rest lower - One medium, rest lower - All low	Risk score

ELEMENTS of Red Hat and Red Hat strategy

- 90% of Fortune 500 are our customers
- Position in downstream and upstream supply chain
- Focus on specific products
- Hybrid work model
- Red Hat culture
- etc.
- 25 ELEMENTS in total

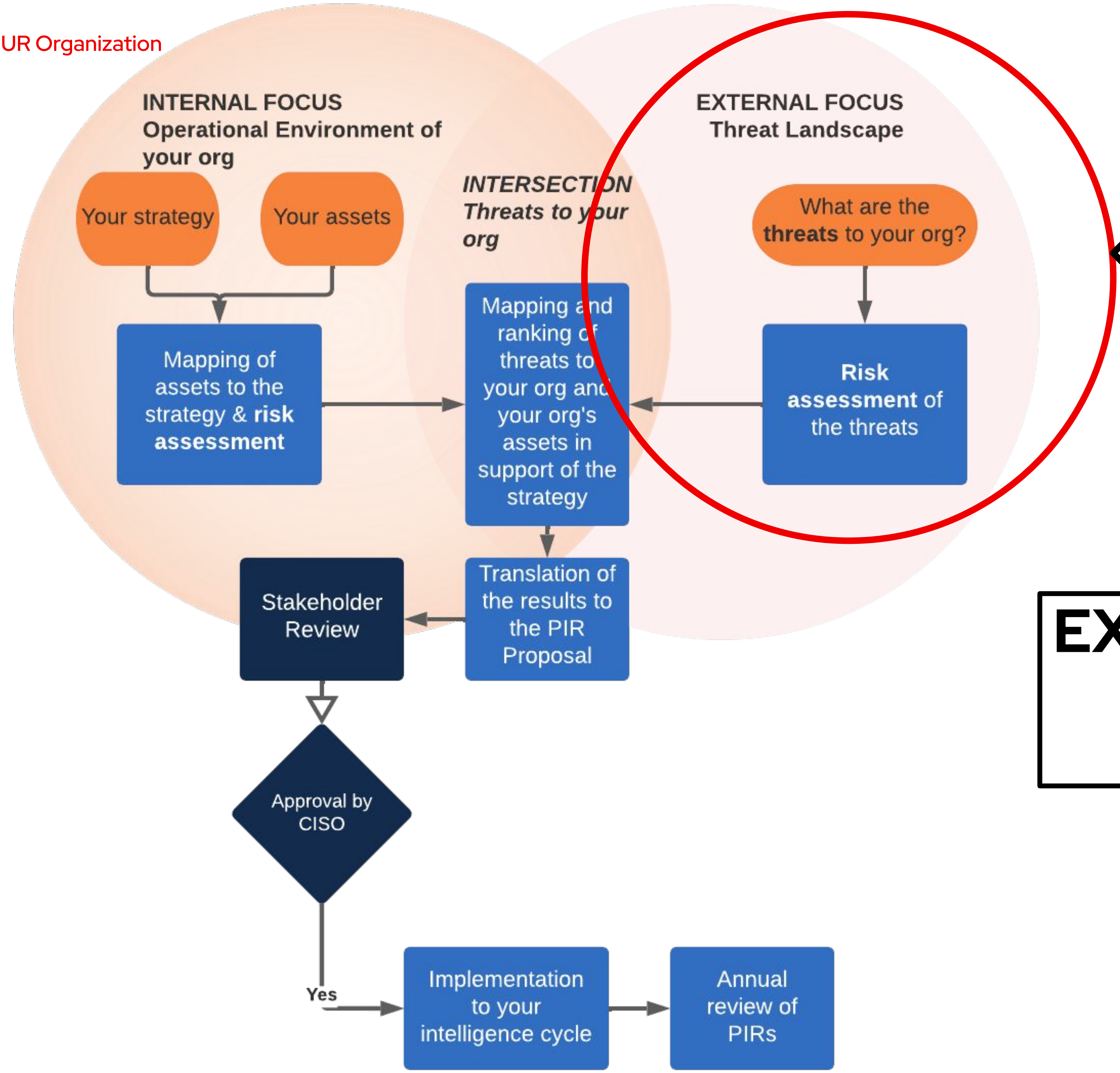
Multiple respondents working individually

MEDIAN risk score of the ELEMENTS

Ranked Top10 ELEMENTS for the next phase

Risk Score of the ELEMENTS & Supporting Assets = Likelihood (Appeal for the attacker) * Impact of attack on the assets

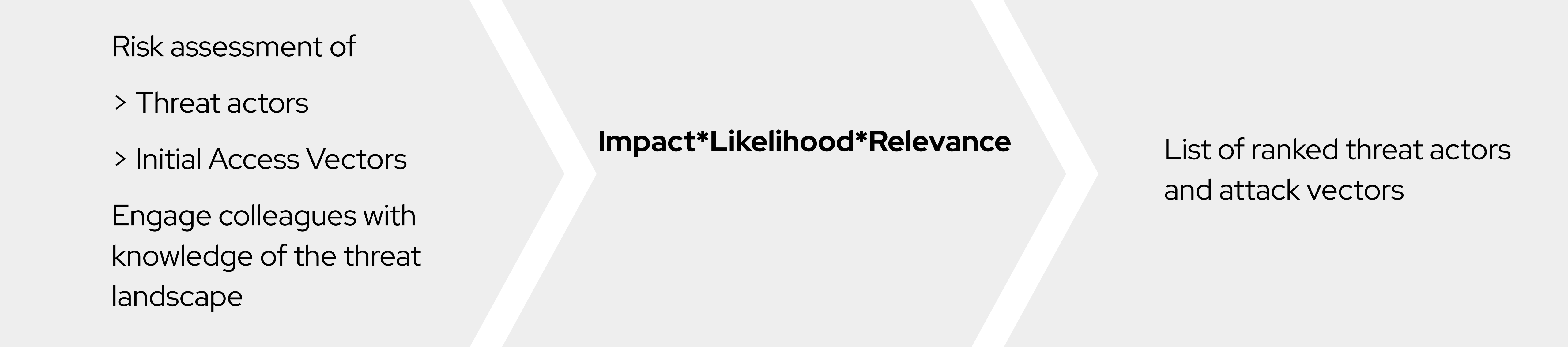
TLP:CLEAR


INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & risk assessment
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the threats to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

EXTERNAL FOCUS of the process

The process of developing PIRs

EXTERNAL FOCUS – Elements of Your Organization



Risk assessment of

> Threat actors

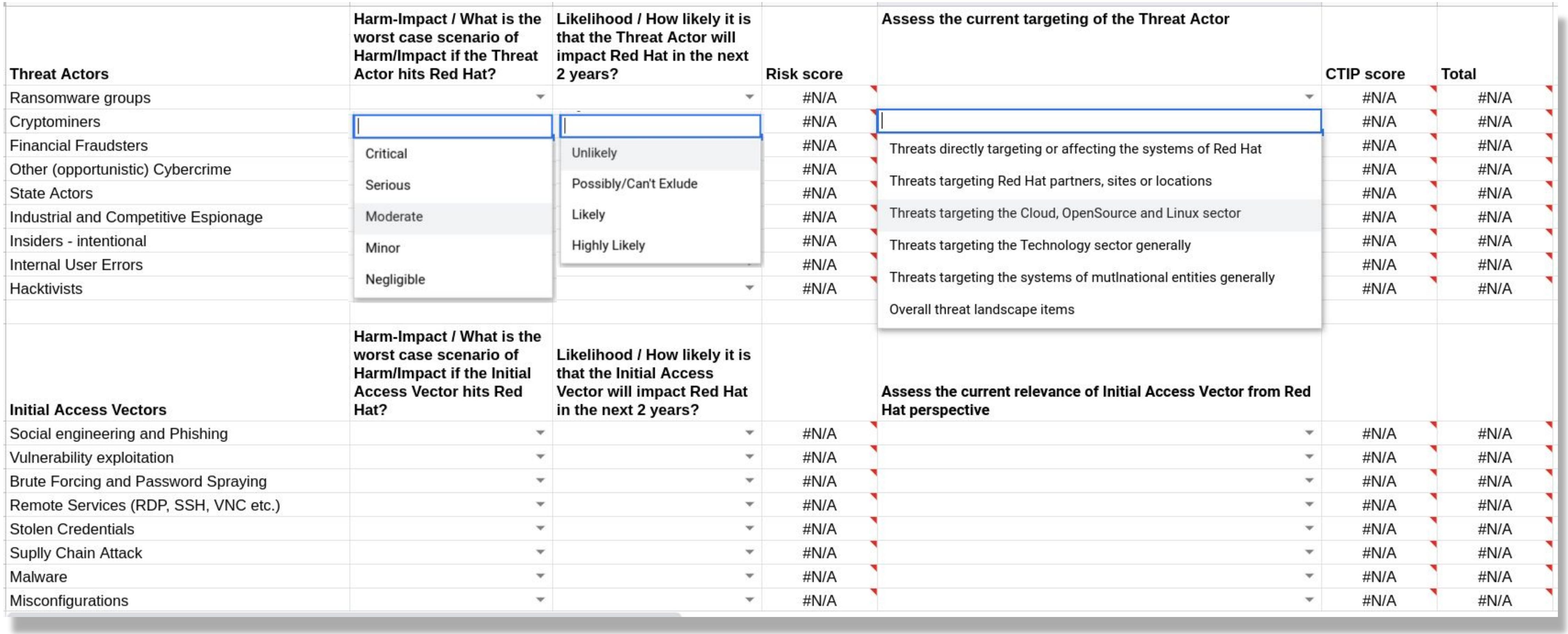
> Initial Access Vectors

Engage colleagues with knowledge of the threat landscape

Impact*Likelihood*Relevance

List of ranked threat actors and attack vectors

EXTERNAL FOCUS – Threat Landscape



Threat Actors	Harm-Impact / What is the worst case scenario of Harm/Impact if the Threat Actor hits Red Hat?	Likelihood / How likely it is that the Threat Actor will impact Red Hat in the next 2 years?	Risk score	Assess the current targeting of the Threat Actor	CTIP score	Total
Ransomware groups			#N/A		#N/A	#N/A
Cryptominers			#N/A		#N/A	#N/A
Financial Fraudsters			#N/A		#N/A	#N/A
Other (opportunistic) Cybercrime			#N/A		#N/A	#N/A
State Actors			#N/A		#N/A	#N/A
Industrial and Competitive Espionage			#N/A		#N/A	#N/A
Insiders - intentional			#N/A		#N/A	#N/A
Internal User Errors			#N/A		#N/A	#N/A
Hacktivists			#N/A		#N/A	#N/A
Initial Access Vectors	**Harm-Impact / What is the worst case scenario of Harm/Impact if the Initial Access Vector hits Red Hat?**	**Likelihood / How likely it is that the Initial Access Vector will impact Red Hat in the next 2 years?**		**Assess the current relevance of Initial Access Vector from Red Hat perspective**		
Social engineering and Phishing			#N/A		#N/A	#N/A
Vulnerability exploitation			#N/A		#N/A	#N/A
Brute Forcing and Password Spraying			#N/A		#N/A	#N/A
Remote Services (RDP, SSH, VNC etc.)			#N/A		#N/A	#N/A
Stolen Credentials			#N/A		#N/A	#N/A
Suplly Chain Attack			#N/A		#N/A	#N/A
Malware			#N/A		#N/A	#N/A
Misconfigurations			#N/A		#N/A	#N/A

- Critical
- Serious
- Moderate
- Minor
- Negligible

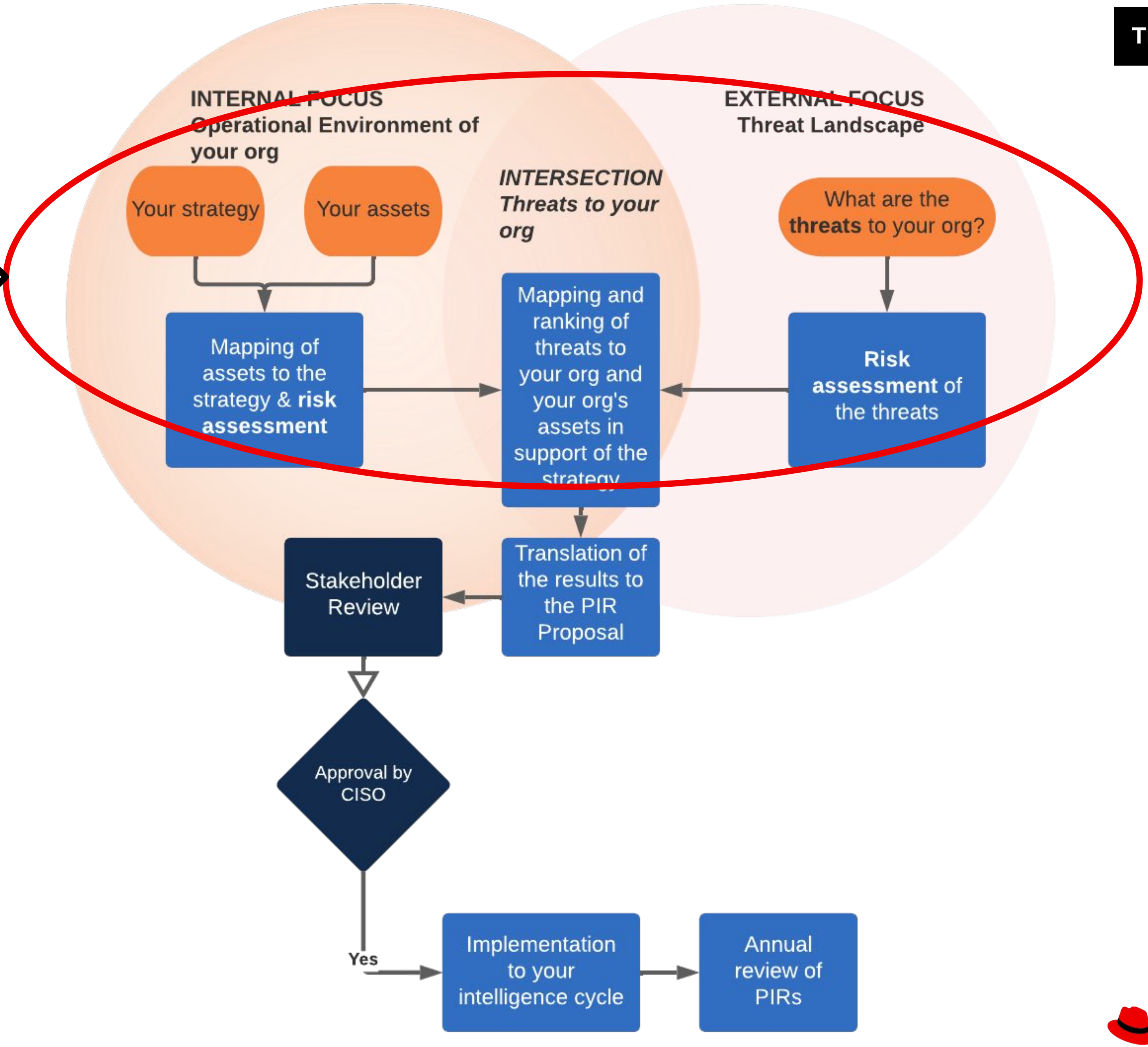
- Unlikely
- Possibly/Can't Exlude
- Likely
- Highly Likely

- Threats directly targeting or affecting the systems of Red Hat
- Threats targeting Red Hat partners, sites or locations
- Threats targeting the Cloud, OpenSource and Linux sector
- Threats targeting the Technology sector generally
- Threats targeting the systems of mutlnational entities generally
- Overall threat landscape items

Inspiration – Andy Piazza: https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11

TLP:CLEAR

COMBINED EXERCISE



INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & **risk assessment**
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the **threats** to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

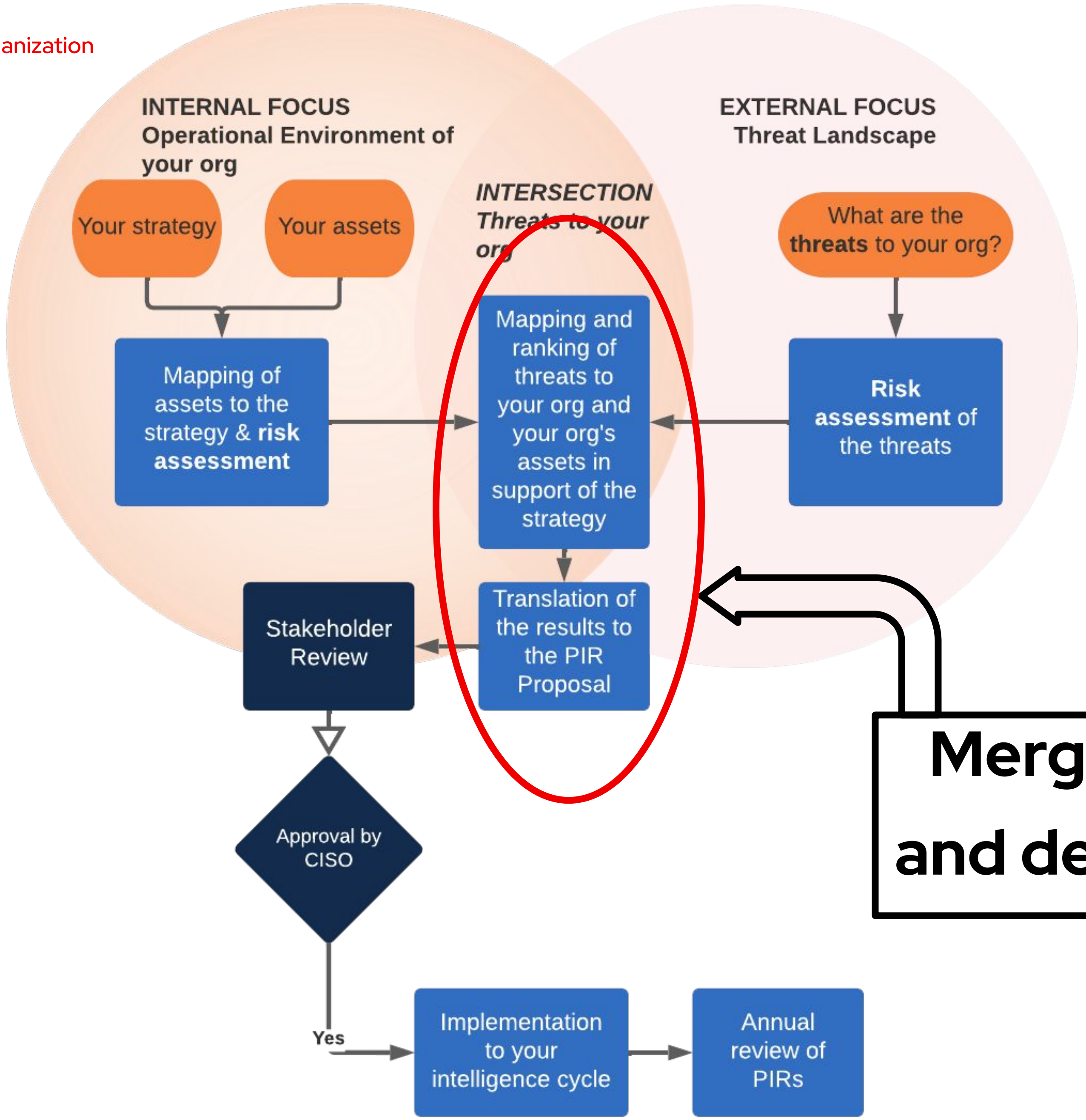
Red Hat

COMBINED EXERCISE

The two exercises can be combined

- Element + Threat Actor + Attack Vector
- Generate you the PIRs almost instantly
- Requires people who know your operational environment, business strategy and the external threats

TLP:CLEAR


INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & risk assessment
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the threats to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

Merging the exercises and developing the PIRs

Red Hat

TLP:CLEAR

Mapping exercise and developing the PIRs

Mapping the **list of ranked threat actors and attack vectors** to the **list of ELEMENTS** representing Red Hat strategy and assets

- Risk score and ranking
- And CTI insight

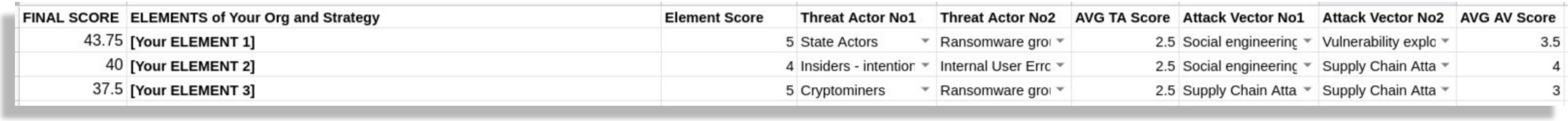
Mapping = ELEMENT + Threat Actor + Attack Vector

Final ranking of PIRs = Element Score * Threat Actor Score * Attack Vector Score

- Translate the result to questions or statements
- You can expand the PIRs in Specific Intelligence Requirements (SIRs)

TLP:CLEAR

Mapping exercise and developing the PIRs



FINAL SCORE	ELEMENTS of Your Org and Strategy	Element Score	Threat Actor No1	Threat Actor No2	AVG TA Score	Attack Vector No1	Attack Vector No2	AVG AV Score
43.75	**[Your ELEMENT 1]**	5	State Actors	Ransomware groı	2.5	Social engineerinç	Vulnerability explc	3.5
40	**[Your ELEMENT 2]**	4	Insiders - intentior	Internal User Errc	2.5	Social engineerinç	Supply Chain Atta	4
37.5	**[Your ELEMENT 3]**	5	Cryptominers	Ransomware groı	2.5	Supply Chain Atta	Supply Chain Atta	3

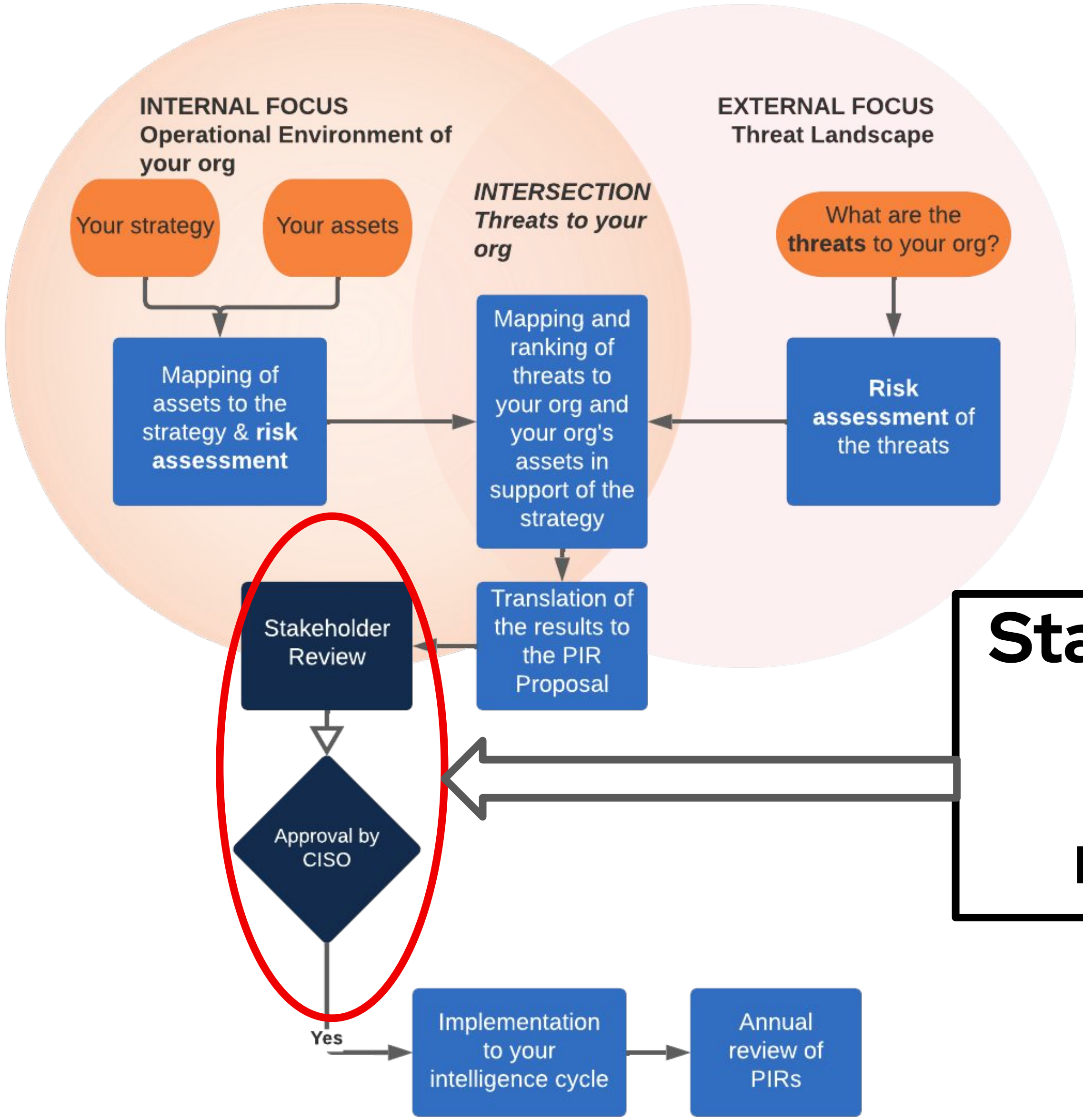
FINAL SCORE = Element Score * Threat Actor Score * Attack Vector Score

Element Score - Top 10 ELEMENTS from the INTERNAL FOCUS exercise
ELEMENTS No. 1 and 2 = 5 points
ELEMENTS No. 3 and 4 = 4 points
ELEMENTS No. 5 and 6 = 3 points
ELEMENTS No. 7 and 8 = 2 points
ELEMENTS No. 9 and 10 = 1 point

Threat Actor (TA) Score
Top 5 TAs from the EXTERNAL FOCUS exercise
No. 1 = 5 points
No. 2 = 4 points
No. 3= 3 points
No. 4 = 2 points
No. 5 = 1 point

Attack Vector (AV) Score
Top 5 AV from the EXTERNAL FOCUS exercise
No. 1 = 5 points
No. 2 = 4 points
No. 3= 3 points
No. 4 = 2 points
No. 5 = 1 point

TLP:CLEAR


INTERNAL FOCUS
Operational Environment of your org
Your strategy
Your assets
Mapping of assets to the strategy & risk assessment
INTERSECTION
Threats to your org
Mapping and ranking of threats to your org and your org's assets in support of the strategy
EXTERNAL FOCUS
Threat Landscape
What are the threats to your org?
Risk assessment of the threats
Translation of the results to the PIR Proposal
Stakeholder Review
Approval by CISO
Yes
Implementation to your intelligence cycle
Annual review of PIRs

Stakeholder review and approval by a responsible leader

Red Hat

Adjust the process to your needs!

Do you know the crown jewels of your org well?

> Threat landscape assessment

Are you not sure about the crown jewels and you have people who know well both the org and the threat landscape?

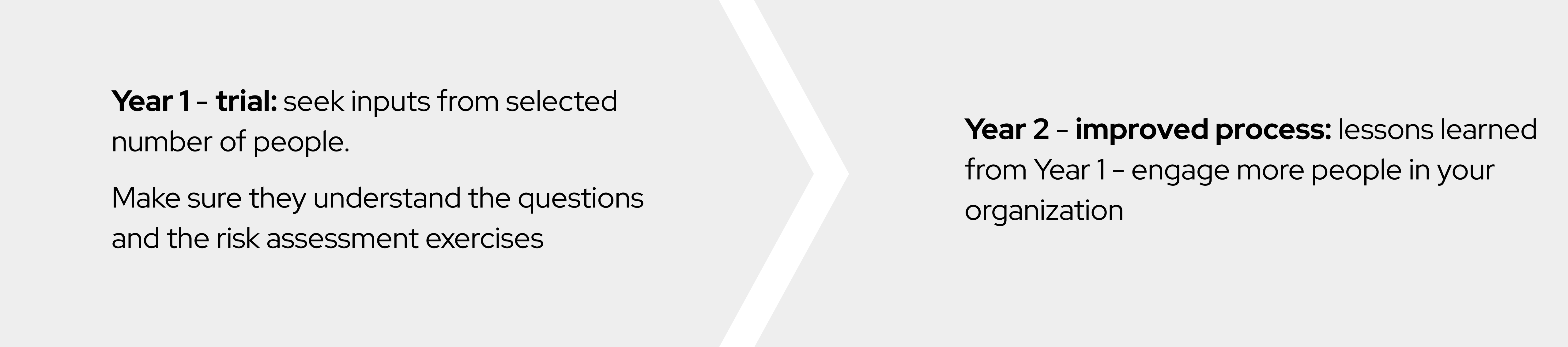
> Combined INTERNAL and EXTERNAL exercise

Are you not sure about the crown jewels and you don’t have people who would have sufficient knowledge of both your org and the threat landscape?

> Separate INTERNAL and EXTERNAL exercise

Process of iterations and improvement

Difficult to have the perfect process on year one



Year 1 – trial: seek inputs from selected number of people.

Make sure they understand the questions and the risk assessment exercises

Year 2 – improved process: lessons learned from Year 1 – engage more people in your organization

TLP:CLEAR

Challenges

- Lack of awareness of the purpose of the PIRs across the organization and even InfoSec
- Find the right balance for the level of detail
- You can easily overcomplicate the whole process and go in too much detail
- You can keep it too high-level and be vague
- Can be resource intensive

Opportunities

- Learn about your organization
- Learn about the threat landscape
- Engage with teams across your organization
- Good to have the PIRs…

TLP:CLEAR

Integration of PIRs into the CTI lifecycle

Integration of PIRs into the CTI lifecycle

- Collection management priorities
- CTI platforms alerting
- Detection priorities
- Threat hunting program priorities
- Long-term analytical deliverables priorities

TLP:CLEAR

Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

Ondra Rojčík

@orojcik

in ondrejrojcik/