TLP:CLEAR

Priority Intelligence Requirements Workshop

How to Set the Direction of Your CTI Program

Ondra Rojcik, Vladimir Janout
CTI Analysts

TLP:CLEAR

Ondra Rojčík

in/orojcik

- CTI Analyst at Red Hat
- Threat Intel analyst since 2006: Czech gov and NATO Intelligence Production Unit; co-founder and Head of Strategic CTI at Czech Cyber Security Agency (NÚKIB)
- Primary focus: analysis & reporting, CTI processes & tradecraft

Vladimír Janout

in/vladimir-janout

- CTI Analyst at Red Hat
- Joined Red Hat in 2021 as intern, after graduating joined full time in 2022
- Primary focus: Operationalization of threat intelligence, intel platforms, SOAR and automation

Red Hat

TLP:CLEAR

Priority Intelligence Requirements Workshop

- Why PIRs
- The Red Hat process
- Who is it for
- Retired version
- v2.0
- ELEMENTS (exercise)
- ASSETS (exercise)
- Adversarial operations (exercise)
- Risk assessment (exercise)
- Operationalization

Red Hat

Why we need PIRs

- The threat landscape is a confusing place
- It is hard to figure out what to focus on
- So many threats out there, so few people on the team

Source: Midjourney

Red Hat

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

The PIRs help to identify the most relevant threats for your organisation

Provides the focus and direction to your CTI team

- Intelligence Requirements & Direction
- Monitoring & Alerting
- Collection Management
- Research, Investigation & Analysis
- Threat Informed Defence
  - Threat Hunting
  - Detection

Why we developed the Red Hat approach

Existing approaches

- Assumption that you know what type of threat actors is motivated to attack the “crown jewels” of your organisation
- The resulting PIRs tend to be general, but **not tailored** enough **for your organization**
- **Focus on external threats** without clearly defined links to your organization and its assets

Defining the Intelligence Requirements: What Does the CTI Community Know about the Process?

Intel471

Feedly

Who is our approach for?

Internal CTI

If you are an internal CTI team

Limited knowledge of threat landscape

Desire to engage stakeholders with great knowledge of your business, but limited knowledge of the threat landscape

Threats to your org

Want to know how threats relate to your organisation

Multiple “crown jewels”

Organisations are often complex and may have various different crown jewels (some you may not even think about)

Or you want to keep it low - within the CTI/InfoSec team

Red Hat

TLP:CLEAR

slido

What is your current relationship with Priority Intelligence Requirements (PIRs)

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

V0000000

TLP:CLEAR

slido

What's the size of your CTI team?

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

V0000000

TLP:CLEAR

slido

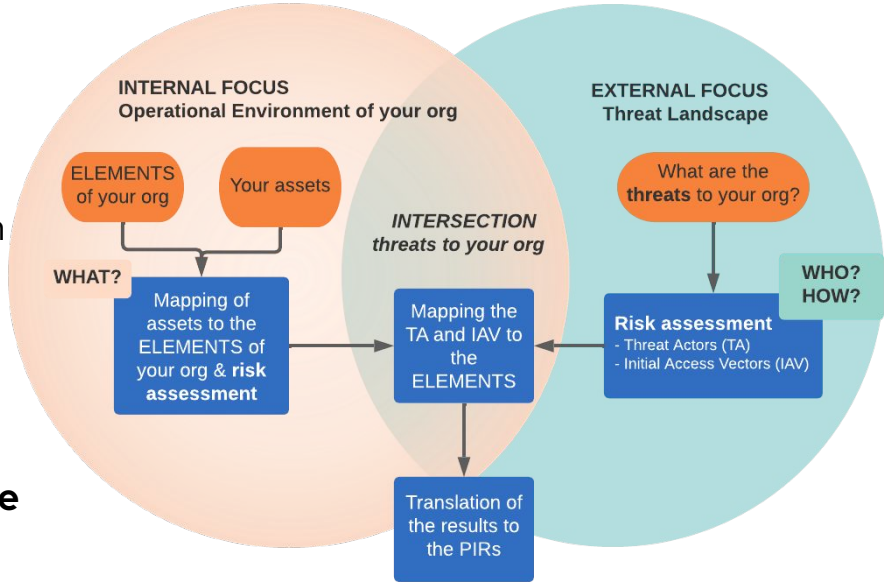
Which option best describes your CTI team's area of focus

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

V0000000

The original - RETIRED - process overview

- An intersection of organization's operational environment and the threat landscape
- High-level risk assessment and adversary evaluation
- Collaborative exercise engaging multiple teams
- **Ambition to provide WHAT, WHO and HOW of the threat landscape**

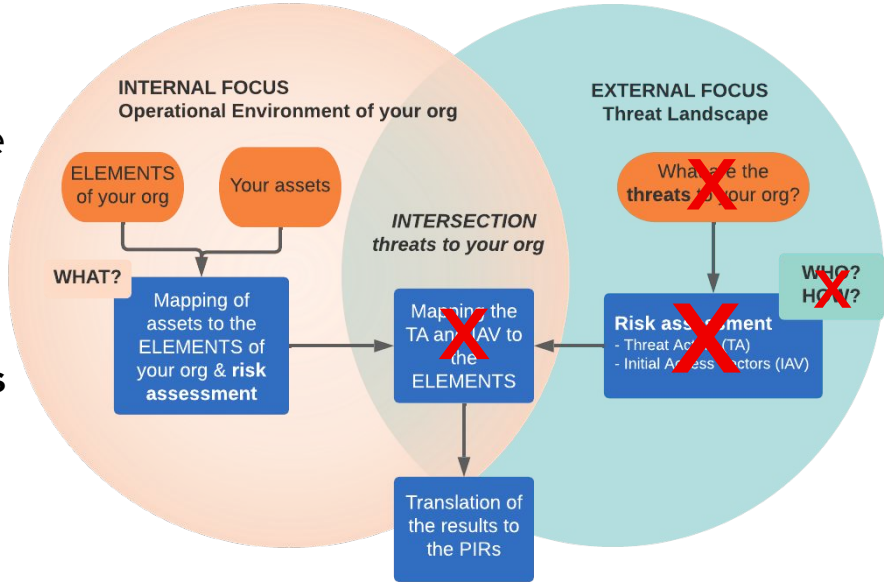


Simplification of the PIR development process

- WHO and HOW are critical Qs, but…
- More focus on the part that provides the most value and is easy to operationalise

WAS: one or two months > NOW: one or two weeks

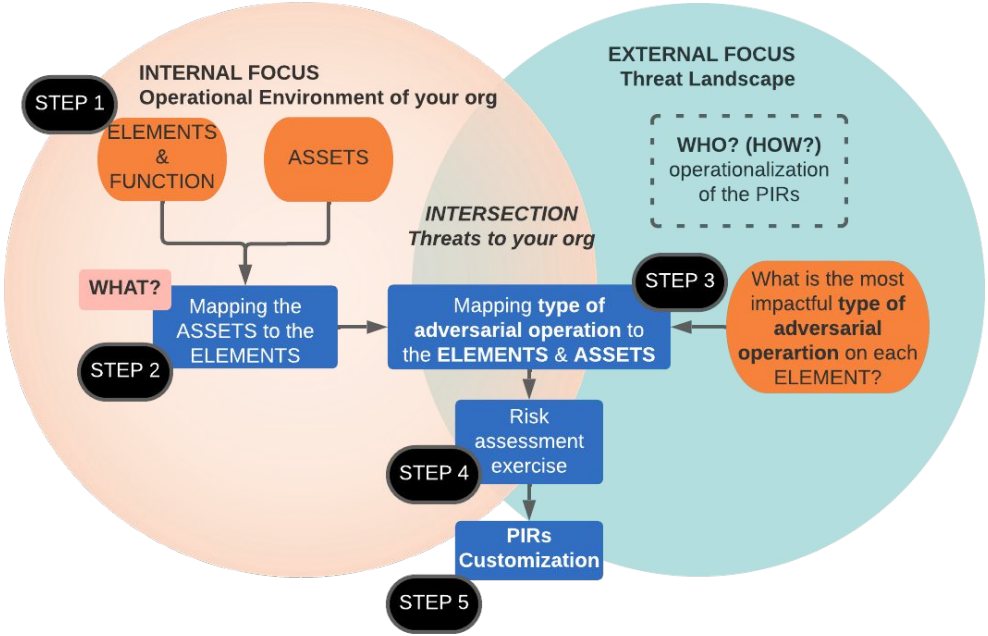
While keeping the parts with the best ROI



Red Hat

RH PIR Development Process 2.0

- ELEMENTS of organisation
- Most of the focus goes inwards
- Identify the crown jewels of your organisation
- The main Threat Landscape part is the "**type of adversarial operation**"
- Is it a Threat Modeling?



Red Hat

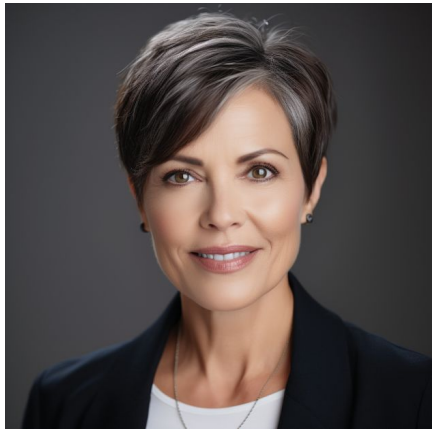
STELLAR Electric

Mock-up company for this workshop

- EU-based electric vehicle (EV) company
- Founded in 2015
- Revenue of 1.344 billion EUR
- 20% longer range compared to competitors
- Production and research facilities located in the EU and China
- Supply chain, sourcing lithium batteries - China, Chile

STELLAR Electric

- Over the last five years revenue has surged by 348%, from €300 million in 2017 to €1.34 billion in 2022.
- In 2022 limitations in battery production facilities
- Growth rate of only 12% for 2022 compared to around 50% in previous years; profit margin 7%



Andrea Jensen
Chairwoman, Stellar Electric

Stellar Electric - **Annual Report**

Strategy and objectives

Innovative Range-Boosting Technology
We remain steadfast in our commitment to innovation. Our primary objective is to develop and refine our proprietary range-boosting technology, setting a new standard for EV range.

Sustainability Leadership
Our strategy goes beyond product excellence. We aim to lead the industry in sustainability, focusing on reducing our carbon footprint and advocating for a greener future.

Software-First Approach
We will adopt a software-first approach to vehicle development, emphasizing the integration of cutting-edge software solutions into our vehicles. This approach will enable us to enhance vehicle functionality, connectivity, and user experience.

Advanced Driver Assistance Systems (ADAS)
Our objective is to develop and implement advanced driver assistance systems that elevate safety, convenience, and autonomous capabilities in our vehicles. We aim to be at the forefront of ADAS technology, continually enhancing features like adaptive cruise control, lane-keeping assistance, and automated parking.

Advanced Safety Features
We will continue to innovate and implement advanced safety features, including collision avoidance systems, pedestrian detection, and emergency braking. These technologies are designed to mitigate accidents and reduce the severity of collisions.

Cybersecurity Resilience
As vehicles become more connected, cybersecurity is a top concern. We will invest in robust cybersecurity measures to protect our vehicles and customer data from potential threats, maintaining trust and safety.

Global Expansion
We seek to expand our global footprint, making our cutting-edge EVs available to consumers in new markets while adhering to local regulations and preferences.

Stellar Electric

Portions of this document have been generated using ChatGPT model developed by OpenAI. Images generated in part by MidJourney AI.

Performance indicators

20%
longer range compared to competitors

95%+
CSI rating each year

12%
of revenue going into research and development

25%
increase in international sales

Range Advancement: Stellar's unique range-boosting technology has delivered a consistent 20% longer range compared to competitors, solidifying our position as an industry leader.

Customer Satisfaction Index (CSI): Our relentless focus on customer satisfaction has resulted in consistently high CSI ratings, exceeding 95% each year.

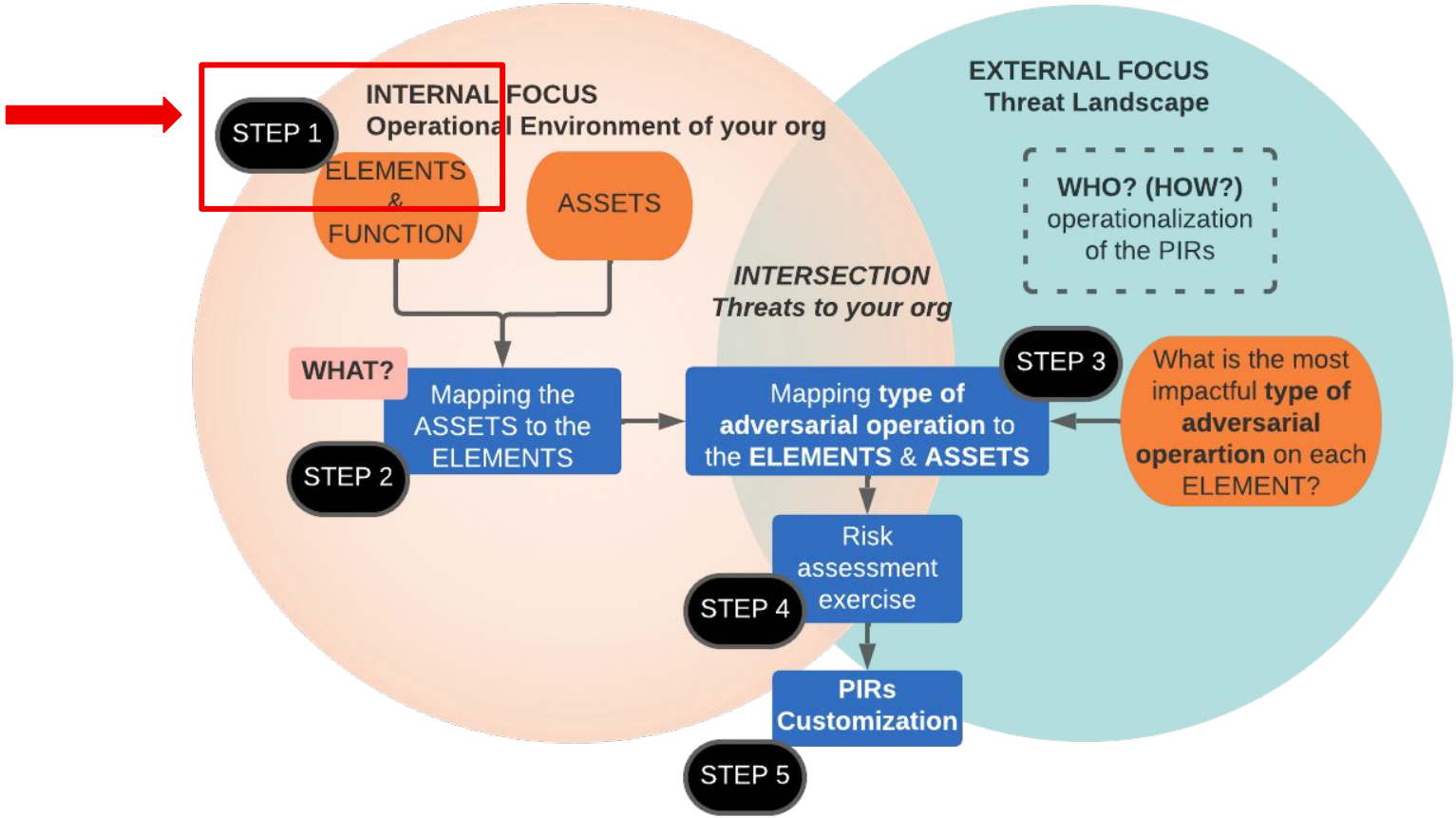
Employee Engagement: We maintain high levels of employee engagement and retention, reflecting our commitment to empowering our workforce.

Research and Development Investment Ratio: Stellar allocates 12% of its revenue to research and development, driving continuous innovation in EV technology.

Market Expansion: Our successful entry into new international markets has contributed to a 25% increase in international sales.

Stellar Electric

Portions of this document have been generated using ChatGPT model developed by OpenAI. Images generated in part by MidJourney AI.


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?) operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 1a core ELEMENTS of your business and strategy (INTERNAL FOCUS)

Extract keywords representing your

- organization
- its strategy
- mission and vision

From high-level strategic documents defining your organization and depicting your organization's strategy

Output: ELEMENTS

Step 1a core ELEMENTS of your business and strategy (INTERNAL FOCUS)

Identify documents from which you can extract ELEMENTS of your business and strategy

- Annual Reports
- Business strategy for next n years
- “About” section of your webpage
- Town hall meetings, presentations by your CEO
- “Who we are” internal reports

Step 1a core ELEMENTS of your business and strategy (INTERNAL FOCUS)

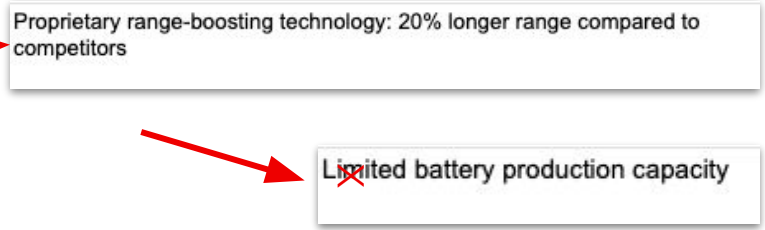
How to define ELEMENTS

- What features **define** your organisation?
- What makes your organization **unique**?
- What are the most important aspects of your **strategy**?
- Why is anyone **buying** your products or services?
- Why are you **ahead** of competitors?
- Should you pay special attention to a particular **product or service**?
- What might the **valuable data** that you have?
    - Data that keeps you ahead of competitors, proprietary information, R&D, data on relations with partners or customers, potentially damaging information

Step 1a core ELEMENTS of your business and strategy (INTERNAL FOCUS)

How to define ELEMENTS

- What features define your organisation?
- What makes your organization unique?
- What are the most important aspects of your strategy?
- Why is anyone buying your products or services?
- Why are you ahead of competitors?
- Should you pay special attention to a particular product or service?
- What might the valuable data that you have?
  - Data that keeps you ahead of competitors, proprietary information, R&D, data on relations with partners or



TLP:CLEAR

ELEMENT

Limited battery production capacity

About

Stellar Electric, an EU-based leader in the electric vehicle (EV) industry, stands at the forefront of sustainable transportation solutions. With a revenue of **1.344 billion EUR**, Stellar has firmly established itself as a EU-based key player in both the European and Chinese markets. Our commitment to innovation and environmental responsibility is echoed in our production and research facilities strategically located in both the EU and China, enabling us to leverage diverse expertise and technologies.

However, in 2022, we faced a significant challenge in the form of capacity limitations in our battery production facilities. These limitations impacted our ability to meet the growing demand for our electric cars, resulting in a growth rate of only **12%** for the year. We acknowledge this issue and are actively investing in expanding our manufacturing capacity to address this bottleneck.

Furthermore, we maintain a global perspective on our supply chain, sourcing lithium batteries not only from China but also from the resource-rich mines of Chile. This approach ensures the quality and reliability of our EVs while supporting. a responsible and sustainable battery supply chain. Stellar Electric is dedicated to redefining the EV landscape, providing eco-conscious consumers in the EU and China with vehicles that merge cutting-edge technology, exceptional performance, and a deep commitment to a greener future.

Our purpose

At Stellar Electric, our purpose is to redefine the electric vehicle (EV) industry through groundbreaking technology. We are dedicated to offering sustainable mobility solutions that not only reduce emissions but also provide our customers with a superior driving experience, backed by a remarkable 20% longer range compared to our competitors.

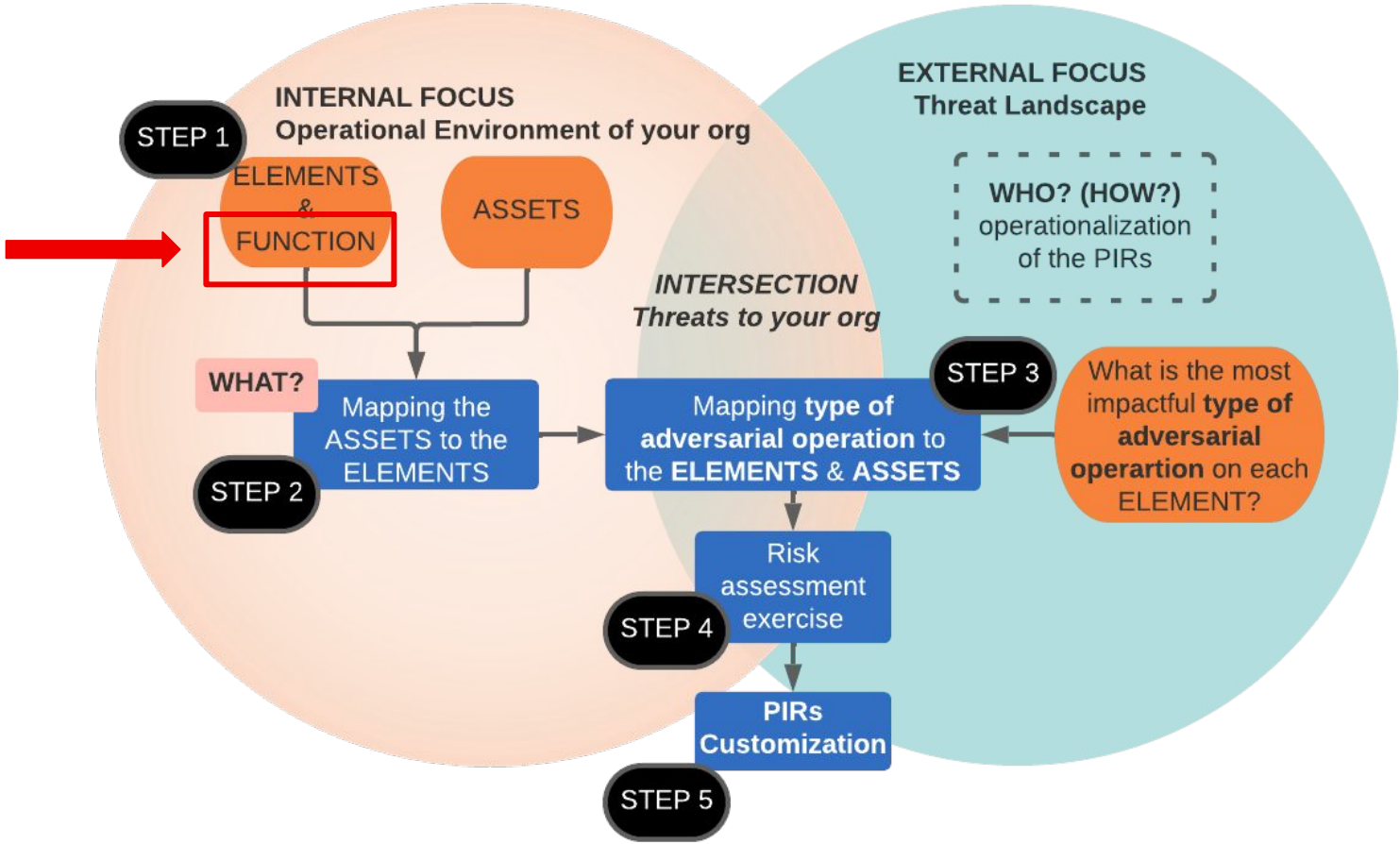
ELEMENT

Proprietary range-boosting technology: 20% longer range compared to competitors

Stellar Electric

Portions of this document have been generated using ChatGPT model developed by OpenAI.
Images generated in part by Midjourney AI.

Red Hat


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization
of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 1b THE FUNCTION (INTERNAL FOCUS)

A	B	C	D
Item No.	**ELEMENTS of STELLAR and STELLAR Strategy**	**THE FUNCTION (what is it about the ELEMENTS that needs to be secured)**	**Supporting ASSETS (mainly technology and data/information)**

THE FUNCTION - provides context to ELEMENTS where the relation to information security is not clear

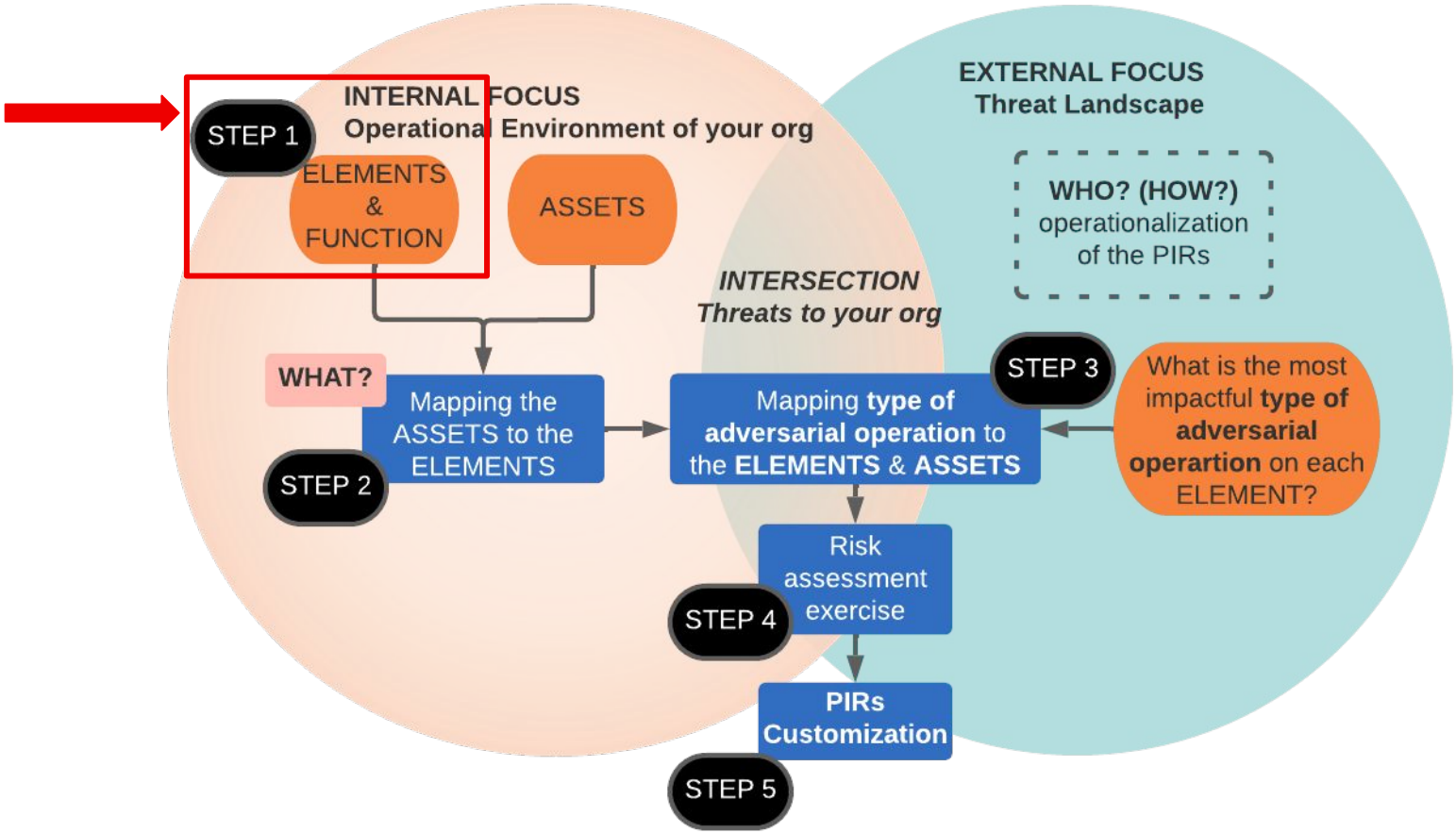
Output: List of ELEMENTS and corresponding FUNCTION

Step 1b THE FUNCTION (INTERNAL FOCUS)

ELEMENTS of STELLAR and STELLAR Strategy - STEP 1	THE FUNCTION - what is it about the ELEMENTS that needs to be secured (STEP 1)
Limited battery production capacity	Up and running battery production
Proprietary range-boosting technology: 20% longer range compared to competitors	Custodian of proprietary data

PIR exercise Link

red.ht/pir


STEP 1
INTERNAL FOCUS
Operational Environment of your org
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 1a & 1b ELEMENTS and FUNCTION exercise

red.ht/pir

15 minutes individual exercise (I.)

Task: identify the ELEMENTS and FUNCTION (2-5) **of STELLAR**

Output: ELEMENTS and their FUNCTION

Step 1a & 1b ELEMENTS and FUNCTION EXERCISE

red.ht/pir

Questions for defining ELEMENTS

- What features define your organisation?
- What makes your organization unique?
- What are the most important aspects of your strategy?
- Why is anyone buying your products or services?
- Why are you ahead of competitors?
- What might the valuable data that you have?
  - Data that keeps you ahead of competitors, proprietary information, R&D, data on relations with partners or customers, potentially damaging information

ELEMENTS = The essence of the organization

FUNCTION = What needs to be secured about ELEMENT

Step 1a core ELEMENTS of your business and strategy (INTERNAL FOCUS)

How to define ELEMENTS

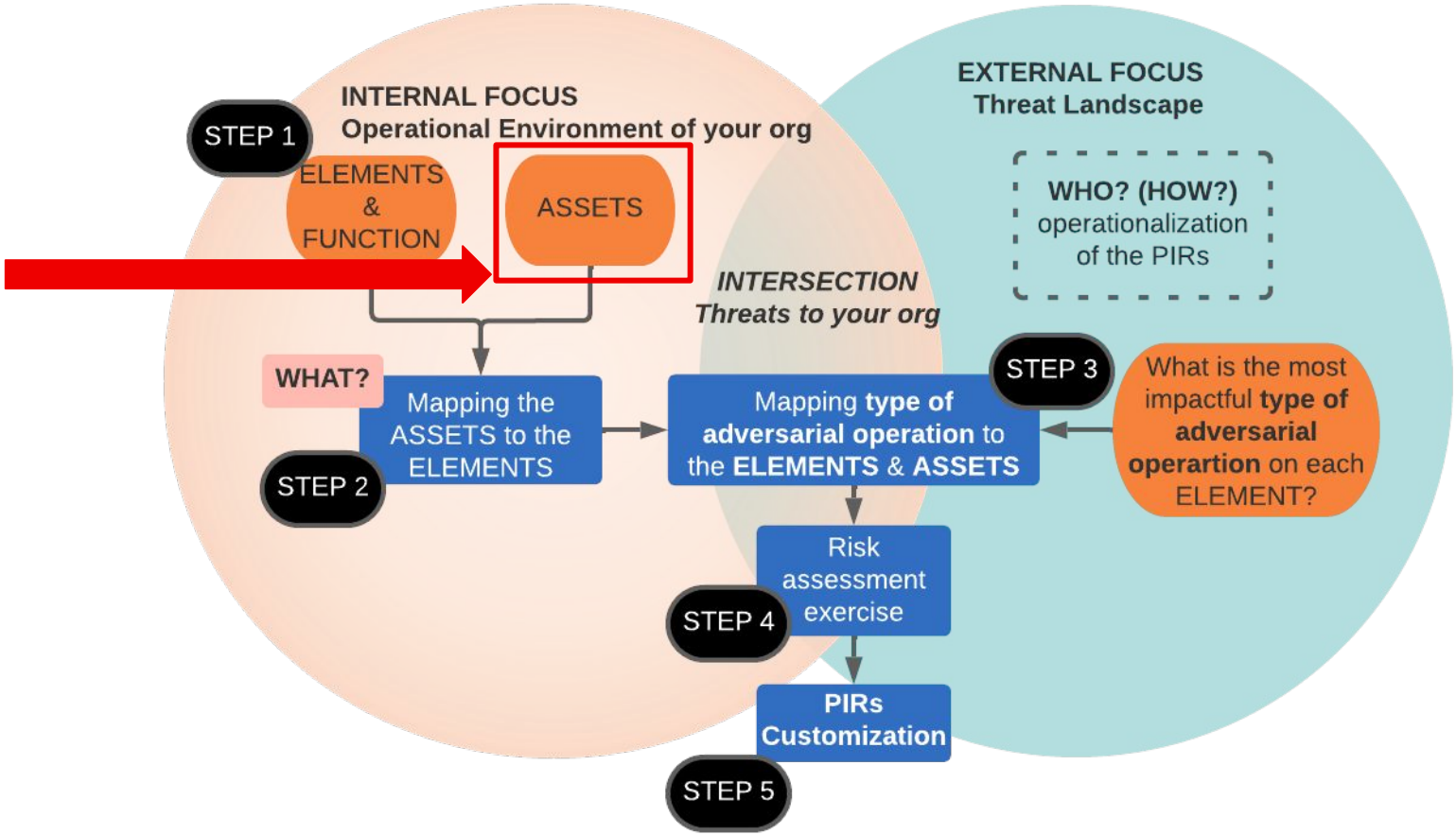
- What are the features of your organisation that define it?
- What makes your organization unique?
- What are the most important aspects of your strategy?
- Why is anyone buying your products or services?
- Why are you ahead of competitors?
- Should you pay special attention to a particular products or services?
- What might be the valuable data that you have?

STELLAR keywords > ELEMENTS

- EU-based, electric vehicle industry company with revenue over 1 billion EUR
- Research and Development in EU and China drives the company success
- Car production in EU and China
- Limited battery production capacity
- Supply chain, spans multiple countries, including China and Chile.
- Proprietary range-boosting technology: 20% longer range compared to competitors
- Public perception of Stellar environmental impact is vital to the brand reputation
- Software-first approach; proprietary In-vehicle software
- Advanced safety features

Step 1b THE FUNCTION – EXAMPLE

ELEMENTS of STELLAR and STELLAR Strategy - STEP 1	THE FUNCTION - what is it about the ELEMENTS that needs to be secured (STEP 1)
EU-based, electric vehicle industry company with revenue over 1 billion EUR	Effective operations at all corporate levels. Uninterupted sales and delivery of electric cars
Research and Development in EU and China drives the company success	Custodian of R&D data
Car production in EU and China	Up and running car production
Limited battery production capacity	Up and running battery production
Supply chain, spans multiple countries, including China and Chile. Any disruptions in the supply chain may result in production delays and increased costs	Safe and secure supplian chains
Proprietary range-boosting technology: 20% longer range compared to competitors	Custodian of proprietary data
Public perception of Stellar environmental impact is vital to the brand reputation	Custodian of sensitive corporate information
Software-first approach; proprietary In-vehicle software	In-vehicle software development and provision
Advanced safety features - technologies to mitigate accidents and reduce the severity of collisions	Development and deployment of vehicle safety fetures


INTERNAL FOCUS
Operational Environment of your org
EXTERNAL FOCUS
Threat Landscape
STEP 1
ELEMENTS & FUNCTION
ASSETS
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 2 ASSET mapping exercise

Supporting Asset
Research and Development Data (R&D)
Operational Technology and Industrial Control Systems (OT&ICS)
Sensitive corporate information
Partner and third party information
Contracts with government entities
Proprietary information
Software development pipeline
Continuous integration and continuous delivery/continuous deployment (CI/CD tools)
All organizational assets

8 minutes individual exercise (II.)

Task: map the most important ASSETS to ELEMENTS

Use examples from the Assets sheet.

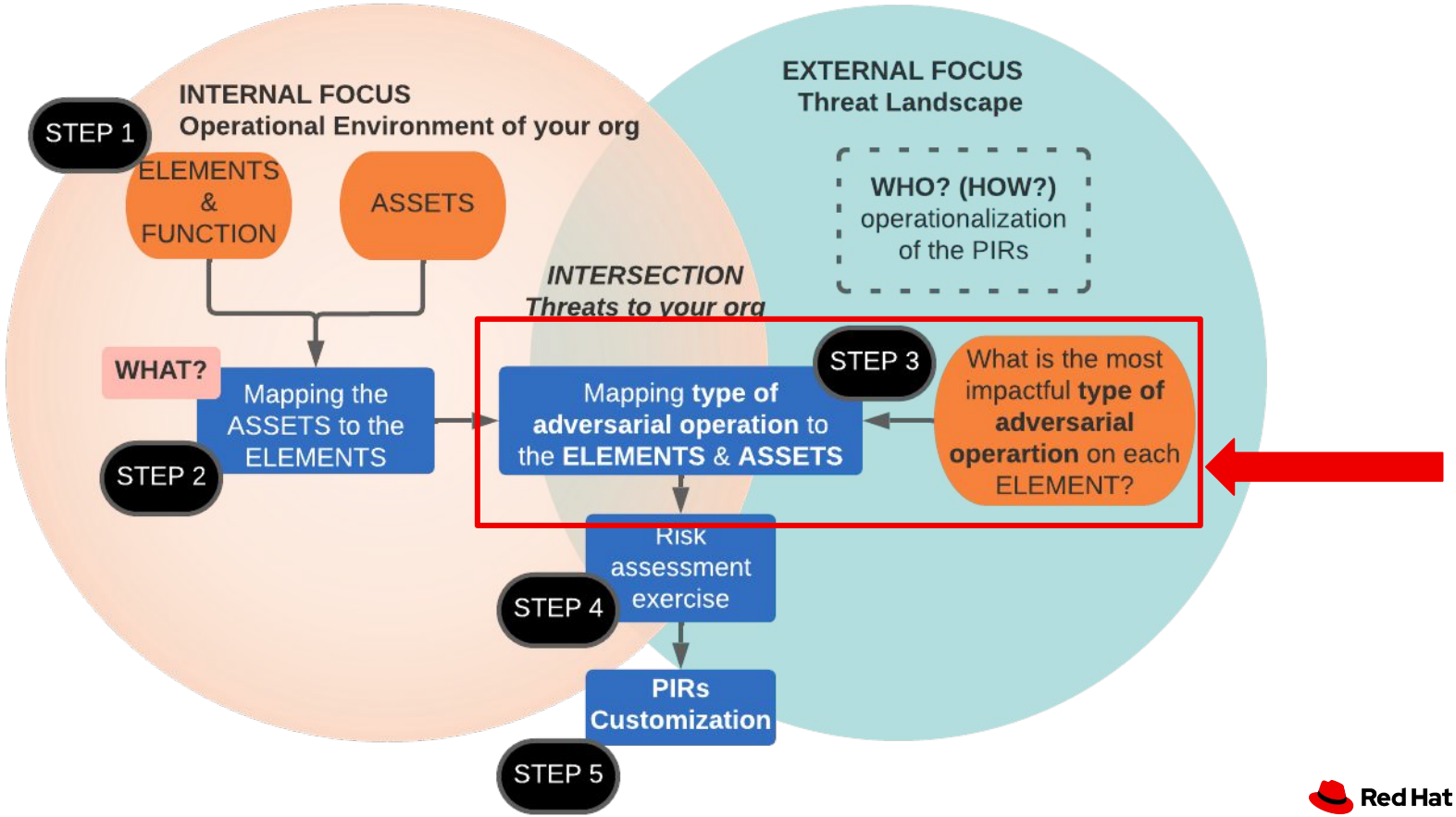
Examples of **Function**/**Asset** relationship:

- **Function: Up and running battery production**
- **Asset: Operational Technology and Industrial Control Systems (OT&ICS)**

Output: "Supporting ASSETS" column in the Sheet listing the ELEMENTS representing your organization and its strategy

Step 2 ASSETS and technologies in support of the ELEMENTS (INTERNAL FOCUS)

ELEMENTS of STELLAR and STELLAR Strategy - STEP 1	THE FUNCTION - what is it about the ELEMENTS that needs to be secured (STEP 1)	Supporting ASSETS (mainly technology and data/information) (STEP 2)
Limited battery production capacity	Up and running battery production	OT&ICS
Proprietary range-boosting technology: 20% longer range compared to competitors	Custodian of proprietary data	Proprietary information


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
STEP 3
Mapping type of adversarial operation to the ELEMENTS & ASSETS
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 3 Mapping types of adversarial operations (EXTERNAL FOCUS & INTERSECTION)

Type of Adversarial Operation	MITRE ATT&CK technique	Keywords for operationalisation
Ransomware	T1486 Data Encrypted for Impact T1490 Inhibit System Recovery TA0010 Exfiltration	ransom, ransomware, encryption, extortion, double extortion, triple extortion, crypto-malware
Business Email Compromise & Fraud	*T1566 Phishing* *T1078 Valid Accounts*	business email compromise, BEC, phishing, spear phishing, whaling, social engineering, financial fraud, copyright
Stolen Information & Espionage	TA0010 Exfiltration	espionage, cyber espionage, exfiltration, industrial espionage, government, confidentiality, classified information, sensitive information, proprietary information, PII, HIPAA
Denial of Service & Availability	T1499 Endpoint Denial of Service T1495 Firmware Corruption T1498 Network Denial of Service T1489 Service Stop ...	DoS, DDoS, availability, shutdown, data wipe, data destruction, sabotage
Resource Hijacking	T1496 Resource Hijacking	resource hijacking, cryptojacking, cryptomining, cryptocurrency, kubernetes
Initial Point of Supply Chain Attack	T1565 Data Manipulation The “Initial Point of Supply Chain Attack” is not “T1195 Supply Chain Compromise” as this MITRE ATT&CK technique is on the “Initial Access” vector side	third-party, vendor, external components, inject malicious code, malicious update, open-source software repositories, manipulated packages, repojacking
Data Manipulation	T1565 Data Manipulation T1491 Defacement	integrity, data manipulation, defacement, software supply-chain, repojacking, malicious code injection, compromised repository, software dependency, CI/CD
Internal User Error	*NA*	*Misconfigured services and systems, misconfigured access and authorization, service or API exposure, accidental leak or modification of data, credentials, secrets, confidential information, corporate data, sensitive data*

Step 3 Mapping types of adversarial operations (EXTERNAL & INTERSECTION)

Type of Adversarial Operation
Ransomware
Business Email Compromise & Fraud
Stolen Information & Espionage
Denial of Service & Availability
Resource Hijacking
Initial Point of Supply Chain Attack
Data Manipulation
Internal User Error

- Arbitrary list
- It can be adjusted to the needs of any organisation
- Internal User Error - an outlier - not a type of adversarial operation
  - Includes **unintentional leaks** sensitive information by an insider
  - Can be a separate category
- Stolen Information & Espionage
  - Includes **intentional leaks** of sensitive information by insider
  - Can be a separate category

Step 3 Mapping types of adversarial operations (EXTERNAL & INTERSECTION)

You **can** use existing frameworks and taxonomies

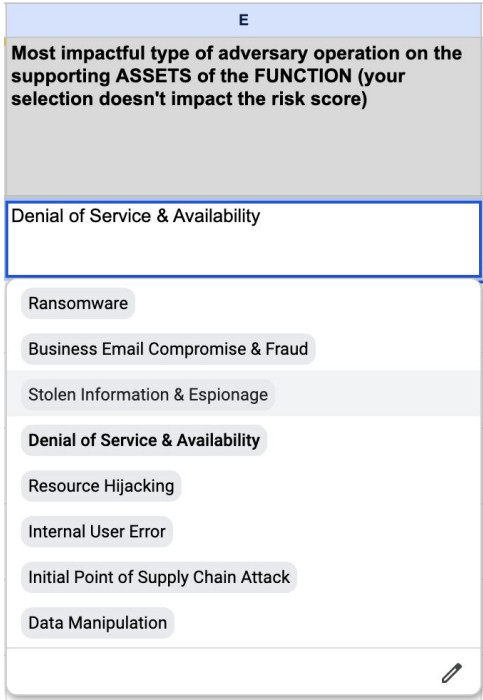
- MITRE ATT&CK
- Confidentiality, Integrity, Availability
- STRIDE
- VERIS Framework
- CAPEC
- ENISA or FIRST taxonomies

Step 3 Mapping types of adversarial operations exercise

10 minutes individual exercise (II.)

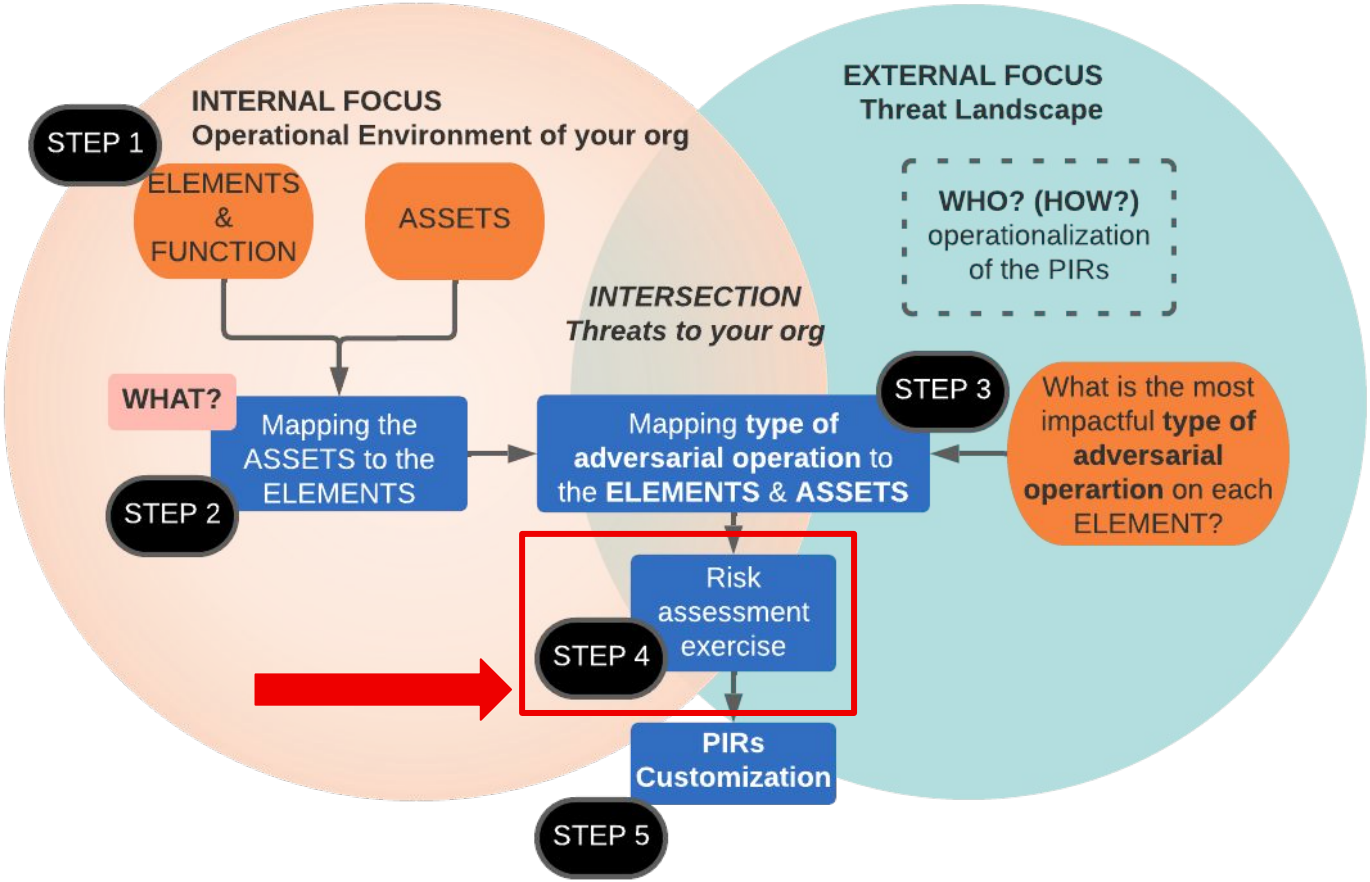
Task: map the most impactful types of adversarial operations to ELEMENT

What type of adversarial operations would most have the biggest impact on an ELEMENT?



Output: Mapped types of adversarial operations to ELEMENTS

Red Hat


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 4 RISK ASSESSMENT

(Likelihood Q) APPEAL of the ELEMENT and supporting ASSET for attackers - consider the worst case scenario

APPEAL for attackers:

- Extremely appealing
- Very appealing
- Moderately appealing
- Slightly appealing
- Not at all appealing

(Impact Q) Consider the worst case scenario of an impact on STELLAR if a threat actor attacks the supporting ASSETS

Impact:

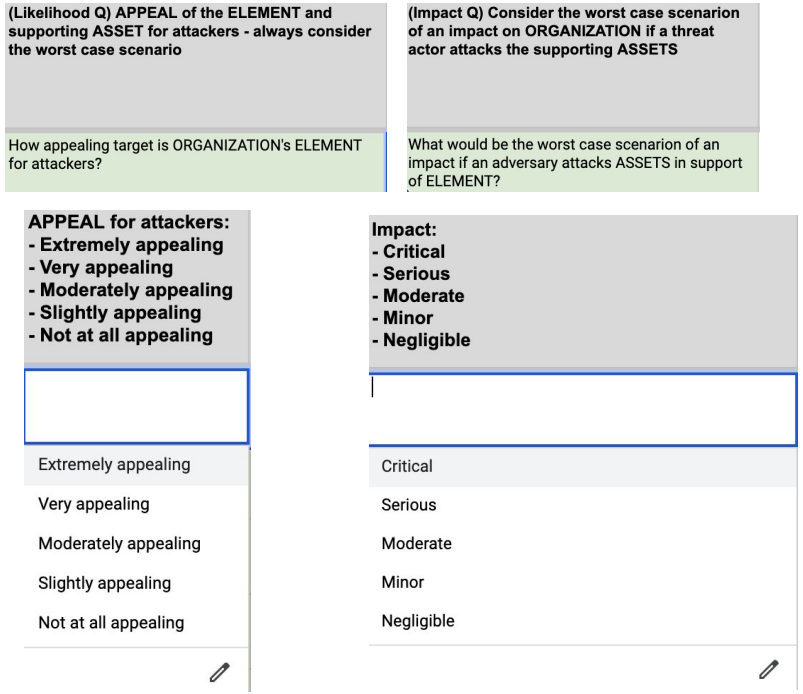
- Critical
- Serious
- Moderate
- Minor
- Negligible

Step 4 RISK ASSESSMENT exercise

10 minutes individual exercise (III.)

Task: risk assessment exercise - likelihood and impact of adversarial operation against an ELEMENT

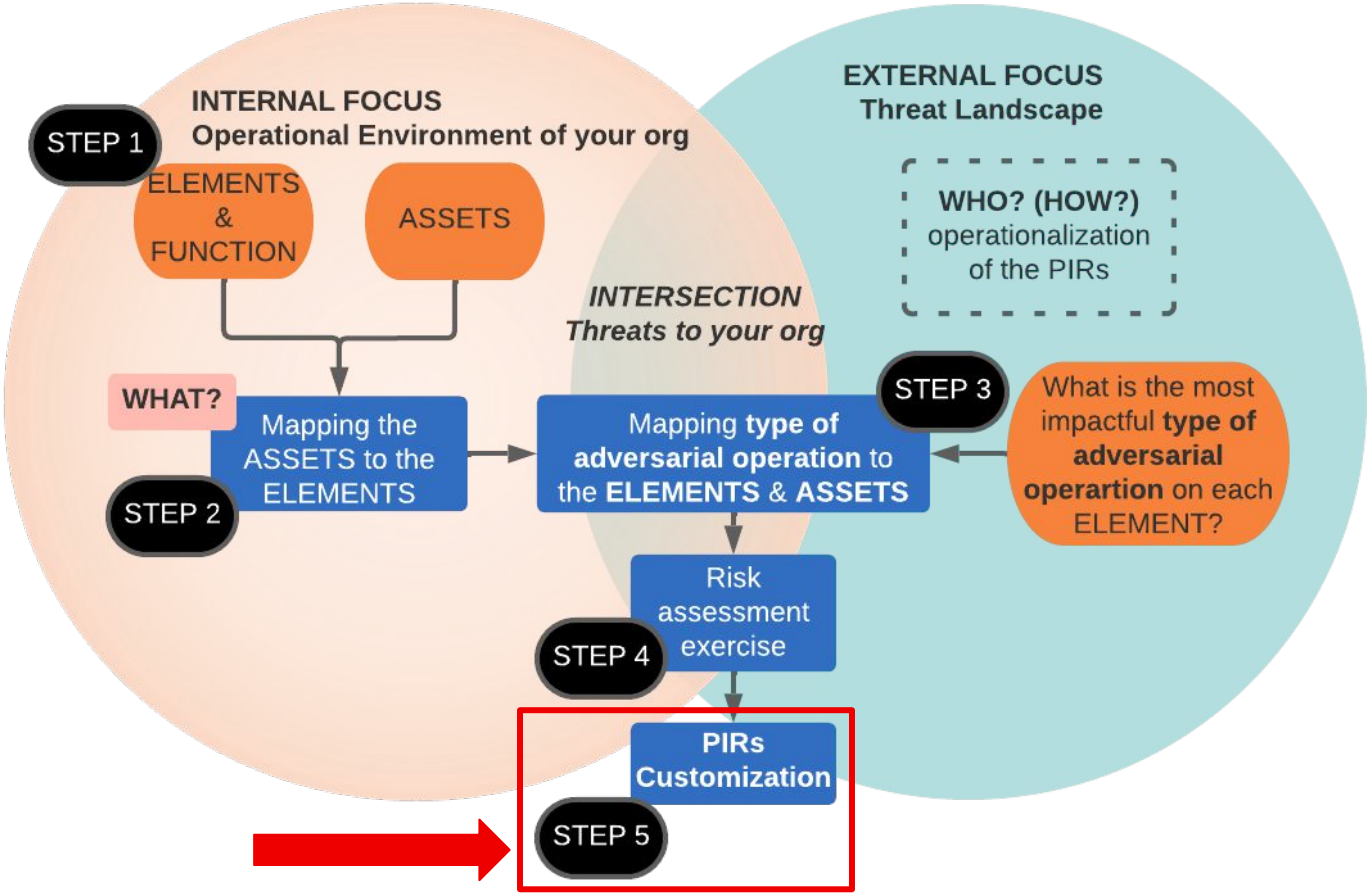
Output: Scored and ranked ELEMENTS and your top PIRs



Step 4 RISK ASSESSMENT

ELEMENTS of ORGANIZATION and ORGANIZATION Strategy	AL of the ELEMENT and r attackers - always consider rio	APPEAL for attackers: - Extremely appealing - Very appealing - Moderately appealing - Slightly appealing - Not at all appealing	(Impact Q) Consider the worst case scenarion of an impact on ORGANIZATION if a threat actor attacks the supporting ASSETS	Impact: - Critical - Serious - Moderate - Minor - Negligible	Risk score
Car production in EU and China	re STELLAR's OT&ICS in on?	Moderately appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of car production in EU and China?	Serious	12
Limited battery production capacity	re STELLAR's OT&ICS in luction?	Moderately appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of limited battery production capacity?	Serious	12
Supply chain, spans multiple countries, including China and Chile. Any disruptions in the supply chain may result in production delays and increased costs	STELLAR's corporate d third party information, ent entities?	Slightly appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of supply chain?	Moderate	6
Proprietary range-boosting technology: 20% longer range compared to competitors	STELLAR's proprietary oosting technology?	Extremely appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of proprietary range-boosting technology?	Serious	20
Public perception of Stellar environmental impact is vital to the brand reputation	STELLAR's corporate of environmental impact?	Slightly appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of public perception of STELLAR environmental impact?	Moderate	6
Software-first approach; proprietary In-vehicle software	STELLAR's in-vehicle software sioning?	Moderately appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of in-vehicle software development and provisioning?	Critical	15
Advanced safety features - technologies to mitigate accidents and reduce the severity of collisions	STELLAR's development and afety fetures ?	Moderately appealing	What would be the worst case scenarion of an impact if an adversary attacks ASSETS in support of development and deployment of vehicle safety fetures ?	Critical	15

Output: Scored and ranked ELEMENTS and your top 5/10 ELEMENTS


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

Step 5 PIRs Customization

Use the ranked list of Top 5/10 ELEMENTS with mapped types of adversarial operations to generate the PIRs.

The PIRs can be in any form that is appropriate for the intended operationalization:

- short statements
- intelligence questions
- requests for information etc.

Output: PIRs

Step 5 PIRs Customization

PIR
1 Proprietary range-boosting technology: 20% longer range compared to competitors Type of Attack: Stolen Information & Espionage, Data Manipulation
#2 Research and Development in EU and China drives the company sucess Type of Attack: Stolen Information & Espionage, Data Manipulation
#3 Software-first approach; proprietary In-vehicle software Type of Attack: Data Manipulation, DoS & Attack on Availability
#4 Advanced safety features - technologies to mitigate accidents and reduce the severity of collisions Type of Attack: Data Manipulation, DoS & Attack on Availability
#5 Car production in EU and China Type of Attack: DoS & Attack on Availability, Internal User Error

- Statements
- Intelligence Questions
- RFIs
- Any other form

Engage multiple respondents > additional “step” > **calculate median score**

Step 5 PIRs Customization

Rephrase the result to statements that can be operationalized if needed

PIR
1 Proprietary range-boosting technology: 20% longer range compared to competitors Type of Attack: Stolen Information & Espionage, Data Manipulation
#2 Research and Development in EU and China drives the company sucess Type of Attack: Stolen Information & Espionage, Data Manipulation
#3 Software-first approach; proprietary In-vehicle software Type of Attack: Data Manipulation, DoS & Attack on Availability
#4 Advanced safety features - technologies to mitigate accidents and reduce the severity of collisions Type of Attack: Data Manipulation, DoS & Attack on Availability
#5 Car production in EU and China Type of Attack: DoS & Attack on Availability, Internal User Error

EU-based, electric vehicle industry company with revenue over 1 billion EUR

- PIR # n Threats to STELLAR based on its revenue, geography, industry and position on the market

TLP:CLEAR

Operationalization

Buckets of Keywords: for each PIRs

Specific Intelligence Requirements (SIRs)

Threat Actors Prioritization: lists of threat actors for individual PIRs

Strategic level

Keywords > Queries and Alerting in TIPs

SIRs > research questions/topics

Tactical level

TAP > TTPs of the priority threat actors

Operationalization is depended on the scope of your CTI team

Operationalization: enrich the PIRs by keywords

Priority Intelligence Requirements		
PIR	**PIR keywords**	**Type of Adversary Operation keywords**
# 1 Proprietary range-boosting technology: 20% longer range compared to competitors Type of Adversary Operation: Stolen Information & Espionage, Data Manipulation		espionage, cyber espionage, exfiltration, industrial espionage, government, confidentiality, classified information, sensitive information, confidential information, proprietary information, PII, HIPAA | integrity, data manipulation, defacement, software supply-chain, repojacking, malicious code injection, compromised repository, software dependency, CI/CD
#2 Research and Development in EU and China drives the company sucess Type of Adversary Operation: Stolen Information & Espionage, Data Manipulation		espionage, cyber espionage, exfiltration, industrial espionage, government, confidentiality, classified information, sensitive information, confidential information, proprietary information, PII, HIPAA | integrity, data manipulation, defacement, software supply-chain, repojacking, malicious code injection, compromised repository, software dependency, CI/CD
#5 Car production in EU and China Type of Adversary Operation: DoS & Attack on Availability, Internal User Error	Operational Technology, Industrial Control System, Industrial Production, Factory, Production Facility, Cars, Vehicles, EV, Car Production	sabotage DoS, DDoS, availability, shutdown, data wipe, data destruction, sabotage | misconfigured services and systems, misconfigured access and authorization, service or API exposure, accidental leak or modification of data, credentials, secrets, confidential information, proprietary technology/information, corporate data, sensitive data

- Buckets of keywords for each PIR
- Your “manual” job - not part of this process

#5 Car production in EU and China
Type of Adversary Operation: DoS & Attack on Availability, Internal User Error

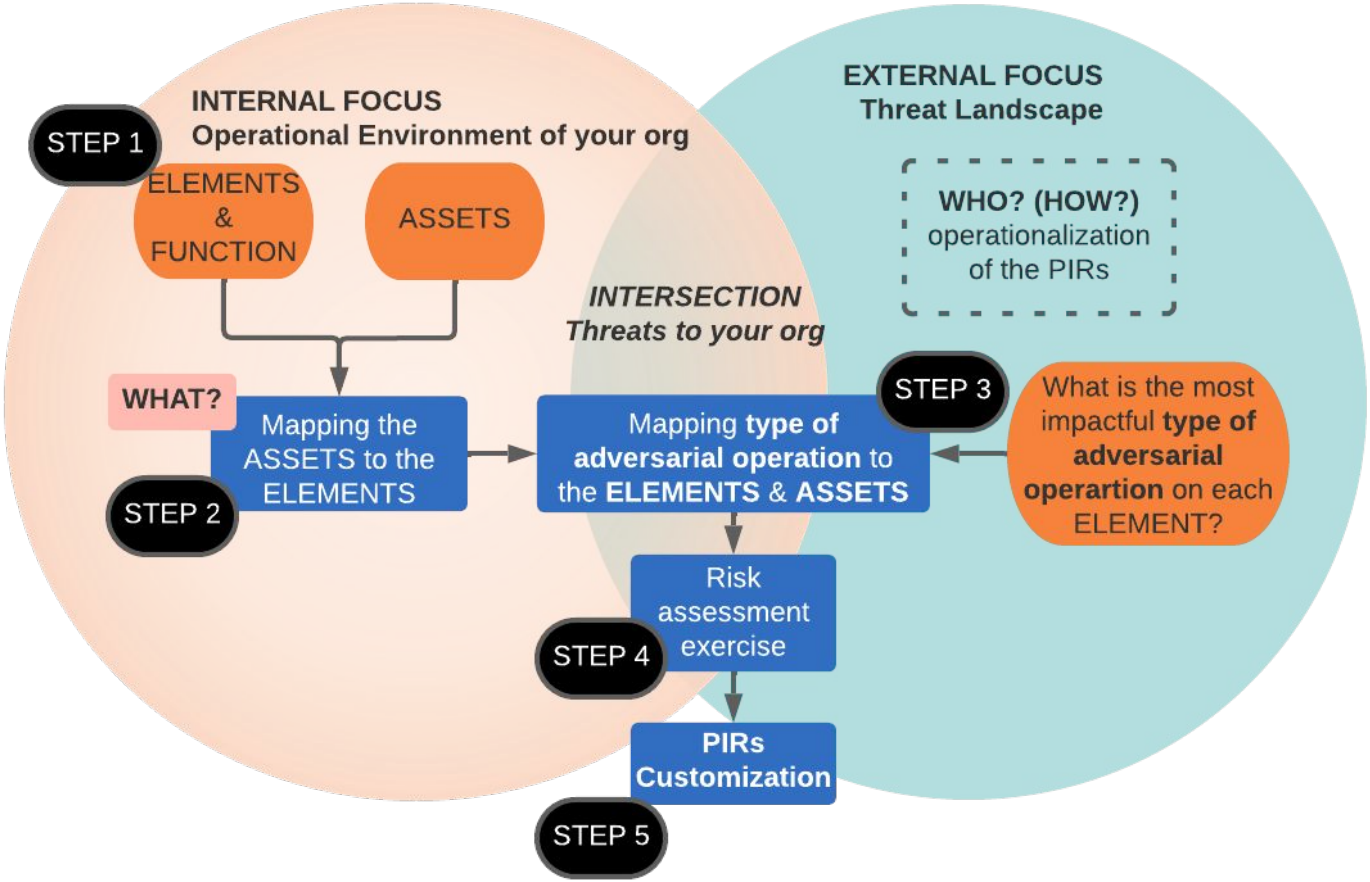
Operational Technology, Industrial Control System, Industrial Production, Factory, Production Facility, Cars, Vehicles, EV, Car Production

sabotage
DoS, DDoS, availability, shutdown, data wipe, data destruction, sabotage | misconfigured services and systems, misconfigured access and authorization, service or API exposure, accidental leak or modification of data, credentials, secrets, confidential information, proprietary technology/information, corporate data, sensitive data

Operationalization

Integration of PIRs into the CTI lifecycle

- Research topics and analytical deliverables priorities
- Collection management priorities
- CTI platforms alerting
- Threat Informed Defence
  - Detection priorities
  - Threat hunting program priorities


INTERNAL FOCUS
Operational Environment of your org
STEP 1
ELEMENTS & FUNCTION
ASSETS
EXTERNAL FOCUS
Threat Landscape
WHO? (HOW?)
operationalization of the PIRs
INTERSECTION
Threats to your org
WHAT?
Mapping the ASSETS to the ELEMENTS
STEP 2
Mapping type of adversarial operation to the ELEMENTS & ASSETS
STEP 3
What is the most impactful type of adversarial operartion on each ELEMENT?
Risk assessment exercise
STEP 4
PIRs Customization
STEP 5

red.ht/pir-feedback

- Workshop materials at **red.ht/pir**
- Feedback form at **red.ht/pir-feedback**
- v1.0 (RETIRED) step-by-step at GitHub > v1.1 incoming
  Developing Priority Intelligence Requirements @ Red Hat

Ondra Rojčík
in/orojcik

Vladimír Janout
in/vladimir-janout