Priority Intelligence Requirements Workshop

How to Set the Direction of Your CTI Program

Ondra Rojcik, Vladimir Janout
CTI Analysts
Ondra Rojčík

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

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
Priority Intelligence Requirements Workshop

Agenda

- 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
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
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
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.
What's the size of your CTI team?

Click Present with Slido or install our Chrome extension to activate this poll while presenting.
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.
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
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?
STEELLAR 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
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 experiences.

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 lead 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 priority. We will invest in robust cybersecurity measures to protect our vehicles and customers 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.

Performance indicators

20% longer range compared to competitors
95%+ CO2 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 Rate: 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.
PIR Workshop
Workshop materials at red.ht/pir

INTERNAL FOCUS
Operational Environment of your org

STEP 1
ELEMENTS & FUNCTION

ASSETS

INTERSECTION
Threats to your org

STEP 2
Mapping the ASSETS to the ELEMENTS

EXTERNAL FOCUS
Threat Landscape

STEP 3
Mapping type of adversarial operation to the ELEMENTS & ASSETS

WHO? (HOW?)
operationalization of the PIRs

STEP 4
Risk assessment exercise

What is the most impactful type of adversarial operation on each ELEMENT?

STEP 5
PIRs Customization
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 customers, potentially damaging information

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

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 were faced due to 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.

Proprietary range-boosting technology: 20% longer range compared to competitors.
INTERNAL FOCUS
Operational Environment of your org

EXTERNAL FOCUS
Threat Landscape

STEP 1
Elements & Function

STEP 2
WHAT?
Mapping the ASSETS to the ELEMENTS

STEP 3
Mapping type of adversarial operation to the ELEMENTS & ASSETS

STEP 4
Risk assessment exercise

STEP 5
PIRs Customization

STEP 3
What is the most impactful type of adversarial operation on each ELEMENT?

STEP 4
Risk assessment exercise

STEP 5
PIRs Customization

Workshop materials at red.ht/pir
### Step 1b THE FUNCTION (INTERNAL FOCUS)

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item No.</td>
<td>ELEMENTS of STELLAR and STELLAR Strategy</td>
<td>THE FUNCTION (what is it about the ELEMENTS that needs to be secured)</td>
<td>Supporting ASSETS (mainly technology and data/information)</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>ELEMENTS of STELLAR and STELLAR Strategy - STEP 1</th>
<th>THE FUNCTION - what is it about the ELEMENTS that needs to be secured (STEP 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited battery production capacity</td>
<td>Up and running battery production</td>
</tr>
<tr>
<td>Proprietary range-boosting technology: 20% longer range compared to competitors</td>
<td>Custodian of proprietary data</td>
</tr>
</tbody>
</table>
PIR exercise Link

red.ht/pir
PIR Workshop

Workshop materials at red.ht/pir

---

**STEP 1**

**INTERNAL FOCUS**
Operational Environment of your org

**ELEMENTS & FUNCTION**

---

**STEP 2**

Mapping the ASSETS to the ELEMENTS

---

**STEP 3**

Mapping type of adversarial operation to the ELEMENTS & ASSETS

---

**STEP 4**

Risk assessment exercise

---

**STEP 5**

PIRs Customization

---

**EXTERNAL FOCUS**
Threat Landscape

---

**WHO? (HOW?)**
operationalization of the PIRs

---

**INTERSECTION**
Threats to your org

---

What is the most impactful type of adversarial operation on each ELEMENT?
Step 1a & 1b ELEMENTS and FUNCTION exercise

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

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

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

EXTERNAL FOCUS
Threat Landscape

STEP 1
Mapping the ASSETS to the ELEMENTS & FUNCTION

STEP 2
WHAT?

STEP 3
Mapping type of adversarial operation to the ELEMENTS & ASSETS

STEP 4
Risk assessment exercise

STEP 5
PIRs Customization

INTERSECTION
Threats to your org

WHO? (HOW?) operationalization of the PIRs

What is the most impactful type of adversarial operation on each ELEMENT?
Step 2 ASSET mapping exercise

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)

<table>
<thead>
<tr>
<th>ELEMENTS of STELLAR and STELLAR Strategy - STEP 1</th>
<th>THE FUNCTION - what is it about the ELEMENTS that needs to be secured (STEP 1)</th>
<th>Supporting ASSETS (mainly technology and data/information) (STEP 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited battery production capacity</td>
<td>Up and running battery production</td>
<td>OT&amp;ICS</td>
</tr>
<tr>
<td>Proprietary range-boosting technology: 20% longer range compared to competitors</td>
<td>Custodian of proprietary data</td>
<td>Proprietary Information</td>
</tr>
</tbody>
</table>
INTERNAL FOCUS
Operational Environment of your org

ELEMENTS & FUNCTION

ASSETS

STEP 1

INTERSECTION
Threats to your org

STEP 2

WHAT?

Mapping the ASSETS to the ELEMENTS

STEP 3

Mapping type of adversarial operation to the ELEMENTS & ASSETS

What is the most impactful type of adversarial operation on each ELEMENT?

EXTERNAL FOCUS
Threat Landscape

WHO? (HOW?) operationalization of the PIRs

STEP 4

Risk assessment exercise

STEP 5

PIRs Customization

Workshop materials at red.ht/pir
# Step 3: Mapping types of adversarial operations

## (EXTERNAL FOCUS & INTERSECTION)

<table>
<thead>
<tr>
<th>Type of Adversarial Operation</th>
<th>MITRE ATT&amp;CK Technique</th>
<th>Keywords for operationalisation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ransomware</strong></td>
<td>T1486 Data Encrypted for Impact</td>
<td>ransom, ransomware, encryption, extortion, double extortion, triple extortion, crypto-malware</td>
</tr>
<tr>
<td></td>
<td>T1490 Inhibit System Recovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TA0010 Exfiltration</td>
<td></td>
</tr>
<tr>
<td><strong>Business Email Compromise &amp; Fraud</strong></td>
<td>T1566 Phishing</td>
<td>business email compromise, BEC, phishing, spear phishing, whaling, social engineering, financial fraud, copyright</td>
</tr>
<tr>
<td></td>
<td>T1078 Valid Accounts</td>
<td></td>
</tr>
<tr>
<td><strong>Stolen Information &amp; Espionage</strong></td>
<td>TA0010 Exfiltration</td>
<td>espionage, cyber espionage, exfiltration, industrial espionage, government, confidentiality, classified information, sensitive information, proprietary information, PII, HIPAA</td>
</tr>
<tr>
<td><strong>Denial of Service &amp; Availability</strong></td>
<td>T1499 Endpoint Denial of Service</td>
<td>DoS, DDoS, availability, shutdown, data wipe, data destruction, sabotage</td>
</tr>
<tr>
<td></td>
<td>T1495 Firmware Corruption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1498 Network Denial of Service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1489 Service Stop</td>
<td></td>
</tr>
<tr>
<td><strong>Resource Hijacking</strong></td>
<td>T1496 Resource Hijacking</td>
<td>resource hijacking, cryptojacking, cryptomining, cryptocurrency, kubernetes</td>
</tr>
<tr>
<td><strong>Initial Point of Supply Chain Attack</strong></td>
<td>T1565 Data Manipulation</td>
<td>third-party, vendor, external components, inject malicious code, malicious update, open-source software repositories, manipulated packages, repojacking</td>
</tr>
<tr>
<td></td>
<td>The “Initial Point of Supply Chain Attack” is not “T1195 Supply Chain Compromise” as this MITRE ATT&amp;CK technique is on the “Initial Access” vector side</td>
<td></td>
</tr>
<tr>
<td><strong>Data Manipulation</strong></td>
<td>T1565 Data Manipulation</td>
<td>integrity, data manipulation, defacement, software supply-chain, repojacking, malicious code injection, compromised repository, software dependency, CI/CD</td>
</tr>
<tr>
<td></td>
<td>T1491 Defacement</td>
<td></td>
</tr>
<tr>
<td><strong>Internal User Error</strong></td>
<td>NA</td>
<td>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</td>
</tr>
</tbody>
</table>
Step 3 Mapping types of adversarial operations (EXTERNAL & INTERSECTION)

- 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
Step 1: Operational Environment of your org

Step 2: Mapping the ASSETS to the ELEMENTS

Step 3: Mapping type of adversarial operation to the ELEMENTS & ASSETS

Step 4: Risk assessment exercise

Step 5: PIRs Customization

**INTERNAL FOCUS**

**EXTERNAL FOCUS**

**INTERSECTION**

Threats to your org

**WHO? (HOW?)**

operationalization of the PIRs

What is the most impactful type of adversarial operation on each ELEMENT?
(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

<table>
<thead>
<tr>
<th>ELEMENTS</th>
<th>AL of the ELEMENT and your attackers - always consider</th>
<th>APPEAL for attackers:</th>
<th>(Impact Q) Consider the worst case scenario of an impact on ORGANIZATION if a threat actor attacks the supporting ASSETS</th>
<th>Impact:</th>
<th>Risk score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Car production in EU and China</td>
<td>are STELLAR’s OT&amp;CS in question?</td>
<td>Moderately appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of car production in EU and China?</td>
<td>Serious</td>
<td>12</td>
</tr>
<tr>
<td>Limited battery production capacity</td>
<td>are STELLAR’s OT&amp;CS in question?</td>
<td>Moderately appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of limited battery production capacity?</td>
<td>Serious</td>
<td>12</td>
</tr>
<tr>
<td>Supply chain, spans multiple countries, including China and Chile. Any disruptions in the supply chain may result in production delays and increased costs</td>
<td>STELLAR’s corporate and third party information, client entities?</td>
<td>Slightly appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of supply chain?</td>
<td>Moderate</td>
<td>6</td>
</tr>
<tr>
<td>Proprietary range-boosting technology: 20% longer range compared to competitors</td>
<td>STELLAR’s proprietary range-boosting technology?</td>
<td>Extremely appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of proprietary range-boosting technology?</td>
<td>Serious</td>
<td>20</td>
</tr>
<tr>
<td>Public perception of Stellar environmental impact is vital to the brand reputation</td>
<td>STELLAR’s corporate perception of environmental impact?</td>
<td>Slightly appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of public perception of STELLAR environmental impact?</td>
<td>Moderate</td>
<td>6</td>
</tr>
<tr>
<td>Software-first approach; proprietary In-vehicle software</td>
<td>STELLAR’s in-vehicle software</td>
<td>Moderately appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of in-vehicle software development and provisioning?</td>
<td>Critical</td>
<td>15</td>
</tr>
<tr>
<td>Advanced safety features - technologies to mitigate accidents and reduce the severity of collisions</td>
<td>STELLAR’s development and safety features?</td>
<td>Moderately appealing</td>
<td>What would be the worst case scenario of an impact if an adversary attacks ASSETS in support of development and deployment of vehicle safety features?</td>
<td>Critical</td>
<td>15</td>
</tr>
</tbody>
</table>

### Output:

Scored and ranked ELEMENTS and your top 5/10 ELEMENTS
**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

- Statements
- Intelligence Questions
- RFIs
- Any other form

Engage multiple respondents > additional “step” > calculate median score
## Step 5 PIRs Customization

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

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

**Rephrase** the result to statements that can be operationalized if needed

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

<table>
<thead>
<tr>
<th>PIR</th>
<th>PIR keywords</th>
<th>Type of Adversary Operation keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 Proprietary range-busting technology: 26% longer range compared to competitors</td>
<td></td>
<td>espionage, cyber espionage, infiltration, industrial espionage, government confidentiality, classified information, sensitive information, confidential information, proprietary information, P: IPA</td>
</tr>
<tr>
<td>#2 Research and development in EU and China drives the company success</td>
<td></td>
<td>espionage, cyber espionage, infiltration, industrial espionage, government confidentiality, classified information, sensitive information, confidential information, proprietary information, P: IPA</td>
</tr>
<tr>
<td>#6 Car production in EU and China</td>
<td>DoS, DDoS, availability, shutdown, data wipe, data destruction, sabotage</td>
<td>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</td>
</tr>
</tbody>
</table>

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