How to Develop Priority Intelligence Requirements for YOUR Organization

Ondra Rojčík
Senior CTI Analyst, Red Hat
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
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/
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
Red Hat’s process of developing PIRs
INTERNAL FOCUS of the process
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

<table>
<thead>
<tr>
<th>ELEMENTS of Red Hat and the Red Hat Strategy</th>
<th>THE FUNCTION (what is it about the ELEMENTS that needs to be secured)</th>
<th>Supporting ASSETS (mainly technology and data/information)</th>
<th>(Likelihood) APPEAL for attackers - always consider the worst case scenario</th>
<th>APPEAL for attackers:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Extremely appealing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Very appealing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Moderately appealing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Slightly appealing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Not at all appealing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact Q</th>
<th>Confidentiality/Integrity/Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>RELEVANCE scale: Critical, High, Medium, Low. Always consider the worst case scenario.</td>
<td></td>
</tr>
<tr>
<td>Confidentiality/Integrity/Availability:</td>
<td></td>
</tr>
<tr>
<td>- One critical, rest lower</td>
<td></td>
</tr>
<tr>
<td>- Three or two critical, rest lower</td>
<td></td>
</tr>
<tr>
<td>- One high, rest lower</td>
<td></td>
</tr>
<tr>
<td>- Three or two medium, rest lower</td>
<td></td>
</tr>
<tr>
<td>- One medium, rest lower</td>
<td></td>
</tr>
<tr>
<td>- All low</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk score</th>
</tr>
</thead>
</table>

**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**
How to Develop PIRs for YOUR Organization

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

Stakeholder Review

Translation of the results to the PIR Proposal

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

<table>
<thead>
<tr>
<th>Threat Actors</th>
<th>Harm-Impact / What is the worst case scenario of Harm/Impact if the Threat Actor hits Red Hat?</th>
<th>Likelihood / How likely it is that the Threat Actor will impact Red Hat in the next 2 years?</th>
<th>Risk score</th>
<th>Assess the current targeting of the Threat Actor</th>
<th>CTIP score</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware groups</td>
<td></td>
<td>Unlikely</td>
<td>i/N/A</td>
<td>Threats directly targeting or affecting the systems of Red Hat</td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Cryptominers</td>
<td></td>
<td>Possibly/Can’t Exclude</td>
<td>i/N/A</td>
<td>Threats targeting Red Hat partners, sites or locations</td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Financial Fraudsters</td>
<td></td>
<td>Likely</td>
<td>i/N/A</td>
<td>Threats targeting the Cloud, OpenSource and Linux sector</td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Other (opportunistic) Cybercrime</td>
<td></td>
<td>Highly Likely</td>
<td>i/N/A</td>
<td>Threats targeting the Technology sector generally</td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>State Actors</td>
<td></td>
<td>Overall threat landscape items</td>
<td>i/N/A</td>
<td>Threats targeting the systems of multinational entities generally</td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Industrial and Competitive Espionage</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Insiders - intentional</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Internal User Errors</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Hacktivists</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
</tbody>
</table>

## Initial Access Vectors

<table>
<thead>
<tr>
<th>Initial Access Vectors</th>
<th>Harm-Impact / What is the worst case scenario of Harm/Impact if the Initial Access Vector hits Red Hat?</th>
<th>Likelihood / How likely it is that the Initial Access Vector will impact Red Hat in the next 2 years?</th>
<th>Risk score</th>
<th>Assess the current relevance of Initial Access Vector from Red Hat perspective</th>
<th>CTIP score</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social engineering and Phishing</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Vulnerability exploitation</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Brute Forcing and Password Spraying</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Remote Services (RDP, SSH, VNC etc.)</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Stolen Credentials</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Supply Chain Attack</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
<tr>
<td>Misconfigurations</td>
<td></td>
<td></td>
<td>i/N/A</td>
<td></td>
<td>i/N/A</td>
<td>i/N/A</td>
</tr>
</tbody>
</table>

How to Develop PIRs for YOUR Organization

1. **INTERNAL FOCUS**
   - Operational Environment of your org
   - Your strategy
   - Your assets

2. **INTERSECTION**
   - Threats to your org
   - Mapping of assets to the strategy & risk assessment
   - Mapping and ranking of threats to your org and your org's assets in support of the strategy

3. **EXTERNAL FOCUS**
   - Threat Landscape
   - What are the threats to your org?
   - Risk assessment of the threats

4. **COMBINED EXERCISE**
   - Stakeholder Review
   - Translation of the results to the PIR Proposal
   - Approval by CISO

5. **Implementation**
   - Yes: Implementation to your intelligence cycle
   - No: Annual review of PIRs
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
How to Develop PIRs for YOUR Organization

Merging the exercises and developing the PIRs
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)
Mapping exercise and developing the PIRs

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

<table>
<thead>
<tr>
<th>FINAL SCORE</th>
<th>ELEMENTS of Your Org and Strategy</th>
<th>Element Score</th>
<th>Threat Actor No1</th>
<th>Threat Actor No2</th>
<th>AVG TA Score</th>
<th>Attack Vector No1</th>
<th>Attack Vector No2</th>
<th>AVG AV Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>43.75</td>
<td>[Your ELEMENT 1]</td>
<td>5</td>
<td>State Actors</td>
<td>Ransomware group</td>
<td>2.5</td>
<td>Social engineering</td>
<td>Vulnerability exploit</td>
<td>3.5</td>
</tr>
<tr>
<td>40</td>
<td>[Your ELEMENT 2]</td>
<td>4</td>
<td>Insiders - intention</td>
<td>Internal User Error</td>
<td>2.5</td>
<td>Social engineering</td>
<td>Supply Chain Attack</td>
<td>4</td>
</tr>
<tr>
<td>37.5</td>
<td>[Your ELEMENT 3]</td>
<td>5</td>
<td>Cryptominers</td>
<td>Ransomware group</td>
<td>2.5</td>
<td>Supply Chain Attack</td>
<td>Supply Chain Attack</td>
<td>3</td>
</tr>
</tbody>
</table>

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
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
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...
Integration of PIRs into the CTI lifecycle

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

ondrejrojcik/