First let's go over the criteria that was set in T3.

1. **Access Method:** Ensuring diverse access methods, including open web interfaces and APIs, is crucial. This criterion remains valid as SMEs and organizations in developing economies may have varying levels of technical expertise and infrastructure capabilities. Simple and straightforward access methods, such as user-friendly web interfaces, enhance accessibility, while APIs allow for more advanced integrations into existing security systems. This flexibility can increase the usability of threat intelligence data across different organizational contexts and technical environments.
2. **Timeliness:** The demand for updates in real-time or nearly real-time is crucial, as cybersecurity dangers transform quickly. SMEs and growing economies can be more exposed to cyberattacks because they may not have strong cybersecurity safeguards yet. When information comes in on time, it helps with the forthcoming proactive defence actions. For example, fixing vulnerabilities by patching them quickly, blocking harmful IP addresses and reducing active threats. Having a threat feed that always gives the latest information greatly improves an organization's capability to react quickly against threats.
3. **Accuracy:** Precise understanding of potential dangers is imperative, as inaccurate information can result in ineffectual or detrimental actions, such as obstructing legitimate traffic or neglecting genuine threats. Dependable and confirmed sources of data are essential in guaranteeing the credibility of threat intelligence. This requires evaluating the validation methods used by the source, the standing of the supplier, and verifying with other reputable sources. Accuracy ensures that resources are used efficiently and that security measures are effectively targeted.
4. **Pricing:** This criterion is especially pertinent for SMEs and organizations in developing economies where budget constraints are common. Free access to threat intelligence data is crucial for making these resources accessible. Pricing should also consider the potential cost of implementation and maintenance of the threat intelligence feeds. Cost-effective solutions, including those offering free tiers with essential features, enable broader adoption and enhance the cybersecurity posture of resource-constrained organizations. Where possible, the value provided by the threat intelligence should be weighed against the cost to ensure it is a worthwhile investment.

Possible additions to the criteria:

1. **Scalability:** Consider whether the threat intelligence solution can scale with the organization's growth. SMEs might expand their operations, and the chosen solution should be able to accommodate increased data and user demands without significant additional costs.
2. **Support and Community:** Evaluate the availability of support and the presence of a user community. Open-source and community-driven platforms often provide valuable support resources and forums where users can share experiences and solutions.
3. **Integration Capabilities:** Assess how well the threat intelligence source integrates with existing security tools and platforms. Seamless integration can streamline the workflow and enhance the overall efficiency of security operations.

Looking at the list given in the IntelMQ VM we can quickly go over what was already there.

Abusix-Expert	API	Real-time	High	Unknown
AttackingNetBlocks-Collector	Web Interface	Near-real-time	High	Free (Open Source)
Bambenek-HTTP-Collector	API, Web Interface	Real-time	High	Free (Open Source)
Blocklist-Apache-Collector	API	Real-time	High	Free
Blocklist-Brutef-Collector	API	Real-time	High	Free
Blocklist-bots-Collector	API	Real-time	High	Free
CIArmy-HTTP-Collector	API	Real-time	High	Free
CZ.NIC-HaaS-HTTP-Collector	API	Real-time	High	Free
Cymru-Expert	API	Real-time	High	Unknown
DNS-Rec-Collector	API, Web Interface	Real-time	High	Free (Open Source)
Dataplane-Parser	API, Web Interface	Real-time	High	Paid
DshieldBlock-Parser	API, Web Interface	Real-time	High	Free (Open Source)
LatestMaliciousDomain-Collector	API	Real-time	High	Free
MalwareUrl-Collector	API	Real-time	High	Free
Malwareurl-Parser	API	Real-time	High	Free
OpenPhish-Parser	API	Real-time	High	Free
SSH-PW-Auth-Collector	API	Real-time	High	Free
Threatminer-Parser	API	Real-time	High	Free
URL-Expert	API	Real-time	High	Unknown
URLhaus	API	Real-time	High	Free
deduplicator-expert	API	Real-time	High	Unknown
feodo-tracker-collector	API	Real-time	High	Free
gethostbyname-expert	API	Real-time	High	Unknown
taxonomy-expert	API	Real-time	High	Unknown

Additions that could be added:

AlienVault OTX (Open Threat Exchange)

- **Access Method:** AlienVault OTX offers a robust API that allows users to programmatically access threat data. This API can be integrated into security tools and workflows, enabling automated ingestion and analysis of threat intelligence.
- **Timeliness:** AlienVault OTX provides real-time updates on new and emerging threats. Subscribers can enlist in particular "pulses" formed by other users or organizations. These pulses encompass indicators of compromise (IOCs) such as pernicious IP addresses, domains, file hashes, and URLs. Subscribed individuals promptly receive notifications as soon as novel data is incorporated into the pulses they track, ensuring they are apprised of emerging menaces.
- **Accuracy:** The threat data in OTX is contributed by a global community of security professionals. This crowdsourced model ensures a wide variety of threat intelligence is available. The OTX community validates the data, which helps to filter out false positives and ensures the accuracy and reliability of the threat information.
- **Pricing:** AlienVault OTX provides SMEs and organizations with limited cybersecurity budgets a valuable source of threat intelligence without any cost, making it a highly sought-after resource.

PhishTank

- **Access Method:** API of PhishTank is what lets developers mix phishing data inside their applications. It gives method to the database of phishing URLs, allowing automatic checks and integrations.
- **Timeliness:** PhishTank has a strong update system in place. It gets new phishing threats from users globally, keeping the database current and showing the most recent activities. The group of users can confirm fresh submissions, making it possible to update the database almost in real time.
- **Accuracy:** PhishTank depends on a group of users to confirm reported phishing URLs. This method, known as crowdsourced verification, guarantees an excellent level of precision and assists in eliminating incorrect reports. PhishTank is a recognized and trustworthy platform within the cybersecurity community, making data more dependable.
- **Pricing:** PhishTank is a tool that people can use without any cost, which means it is available to anyone - be it an organization or individual. This kind of openness helps in promoting wide participation and exchange of phishing threat knowledge.

CIRCL (Computer Incident Response Center Luxembourg)

- **Access Method:** CIRCL provides threat intelligence through MISP (Malware Information Sharing Platform & Threat Sharing) feeds. MISP is an open-source threat intelligence platform used for sharing, storing, and correlating indicators of compromise.
- **Timeliness:** CIRCL regularly updates its threat intelligence feeds. As a governmental CERT, CIRCL ensures that the data is current and provides timely information on

emerging threats. CIRCL also focuses on reporting critical incidents and major threat activities, ensuring that organizations are aware of significant threats in a timely manner.

- **Accuracy:** CIRCL is maintained by a governmental Computer Emergency Response Team, which ensures a high level of trust and reliability in the data. The threat intelligence provided by CIRCL is carefully validated and vetted, ensuring its accuracy and relevance to the cybersecurity community.
- **Pricing:** CIRCL's threat intelligence feeds are available for free, making them accessible to various organizations.

IBM X-Force Exchange

- **Access Method:** IBM X-Force Exchange provides an API that allows for automated access to its vast repository of threat intelligence data. This API can be used to integrate threat intelligence into security operations and response workflows.
- **Timeliness:** IBM X-Force Exchange offers real-time updates on global threats and vulnerabilities, ensuring that users have access to the latest intelligence. The platform covers a wide range of threat intelligence, including malware, vulnerabilities, threat actor activities, and security news.
- **Accuracy:** The threat intelligence is curated and analysed by IBM's security research team, ensuring high accuracy and reliability. The platform aggregates data from various sources, including open-source intelligence and proprietary IBM research, to provide a comprehensive view of the threat landscape.
- **Pricing:** IBM X-Force Exchange offers a free tier that provides access to a substantial amount of threat intelligence data. Paid plans are available for more extensive data access and higher API request limits.