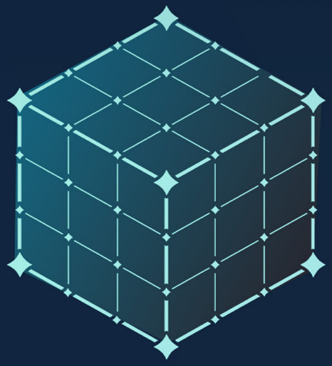
THREATQUOTIENT™

Using ThreatQ™ In Air-Gapped Environments



Contents

1) OVERVIEW

At ThreatQuotient, we increasingly receive requests from our customers and prospects to assist with the use of threat intelligence in air-gapped environments, where the network requires complete separation from external internet and network connections. This is a challenging request for many threat intelligence feeds and platforms as many of these capabilities require some form of internet connection to work correctly or to their fullest capability.

This document describes and addresses many of the common considerations that influence the design and implementation of a Threat Intelligence Platform (TIP) – in this case, the ThreatQ Platform – within Air-Gapped Environments.

The document is split into the following two separate sections:

- Considerations for Threat Intelligence in Air-Gapped Environments
- Implementing ThreatQ in an Air-Gapped Environment

2) CONSIDERATIONS FOR THREAT INTELLIGENCE IN AIR-GAPPED ENVIRONMENTS

2.1 CONSIDERATION 1 – EFFECTIVE PLACEMENT

Threat data can be captured from both internal and external sources, each with their own individual challenges when working within an air-gapped environment. In both cases, the effectiveness of a TIP will boil down to placement within the architecture.

Internal sources of threat data normally include other security tools, such as the SIEM, ticketing system and vulnerability assessment solution. These tools each have specific security restrictions and are normally placed in a protected zone within the infrastructure. It is essential to consider these tools as viable sources of threat data as they add layers of context that an external source cannot, particularly with respect to the relevance of threat data within the context of business requirements/needs.

External sources of threat data are generally provided by a combination of feeds, data enrichment and cloud-based data analysis tools. These sources of data are typically made available by a web-based API, emails and other common transfer mechanisms that are regularly fed into the environment. External sources offer valuable insight into global threat data and should also be considered a key part of any TIP.

A successful implementation of a TIP will leverage a combination of both internal and external sources of data. It is, therefore, imperative that the architectural placement of the platform be carefully considered to take advantage of both source types without introducing security implications for the wider environment.

2.2 CONSIDERATION 2 – ARCHITECTURE OF THE THREAT INTELLIGENCE PLATFORM

All TIP providers offer an ‘on-premises’ solution to some degree. However, it is important to note that an ‘on-premise’ solution does not necessarily mean that it will work effectively in an air-gapped environment. With that in mind, there are some important considerations that are generally glossed over by many providers.

First, we must consider the architecture of the platform. Many of the TIP platforms were designed principally for cloud-based use. These platforms have been migrated to fit an 'on-premises' use case. As such, they often require multiple components to effectively replicate their cloud-based counterparts. These additional components introduce layers of complexity into the architecture to meet the 'on-premises' use case.

Second, it is important to clearly understand the functionality that is offered by the TIP. Many TIP vendors will offer an 'on-premise' capability. After further investigation, however, it may be noted that the 'on-premise' offering may be less feature-rich or will require an internet connection for some features to work correctly. Additionally, the 'on-premises' capability may just be a stub to provide integrations between their cloud-based solution and your internal architecture; your data may not stay on-premises.

An effective air-gapped solution must offer access to the full product feature set without the need for multiple, additional components or an external internet connection.

2.3 CONSIDERATION 3 – UPDATES

Updates are an important part of any TIP. The updates will enable new functionality and patch any newly discovered security vulnerabilities. An air-gapped solution must be able to receive updates on a regular and timely basis and should involve simple installs that keep the entire TIP architecture in line with custom functionality.

2.4 CONSIDERATION 4 – ENRICHMENT AND ANALYSIS SOURCES

A key feature of the TIP is the provision of a data enrichment and analysis capability. This capability (known as "Operations" in ThreatQ) offers enrichment of threat data from both internal and external sources. There are several points to consider when leveraging enrichment capabilities, including:

Do you plan to utilize both internal and external enrichment sources?

There are multiple different types of enrichment sources that a TIP may use. These range from internal sources, such as the SIEM or log repository, to external sources, such as VirusTotal, DomainTools or Emerging Threats. Both types can offer value to TIP users and should, therefore, be considered when architecting an environment. In both cases, placement of the TIP is essential to ensure that enrichment capabilities may be leveraged without compromising the security of the wider environment.

Is there a requirement to anonymize enrichment requests to avoid identification of their source?

In some environments, particularly those that are air-gapped, it is important to avoid sharing any critical data beyond an organization's boundaries. This can occasionally be a challenge when leveraging external enrichment tools, as some tools will share details about the requests that are made with their wider user community. In these scenarios, consideration must be made as to whether to enable external enrichment capabilities. If they are to be enabled, then a deeper understanding may be required with respect to how these tools will interact with the TIP and what information may be gleaned by exposing the intelligence your organization is looking at.

Should enrichment be performed on-demand (manually), automatically or a combination of both?

Many external enrichment tools will implement a quota on the number of requests that may be made of their service in a given time period. Normally, it is possible to increase these quotas at a cost. Therefore, it is worth considering how these enrichment tools should be used.

There are many different use cases for such tools. Enrichment tools may be used on-demand, automatically and in a hybrid configuration. On-demand enrichment requires a user to manually request that a specific indicator or set of indicators be enriched. This is a useful mechanism when quotas are low, but reduces autonomy. Automated enrichment significantly improves autonomy, but runs the risk of enriching data that is of little value to the business and results in consuming valuable quota unnecessarily. A hybrid solution offers a balance between both manual and automated solutions. This type of solution is more complex to configure but increases control over which indicators are enriched automatically while still maintaining a degree of autonomy and reducing analyst workload.

Which enrichment sources should be used?

There are many enrichment sources that are available. Enrichment sources share a few traits with threat intelligence feeds. Therefore, it is worth understanding the type and focus of the data that the enrichment service offers and determining which adds the most value to the air-gapped environment. Each service will offer different data sets which may or may not be valuable to the business. Examples of variations include political, geographical and industry learnings, as well as functional differences in terms of the data that is returned.

Which analysis capabilities should be used?

Analysis capabilities may be leveraged by a TIP to further expand the portfolio of functions available to the analyst beyond the look-ups that can be expected from traditional enrichment sources. Analysis capabilities may be located inside the network as well as outside. A typical example of such a tool is the capability to submit an indicator to a dynamic analysis engine for detonation with results returned to the TIP on completion.

How will requests be made?

Enrichment services will return data once such a request is made from the source. This concept applies to the TIP also. Use of enrichment technologies can break the air-gap model if such enrichment requests are made directly from the TIP platform. It is still feasible to leverage enrichment tools, but it is important to understand what options are available for facilitating enrichment requests as well as any environmental or security restrictions that may be in place.

2.5 CONSIDERATION 5 – INTEGRATIONS

Figure 1 shows a typical high-level overview of the ThreatQ TIP. An effective TIP should implement three core concepts: the Threat Library™, Adaptive Workbench™ and Open Exchange™. A TIP should have the ability to ingest threat data from multiple sources into a single data model (Threat Library). Once ingested, it should be possible to nurture the threat data to better fit business requirements (Adaptive Workbench). Finally, it should be possible to build or implement bi-directional integrations with other security technologies (Open Exchange).

Air-Gapped environments benefit from the same model. When integrations are implemented, the data from external sources has increased value, providing the ability to:

- Correlate external threat data with events that are occurring within the air-gapped environment.
- Improve the relevance of the externally sourced data by providing a self-tuning feedback loop that constantly evaluates and updates data scores based on the events that are occurring within the air-gapped environment.
- Implement a single consistent source of threat data that offers a common view of threat data across the air-gapped environment.
- Improve collaboration between security teams when working with threat intelligence by supplying threat intelligence to the tools and workflows used by various teams.

It is beneficial to understand if and how you would like to integrate threat data into your air-gapped environment. This understanding will better guide the architectural decisions that you make and will simplify the deployment process.

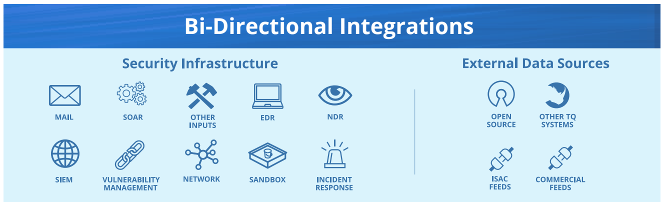


Figure 1. Integrations within ThreatQ

2.6 CONSIDERATION 6 – SPLITTING THREAT INTELLIGENCE PLATFORM FUNCTIONS

In many cases, it may be necessary to split the core functions of the TIP when designing for an air-gapped environment. This decision is generally informed by the placement and associated functional decisions for the environment.

There are several concepts to consider when determining how or whether to split a TIP implementation into separate functions, including:

Ingestion of threat data

A key premise of a TIP is the ingestion of threat data from external sources. Many of these sources offer limited methods of integration (predominantly by authenticated API over an internet connection). Therefore, it is not uncommon to start by placing a TIP in a zone that has direct or proxied access to the internet. This enables the TIP to consume and regularly update threat data from your preferred sources. The internet connection would break the premise of an air-gapped environment. Therefore, it is feasible to separate the ingestion of threat data into its own independent function.

Working with threat data in an air-gapped environment

A second common split of functionality is defined by a user's requirement to work with threat data in a safe and secure context that has no risk of spread beyond the boundaries of the air-gapped environment. In this scenario, it is typical to implement a standalone TIP that takes an aggregated feed of threat data from a trusted source. The feed could be provided via a data diode (that allows ingestion of data only) or via another source, such as a directory where updated feed data is placed (useful when manually transferring data between environments).

Enrichment and analysis

Enrichment and analysis can be powerful capabilities when added to a TIP. There are some challenges when implementing a TIP in an air-gapped environment (as described in Section 2.4). To address these challenges, some TIP environments implement additional functionality to help aggregate, anonymize and transfer enrichment requests from an air-gapped environment to external enrichment services via the public internet, returning the results to the internal TIP once the requests are complete.

2.7 CONSIDERATION 7 – TIMELINESS OF DATA DELIVERY FROM EXTERNAL SOURCES

The requirement to air-gap a TIP results in a lack of access to the externally facing services that are useful in the day-to-day operations that use threat intelligence (e.g., access to external enrichment sources). It is still possible to leverage external services as a source of threat data and enrichment, but timeliness must be considered when doing so.

Many of the solutions that provide access to external services from an air-gapped environment may require the implementation of a transfer process. The transfer process will vary depending on your specific security and environment requirements for the air-gapped solution. In some cases, a technical solution (such as a data diode) may be feasible, but, in others, a more manual solution (such as manually transferring data between environments) may be required. Each chosen solution will influence the timeliness with which data will be made available to an air-gapped environment.

It is, therefore, important to consider the timeliness requirements for a TIP, including:

- How quickly should data be made available from external sources to the database of the internal solution?
- How quickly should enrichment requests be performed on data from external sources?
- Are there any compromises in the timeliness of data delivery that can be made? What are they?
- How do the timeliness requirements affect enrichment or intelligence source request limitations?

It is important to understand that there is a trade-off to be made between the confidentiality of a system's data and the timeliness of access to and consumption of data from externally facing sources. The higher the confidentiality of a system, the more likely it is that timeliness of data delivery will decrease. This is principally because additional security measures (such as air-gaps) may add additional complexities into the data delivery process.

3) IMPLEMENTING THREATQ IN AN AIR-GAPPED ENVIRONMENT

3.1 STEP 1 – INGESTING THREAT INTELLIGENCE DATA

The first step to building a TIP in an air-gapped environment requires successful capture of threat data from your chosen feeds.

A high-level overview of the configuration is shown in Figure 2. In this example, a ThreatQ instance has been placed in a network zone that is accessible to the internet either directly or via proxy.

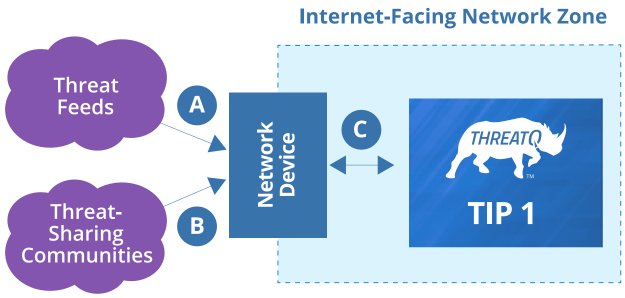


Figure 2. Ingesting Threat Data from External Feeds

There are multiple, different methods of accessing threat data from external sources. Traditional feeds (Reference A in Figures 2-6) may be pulled into the TIP on a regular basis (configurable). Such feeds may include a variety of different formats ranging from traditional API-based feeds to other types that are based on standards like STIX/TAXII.

In addition, the TIP will be able to work closely with sharing communities (Reference B in Figures 2-6). ThreatQ can both import and export data from these communities. Data may be selectively exported or not exported at all if preferred. Many of these communities will leverage a common platform (e.g., MISP) or may even offer direct integration directly with the TIP. ThreatQ fully supports both of these approaches.

All data is aggregated and normalized into a common flexible data model, known as the Threat Library (Reference C in Figures 2-6). ThreatQ does not restrict its users to a standard (e.g., STIX). Instead, ThreatQ offers compatibility with any standards that the business would like to leverage. All threat data will be mapped to ThreatQ's data model. This model (known as the Threat Library) allows you to define a taxonomy for the threat data and its tags and attributes that meets your unique business requirements.

3.2 STEP 2 – ESTABLISHING A TIP IN THE AIR-GAPPED ENVIRONMENT

The second step is to establish a TIP presence in the air-gapped environment. A transfer mechanism must be established between the externally facing instance that was built in Step 1 and the TIP in the air-gapped environment.

Figure 3 shows how ThreatQ is implemented in an air-gapped environment. ThreatQ leverages a mechanism called Air-Gapped Data Sync (AGDS) to effectively transfer threat data from one instance to another. This methodology is designed to support air-gapped environments and has been implemented with both data diodes and manual transfer approaches. Crucially, the AGDS methodology supports a one-way flow of data between the internet-facing instance and the air-gapped instance of ThreatQ. Specifically, threat data will be exported from TIP 1 and passed to the transfer mechanism (Reference D in Figures 3-6). The transfer mechanism (in this case AGDS) will enable transfer of the data to the air-gapped environment. Once successfully transferred, the AGDS will upload the new data into the Threat Library in TIP 2 (Reference E in Figures 3-6).

Users will be provided access to TIP 2, which will act as their primary source of threat intelligence data. User access is provided via the Web GUI over 443/tcp.

3.3 STEP 3 – INTEGRATING WITH INTERNAL TOOLS

The third step requires connecting third-party tools (such as the SIEM or IR Ticketing solution) to the ThreatQ instance (TIP 2). These connections ensure that ThreatQ can provide contextually relevant threat data to critical security tools as well as access to internal enrichment sources within the air-gapped environment. Figure 4 shows an example of how this might be configured.

ThreatQ leverages its Open Exchange to build bi-directional integrations with third-party technologies (Reference G in Figures 4-6). These integrations can take many different forms, including:

SIEM Integration

ThreatQ can provide a nurtured and filtered set of threat data to the SIEM. This data set may be customized to meet specific business requirements. ThreatQ will reduce the amount of less valuable threat data that is sent to the SIEM. This will allow SOC analysts to focus more of their time dealing with potential threats rather than dealing with false positives.

Most SIEM integrations also include the ability to run actions on the threat data in ThreatQ. This includes actions such as adding indicators, marking indicators as false positives and searching for related indicators.

Ticketing Integration

ThreatQ may be integrated with ticketing systems. This enables the process of incident-driven analysis of threat data as well as many other features. ThreatQ may be used to automatically populate tickets with relevant threat data from its Threat Library. Certain ticketing systems offer support for users to perform actions on ThreatQ from within the ticketing system itself. Common features include marking indicators as false positives, looking for related indicators and adding new indicators into ThreatQ.

Vulnerability Assessment

ThreatQ can leverage vulnerability data (such as CVE information) from a range of different sources. This information may be used to enhance the context and relevance of the threat data within the TIP. If the TIP is integrated with asset management or configuration management databases (CMDBs), organizations can support risk calculations and patch prioritization by aligning severity of vulnerability (external threat reporting) with presence in the environment (vulnerability scanning) with asset value/business impact (CMDB). Typical sources of data include:

- Internal Vulnerability Assessment tools
- External sources, such as the National Vulnerability Database (NVD)
- Certain threat feeds

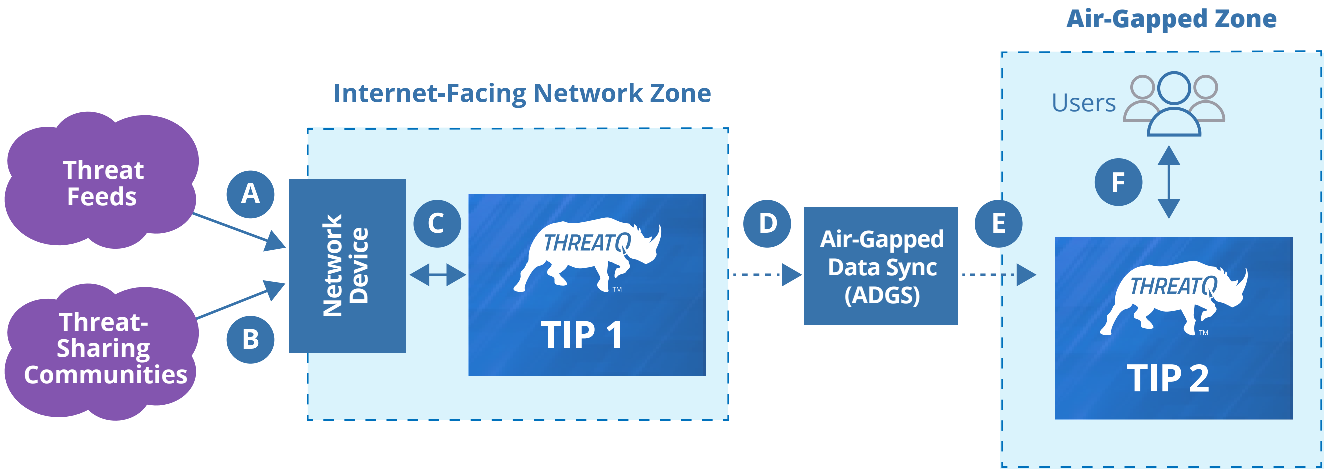

Air-Gapped Zone
Internet-Facing Network Zone
Threat Feeds
Threat-Sharing Communities
A
B
Network Device
C
THREATQ
TIP 1
D
Air-Gapped Data Sync (ADGS)
E
Users
F
THREATQ
TIP 2

Figure 3. Implementing an Air-Gapped TIP

3.4 STEP 4 – PROVIDING EXTERNAL ENRICHMENT CAPABILITIES

The fourth and final step enables the air-gapped TIP to leverage external enrichment sources in either an automatic or manual way. As shown below, there are several possible ways to execute Step 4 depending on business requirements. These enrichment options may also be combined, if required.

3.4.1 AUTOMATED ENRICHMENT

Many enrichment sources will support the use of automated enrichment in ThreatQ. These enrichment capabilities may be implemented very simply in the existing infrastructure.

Figure 5 shows an infrastructure where automated enrichment has been applied. Threat data is downloaded into TIP 1 (internet-facing TIP) in the usual manner. A subset of the ingested data can be specified through a configuration file (for example, only enrich IP Addresses or only enrich indicators related to Adversary APT1).

A periodic process (Reference H in Figures 5-6) will then apply a set of chosen enrichment tools against the new data set and automatically incorporate the results into the data set. All communications with the externally facing enrichment sources will be performed directly from the internet-facing TIP.

Enriched threat data will be transferred back automatically to TIP 2 using the processes that were set up in Step 2.

Additional automation is also possible through ThreatQ TDR Orchestrator, an optional product of the ThreatQuotient Solution Suite.

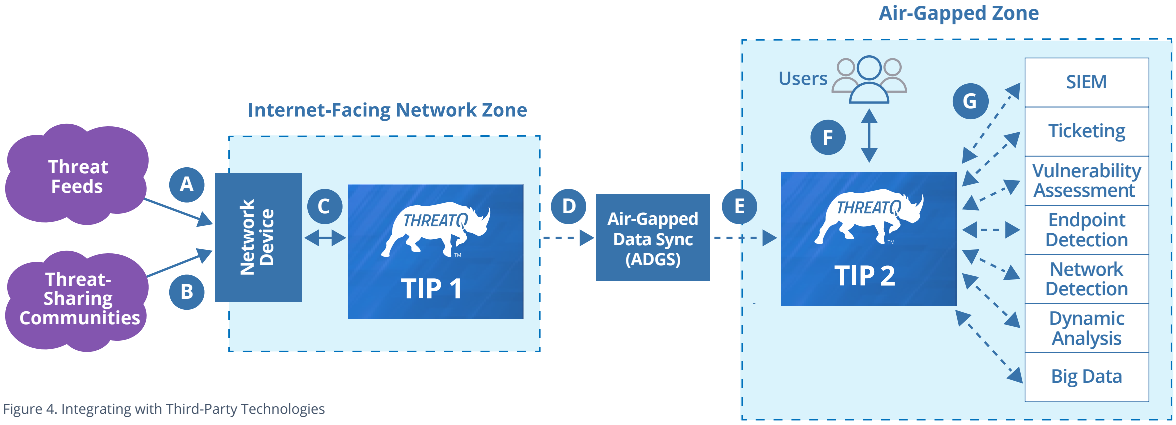


Figure 4. Integrating with Third-Party Technologies

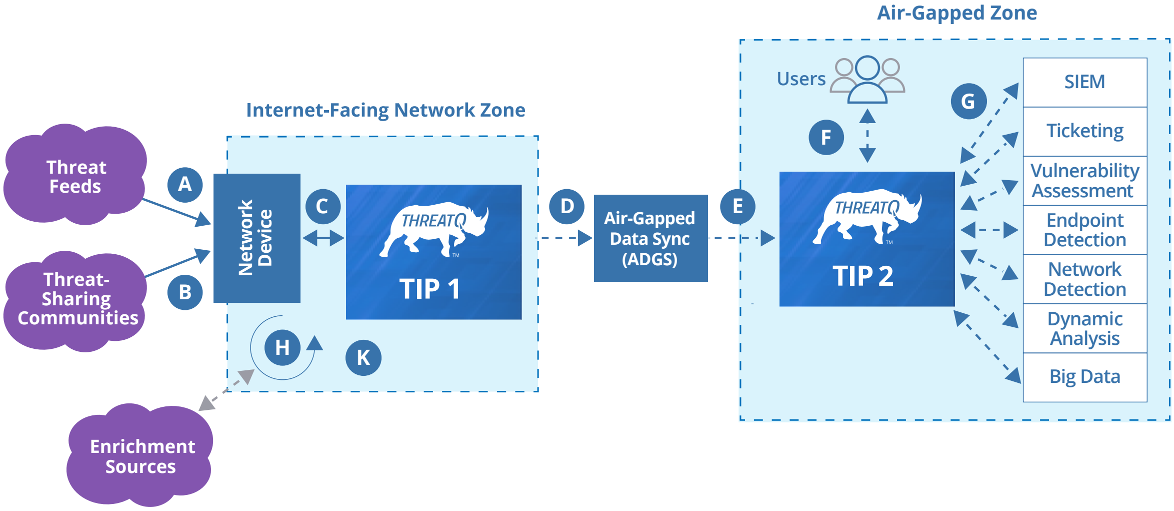


Figure 5. Implementing Automated Enrichment

3.4.2 MANUAL ENRICHMENT

The requests for manual enrichment would normally originate from the TIP in the air-gapped zone, as this is the location where users will access and use the threat data. Manual enrichment techniques must consider the security constraints that are associated with air-gapped environments.

Figure 6 shows the implementation of manual enrichment into the infrastructure. Manual enrichment requests are periodically collected from the TIP in the air-gapped zone and are transferred to a location where enrichment transfers may take place (Reference I in Figure 6). A process for Enrichment Request Transfer is then implemented. This process will vary and may include a technical (automated transfer) or manual solution (manual transfer) depending on the security constraints within the environment. (Please refer to Consideration 7 for more details.) Once the requests have been successfully transferred, a separate process (Reference J in Figure 6) will pull the requests from the transfer location and upload them into ThreatQ in preparation for enrichment. ThreatQ will then periodically pass the data to the chosen enrichment sources for enrichment and incorporate the results into the data set in TIP 1 (Reference K in Figure 6).

Enriched threat data will automatically be transferred back to TIP 2 using the processes that were set up in Step 2.

3.4.3 A NOTE ON 'ANONYMIZATION' OF ENRICHMENT REQUESTS

Several enrichment sources are known to share data on the indicators that have recently been enriched using its services. This can be a challenge for organizations that would like to make their requests confidential. This creates a trade-off between the benefits of using a service and the potential implications of sharing visibility of enrichment requests with an unknown group of stakeholders. It is possible to mitigate this issue to a degree by using the process of 'anonymization' of enrichment requests.

Any enrichment requests that are provided by automated or manual enrichment may be mixed with an additional set of random requests from the Threat Library in TIP 1 or TIP 2 prior to being sent to the externally facing enrichment source. This has the effect of adding noise to the enrichment requests, which, in turn, provides a degree of mitigation when confidentiality of requests is desired.

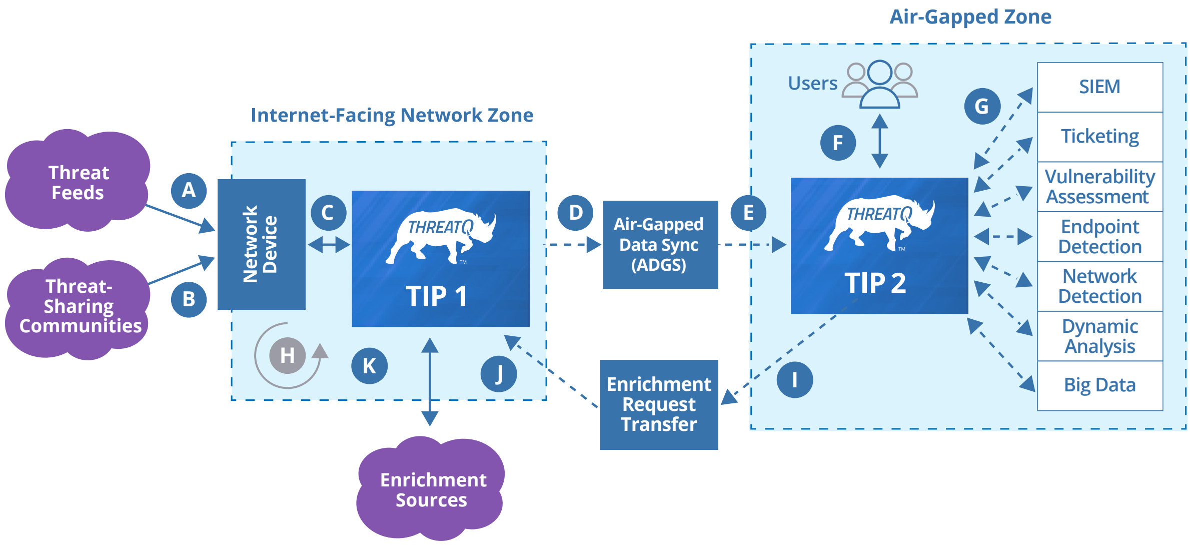


Figure 6. Implementing Manual Enrichment

CONCLUSION

The use of threat intelligence in air-gapped environments presents several challenges. Organizations with such a requirement need to consider several factors, including the placement and architecture of the TIP as well as how to maximize the value given external connectivity restrictions.

ThreatQ is designed to provide organizations with flexibility in how they deploy and use a TIP to meet their specific security and environment requirements. With thoughtful consideration to the desired capabilities and associated trade-offs, even security operations teams in highly regulated environments can use ThreatQ to aggregate, analyze and act on threat intelligence to accelerate security operations and mitigate cyber risk.