TRUSTED PARTNER NETWORK

ME - ISAC 101

Media + Entertainment Information Sharing Analysis Center

PRIVILEGED AND CONFIDENTIAL

Table of Contents

1. What is an ISAC & ISAC Benefits
2. Threat Intel Overview & Services
3. Operating Model
4. Proactive Preventative Blocking
5. Data Flows
6. Timeline
7. Secure vs Threat Intel Portals

TRUSTED PARTNER NETWORK

An ISAC is a member-driven non-profit organization that serves as the focal point for collection, analysis, and dissemination of risk and threat information among its members.

Benefits of an ISAC

Provides a means of communication and collaboration on cyber threat and incident data to raise the defensive posture

Threat Intel Fusion Center
Curated feeds of threat indicators to drive defensive tools, reports, alerts, and bulletins on emerging threats

Collaboration Platform
Email lists, online chat/forum and document repository

Training and Outreach
Summits, meetings, classes, webinars, newsletters, best practices, guides, and advisory services

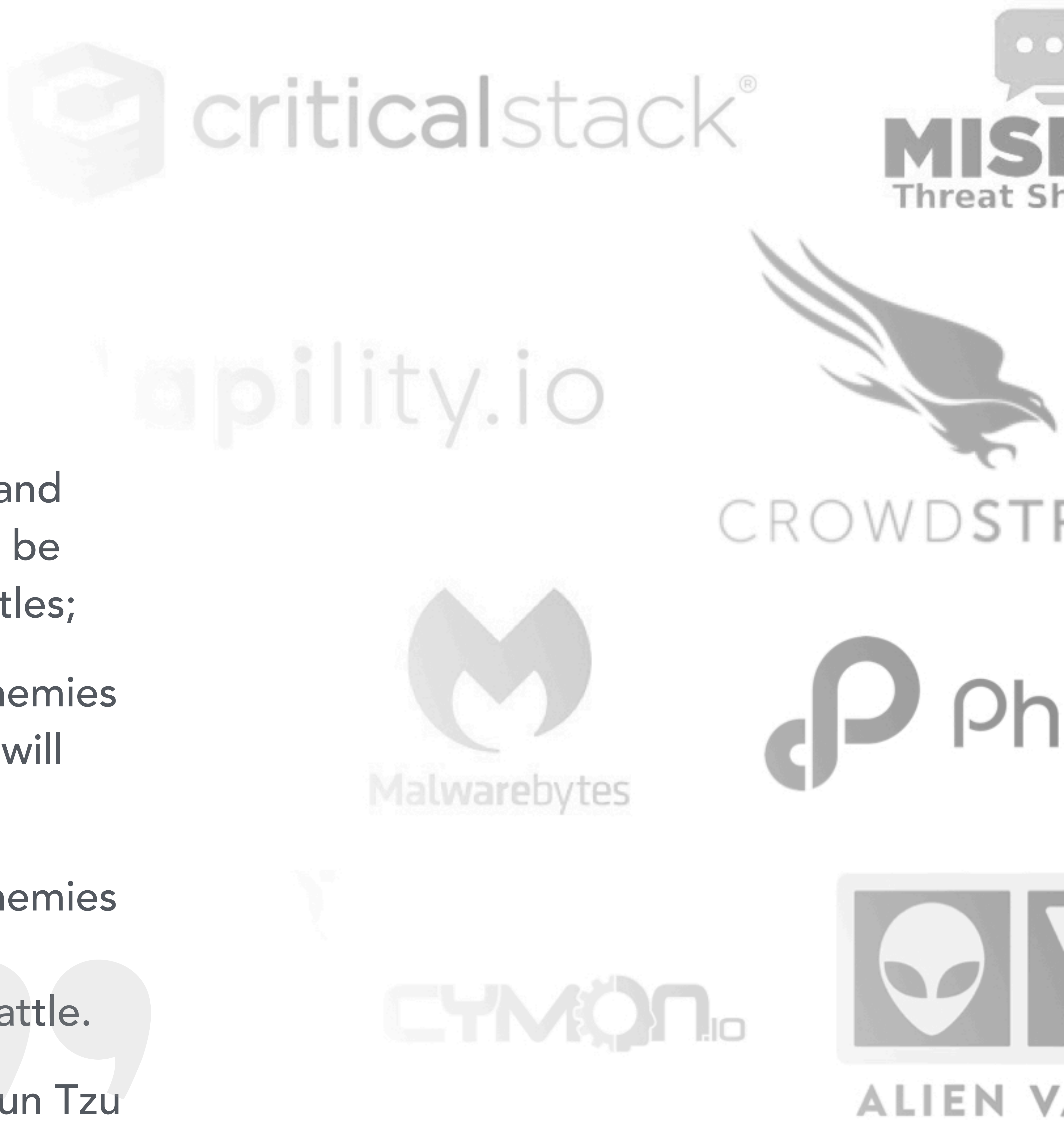
Threat Intel Overview

Offense Informs Defense

Create a Better Informed Defensive Strategy

Informed Defense Enables a Proactive Defense

> If you know your enemies and know yourself, you will not be imperiled in a hundred battles;
>
> If you do not know your enemies but do know yourself, you will win one and lose one;
>
> If you do not know your enemies nor yourself, you will be imperiled in every single battle.
>
> - Sun Tzu



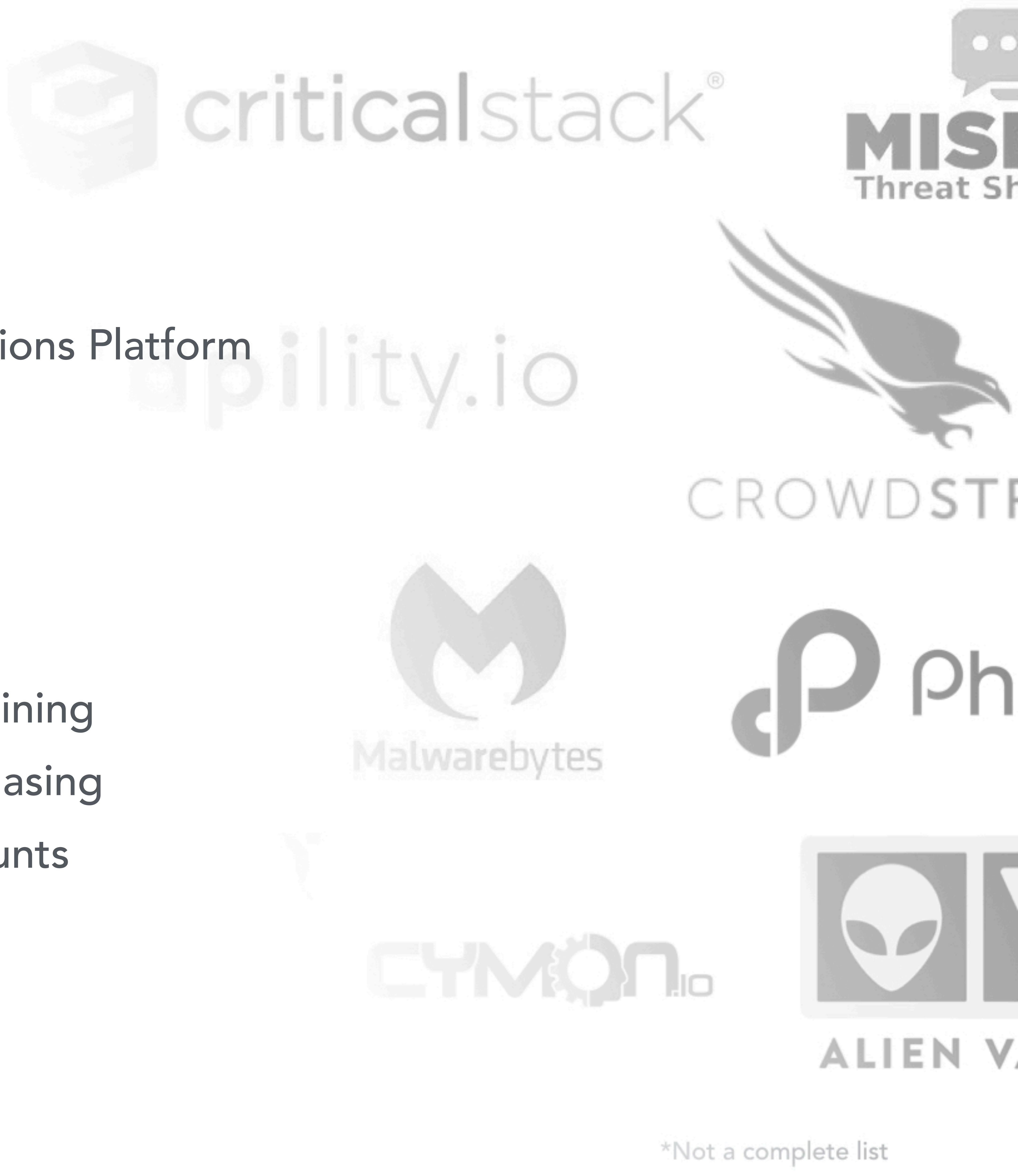
*Not a complete list

Threat Intel Services

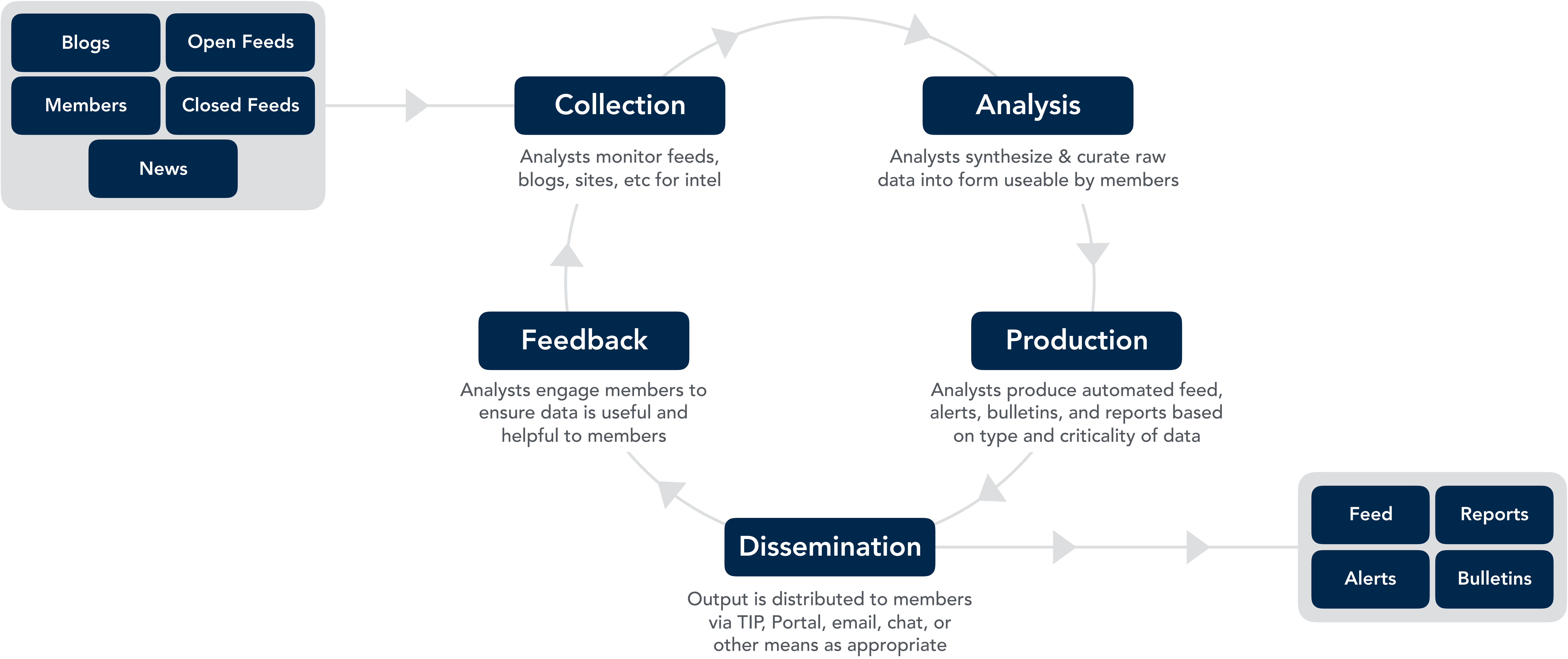
- Machine-readable Threat Intel feed
- Access to Threat Intel Portal
- Threat Alerts
- Threat Bulletins
- Regular Threat Intel Reports
- Security Newsletter
- Security Meetings at Summits
- Industry Best Practices
- Access to Secure Document Repo
- Access to Threat Intel encyclopedia

- Secure Communications Platform
- CISO Forum
- InfoSec Forum
- Anti-Piracy Forum
- Physical Sec Forum
- Custom Industry Training
- Coop Training Purchasing
- Coop Vendor Discounts

*Not a complete list



Operating Model



Blogs

Open Feeds

Members

Closed Feeds

News

Collection

Analysts monitor feeds, blogs, sites, etc for intel

Analysis

Analysts synthesize & curate raw data into form useable by members

Production

Analysts produce automated feed, alerts, bulletins, and reports based on type and criticality of data

Dissemination

Output is distributed to members via TIP, Portal, email, chat, or other means as appropriate

Feedback

Analysts engage members to ensure data is useful and helpful to members

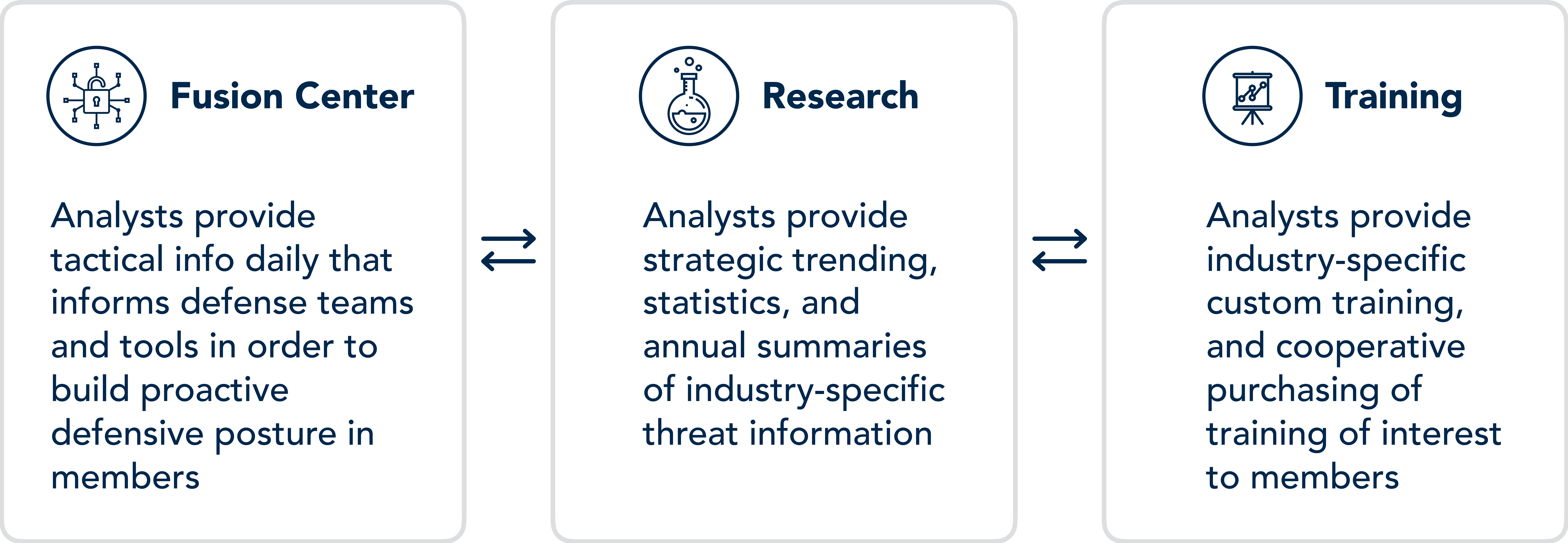
Feed

Reports

Alerts

Bulletins

Operating Model



Fusion Center

Analysts provide tactical info daily that informs defense teams and tools in order to build proactive defensive posture in members

⇄

Research

Analysts provide strategic trending, statistics, and annual summaries of industry-specific threat information

⇄

Training

Analysts provide industry-specific custom training, and cooperative purchasing of training of interest to members

Proactive Preventative Blocking

1 **Attack Occurs and is Reported**
(TIP, Blog, etc.)

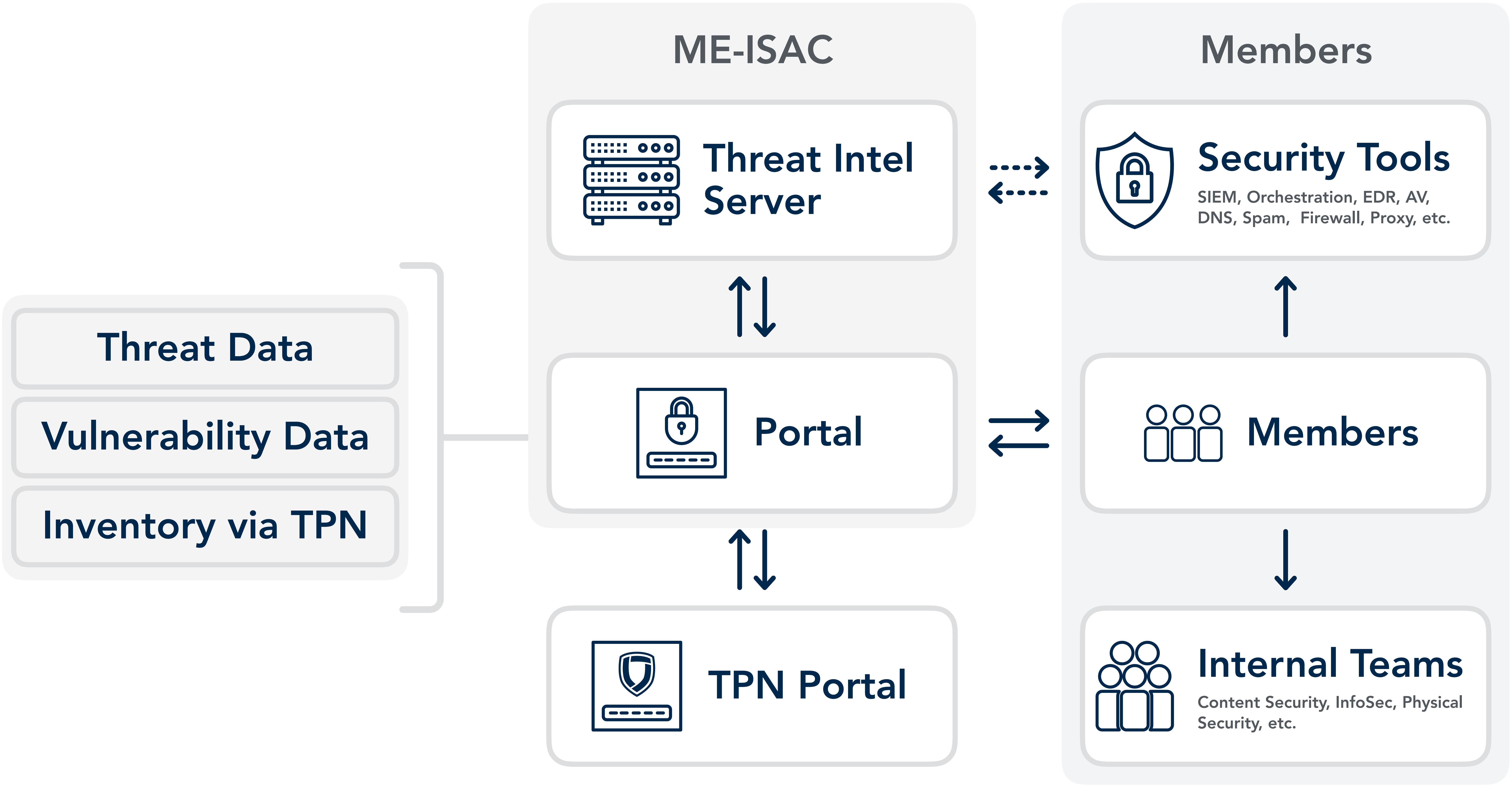
2 **Threat Intel team correlates and deduplicates alerts**
to provide single view of incident and extracts indicators (IP, DNS, email, etc.)

3 **Feed provides indicators to members in machine-readable format**

4 **Indicators entered into appropriate devices as block rules**
(Firewall rules, DNS blackholing, web proxy filters, spam filters, AV, etc.)

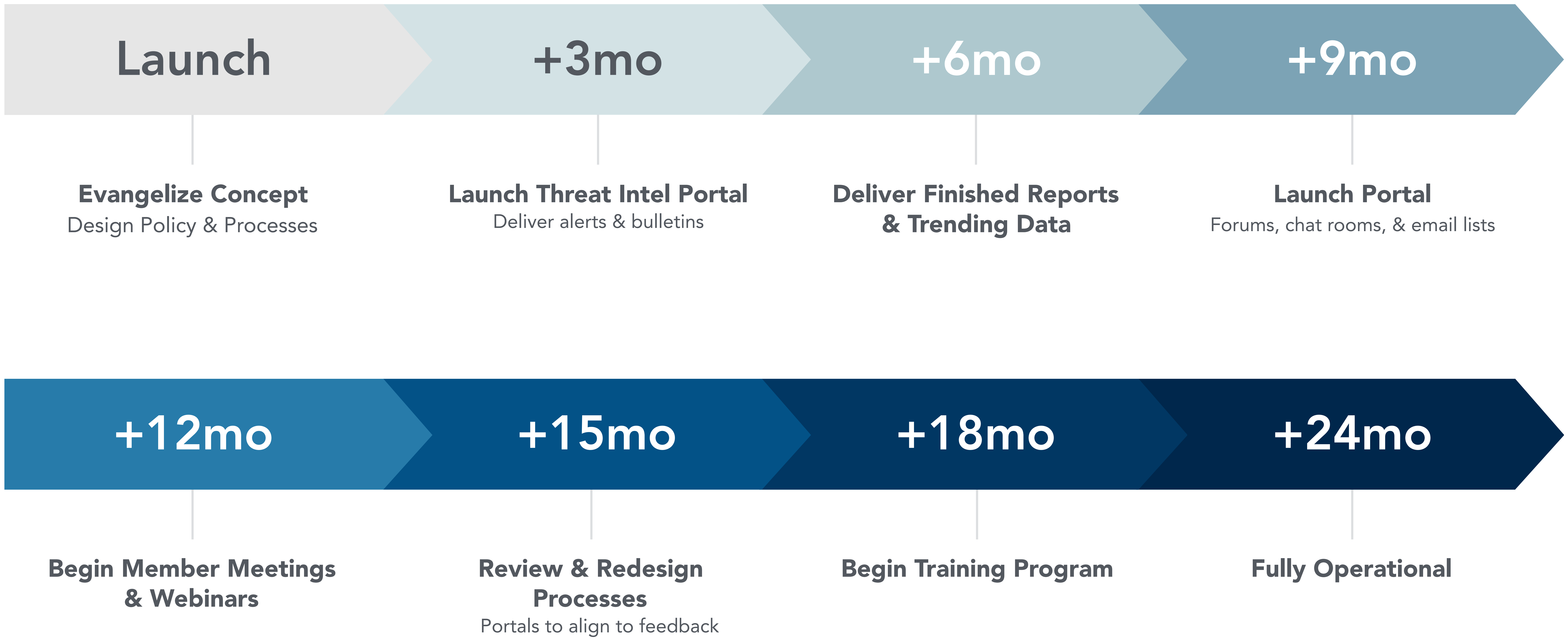
5 **Member is now inoculated from attack before it happens to them**

Data Flows



ME-ISAC
Threat Intel Server
Portal
TPN Portal
Members
Security Tools
SIEM, Orchestration, EDR, AV, DNS, Spam, Firewall, Proxy, etc.
Members
Internal Teams
Content Security, InfoSec, Physical Security, etc.
Threat Data
Vulnerability Data
Inventory via TPN

Timeline Launch to Fully Operational



Launch

Evangelize Concept
Design Policy & Processes

+3mo

Launch Threat Intel Portal
Deliver alerts & bulletins

+6mo

Deliver Finished Reports & Trending Data

+9mo

Launch Portal
Forums, chat rooms, & email lists

+12mo

Begin Member Meetings & Webinars

+15mo

Review & Redesign Processes
Portals to align to feedback

+18mo

Begin Training Program

+24mo

Fully Operational

Portals Secure vs Threat Intel

Secure Portal

Provides document repository, secure communications, and focal point for ISAC activities

Secure, Out-of-Band Communications

Alternative to email / chat, but operates like email / chat
Individual-to-individual, -to-group, -to-community

Wiki-like Encyclopedia of Threat & Risk Data

Community editable repository of threat groups, piracy groups, etc.

Secure Document Repository

White papers, Intel reports, Advisories, etc.

Threat Intel Portal (TIP)

Provides fusion of multiple disparate intel sources, structured API feed to data for machine ingest of intel, and a means for members to interact with the intel

Machine-readable Feed of Threat & Risk Data

STIX/TAXII formatted combined feed from various data sources

Members Consume Data via

- SEIM – provides context & alert triggers
- Orchestration Tool – provides automated updates to firewall rules, etc.
- Manually – search for more information about an indicator

TRUSTED PARTNER NETWORK

PRIVILEGED AND CONFIDENTIAL