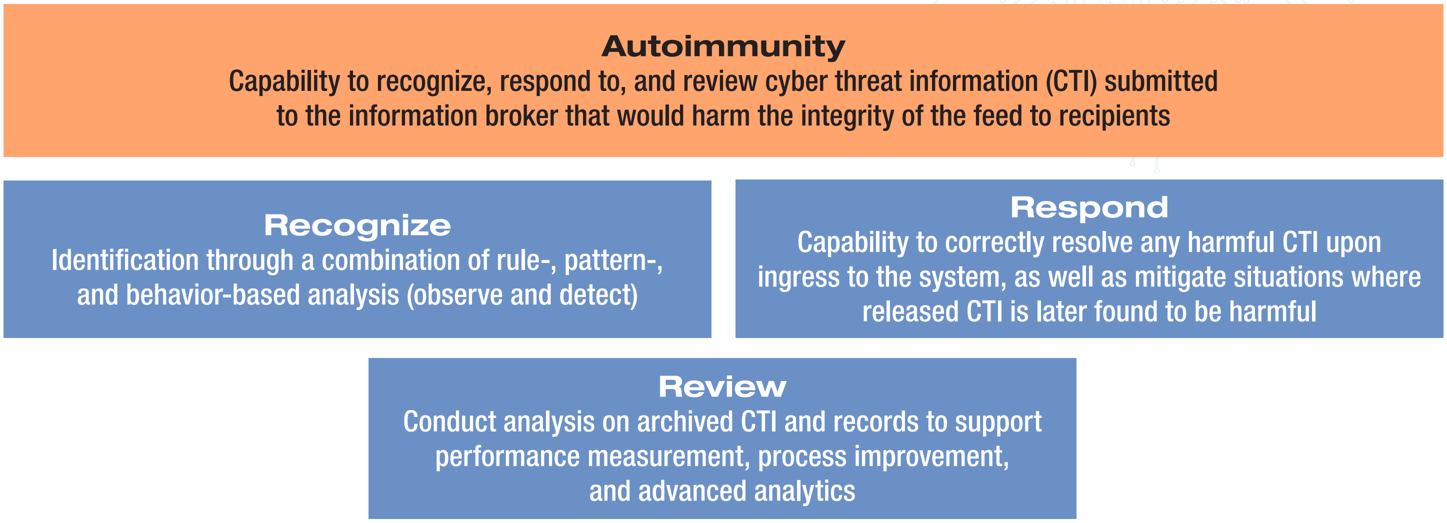
Integrated Adaptive Cyber Defense

Autoimmunity for Cyber Threat Information Sharing

What Is Autoimmunity?



Autoimmunity
Capability to recognize, respond to, and review cyber threat information (CTI) submitted to the information broker that would harm the integrity of the feed to recipients

Recognize
Identification through a combination of rule-, pattern-, and behavior-based analysis (observe and detect)

Respond
Capability to correctly resolve any harmful CTI upon ingress to the system, as well as mitigate situations where released CTI is later found to be harmful

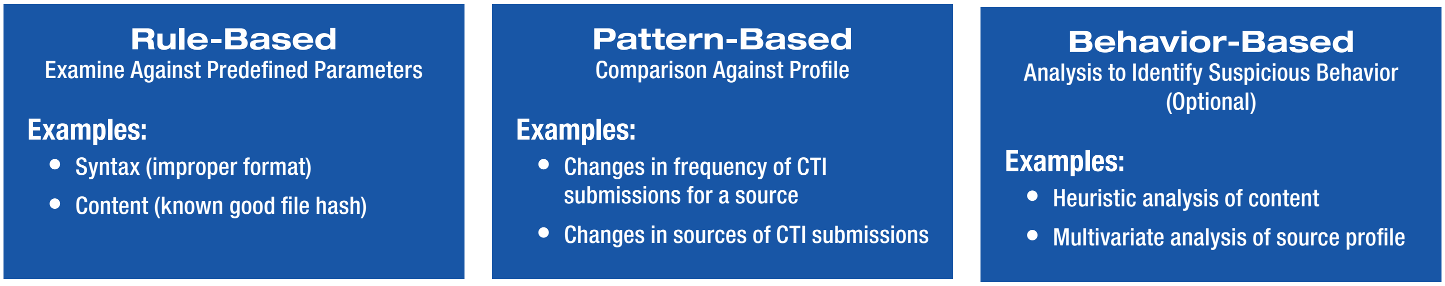
Review
Conduct analysis on archived CTI and records to support performance measurement, process improvement, and advanced analytics

Figure 1. Definition of Autoimmunity

The Autoimmunity Process

Recognition Phase

The first step in the autoimmunity process is for the information broker to properly identify CTI that is not appropriate, suspicious, or potentially harmful. The Johns Hopkins University Applied Physics Laboratory (JHU/APL) recommends that all CTI undergo both rule-based and pattern-based analysis. Behavior-based analysis can also be used if the information broker has the technical capabilities.



Rule-Based
Examine Against Predefined Parameters

Examples:
- Syntax (improper format)
- Content (known good file hash)

Pattern-Based
Comparison Against Profile

Examples:
- Changes in frequency of CTI submissions for a source
- Changes in sources of CTI submissions

Behavior-Based
Analysis to Identify Suspicious Behavior (Optional)

Examples:
- Heuristic analysis of content
- Multivariate analysis of source profile

Figure 2. Three Analysis Types with Examples for Recognition Phase of Autoimmunity

Response Phase

After completion of the Recognition Phase, submitted CTI is deemed appropriate for dissemination or flagged as either inappropriate for dissemination or potentially harmful. JHU/APL recommends that no flagged CTI should automatically advance toward dissemination without an analyst first having an opportunity to review it.

Review Phase

JHU/APL recommends that the information broker store all CTI, analysis results, and disposition actions. The stored data can facilitate more advanced analysis such as auditing, process improvement, and advanced data analytics (e.g., trend analysis).

http:// https://secwww.jhuapl.edu/iacd @IACD_automate https://www.linkedin.com/groups/8608114 icd@jhuapl.edu