Center for Threat Informed Defense

CTI Blueprints

A Report Standardizing Tool

CTI Blueprints helps Cyber Threat Intelligence (CTI) analysts create high-quality, actionable reports more consistently and efficiently

What common problems do CTI analysts face?

- New analysts struggle to learn report writing due to the **lack of standardized guidance.**
- Analysts **lack a repeatable process** to create actionable reports regardless of author.
- Analysts **struggle to create actionable reports** that address specific stakeholder intelligence requirements.
- **Manual processes** in report creation cost analysts time and resources.
- Most CTI is shared in an **unstructured, unstandardized** way.

Driving Innovation

1. Templates –Report templates with prescriptive guidance baked-in to help analysts create actionable intelligence for specific audiences in a repeatable fashion. Each template is designed to support one of four goals: Know, Find, Change, and Inform. The following are CTI Blueprint report templates:

Threat Actor Report

- Know – Living encyclopedia maintained by the intel team to help tactical teams understand the threat actor and inform follow-on actions.

Intrusion Analysis Report

- Find – Support active hunting and incident response operations.

Campaign Report

- Change – Highlight new information related to a threat actor or capabilities.

Executive Report

- Inform – Inform senior decision makers about a risk or decision regarding strategic problems.

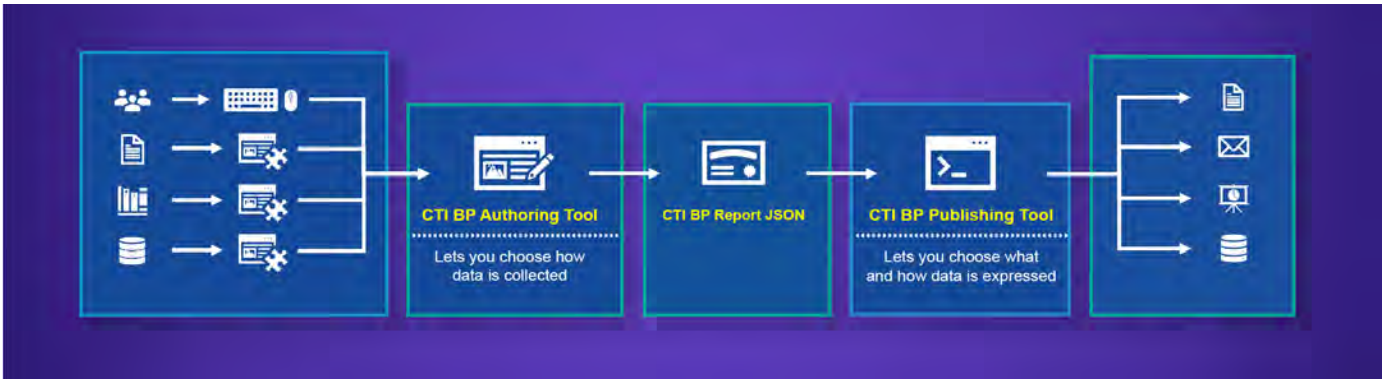
Template & Sample Reports

2. Sample Reports – Templates filled with sample data to provide analysts an example of what a report would look like, following best practices outlined by CTI Blueprints.

3. Software Tool – Analysts can create and publish templates using the free software tool. Users can do the following:

- Generate human-readable assets, such as PDF, E-mail, PowerPoint.
- Generate a JSON file for machine-to-machine readability.
- Integrate with existing workflow by choosing how data is entered, what data is published, and how data is expressed.
- Save time, support repeatability, and reduce user error with plugins allowing for automatic table fill, connections to MITRE ATT&CK, and integration with Attack Flow and D3FEND.
- Extensible framework can be built out to import IOCs from existing TIPs, perform differential analysis on IOCs, etc.

CTI Blueprints Tool Suite



CTI Blueprint Goals

- Advance the quality and standardization of CTI reporting
- Further analytic rigor in the CTI community
- Make it easier to consume and share CTI
- Reduce manual processes in report building
- Support increased integration between CTI teams and their stakeholders to enable better outcomes

What CTI Blueprints is NOT

- Threat Intelligence Platform
- Replacement for STIX or other structured languages
- Tool to create fully stylized reports beyond a basic export and editing function

Get Started

- Visit our Github Page for more information on the project and to access the templates and sample reports: **https://github.com/center-for-threat-informed-defense/cti-blueprints**
- Access the tool here: **https://github.com/center-for-threat-informed-defense/cti-blueprints**

How Can I Get Involved?

- Provide feedback on the templates and tool on Github, or reach out to our team directly at **ctid@mitre-engenuity.org.**
- Help us develop additional plug-ins for the community or provide additional plugin suggestions. A running list of suggested plug-ins can be found on our Github page at: **https://github.com/center-for-threat-informed-defense/cti-blueprints/wiki/Development#suggested-plugins**