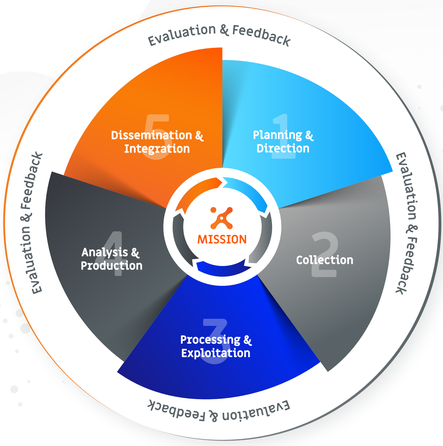
ThreatConnect

Aligning the Intelligence Cycle with ThreatConnect

PLATFORM FEATURES & CAPABILITIES

The Intelligence Cycle & ThreatConnect Platform

The Intelligence Cycle is a six-step methodology adopted by various worldwide public and private organizations to create and circulate intelligence products in support of their mission objectives. The capabilities and features included with the ThreatConnect Platform enable and streamline the execution of this process. Here, each phase of the cycle is briefly defined, followed by the features and capabilities aligned to each phase.



1 Planning & Direction

"Establish the consumer's intelligence requirements and plan intelligence activities accordingly."

- Guide intelligence program development via a library of Resources to include a Knowledge Base; TIP and SOAR eBooks; the Diamond Methodology; and the Threat Intelligence Maturity Model (TIMM)
- Facilitate the tracking of intelligence requirements via Tags, Attributes (prebuilt or custom), and Dashboards
- Bolster a collection plan via integrated open sources, closed sources, internal sources, and intelligence sharing communities; Enable a team workflow via tasks and notifications
- Define a strategy for rating the Threat & Confidence of indicators and excluding unwanted noise; Define custom indicators

2 Collection

"Gather the raw data required to produce the finished product."

- Activate prebuilt OSINT feeds; evaluate their quality via report cards; tap into Technical Blogs and Reports; leverage analyst-curated ThreatConnect Intelligence; and integrate premium threat intelligence
- Acquire operational environment data via integrations focused on Deception, Endpoint Detection & Response (EDR), Network Security, Security Information and Event Management (SIEM), and Vulnerability Management
- Connect to STIX-TAXII feeds via an inbound TAXII client
- Ingest phishing emails and indicators via Phishing and Feed Mailboxes; scrape web pages via an HTTP Feed; parse CSV files; and upload malware to a malware vault
- Manually create indicators and groups; import structured indicators, unstructured indicators, signatures, and emails; or search through unstructured data to add new indicators
- Monitor and import adversary infrastructure via Tracks
- Conduct Brand Monitoring activities via the Domain-Spinning Workbench
- Leverage PlayBooks or build custom apps to collect from a multitude of assets such as an RSS feed, signature provider, or compromised accounts repository (to name a few)
- Ingest indicators via System or Contextually aware Spaces apps such as the VirusTotal App

3 Processing & Exploitation

"Convert the raw data into a comprehensible format that is usable for production of the finished product."

- Assemble data elements into the ThreatConnect Data Model via automated and manual methods
- Illuminate data context by applying metadata in the form of Associations, Tags, Attributes, and indicator ratings
- Automatically deprecate indicator confidence ratings over time
- Leverage markup and markdown to format data elements
- Enrich indicators via integrations focused on Enrichment & Analysis, Malware Analysis, and Orchestration
- Enrich data via Automated Data Services such as DNS resolutions, Whois information, and IP Geolocation services
- Process email bodies and headers via Email Scoring Rules
- Automate various processing and exploitation methods via PlayBooks

4 Analysis & Production

"Integrate, evaluate, analyze, and prepare the processed information for inclusion in the finished product."

- Browse, filter, and save queries for Indicators, Groups, Tags, Tracks, Victims, and Victim Assets
- Exploit advanced filtering methods via the ThreatConnect Query Language (TQL)
- Leverage saved queries and TQL in Dashboards to visualize results
- Assess indicator risk via ThreatAssess and Collective Analytics Layer (CAL) insights, and Investigation Links
- Pivot on data associations via Browse Screen, Details Screen, Graph View, and Attributes
- Analyze indicators via System or Contextually aware Spaces apps such as the VirusTotal App
- Execute UserAction Triggers via PlayBooks
- Manually set indicator Threat and Confidence ratings and Indicator Status
- Model file behavior to illustrate dropped files or network behavior
- Report False Positives to avoid inadvertent incident response activities
- Follow and notify on changes to Indicators, Groups, Tags, Tracks, Victims and other items
- Evaluate data sensitivity and apply Security Labels
- Interface with the ThreatConnect RestAPI using third-party reporting tools to facilitate intelligence product development

5 Dissemination & Integration

"Deliver the finished product to the consumer that requested it and to others as applicable."

- Establish a ThreatConnect TAXII Server or outbound TAXII Client
- Share across ThreatConnect instances via the Cross-Intel Sharing App and Publish feature
- Share intelligence internal to a ThreatConnect instance by posting comments, configuring notifications, and contributing to communities and sources
- Send email or Slack messages via a PlayBook
- Generate a PDF document for an Adversary, Campaign, Event, Incident, Intrusion Set, Report, or Threat
- Manually Export indicators to a CSV file from the UI or establish a persistent, regularly updated HTTPS-based URL to periodically download an Indicator CSV to a third-party integration
- Grant privileged access to the ThreatConnect RestAPI via an API account to allow applications to pull, push, and present data

6 Evaluation & Feedback

"Continually acquire feedback during the Intelligence Cycle and evaluate that feedback to refine each individual step and the cycle as a whole."

- Measure intelligence performance and effectiveness via Incident Response & Ticketing integrations and Case Management solutions
- Evaluate PlayBook Return on Investment metrics
- Acquire operational environment situational awareness via API account observations and false positives
- Define CTI metrics and create custom metrics for a DashboardAutomate various processing and exploitation methods via PlayBooks

*** Intelligence Cycle Overview provided by the Director of National Intelligence (DNI) Office*

Director of National Intelligence. (2013). U.S. National Intelligence; An Overview. Retrieved from https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf

ThreatConnect