



Empowering DFIR through automation and orchestration

Enhancing your artifacts with
Threat Intelligence

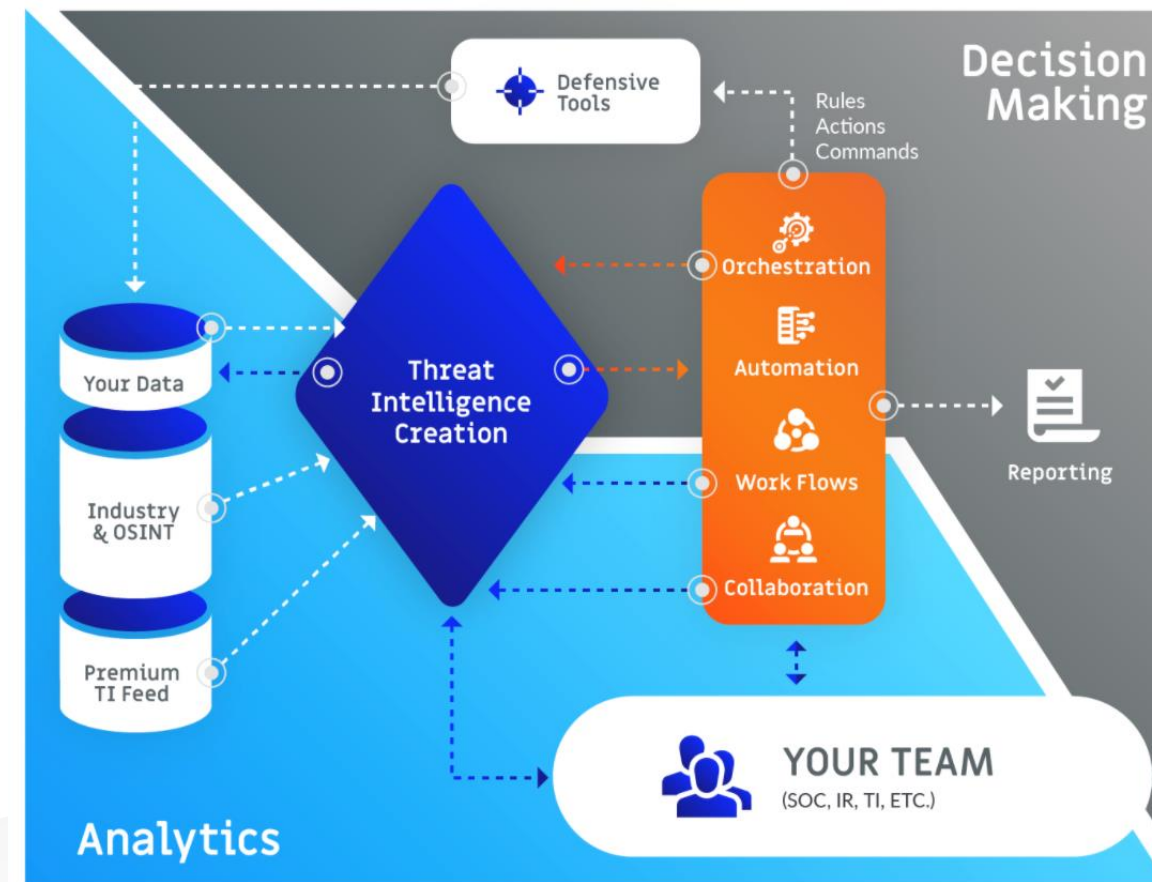


ThreatConnect.com

Copyright © 2020 ThreatConnect, Inc.

Power of Intelligence

- Contextual awareness
- Domain bit squatting detection
- Malicious/suspect domain registration
- Adversary profiles
- Enrich your environment



How can threat intelligence enhance DFIR and what does it mean?

Intelligence

Exists to inform decisions for security operations, tactics, and strategy

Operations

Captures data on adversaries, attacks & attempts that can be refined into intelligence

Why Automate?

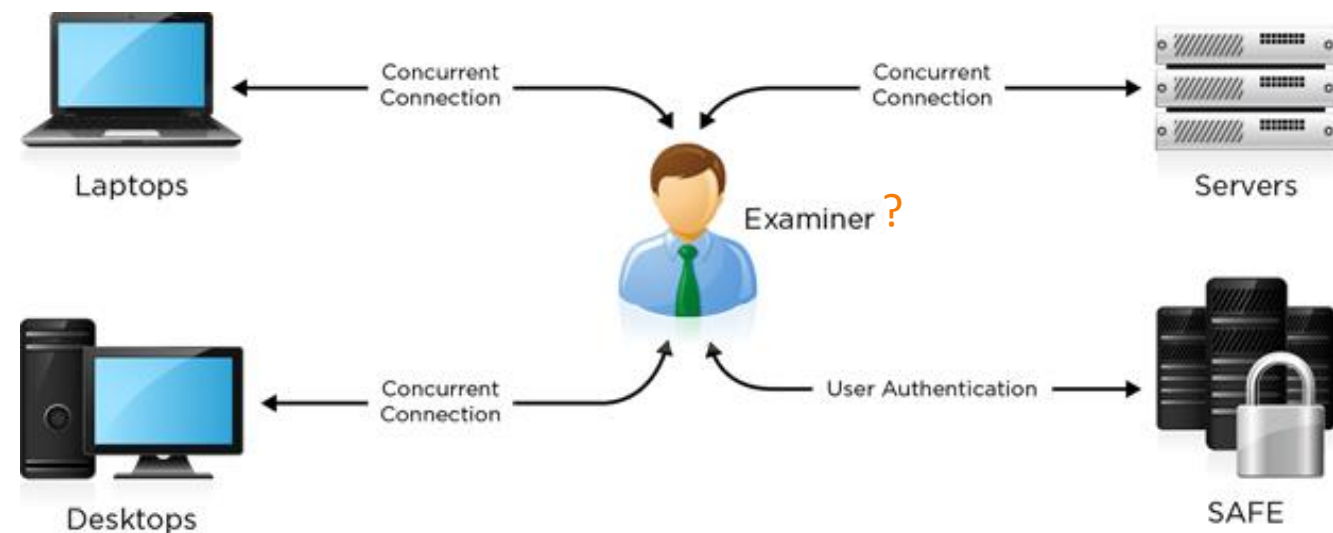
Sounds really complicated

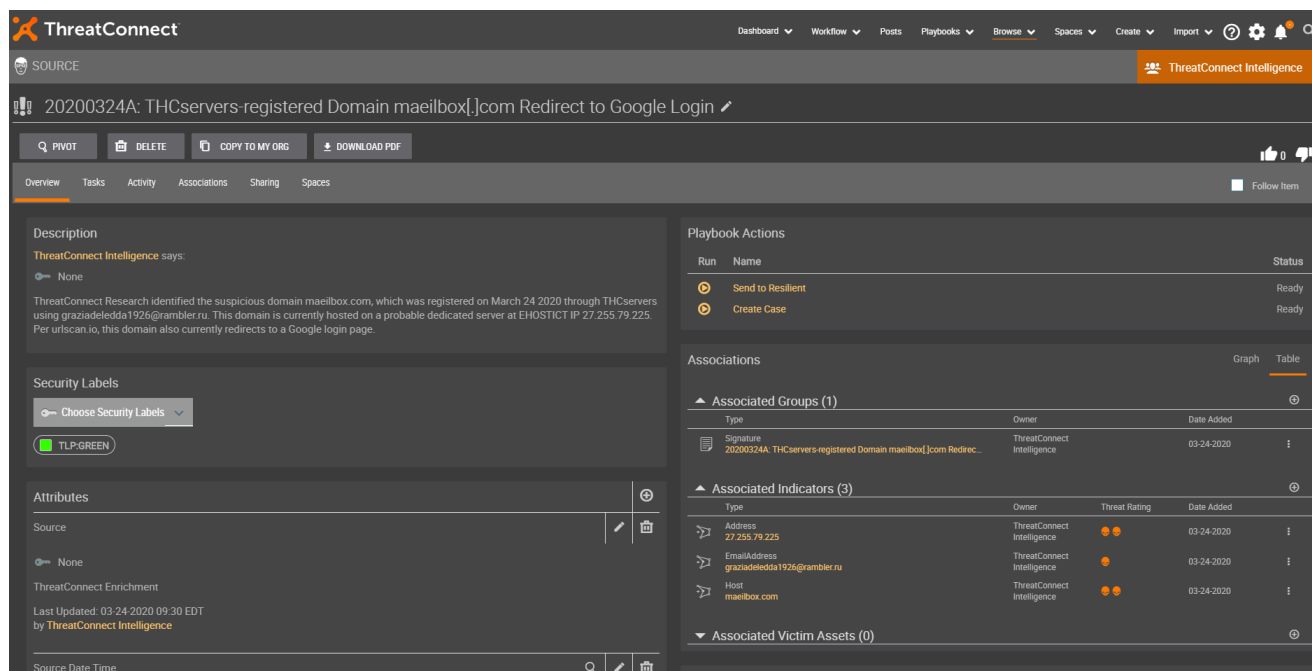
How much time does it take?

How repeatable is it?

What does DFIR Process Automation look like?

- User Action based acquisition
- Runbook/playbook via SOC/TI
- Process can be started as a step in the workflow or runbook in a case





The screenshot displays the ThreatConnect interface for a specific source. The top navigation bar includes links for Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, and a search icon. The source ID is 20200324A, and the title is 'THCservers-registered Domain maelbox[.]com Redirect to Google Login'. Below the title are buttons for PIVOT, DELETE, COPY TO MY ORG, and DOWNLOAD PDF. The left sidebar shows tabs for Overview, Tasks, Activity, Associations, Sharing, and Spaces. The main content area is divided into several sections:

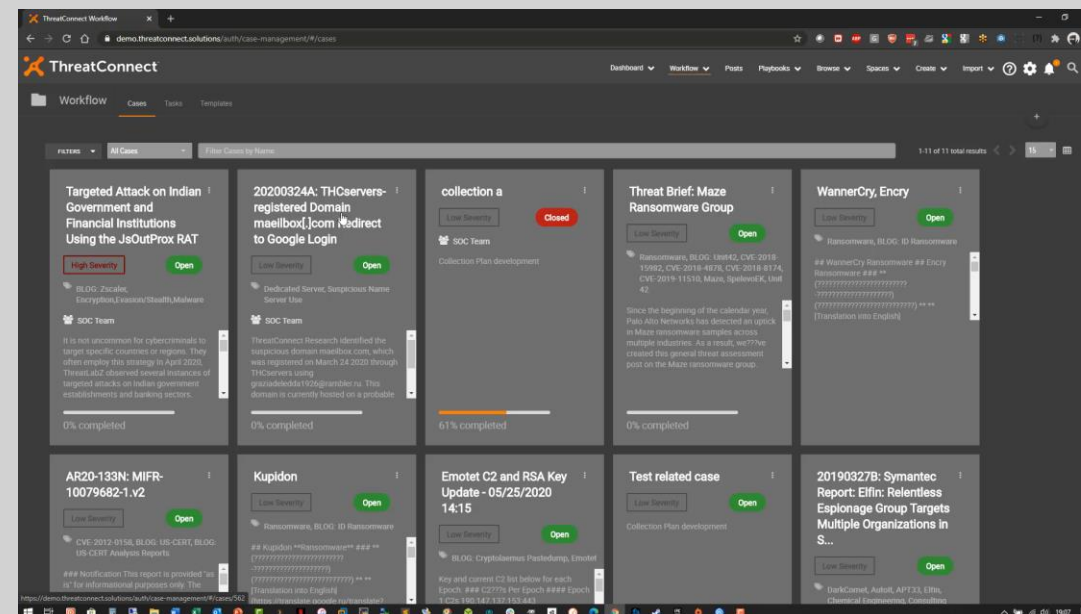
- Description:** A text block stating that ThreatConnect Research identified the suspicious domain maelbox.com, which was registered on March 24, 2020, through THCservers using graziadeledda1926@rambler.ru. It also mentions that the domain is currently hosted on a probable dedicated server at EHOSTICT IP 27.255.79.225 and currently redirects to a Google login page.
- Security Labels:** A section with a 'Choose Security Labels' dropdown and a 'TLP:GREEN' label.
- Attributes:** A section showing the source name, a 'None' status, and a 'ThreatConnect Enrichment' section with a 'Last Updated' timestamp of 03-24-2020 09:30 EDT by ThreatConnect Intelligence.
- Playbook Actions:** A table with two actions: 'Send to Resilient' and 'Create Case', both with a 'Ready' status.
- Associations:** A section with two tables:
 - Associated Groups (1):** A table with columns Type, Owner, and Date Added. It shows one group: 'Signature 20200324A: THCservers-registered Domain maelbox[.]com Redirec...' with Owner 'ThreatConnect Intelligence' and Date Added '03-24-2020'.
 - Associated Indicators (3):** A table with columns Type, Owner, Threat Rating, and Date Added. It shows three indicators: 'Address 27.255.79.225', 'Email address graziadeledda1926@rambler.ru', and 'Host maelbox.com', all with Owner 'ThreatConnect Intelligence' and Date Added '03-24-2020'.
- Associated Victim Assets (0):** A section with a table showing no associated victim assets.

- Repeatable process
- Automated Case creation
- Investigate and gather before creating a forensic case
- Quicker collection
- Shorter case creation times

Analyst Driven Automation

Workflow Driven Automation

- Repeatable process
- Automated Case creation
- Ability to do more in a shorter period of time
- Live Forensics
- Automated timelines



More information is always better



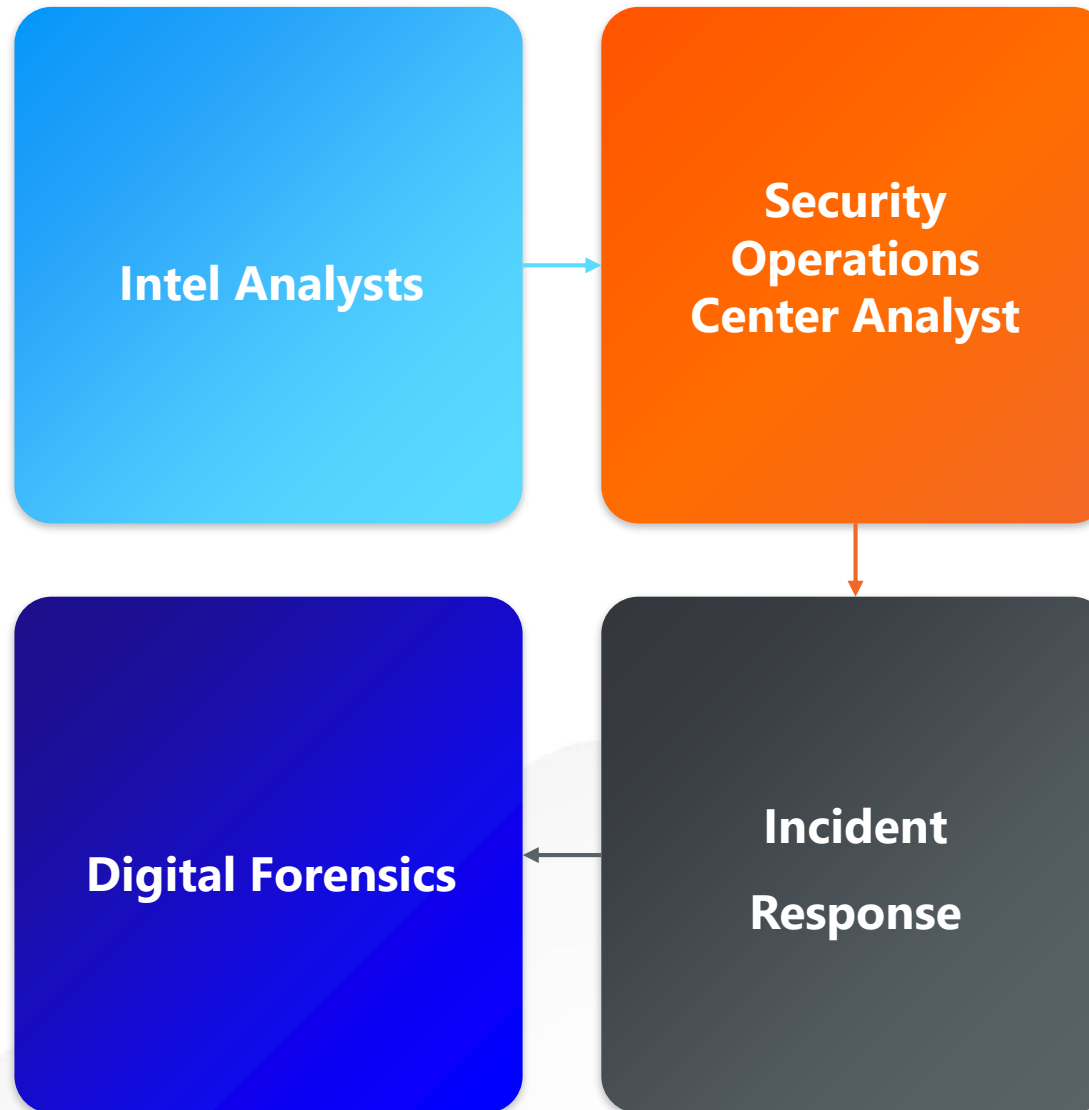
Save analyst time and eliminate redundancy



Automating processes for standardization and quicker decision making



Kick off Automations for response actions based on analysis results



Benefits of Automated Incident Response and Digital Forensics

- Quicker response times
- Greater investigation time
- Ability to do more in a shorter period of time
- End to end information flow from Intel Analyst to Forensic Examiner
- Live Forensics
- Automated timelines



Thank You

ThreatConnect.com

ThreatConnect.com

Copyright © 2020 ThreatConnect, Inc.

