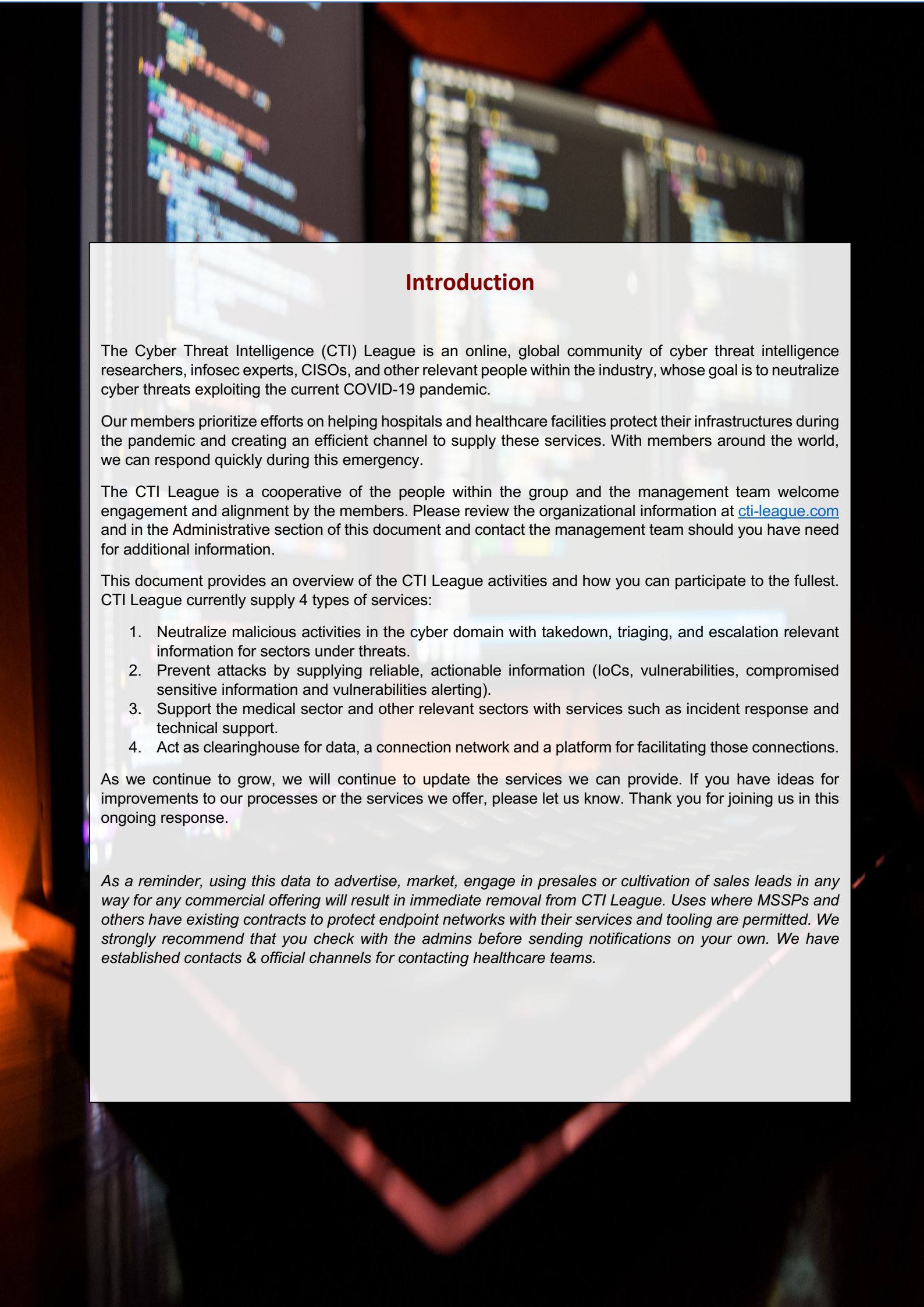
CTI League

Playbook

May 2020

Contents



Introduction

The Cyber Threat Intelligence (CTI) League is an online, global community of cyber threat intelligence researchers, infosec experts, CISOs, and other relevant people within the industry, whose goal is to neutralize cyber threats exploiting the current COVID-19 pandemic.

Our members prioritize efforts on helping hospitals and healthcare facilities protect their infrastructures during the pandemic and creating an efficient channel to supply these services. With members around the world, we can respond quickly during this emergency.

The CTI League is a cooperative of the people within the group and the management team welcome engagement and alignment by the members. Please review the organizational information at cti-league.com and in the Administrative section of this document and contact the management team should you have need for additional information.

This document provides an overview of the CTI League activities and how you can participate to the fullest. CTI League currently supply 4 types of services:

1. Neutralize malicious activities in the cyber domain with takedown, triaging, and escalation relevant information for sectors under threats.
2. Prevent attacks by supplying reliable, actionable information (IoCs, vulnerabilities, compromised sensitive information and vulnerabilities alerting).
3. Support the medical sector and other relevant sectors with services such as incident response and technical support.
4. Act as clearinghouse for data, a connection network and a platform for facilitating those connections.

As we continue to grow, we will continue to update the services we can provide. If you have ideas for improvements to our processes or the services we offer, please let us know. Thank you for joining us in this ongoing response.

As a reminder, using this data to advertise, market, engage in presales or cultivation of sales leads in any way for any commercial offering will result in immediate removal from CTI League. Uses where MSSPs and others have existing contracts to protect endpoint networks with their services and tooling are permitted. We strongly recommend that you check with the admins before sending notifications on your own. We have established contacts & official channels for contacting healthcare teams.

CTI League Goals

The Cyber Threat Intelligence (CTI) League is an online, global community of cyber threat intelligence researchers, infosec experts, CISOs, and other relevant industry stakeholders whose goal is to neutralize cyber threats exploiting the current COVID-19 pandemic.

The CTI League goals can be divided into three core goals – neutralization, prevention, support – detailed in the 'Activities' chapter. Neutralization is the most valuable process, lawfully taking down criminal infrastructure to deny threat actors these capabilities and escalating as appropriate to the relevant law enforcement agency or governmental entity for further steps.

We can only act on intelligence published or facilitated through the CTI League channels. Therefore, CTI League members are encouraged to share information with the community (Cyber Threat Intelligence Community of Sharing) so we can take action and support our stakeholders, like hospitals, laboratories, healthcare facilities, global organizations, governmental entities.

Neutralize

The CTI League operates to **neutralize** malicious activities executed by threat actors exploiting the current pandemic to stop attacks against known and unknown targets. These attacks leverage infrastructure, such as command and control servers, phishing domains, and websites. Lawfully taking down their infrastructure disrupts their ability to conduct criminal activities. Here are some examples:

- Filing an abuse complaint with a registrar about domains used for fraudulent purposes may result in it being "frozen" and unavailable for criminal activity.
- Notifying companies whose sites have been hacked to host command and control servers can result in the company cleaning off the criminal content.

Prevent

The CTI League works to **prevent** cyber attacks against our stakeholders by alerting them to exposed vulnerabilities or impending attacks. The prevention process includes identifying vulnerabilities or attack infrastructure, sharing the indicators in the relevant channel, and alerting the targeted organization if identified. Here are some examples of prevention processes:

- Alerting our stakeholders about vulnerabilities or compromised information and infrastructure
- Creating a database of malicious indicators of compromise for blocking (via both MISP and GitHub repository)
- Alerting about trends and patterns regarding the pandemic in the cyber domain
- Creating a database of hunting queries for alerting systems

Support

The CTI League offers cyber-protection support to our stakeholders and helps them harden their infrastructure, improving their protection abilities. The CTI League members receive support applications from the medical sector and offers advice and guidance to mitigate and respond to attacks. Here are some examples of the supporting processes:

- Creating a safe and secure infrastructure for CTI League activities
- Generating reports for stakeholders and updating them about ongoing attack trends regarding their organizations, such as significant information from underground-based platform (darknet)

The following chapter is a guide for our tools and services in the CTI League. If you have any additional question, please send a message to one of the management team: Ohad Zaidenberg, Nate Warfield, Marc Rogers, and Chris Mills. To find the playbook in the league, type @playbook.

Slack

The CTI League platform is currently Slack. This chapter provides an overview of operating CTI League platform. The CTI League's developer members are working 24/7 to create a secure and simple system to facilitate t the CTI League mission.

While joining Slack, our welcome workflow will send the new user the following message:

> Hi @User! Please read me as this will answer many of the questions our new members have when joining!
>
> Welcome to CTI League! As you explore, please check channels for pinned messages and do not be afraid to ask questions - this is a very busy group, but everyone here is helpful.
>
> Please be sure to read our Code of Conduct: https://cti-league.com/code-of-conduct/ - this is a trust group and violating any of our policies will result in immediate removal.
>
> The League is a platform for connecting people - we started it to connect InfoSec professionals with medical groups who could use a helping hand either with threat intel data, IOC triage, URL takedowns, etc. and this is expanding into other areas (education, infrastructure, etc.).
>
> To get the most from the League, you need to be active: ask for help, ask for information, help others out as you can. Our bot-fed channels are there to provide data; how to utilize the data may require assistance from League members. Do not be afraid to ask questions! There is a lot going on and we want to you to get the most out of the League as possible while respecting your other time commitments.
>
> #1-announcements has our playbook & information on our bots - you can type @playbook in any channel to have it sent to you.
>
> We ask that you use at least your real first name in your Slack handle and if you are comfortable, the organization you work for (like <Name @Organization>).
>
> When joining, please add yourself as a contact for your organization, especially if you can help in any official manner (takedowns, point of contact, etc.). This helps other League members find you if actionable data is found for your organization or if they need your help taking down a bad actor, shutting off C2 infrastructure, etc.
>
> ContactsBot accepts the following commands:
>
> /add_contact [organization] - Adds yourself as a contact for the org specified.
>
> /list_contacts [organization] - Lists the contacts for the org specified.
>
> /list_orgs - Returns the list of organizations that have contacts registered.

The CTI League community encourages its members to take active part in advancing the league's ability to help the medical sector. The management team suggestion box is open 24/7; we kindly welcome them. CTI League members can use the suggestion slash command /ideanew to submit a new idea for the management team.

Whether you have any administration process improvement, want to develop some service for helping the medical sector, or want to help the League be better and efficient for the rest of the members - We are here for you!

If you want to help the CTI League management team with missions we have as a league, please check new volunteering positions in CTI League board (current channel - *#1-volunteering-board*).

Code of Conduct

Please review CTI League code of conduct. All members are held accountable to this code.

https://cti-league.com/code-of-conduct/

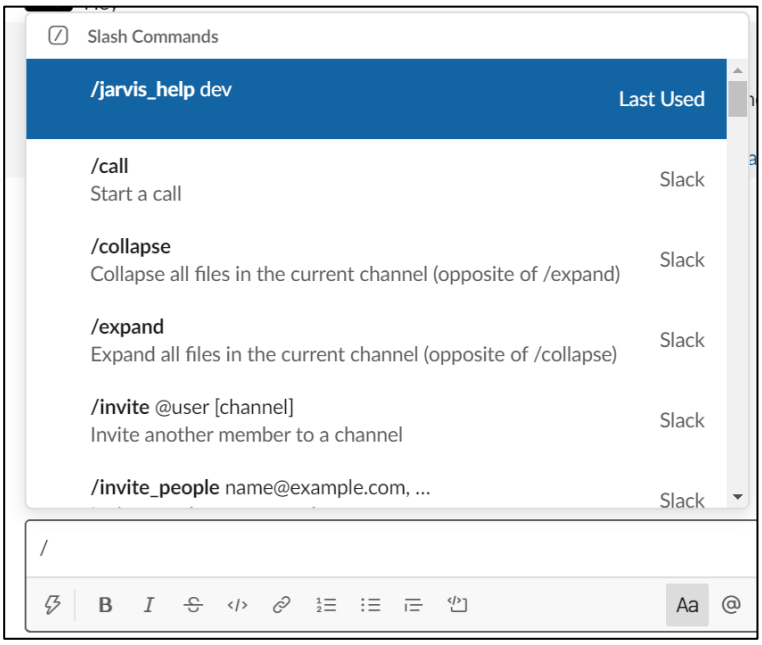
Channel Numbering Method

The CTI League platform is a slack with multiple channels. Most of the channel are public, while some of which are private and dedicated for specific issues.

Channel Numbering Method		
Number	Meaning	Current Channels
1	General channel for communication with the league, introduction by new members, and announcements by the management team	#1-announcements #1-intorduction #1-general #1-volunteering-board #1-general-help
2	CTI League requests – in these channels, our members can facilitate the information and protect the medical sector	#2-ioc-triage #2-takedown-requests #2-medical-vuln-triage #2-request-for-information #2-law-enforcement-escalations #2-help-requests #2-contacts-at #2-anonymous-iocs-report
3	Streaming information by of the CTI League	#3-medical-infra-vuln-stream #3-phishing-attachments #3-covid-suspicious-domains #3-hunting-queries #3-network-monitoring
4	Supporting channels, Darknet and Disinformation	#4-medical-sector-supporting #4-infrastructure-support #4-ir-requests #4-disinformation #4-darknet #4-iocs #4-github-requests-assistance
5	Databases, Feeds, Malware Analysis	#5-hunting-queries-database #5-android-malware-analysis #5-linux-malware-analysis #5-mac-malware-analysis #5-android-malware-analysis #5-sms-analysis #5-feeds
6	OSINT and random channels	#6-osint-misp #6-osint-network #6-random #6-news-covid19

Bots

The main workflow of the League is enabled with bots – such as our main bot Jarvis and or ticketing bot D3PO. To communicate with a bot, you need to use slash command, simply by typing '/' at the channel.



The CTI League members can use the slash command '/jarvis_help' to receive information for Jarvis bot. Following, a list of available commands:

/jarvis_help vulnerabilities

/jarvis_help takedowns

/jarvis_help supporting medical

/jarvis_help supporting infrastructure

/jarvis_help triage

/jarvis_help law enforcement escalations

/jarvis_help requests for info

/jarvis_help malware analysis

/jarvis_help contact info

/jarvis_help hunting queries

/jarvis_help iocs

/jarvis_help incident response

/jarvis_help phishing

Jarvis - Main CTI-League Bot

- Help commands, Channel Info, and Slack Butlerin

Available System Commands	
Query	Command
/add_contact <organization>	Add yourself as a contact for the specified organization
/del_org <organization>	Removes organization you are a member of
/leave_org <organization>	Remove yourself as a contact for an organization
/list_contacts <organization>	List contacts of specified organization
/list_org <search parameter>	List organizations who have contacts registered
/mod_org <exiting org>	Rename existing organization
/my_orgs	List the organizations you are contact for

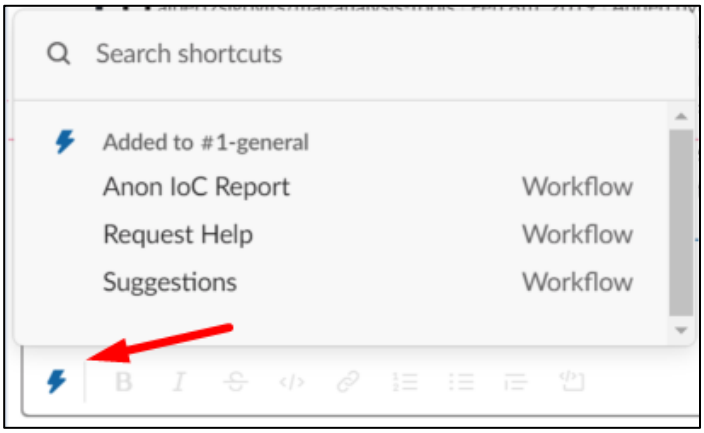
D3PO - RFI Ticket Bot

- Requests for information are managed through the D3.Intel Ticket proprietary backend
- Associated Slash Commands are used for the management lifecycle of RFI Ticket Requests

See more about D3PO in takedown and information request sub-chapter.

Workflows

The CTI League uses workflows in some of it process. Workflow is an automated version of a multi-step task or process, which can be found by pressing the blue lightning:



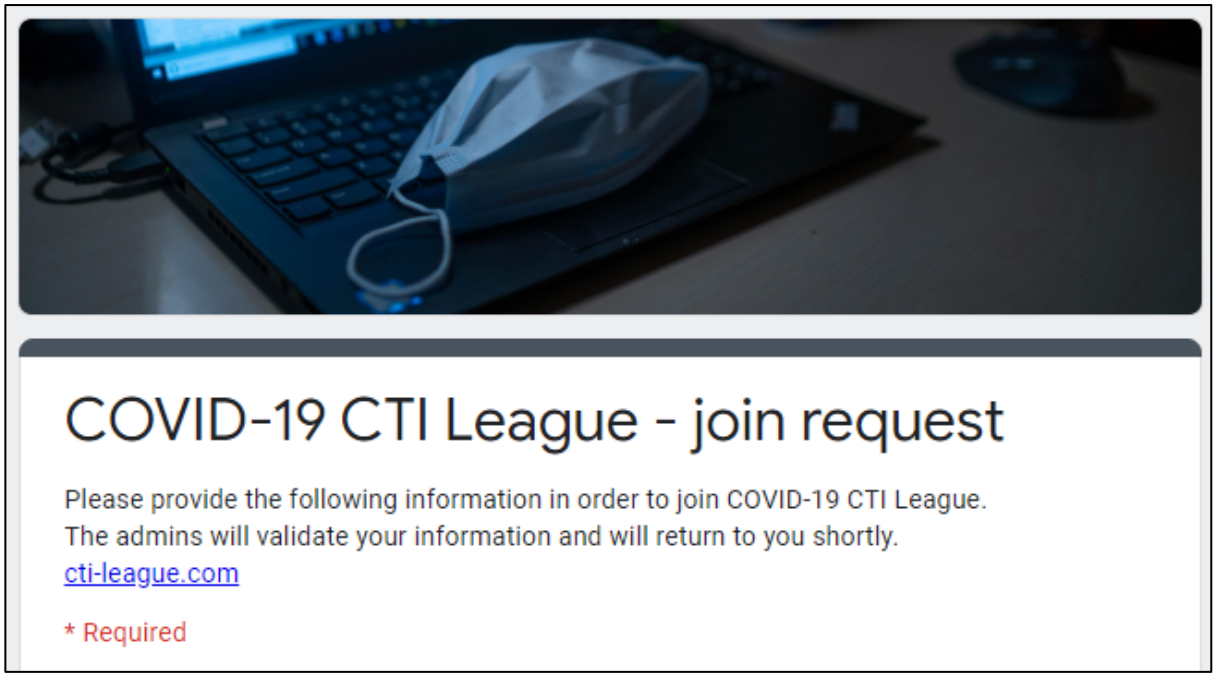
Note that you can find workflow only in its dedicated channel. Here is a list of the current workflows available in the League:

- Anonymous IoC report
- I want to volunteer
- Hunting Queries Sharing
- Darknet Escalation Request
- Indicator of Compromise Triage
- Attachments Triage
- Vuln Stream Keywords
- Help Request

Adding New Members

The CTI League welcomes cyber threat intelligence experts from all around the world. To add a new member for the league, please fill the form in our website:

cti-league.com



The CTI League management team review the requests, validate potential members, and accept qualified people.

Privacy Statement

Please review the CTI League privacy statement:

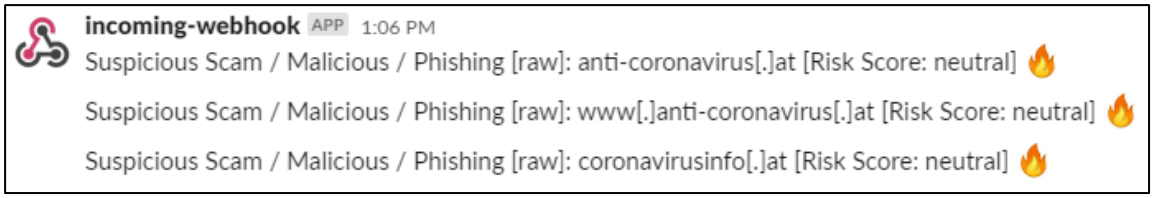
https://cti-league.com/cti-league/privacy-policy/

Cyber Threat Intelligence Community Sharing

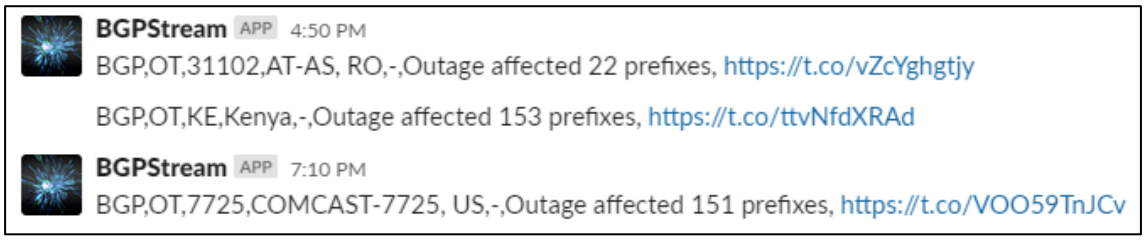
The CTI League is a clearinghouse for data, a connection network and a platform for facilitating those connections. These connections enable our members to find the best Point of Contact for their need. We receive and concentrate data from three types of places using automated and manual methods in our Slack workspace:

1. CTI League monitoring streaming. Available streaming):
    a. Medical infrastructure vulnerabilities in Shodan and Censys (Channel current name: medical-infra-vuln-streaming). Please see more in 'Support' chapter.
    b. Phishing attachments submitted to VT (Channel current name: phishing-attachments)

    c. Phishing domains and subdomains repositories (Channel current name: covid-phishing)



    d. BGP route changes (Channel current name: network-monitoring)



2. Feeds and external services
3. Information sharing by CTI League members

Sharing Information

The CTI League members can share relevant data for the medical sector within the league's relevant channel, whether they identified the information or tracked it in a feed (Channel current names: iocs, feeds). The CTI League members are encouraged to share information with the other members. Here is a table explaining the relevant channels for information sharing:

Information Sharing Channels		
Channel	Information	Type
#4-hunting-queries-database	Hunting queries identifying cyber-attacks regarding the current pandemic	Yara Rule, Sigma Rule
#4-iocs channel	Indicators of compromise of cyber-attacks exploiting the pandemic (using the virus as a decoy method or targeting the medical sector for example)	Domain, IP, URL, Hash
#4-darknet	Information and findings from the Dark web regarding medical organizations or about threats	Compromised data, Trends, Alerts, CVEs
#4-disinformation	Disinformation campaigns and fake news infrastructures	Domain, IP, URL, Campaign
#5-feeds	Feeds relevant for cyberattacks, IoC, Logbooks	Articles, Feeds, IoC

The CTI League is creating a repository of indicators relevant to the current pandemic. The CTI League management team is providing the medical sector:

1. GitHub dedicated to the medical sector, which in, we are creating a database of block lists, hunting queries and prevention methods.
2. MISP integration – streaming information from the league to a dedicated MISP.

Moreover, based on this data, the members enrich the league knowledge of trends and recent cyber-attacks regarding the current pandemic.

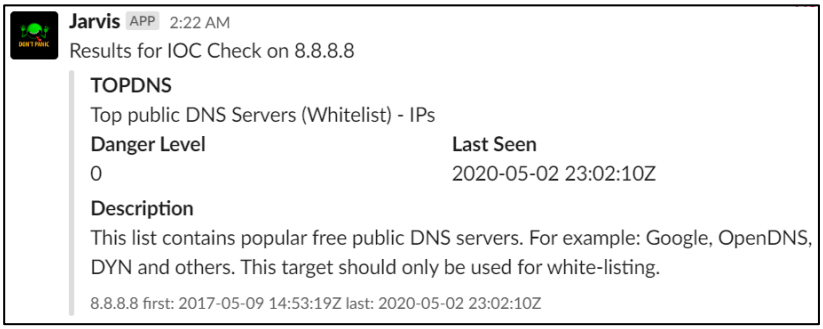
The CTI League members can request for information as well. Please check 'Information Request' sub-chapter.

Information Request

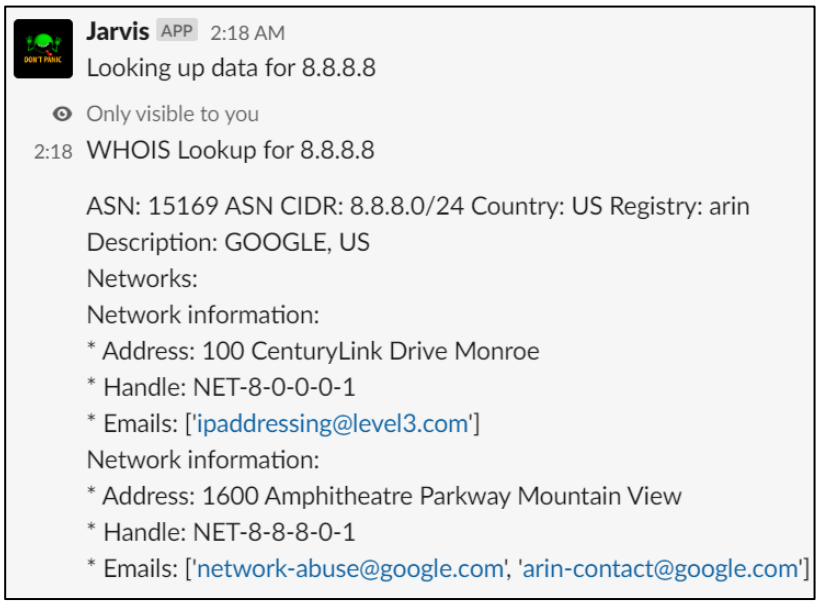
The CTI League members can use the league to collect information about entities regarding their investigations and get help from other expert members within the Request for Information (RFI) channels:

1. Information request:
    a. Using Jarvis, Main CTI-League Bot, with the slash command:

    /checkioc - Checks IoCs on ThreatSTOP database



/whois-ip – Checks Whois, Greynoise.io and VirusTotal data for IP address using Cortex system

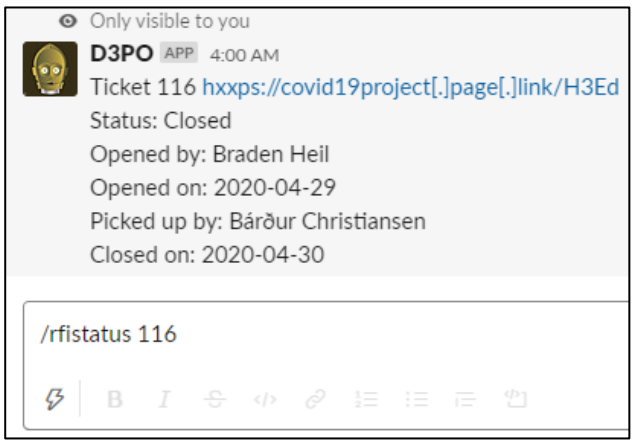


b. Using D3P0, the RFI Ticket Bot - Requests for Information are managed through the D3.Intel Ticket backend. Associated Slash Commands are used for the management lifecycle of RFI Ticket Requests.

Available Slash Commands	
Query	Command
/rficlose	Close a request
/rficlosedcount <last x days>	Displays count of tickets closed in a period
/rficlosedlist <last x days>	List closed tickets over time
/rfinew	Submit a request for information
/rfiopenlist	Lists open and in progress tickets
/rfireply <ticket number>	Reply to a request

/rfisearch <search thing>	Fuzzy search for ticket description
/rfistatus <ticket number>	Status of one ticket

Here is an example for checking status of a request:

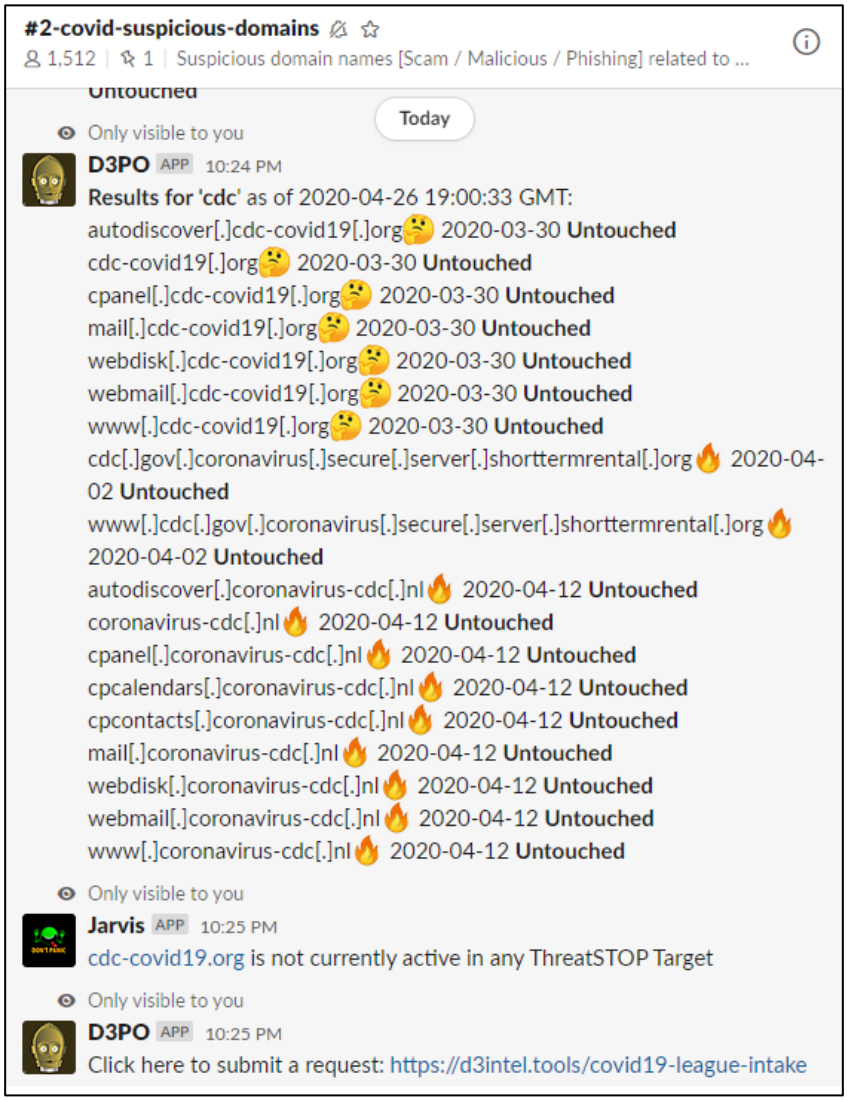


Suspicious Domains Search

The CTI League members can use the suspicious domains streaming channel to captures investigations of suspicious domains and their dispositions. Optionally, it generates a subsequent takedown request.

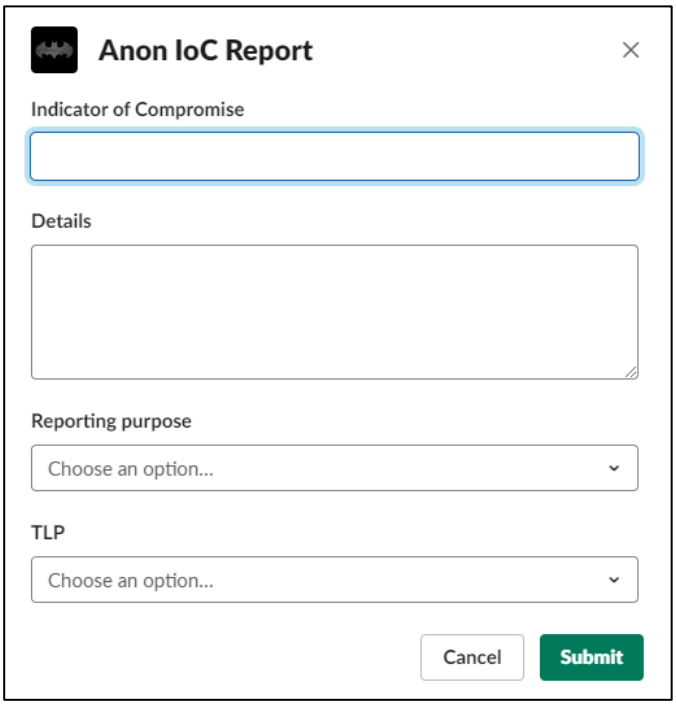
Available Slash Commands	
Query	Command
/suspicioussearch <searchString (optional last X days)>	Conducts a fuzzy search for domains *#2-covid-suspicious domains*
/suspiciousreply <searchString (optional last X days)>	Creates a submission link based on your search
/suspiciousclosenotakedown <ticketnumber>	Closes the suspicious domain ticket
/suspiciousclosewithtakedown <ticketnumber>	Closes the suspicious domain ticket and creates a takedown request ticket in *#4-takedown-requests*

Here is an example of preforming a full investigation via CTI League bot:



Anonymous IoC Reporting

The CTI League allows members to share information with each other in the way they want to. CTI League members can share data anonymously with the community, without attribution of the publisher. We understand some information cannot be attribute to the publisher while it is too sensitive. The CTI League can use the workflow in *#1-general channel*.



The CTI League is based on trust, and the publisher is required to vet the information before publishing. To make sure the reports are accurate, only the management team will have access to the identity of the publisher.

Malware Analysis

The CTI League is a community of cyber threat intelligence experts. The league offers to its members a platform for sharing information and consulting others regarding ongoing malware analysis researches. Our members can find the following platforms:

- Windows malware analysis
- Mac malware analysis
- Linux malware analysis
- Android malware analysis
- SMS Analysis

Cyber-Attack Neutralization

General

The CTI League's primary goal is to neutralize cyber threats exploiting the current COVID-19 pandemic. Our members can choose the best path to achieve this goal:

1. **Takedown** – CTI League members can raise a takedown request for removal of a website, web page, or file from the Internet.
2. **Triage** – CTI League members can help the medical sector with triage indicators. Triage definition: "high priority indicator of compromise to investigate in the medical sector networks and to block".
3. **Law enforcement escalations** – CTI League members can escalate relevant cyber-attack, malicious activity, or critical vulnerabilities to law enforcement agencies and national CERTs.
    a. To submit takedown request - Use 3DP0 bot (see Takedown chapter).
    b. To receive data about requests, the Law enforcement members can check the law enforcements escalation channel.

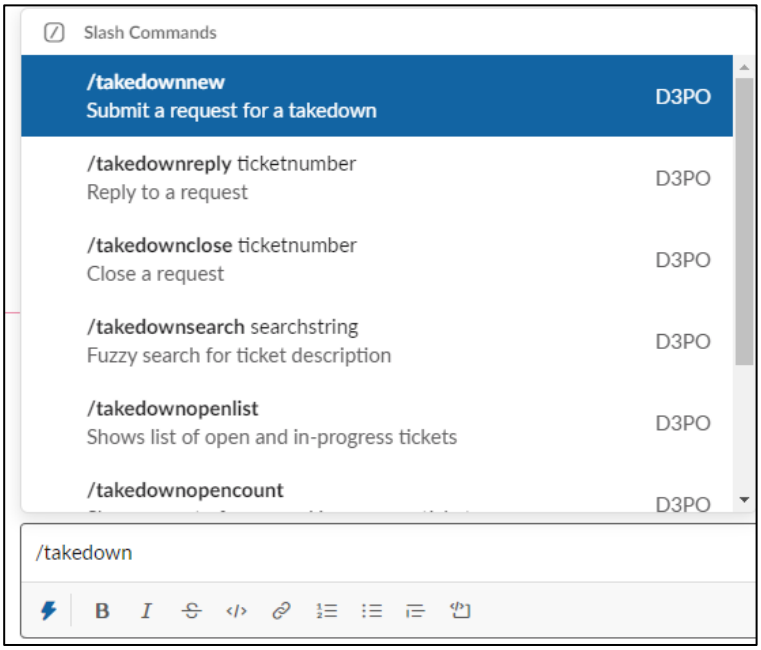
Takedown

The CTI league wishes to remove any relevant threat from the internet. The CTI League options for take down IoCs:

- Helping with the takedown process, check "Takedown" channel.
- Using D3P0, our Ticket Bot – Take down requests are managed through the D3.Intel Ticket backend. Associated Slash Commands are used for the management lifecycle of Takedown Ticket Requests.

Available Slash Commands	
Query	Command
/takedownclose <ticket number>	Close a request
/takedownclosedlist <last x days>	List closed tickets
/takedownnew	Submit a request for a takedown
/takedownopenlist	Shows list of open and in-progress tickets
/takedownopencount	Shows count of open and in progress tickets
/takedownreply <ticket number>	Reply to a request
/takedownsearch <search string>	Fuzzy search for ticket description

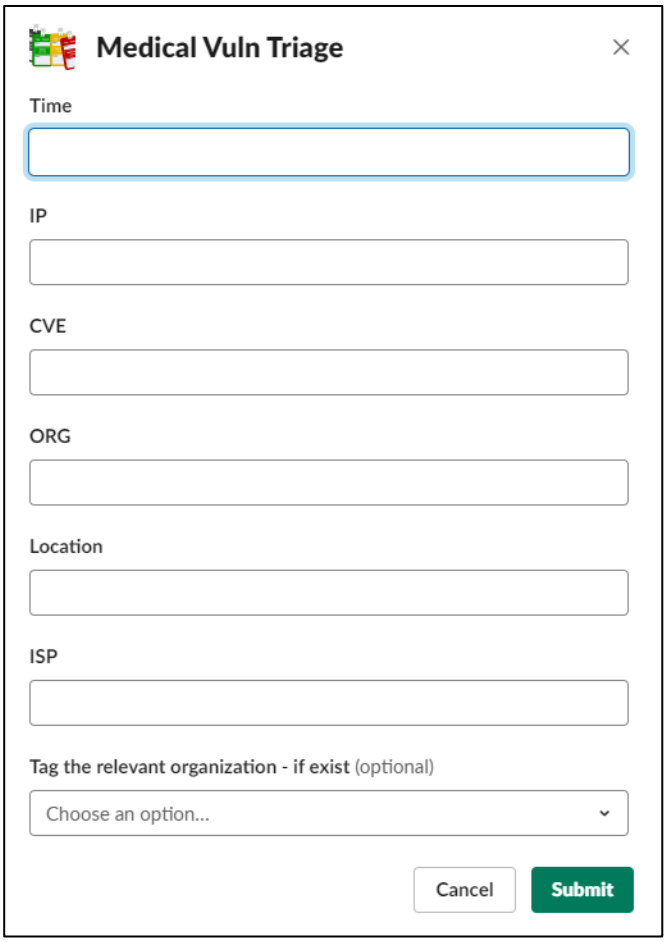
Here is an example for the different takedown slash commands:



Triage

The CTI League members can triage any indicator or vulnerability to the medical sector using the triage channels. Moreover, our members can use a simple workflow within the relevant feed's channel. Triage process is prioritizing indicator of compromise to investigate in the medical sector networks and to block and flag for antivirus analysis.

For example, the CTI League can identify vulnerabilities with our streaming system, and triage it with the workflow at the same channel. Other members that would like to help with the process at *#ioc-triage* channel.



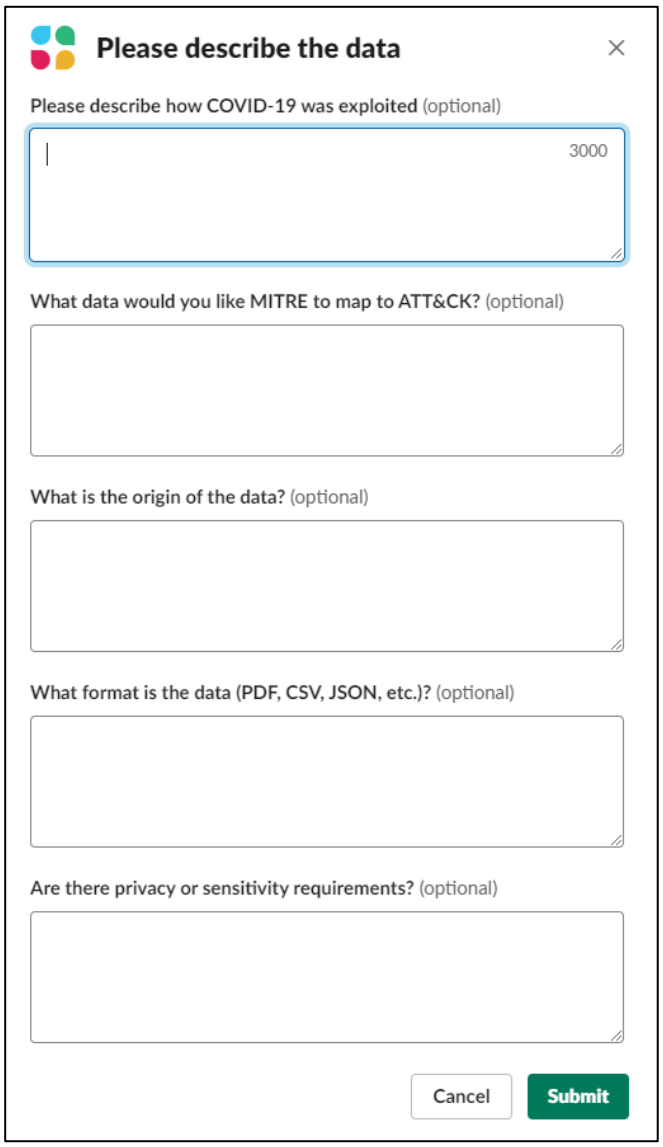
Law Enforcement Agencies Escalation

As the CTI League members receive reports of suspicious domains, compromised infrastructures, and other cyber-attacks by malicious actors, our 24/7 online members triages these reports. Once verified, we work to take down or eliminate threats, escalating to CERTs and law enforcement agencies as necessary. Examples of relevant issues for escalation:

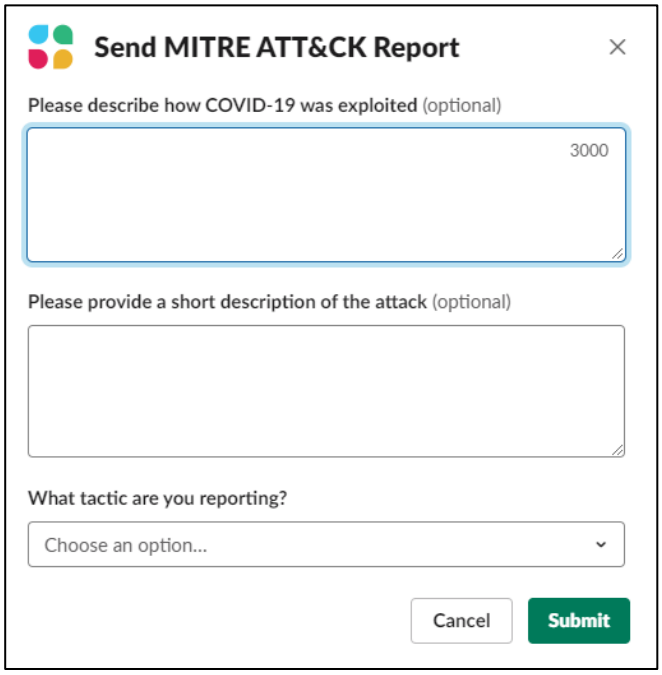
- Criminal activity in the cyber domain
- Threats against national security
- Takedown process would not be effective (in international campaigns for example)
- Urgent reporting to a medical facility
- Issues impacting government infrastructure
- Large scale information relevant to a specific country or individual that support the public (such as hospitals)

MITRE ATT&CK

MITRE is collecting data to analyze in the context of ATT&CK. They are also available to help you map your intel to ATT&CK. CTI League collaborates with MITRE and invites its members to contact MITRE using the two Slack workflows described below. Please mark your data with its sensitivity level (TLP: Green, etc.). "MITRE ATT&CK Help": Reporting about intel and mapping it to ATT&CK, you can submit a request. A MITRE analyst will follow-up with you and help you through the process.



"Submit MITRE ATT&CK Report": MITRE ATT&CK is receiving submissions on attacks where the cyber threat took advantage of COVID. Please submit any information you have on how they gained Initial Access while exploiting COVID, or what they did afterwards. If you wish them to contact you for further details or file submissions, please let them know in your description. Ideally, the submissions should already be mapped to ATT&CK. If it is not, feel free to use the previously described workflow to request their help with the mapping process.



Additionally, MITRE accepts submissions of raw data that is already mapped to ATT&CK through the ATT&CK Sightings project. Details here: https://attack.mitre.org/resources/sightings/

Support

The CTI League members handle domains and network profiling for medical organizations. We offer the medical sector and the relevant organizations two types of support:

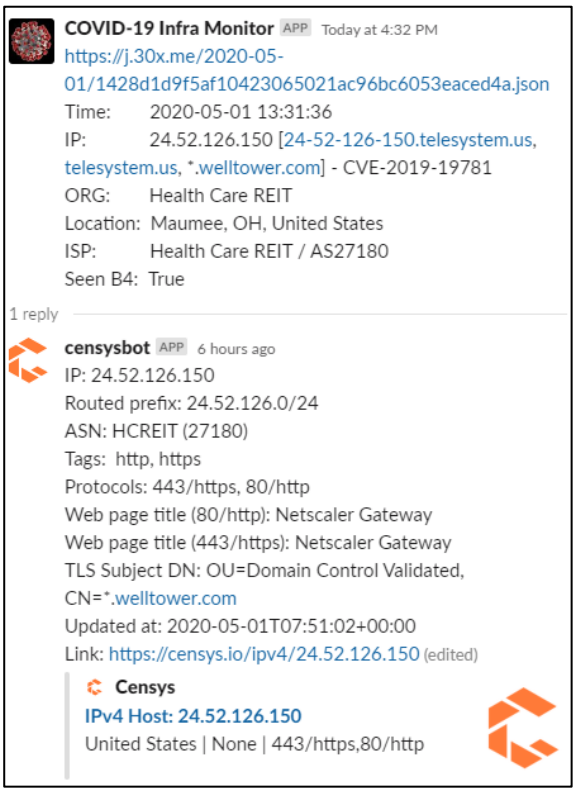
1. Medical sector support
2. Infrastructure support

Medical Sector Support

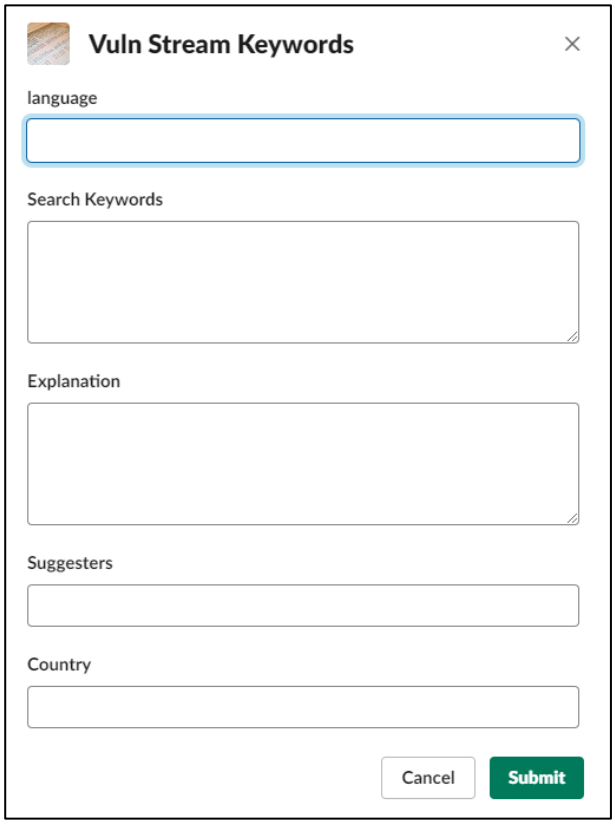
The CTI League offers support to protect critical infrastructure, especially those running in medical institutions, healthcare providers and their supporting organizations (testing laboratories, equipment suppliers, infrastructure providers etc.).

Vulnerabilities Streaming

The CTI League provides the medical sector and relevant organizations (such as national CERTs) 24/7 streaming of infrastructure vulnerabilities in organizations important to our mission. CTI League members can find this streaming in *#2-medical-infra-vuln-stream*. The system identifies medical infrastructure vulnerabilities using data from Shodan and Censys.



Each day, we identify thousands of vulnerable servers within relevant organizations, vet them within our systems, and engage the appropriate partners to notify the affected parties. Currently, we are searching information with 8 languages (English, Polish, German, French, Spanish, Dutch, Slovak, Czech). CTI League would like to expand its keywords for additional languages, for that, please check the workflow in *#2-medical-infra-vuln-stream*.



Law enforcement agencies and CERTs can receive this data automatically by email or webhook. Please contact the management team if you are from one of these organizations and would like to receive this data.

Darknet

The CTI-League searches both Clean Web and Dark Web to find valuable information. The CTI League Darknet Members monitor thousands of underground networks, covering every geographic location for COVID-19 and healthcare industry targeting. Some of these networks include:

1. Cybercriminal forums
    - Invite-only dark web forums
    - Paid entry darknet forums
    - Clearnet hacking forums
    - Carding forums
    - Forums focused on trading and selling breached databases
2. Cybercriminal marketplaces
    - RDP and compromised servers' marketplaces
    - General fraud marketplaces
    - Credit card marketplaces
3. Leak sites
    - Tor leak repositories
    - Tor wikis
    - Data breach sites
    - Ransomware leak sites
4. Paste Sites
    - Pastebin
    - Ghostbin
    - Deep Paste
    - Pastr.io

- Pastemo

5. Underground Social Media Channels (Currently in English and Russian)
    - QQ
    - Telegram
    - WhatsApp
    - Twitter

Through manual and automated research, the CTI League members can alert our partners such as law enforcement and the healthcare industry to any specific COVID-19 related cyber threats discovered in underground networks. Through collaboration with MITRE ATT&CK framework, we can predict trends by threat mapping recent cyber-attacks regarding the current pandemic.

The CTI League members can request for information if they are interested in any underground related findings, threat actor personas, marketplaces, forums, etc. Please check Request for Information (RFI) standard format for submitting requests to the Darknet members' group. This standard form includes a questionnaire for the requesting party to include a detailed description of the ask, along with any relevant keywords that can aid the Darknet members' group in our search.

Support Application

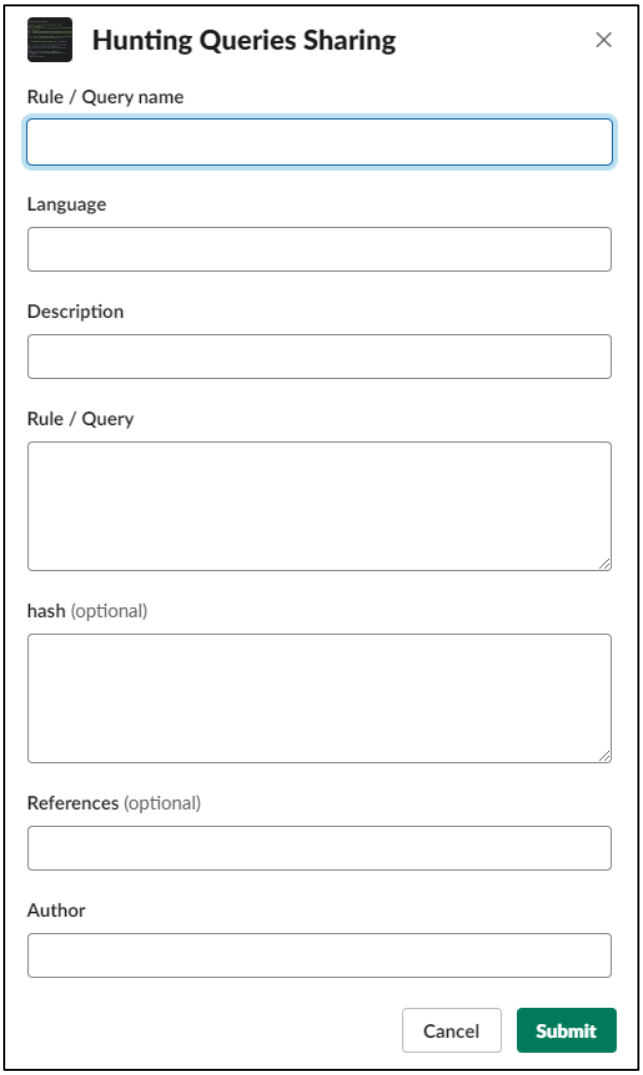
The CTI League members receive support applications from the medical sector. The information is transferred to the relevant channel via the following methods:

1. Formal application from a medical organization for support. The management team will publish cases we receive from the medical sector, and the league can help on these requests. In order to submit an official request, the medical sector can send an email to the following address: info@cti-league.com
2. Raising issues within the relevant channel by one of the CTI League members. Our members receive reports on relevant support requests from the medical sector and share the request in the relevant channel. We encourage our members to use the league for helping with medical sector support requests.
3. A call for support from national / medical sector CERTs. We encourage CERTs to raise a support requests for the medical organizations within their countries.

In the medical support relevant channel, our league members can share methods and tools to help the medical sector. Handling domains and network profiling for the medical sector are the ongoing activities in the channel.

Hunting Queries

The CTI League creates a hunting queries database for the medical sector. The medical sector can receive the database for free and prevent attacks with it. CTI members are encouraged to share relevant hunting queries and rules via a workflow in hunting queries channel (current channel: hunting-queries-database).



Further, the hunting queries, such as Yara and sigma rules or queries for APT scanner will be shared with the medical sector via our GitHub.

GitHub Project

The CTI League gives medical sector systems multiple options for receiving data from the league. One of these options is via our GitHub. The information in the GitHub repository can be divided into 2 sections:

1. Public release - Files vetted and approved for the public, contains blocklists by hash, IP, and domain, and list of known bad actors. This option is open for publication for anyone in need. In this Git our members can find:
    a. Vetted blocklists based on IP address, domains, and hash values for blocking.
    b. A PiHole feed for inclusion into the PiHole software as a blocklist that reflects the data in the domain blacklist.
    c. A compilation of links to information from the CDC and other sources containing information about health and safety.

    https://github.com/COVID-19-CTI-LEAGUE/PUBLIC_RELEASE
2. Limited (private) release- A reliable database of blocklists, vulnerabilities and sensitive information that is presented within GitHub for CTI League members only. Following is a list of the channels and a short explanation about each one:

    Private Block list: INTERNAL ONLY blocklist that have not been verified yet.

https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_BLACKLISTS

Private Allow list: INTERNAL ONLY allow list that have not been verified yet.

https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_WHITELISTS

Private Medical Infrastructure vulnerabilities: Enriched data offered by country separated list of IPs, taken from the vulnerabilities stream. In this repository you can find lists from vulnerable hosts attributed to medical/hospital-orgs, based on keywords in their hostnames or network-info. The lists are separated by country and generated each day (these are not IOCs).

https://github.com/COVID-19-CTI-LEAGUE/PRIVATE_Medical_infra_vuln

Infrastructure Support

The CTI League offers infrastructure support to protect critical infrastructures, especially those found in medical or health-related organizations.

In the relevant channel, the CTI League creates discussions around availability and capacity, enriching the knowledge of the league about trends, vulnerabilities, and capabilities. In several weeks the CTI League will present guide and tips valuable for protection medical organization network.

Vulnerabilities Streaming

CTI League is looking to expand into more sectors under threat due to the Corona Virus. Currently, it allows medical organizations, national CERT teams and law enforcement to subscribe to the custom subset of streams that is published to Slack channel. The filtering allows to further filter the stream based on country/region/city, vulnerability, ASN, IP range, CVSS score, etc. The system is currently in final testing stage with several early adopters. We intend to open it up for wider consumption shortly and will announce it through Slack once available.

Compromised Data

CTI League members identify compromised credentials relevant to the medical and other related sectors within the internet and the dark web. These credentials can be used for hacking the compromised organization, blackmailing, or as a platform for future attacks by the threat actor. When we find a match on either Microsoft Account (consumer) or Azure Active Directory (Commercial), we place those users into a compromised account workflow. Here are examples for compromised data:

- Data stolen from breached sites and network
- RDP, SSH, and any type of services is offer for sale in the Dark web

To search for data in the CTI League TLP:RED dataset from cybercrime RDP shop, use the slash command /uas.

Reminder that TLP:RED is not for disclosure and is restricted to participants only.

The CTI League can report about compromised data at one of the support channels (#4*) or escalate it to the law enforcement agencies within *#2-law-enforcement-escalation*. For example, reporting about compromised offer for sale in the dark web should be reported at *#4-darknet* channel. If the compromised data identified is sensitive, the members can reach out to one of the management team for further steps.

Incident Response

The CTI League members can help the medical sector with handling of ongoing events by incident response request. When medical sectors are under attack, our members can help with the incident response process which include identification, analysis and response to the specific threat.

Disinformation

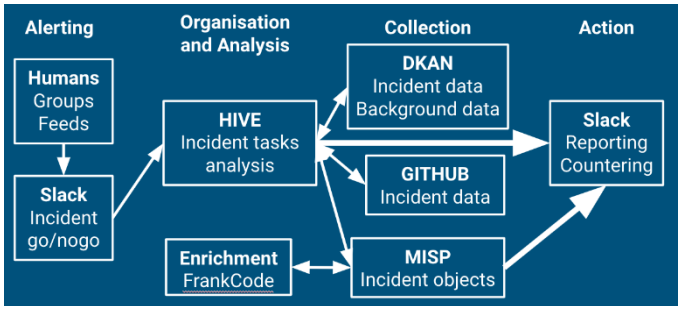
The CTI League is able to neutralize threats in the cyber domain regarding the current pandemic, including disinformation. The mission of this effort is to find and track new disinformation incidents, analyze the information, and coordinate the mitigation /termination of these incidents. The disinformation team:

- Finds, tracks, and responds to disinformation incidents
- Adapts the technology we need to do that better/faster
- Develops the processes we need to enable more people to participate in our response

Team coordination:

- Slack channel #4-disinformation
- Team discussion/training on zoom Wednesday and Saturday at 4-5 PST / 7-8 EST
- Team README and startup guide
- Team playbook: [The Big Book of Disinformation Response](#)[1]

Workflow



Disinformation analysis has overlaps with other incident response methods, and we try to keep tools, processes, and outputs as similar as possible. We will continue to reach out to other CTI League teams to explore connections. Our current process (above) uses HIVE to organize tasks around each disinformation incident and its connections to previous incidents, actors, artefacts etc.

Alerts come in from connected disinformation groups (Covid19Disinformation, Covid19Activation), CTI League members, and existing feeds. They are triaged for volume and relevance before being activated as incidents. The full incident process is described in the Big Book of Disinformation Response, but is a combination of collection, enrichment and analysis of social media artefacts and narratives, with emphasis on TTPs, incident objects and how to report or counter any of incidents that we find.

The CTI League is working on connected workflows, including narrative tracing across incidents and using the tools inside HIVE and MISP.

[1] https://docs.google.com/document/d/1XimTUfZlxfZBBgka-_DQYsXTEgz-GuFfym5MHdva-5g/edit?usp=sharing

Tech Stack

The CTI League disinformation team uses the following tech stack.

Tech Stack		
Name	URL	Type
HIVE	https://hive.thlab.ninja/	Task / Project Management
'Clean' MISP	https://covid-19.iglocska.eu	Reported Objects
'Dirty' MISP	https://misp.cogsec-collab.org	Objects Under Analysis
DKAN	https://data.cogsec-collab.org	Data Repository
GitHub	https://github.com/orgs/COVID-19-CTI-LEAGUE/teams/cti-disinformation	Kanbans and Datastore
Google Drive	https://drive.google.com/drive/u/2/folders/1MtsIfmYEAh9bH8A5OX9nb8xoZ6qCe2g_	Team Notes

Version History

Version	Date	Change Summary
1.0	4/13/2020	Initial release
2.0	5/12/2020	Version 2 – May 2020