



**LEAGUE**

*The success of the CTI-League is driven entirely by its diverse membership and the cross-industry and law enforcement collaboration within.*

# LE Collaboration

**The success of the CTI-League is driven entirely by its diverse membership and the cross-industry, government and law enforcement collaboration within.**

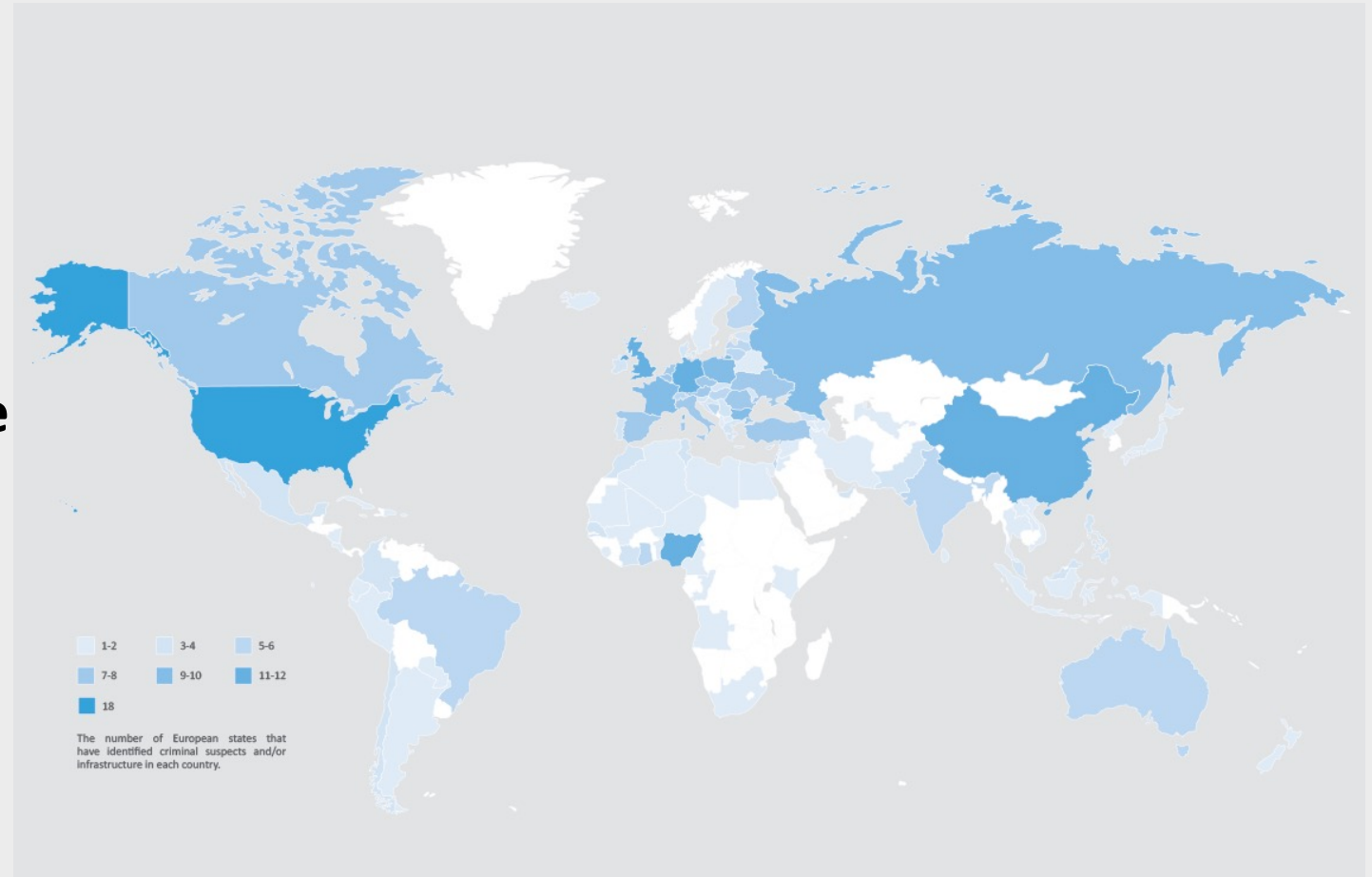
- First, ./whoami
- Marc Rogers
- CTI League Co Founder
- Head of Security for DEF CON
- VP Cybersecurity Strategy Okta



# Collaboration – Why?

We all have the same goal. Lets get on the same team.

- **Cybercrime is a global problem.**
- **Cybercrime respects no borders, laws or pandemics.**
- **Cybercriminals constantly evolve their tactics, techniques and procedures.**
- **Cybercriminals already collaborate. They share intelligence, tools, code, assets.**



Source: UN Statistics via Europol

# Collaboration – Why?

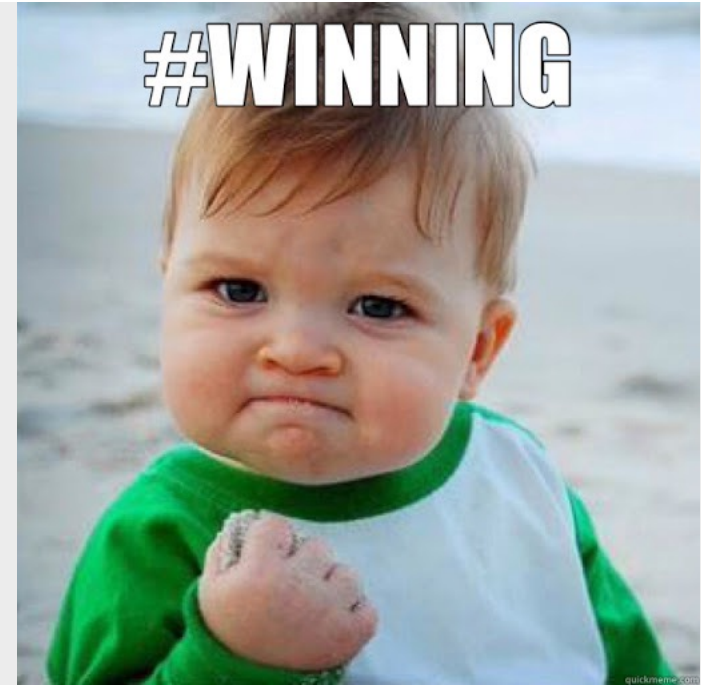
We all have the same goal. Lets get on the same team.

- We all have something to bring to the table.
- Whether our goal is to protect by preventing something from happening or to disrupt and break down an existing campaign – We need the whole picture.
- Silos are a problem. Some may be unavoidable but
  - Organizational silos
  - National silos
  - Policy/Classification based silos
  - Privacy based silos
- Trust and collaboration can be powerful weapons.
  - We all have finite resources
  - Collaboration is a force multiplier

# LE Collaboration

## What does success look like?

- Deconfliction of activities.
- Maintenance of a high level of trust.
- Active participation with a wide range of objectives.
  - LE objectives
  - CTI objectives
  - Gov objectives
  - Industry objectives
- Clearing the playing field
- Similar end goals, different journeys – preservation of evidence.
- Collection of \*useful\* intelligence/evidence
- Export of intelligence in a refined, manageable state and volume.



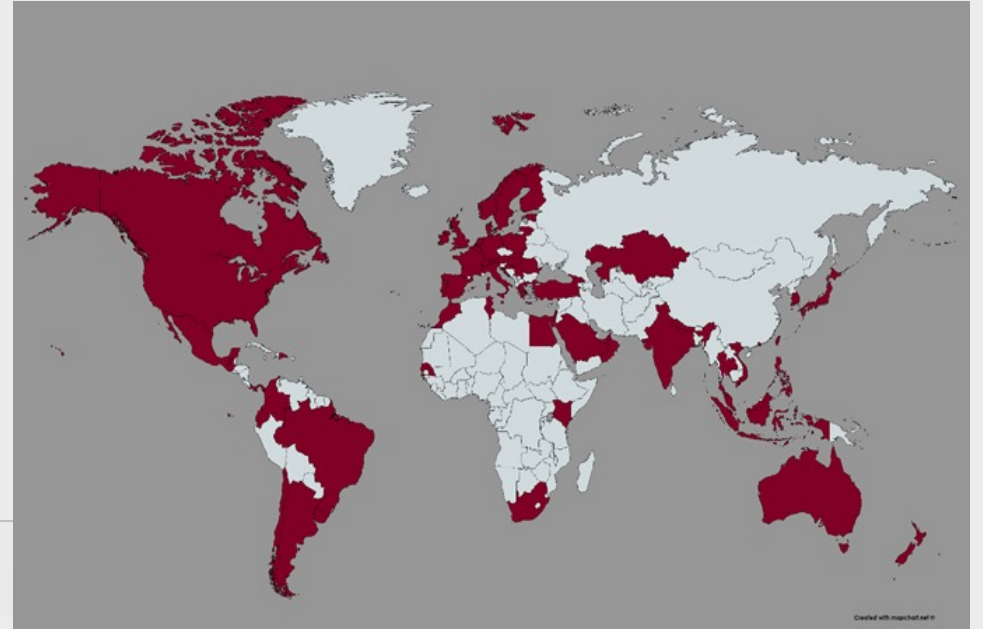
# Where are we today?

1500+ members volunteering.

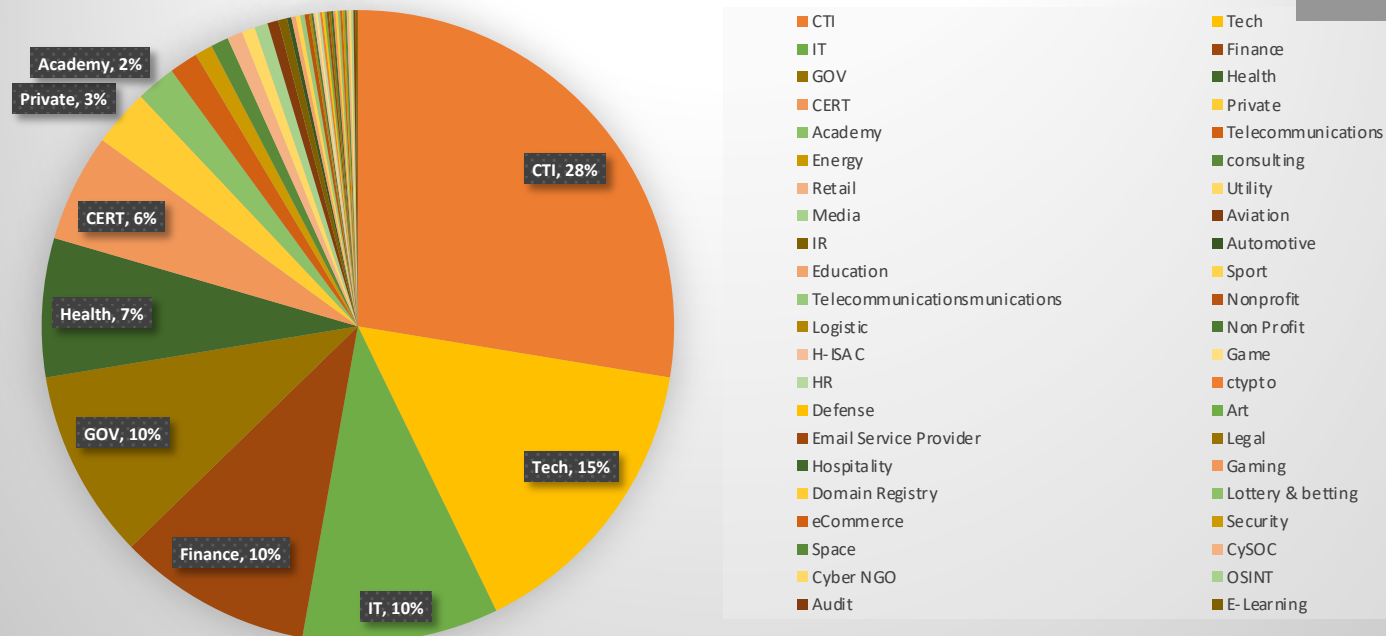
>80 countries

22 Timezones

>44 sectors, >10% LE/Gov




CTI League Volunteers Sectors





# Information sharing

- We have a great platform for information sharing.
- Channels are good places for information exchange but too noisy for LE.
- We need to increase our output of specific information.
- CTI League playbook documents all the tools, bots, feeds and processes available.

 **Anon IoC Report** ×

Indicator of Compromise

Details

Reporting purpose  


Choose an option...

TLP  

Choose an option...

Cancel

Submit

 **Send MITRE ATT&CK Report** ×

Please describe how COVID-19 was exploited (optional)  

3000

Please provide a short description of the attack (optional)


What tactic are you reporting?  

Choose an option...

Cancel

Submit

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

 **Medical Vuln Triage** ×

Time

IP

CVE

ORG

Location

ISP

Tag the relevant organization - if exist (optional)  

Choose an option...

Cancel

Submit

# Engaging with LE

- We have PoC's from multiple agencies, you can identify them from their slack handle or by going directly into # 2-Law-Enforcement-Escalations-Channel
- We have the # 2-Law-Enforcement-Escalations-Channel
- We have escalation tools integrated into D3PO
  - /lenew – generates an LE escalation form (All)
  - /lereply – respond to ticket (LE only)
  - /leclose – close ticket (LE only)
  - /leopenlist – show all open tickets (LE only)
  - and more.... (see channel or ask for more info)

**Law Enforcement Escalation**

Your slack user name:

Summary/Title:

Incident Type

Objective

Why do you believe it is illegal

Location of victim

Location of Suspect

Information about suspect to aid in identification

Do you have documentation available?

Description of documentation

Can LE contact you?



LE Feedback

# How are we doing so far?

## Good

- Useful Threat Intel/IOCs, Alerting and integrations.
- Escalation pathways & tools have worked.
- Darknet Intel has been especially good.
- Good victim notification coordination across multiple agencies.
- Solid action taken to neutralize threats
- Information from CTI League has augmented information produced elsewhere.
- Helped highlight the pivot from virus/pandemic related targeting to economic stimulus/unemployment targeting.
- Perspective and intelligence from groups like CTI has been useful for long running COVID LE investigations (which most tend to be).



**NEEDS**



**IMPROVEMENT**

## Room for improvement.

- Referral system is good but its difficult to know when (and where) new referrals are located.
- Centralization of referrals would be good.
- Most integration and alerting is only good if you already know target IPs, would be good if it could be done on TTPs or other signatures.
- There is A LOT and its hard to know where to start.
- It is difficult to keep track of 20+ channels, so easy to miss key intel.
- Everyone has a slack so 20 channels across multiple slacks doesn't scale.
- Methods to help gather or create some sort of digest of information would be appreciated.
- Daily or weekly summaries would be useful

# Challenges

- Infosec has scored a few own goals with disclosure recently.
  - Red and Blue need to find a way to coordinate disclosure better.
  - Time from notice to PoC is frequently a matter of hours
  - We need to stop helping the bad guys!
- Patch uptake is poor and it isn't improving.
  - Many major institutions have huge vulnerabilities
  - Small institutions are understaffed and under resourced
  - Support coverage is great in western countries less so elsewhere
- Too often we think about vulnerabilities when we should be thinking about entire systems.
  - What's the point in reinforcing the door if the walls have cracks?
  - Vulnerability management needs to evolve
  - Risk score need to use context

What Next?

# Future Thinking

- Future engagement and activity - Thinktanks
- Long term information sharing strategies.
- Future targeting
  - Global events?
  - Disasters?
  - National events?
  - Specific Campaigns?
- Keep a narrow focus or broaden scope?  
Whatever happens we need to ensure the output remains focused.
- Collection of useful intelligence
- Export of intelligence in a refined, manageable state and volume.



# Thank You!

Further information:

[HTTPS://CTI-League.com](https://CTI-League.com)

[marc@CTI-League.com](mailto:marc@CTI-League.com)

[info@CTI-League.com](mailto:info@CTI-League.com)

@CTIleague

