Team Cymru

Community Services

The “What/Why/How”

AGENDA

Introductions

Who is Team Cymru?

Overview of Community Services

Bogons

UTRS™ (DDOS mitigation service)

NIMBUS™ Threat Intelligence

DNB, Dragon News Bytes

IP to ASN Mapping Tools

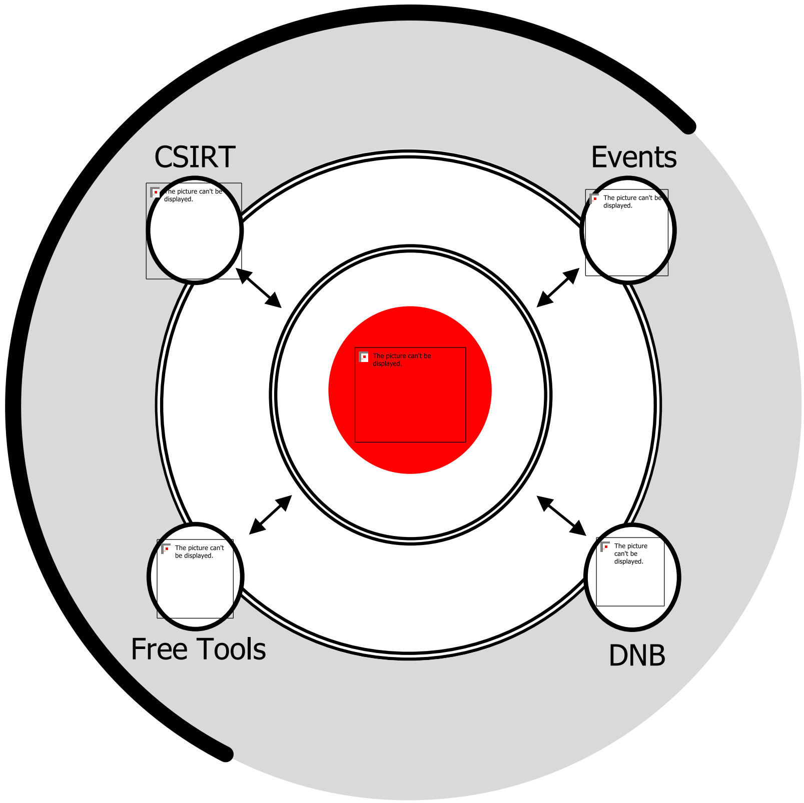
MHR, Malware Hash Registry

CAP, CSIRT Assistance Program

The picture can't be displayed.

INTRODUCTIONS

Team Cymru



Who we Are

We uncover the who, what, when, where and why of malicious behavior.

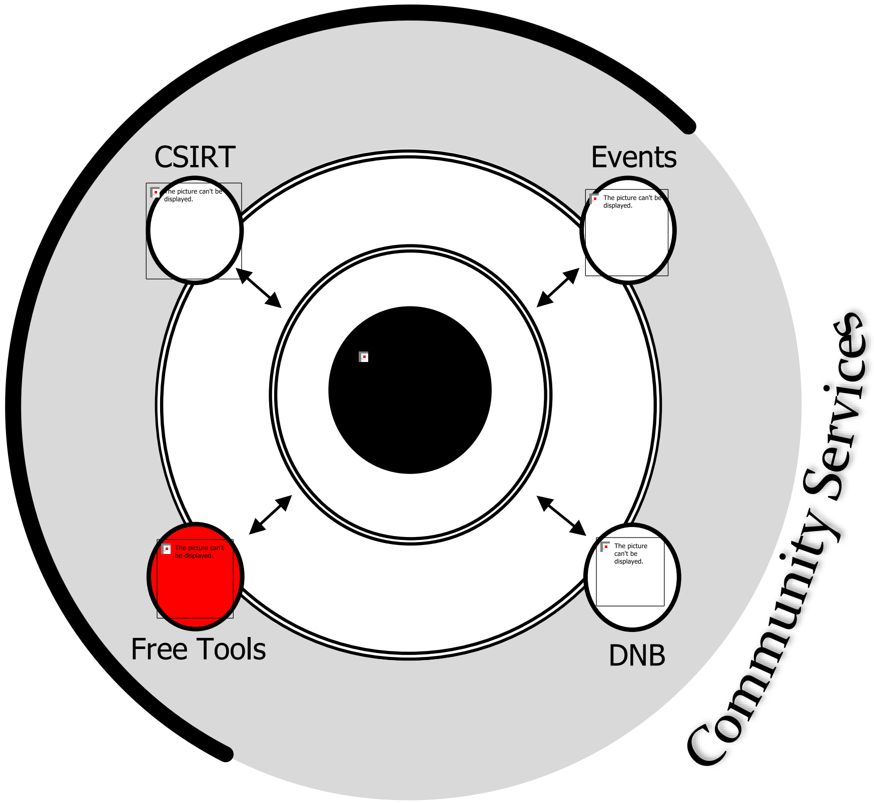
15+ years of service to network defenders, internet operators and cybercrime investigators worldwide.

- Free services for ISPs, hosting providers and CSIRTs
- Unmatched eco-system of data sharing and collaboration partnerships worldwide
- Work with 140+ CSIRT teams in 86+ countries
- Relied on by many security vendors, Fortune 100 companies, and public sector teams.

Team Cymru is comprised of former…

- Members of national and industry CSIRT teams
- Law enforcement
- Analysts from research, education, private and public sectors
- ISP backbone engineers
- Fortune 500 enterprise network engineers
- Penetration testers
- Military – US and allied nations
- Frontend, backend, gaming, web app, kernel, high-performance computing and big data developers and system engineers

Outreach



CSIRT
Events
The picture can't be displayed.
The picture can't be displayed.
The picture can't be displayed.
The picture can't be displayed.
Free Tools
DNB
Community Services

Free Tools

Solutions provided by Team Cymru

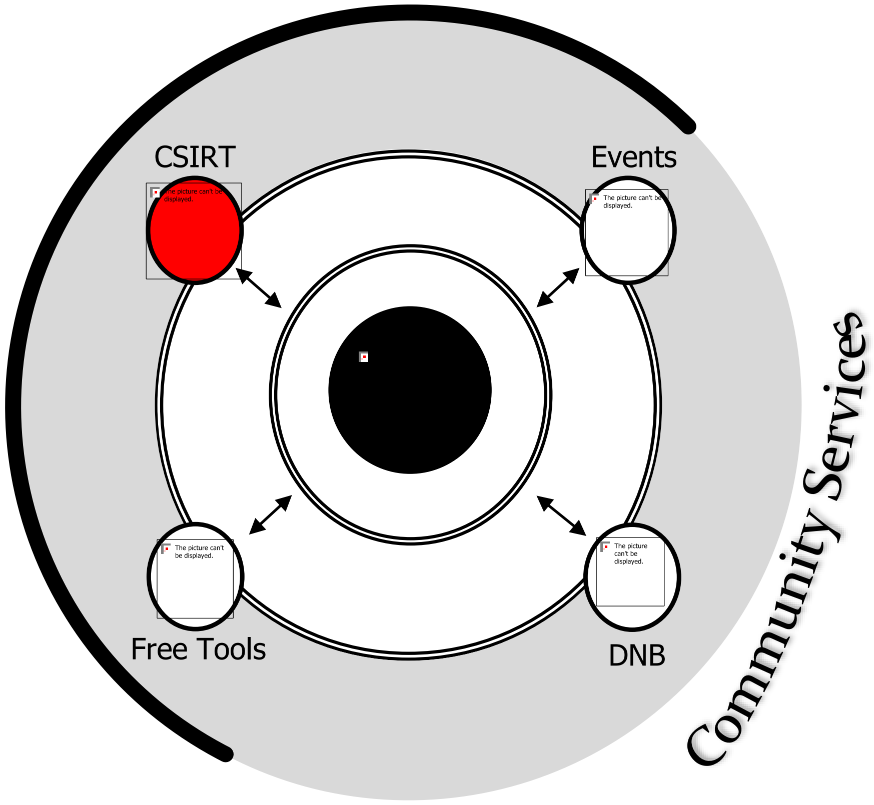
Nimbus Threat Monitor: Kibana-based appliance that integrates our insight about malicious activity on your network, with near real time alerting

Unwanted Traffic Removal Service (UTRS): A system that helps mitigate large infrastructure attacks by leveraging an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions that automatically distributes verified BGP-based filter rules from victim to cooperating networks.

IP To ASN Mapping Project: A query interfaces that allow for the mapping of IP addresses to BGP prefixes and Autonomous System Numbers (ASNs), based on BGP feeds from our 50+ BGP peers. Updated every 4 hours, this data is available through traditional WHOIS (TCP 43), DNS (UDP 53), HTTP (TCP 80), and HTTPS (TCP 443).

Malware Hash Registry (MHR): Similar to the Team Cymru IP address to ASN mapping project, the Malware Hash Registry (MHR) project is a look-up service with an added benefit: you can query our service for a computed MD5 or SHA-1 hash of a file and, if it is tracked malware, we return the last time we have seen it along with an approximate anti-virus detection percentage.

Outreach


CSIRT
The picture can't be displayed.
Events
The picture can't be displayed.
The picture can't be displayed.
Free Tools
The picture can't be displayed.
DNB
Community Services

CSIRT Assistance Program

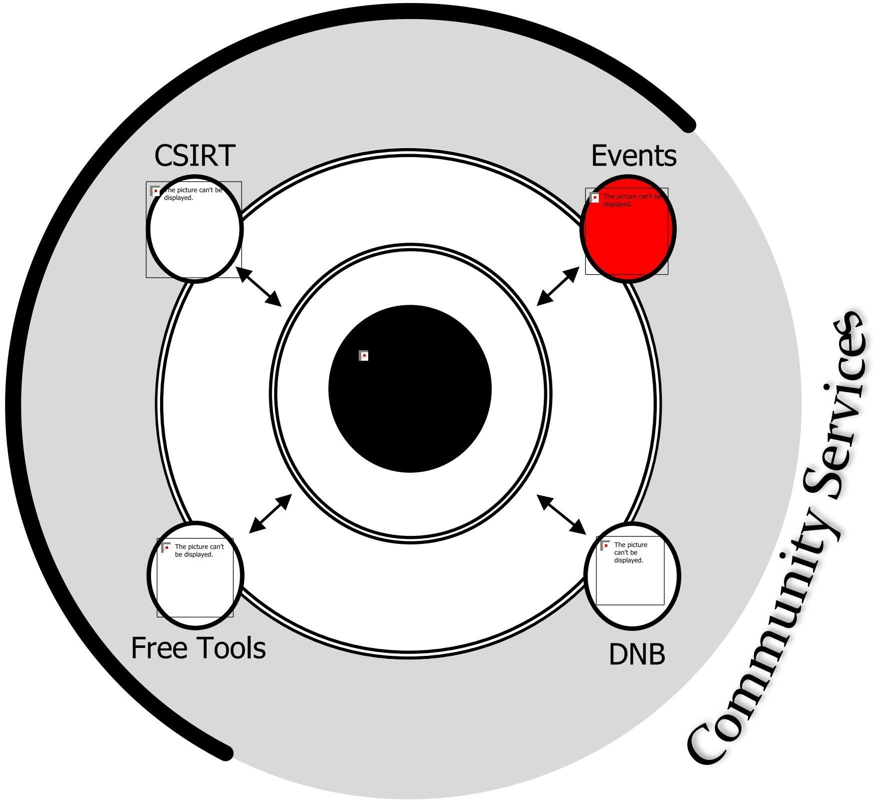
Free Threat Intel for Non-Commercial National and Regional CSIRT Teams.

Team Cymru works with national and regional CSIRT teams globally by sharing our world-class threat intelligence. We provide this unique Pure Signal™ intelligence at no cost to you. We want to help secure the Internet, and we want to keep you informed of what we see in your region

We provide intelligence on a variety of categories:

Bots / Controllers
Brute-Force
Darknet
Honeypot
Open Resolvers
Phishing
Scanners
Spam
Proxies

Outreach


CSIRT
The picture can't be displayed.
Events
The picture can't be displayed.
Free Tools
The picture can't be displayed.
DNB
The picture can't be displayed.
Community Services

Events

Team Cymru Conferences

We hold a series of Regional Information Security Events (RISE), as well as an annual conference called Underground Economy. These are exclusive events, centered on threat intelligence, cyber crime and cyber security issues, that include TLP-Amber and -Red case studies. In order to register for one of these events, please apply via the links below, and we will contact you with further instructions.

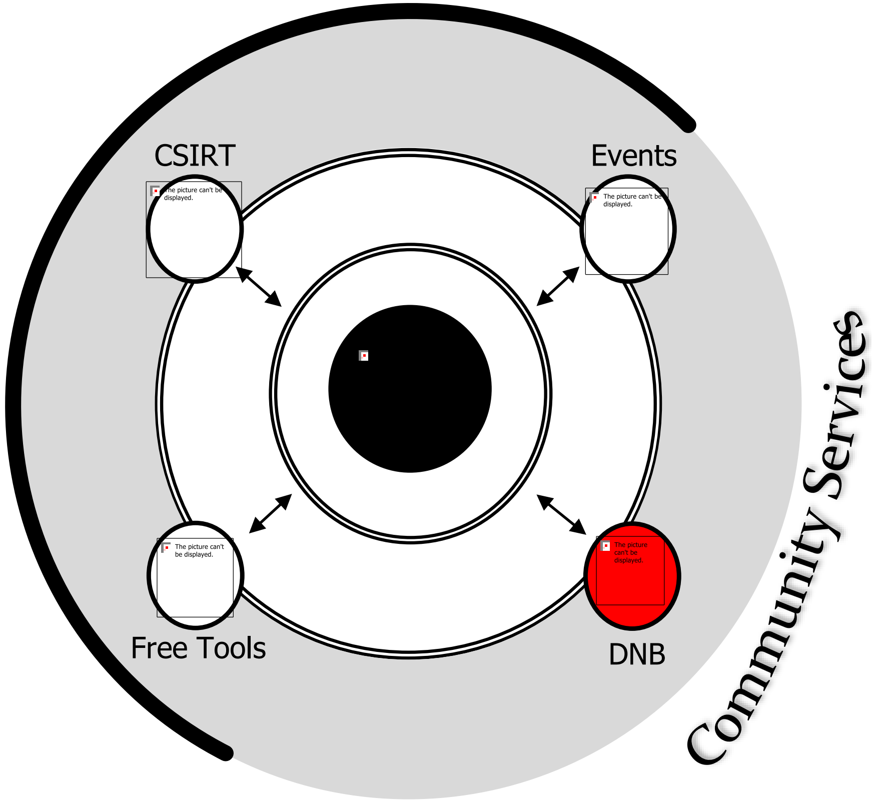
Team Cymru Webinars

We have a ongoing series called ‘Dragons Den’ where we talk with industry experts about current trends, participate in and sponsor regional events (e.g PacNOG), and host webinars around the globe to help keep communities up to date on what we are working on and seeing in the world of information security / intelligence.

Event Schedules

Visit our events page https://team-cymru.com/company/events/ follow us on Twitter @teamcymru and LinkedIn https://www.linkedin.com/company/team-cymru/

Outreach



Dragon News Bytes

Curated Information Security News provided by Team Cymru

Dragon News Bytes is a private and restricted mailing list that distributes Information Security news articles. These articles may come from newspapers, magazines, and other online resources, as well as from Team Cymru's own research.

We will endeavor to tag the subject line with [DNB] and at least one other tag to suggest the topic:

[APT] – Advanced Persistent Threat, Nation State hacks and malware

[ARREST] – News of arrests, court matters and sentencing for InfoSec criminals

[ATTACK] – DDoS, defacements and criminal 'hacks'

[HACKTIVISM] – Anonymous, #OpAnything plus anything related to online protests

[MALWARE] – Viruses, botnets and other stuff we know you love

[MOBILE] – Anything related to Android, iOS Security

[POLICY] – Anything related to InfoSec policies, guidance and procedures

[PRIVACY] – Related to anything that impacts your personal privacy, OPSEC, data breaches, and information disclosures

[RESEARCH] – Papers and other new analysis and insight

[TIPS] – Anything else we can't categorize otherwise

[VULNS] – Anything related to vulnerabilities, patching, etc

BOGON’s

BOGON’s Module Overview

- What are BOGON’s ?
- What problem(s) are we helping to solve ?
- Requirements to signup for the BOGON Service.
- How to signup for the BOGON Service.
- How to implement BOGON Service on your network.
- Questions ?

What are BOGON's

- BOGON's are netblocks that should not be reachable or routable on the public internet.
- The following are part of the Basic BOGON's dataset:
  - RFC 1918, RFC 5735 and RFC 6598
  - IP address blocks that have not been assigned to a RIR
- The following make up our Full BOGON's dataset:
  - All the addresses in the Basic BOGON dataset
  - RIR address blocks that are currently not allocated or assigned

What problem are we helping to solve

- Internet routers that face the public internet should only forward traffic with valid IP's
- Manually maintaining filters (ACL's) and keeping them updated is a time consuming and error prone task. Cymru Bogon's solves this.
- We provide a unified and validated near realtime list of IP addresses that should NOT be reachable on the public internet.
- We provide this via BGP, DNS, and HTTPS (wget txt data)

Requirements to signup for BOGON's

- **Data via HTTPS or DNS does not require any signup.**
- **Data via BGP feed requires the following signup information:**
  - **Full Name**
  - **ASN and Peering IP**
  - **Email and Company Name**
  - **Router that can handle up to 250,000 prefixes and eBGP Multi-Hop**

How to signup for BOGON's service

- For the BGP feed goto the following link and complete the form

  https://www.team-cymru.com/bogon-networks

- You will need your complete name, company name, email address
- You will also need your public ASN and the IP address you wish to peer with.
- Once you submit this information, our staff will review and validate the information. If everything is in order you will get an email with the BGP peering details.

How to implement BOGON's in your network

- Implementing BOGON's in your network is pretty straight forward.
- For HTTPS / DNS methods you will need to integrate these queries into your existing tools. The specifics are ICB
- For BGP integration, you will create a BGP neighbor session on your router and setup a route-map or prefix filter that tags the incoming route announcements so those routes goto /dev/nul
- We have lots of examples available on our web site.

QUESTIONS ?

NIMBUS™
Network Threat Intelligence

NIMBUS™ Module Overview

- What is NIMBUS?
- What problem(s) are we helping to solve ?
- Requirements to signup for the NIMBUS Service.
- How to signup for the NIMBUS Service.
- How to implement NIMBUS Service on your network.
- Questions ?

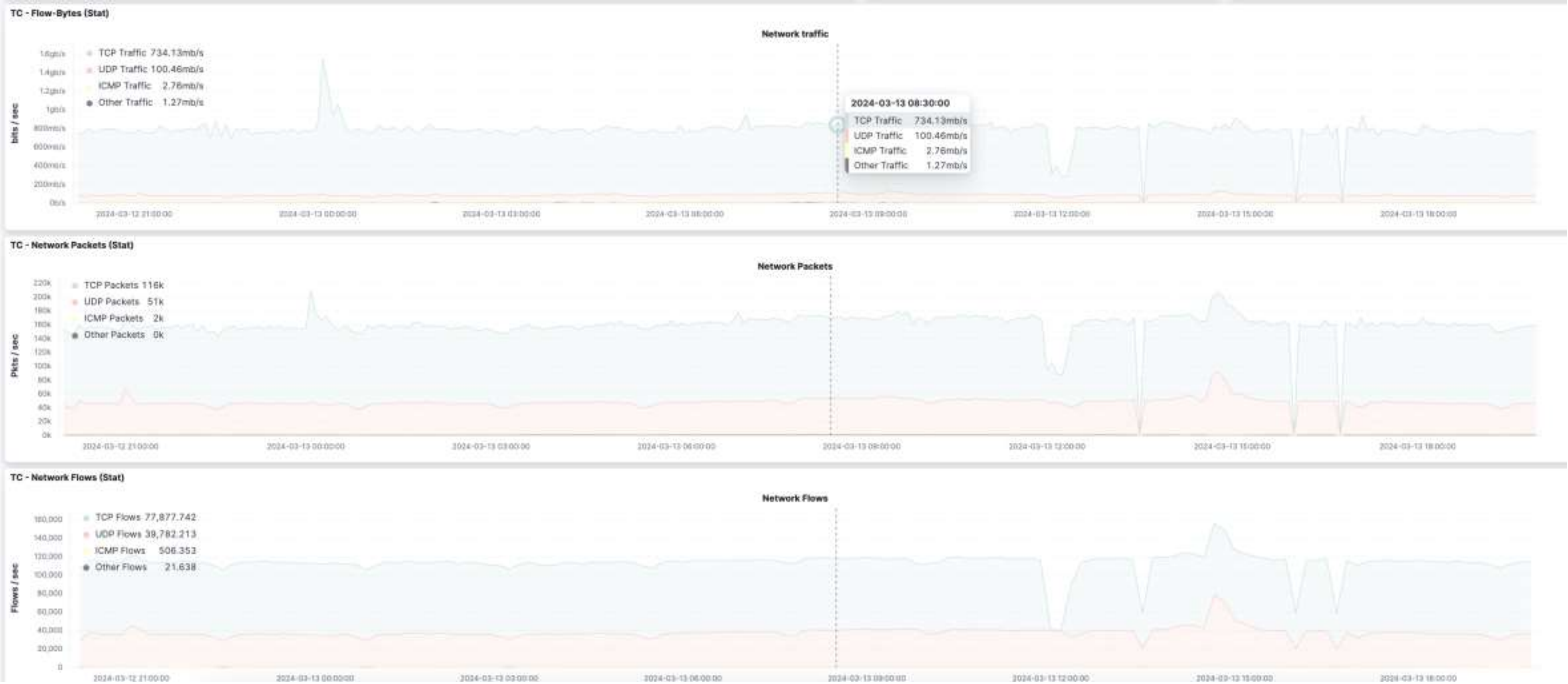
What is NIMBUS™

- NIMBUS is Team Cymru's ISP and Hosting Company focused Threat Intelligence system.
- We take our unique and one of a kind IP reputation data and automatically correlate it with your network flows.
- This then enables us to tell you about malicious traffic on your network.

https://www.team-cymru.com/nimbus-threat-monitor

What is NIMBUS

- Clients access the real-time threat information via a Kabana web interface.
- Using Kabana allows you, the user to customize your dashboards, enabling you to see the information most important to you.


TC - Flow-Bytes (Stat)
Network traffic
bits / sec
1.6gb/s
1.4gb/s
1.2gb/s
1gb/s
800mb/s
600mb/s
400mb/s
200mb/s
0b/s
TCP Traffic 734.13mb/s
UDP Traffic 100.46mb/s
ICMP Traffic 2.76mb/s
Other Traffic 1.27mb/s
2024-03-13 08:30:00
TCP Traffic 734.13mb/s
UDP Traffic 100.46mb/s
ICMP Traffic 2.76mb/s
Other Traffic 1.27mb/s
2024-03-12 21:00:00
2024-03-13 00:00:00
2024-03-13 03:00:00
2024-03-13 06:00:00
2024-03-13 09:00:00
2024-03-13 12:00:00
2024-03-13 15:00:00
2024-03-13 18:00:00
TC - Network Packets (Stat)
Network Packets
Pkts / sec
220k
200k
180k
160k
140k
120k
100k
80k
60k
40k
20k
0k
TCP Packets 116k
UDP Packets 51k
ICMP Packets 2k
Other Packets 0k
2024-03-12 21:00:00
2024-03-13 00:00:00
2024-03-13 03:00:00
2024-03-13 06:00:00
2024-03-13 09:00:00
2024-03-13 12:00:00
2024-03-13 15:00:00
2024-03-13 18:00:00
TC - Network Flows (Stat)
Network Flows
Flows / sec
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
TCP Flows 77,877.742
UDP Flows 39,782.213
ICMP Flows 506.353
Other Flows 21.638
2024-03-12 21:00:00
2024-03-13 00:00:00
2024-03-13 03:00:00
2024-03-13 06:00:00
2024-03-13 09:00:00
2024-03-13 12:00:00
2024-03-13 15:00:00
2024-03-13 18:00:00

What problem(s) are we helping to solve?

- Team Cymru NIMBUS helps solve the following kinds of problems
  - Quickly identify compromised hosts on your network
  - Who is consuming valuable bandwidth for malicious purposes ?
  - Prioritize remediation based on our near real-time information
  - Protect your customers
  - Reduce operational costs and improve your brand.
- All of this and more at no-cost to our partners.
- When you join NIMBUS you join a unique community that is focused on helping save and protect human lives!
- Become an Internet Hero!!

Requirements to signup for NIMBUS

- You must be a network operator
- You must have a publicly assigned ASN by your RIR
- You must be running BGP on your network
- You must be able to export netflow records

How to signup for NIMBUS

- Signing up for NIMBUS is straight forward:
  - Goto the web site https://www.team-cymru.com/nimbus-signup
  - Complete the form with the following information:
    - First and Last Name
    - Company Name
    - Your company email address (generally we do not accept free email addresses)
    - Mobile Phone number (for our realtime WhatsApp notifications / support)
    - Job Title
    - Public ASN as allocated by your RIR
    - You need to agree to our Terms and Conditions

- Once the form is submitted our team will validate the information and quickly get back to you via email

How to implement NIMBUS in your network

- Once you are approved for NIMBUS implementation is easy.
- You will configure your network edge / border router to export network flow information to our cloud-based collector.
- Once we see flow records arriving, we will then provide you with the control panel login credentials.
- It is important that we see flows within 5 calendar days after approval or the session may be deleted, and you would have to start over.
- We will then schedule a training session via Zoom

QUESTIONS ?

Dragon News Bytes

Curated Cyber Security News and Information

DNB Module Overview

- What Dragon News Bytes?
- What problem(s) are we helping to solve ?
- Requirements to signup for the DNB Service.
- How to signup for the DNB Service.
- How to implement DNB Service on your network.
- Questions ?

What is Dragon News Bytes

Dragon News Bytes is a private and restricted mailing list that distributes Information Security news articles. These articles may come from newspapers, magazines, and other online resources, as well as from Team Cymru's own research.

https://www.team-cymru.com/dnb

What problem are we helping to solve?

- Sorting thru the high volume of news and information articles
- Get you actionable, current, relevant news and related information quickly.
- Our team sifts thru hundreds of research papers, articles, press releases, breach notices, data dumps, etc. each day looking for and sorting this information into condensed posts.
- Think of it like a President's Daily Brief, it's a summary with links to the details.
- We give you the BLUF (Bottom Line Up Front)

Requirements to signup for DNB

- In order to signup for DNB you need to complete an application.
- Generally, you must signup from a corporate email address.
- Your application will be vetted by our team.
- Once approved you will begin to receive email from DNB.

How to signup for Dragon News Bytes

- **Signing up is very straight forward and takes just a couple of minutes.**
- **Goto https://www.team-cymru.com/dnb**
- **Scroll down to the bottom and click on “SUBSCRIBE NOW”**
- **Complete the application form**
- **Our team will complete the needed internal steps and get back intouch shortly.**

How to implement DNB in your org?

- Recommend that you create an email filter and put DNB emails into a specific folder. Helps sort them from the noise.
- You might wish to filter based on our Subject headers, so that you can catch topic areas that are important to you
- Recommend that each morning you have a cup of java / tea and spend 10 minutes looking thru the latest emails and seeing if any of them are relevant to your operations.
- Forward email and info internally to those that can better act on relevant issues.

QUESTIONS ??

IP to ASN Services

Various data mapping services

IP to ASN Mapping Module Overview

- What is IP to ASN Mapping?
- What problem(s) are we helping to solve ?
- Requirements to signup for the IP to ASN Mapping Service.
- How to signup for the IP to ASN Mapping Service.
- How to implement IP to ASN Mapping Service on your network.
- Questions ?

What is IP to ASN Mapping Service?

- The service enables a way to map network identifiers:
  - https://www.team-cymru.com/ip-asn-mapping
    - BGP Origin ASN
    - BGP Peer ASN
    - BGP Prefix
    - Prefix Country Code (assigned)
    - Prefix Registry (assigned)
    - Prefix Allocation date
    - ASN Country Code (assigned)
    - ASN Registry (assigned)
    - ASN Allocation date
    - ASN Description

What problems are we helping to solve?

- We are enabling quick mapping of network identifiers to useful information.
- We do the heavy lifting of getting data from all of the RIR's, more than 50+ BGP peers and other sources.
- We compile this into an easy, automated way of querying info.
- We refresh the information every 4 hours.
- Easy way to map a large number IP's to ASN's for example.
  - This enables seeing if a specific ASN is the source of problems

Requirements to sign up for service

- Generally anyone can use the service as long as:
  - You understand this is NOT a GEOLocation service.
  - You do not abuse the service with high query rates
    - If you have a specific need or concern please reach out to us and we will work with you.

How to signup for service

- There is no specific procedure to sign up for the service.
- You can read more about the interfaces here

https://www.team-cymru.com/ip-asn-mapping

How to implement the service in your org

- Implementation into your network is via several different methods.
  - HTTPS Queries (secure and encrypted, single queries)
  - WHOIS Queries (great for low to moderate volume)
  - DNS Queries (great for higher volume queries)

How to implement the service in your org

- **Using the HTTPS Query Method**
  - **https://asn.cymru.com/**
  - **The webpage is a proxy interface to the whois method**

How to implement the service in your org

- **Using the Whois query method**
  - **You can manually create a command line such as:**

```
whois -h whois.cymru.com " -v 216.90.108.31 ”
```

  - **Which will return the following:**

```
AS   | IP            | BGP Prefix      | CC | Registry | Allocated  | AS Name
23028| 216.90.108.31| 216.90.108.0/24 | US | arin     | 1998-09-25 | TEAM-CYMRU, US
```

How to implement the service in your org

- Using the whois query method:
  - You can also create an ascii text file that contains the data you wish to look up.
  - You then use GNU-NetCat to feed that to the whois server and in return you get a stream of responses.

How to implement the service in your org

- **Using the whois / netcat query method**
  - **Text file with the following data**

```
begin
68.22.187.5
207.229.165.18
198.6.1.65
End
-----------------------------------
```

```
netcat whois.cymru.com 43 < test.txt
Bulk mode; whois.cymru.com [2022-09-06 19:04:04 +0000]
23028   | 68.22.187.5       | TEAM-CYMRU, US
6079    | 207.229.165.18    | RCN-AS, US
701     | 198.6.1.65        | UUNET, US
```

How to implement the service in your org

- **Using the DNS query methods:**
  - **You can query a number of different DNS zones for different data**

origin.asn.cymru.com.	**Map IPv4 / Prefix to an origin ASN**
origin6.asn.cymru.com	**Map IPv6 prefix to an origin ASN**
peer.asn.cymru.com	**Map IPv4 prefix to possible peer ASN**
asn.cymru.com	**Provide details on a specific ASN**

```
dig as17263.asn.cymru.com txt +short

"17263 | US | arin | 2000-08-14 | TN-ASN-NM, US"
```

QUESTIONS ?

MHR – Malware Hash Registry

MHR Module Overview

- **What is MHR Service?**
- **What problem(s) are we helping to solve ?**
- **Requirements to signup for the MHR Service.**
- **How to signup for the MHR Service.**
- **How to implement MHR Service on your network.**
- **Questions ?**

What is the MHR Service?

- MHR or Malware Hash Registry, is comprehensive dataset of malware from around the globe.
- The dataset is based on 30+ antivirus databases from around the globe.
- The dataset also contains 8+ years of Team Cymru's malware intelligence research. This is a force multiplier.
- Easy to integrate into existing work-flows
- More info https://www.team-cymru.com/mhr

What problem are we helping to solve?

- Reducing workload when researching malware hashes
- Single query to MHR vs many queries to different systems
- Near real-time results
- Easy integration into existing systems and work-flows.
- Improve email attachment security
- Improve file storage security.

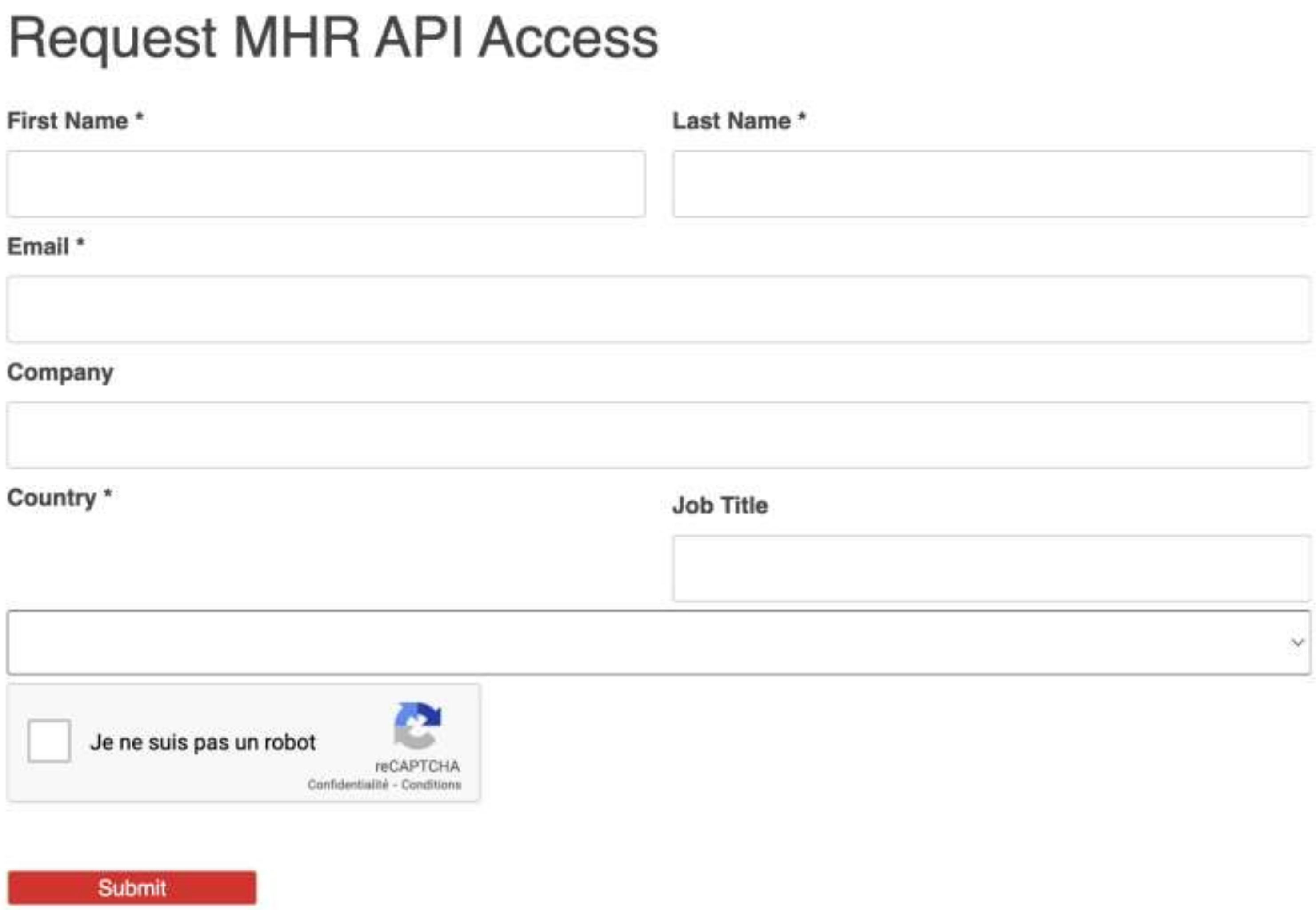
Requirements to signup for MHR

- **Must be at least one of the following types of users:**
  - **Network Security**
  - **Researcher / Analysts**
  - **Incident Response**

- **To use the REST-API interface you will need to complete and application and be approved.**
- **All low volume access is available via public facing interfaces**

How to signup for the MHR Service

- You can sign up for the REST-API access via the web
- Goto https://hash.cymru.com/signup
- Complete the form and submit it.
- Our team will review and validate the information and respond



Request MHR API Access

First Name *

Last Name *

Email *

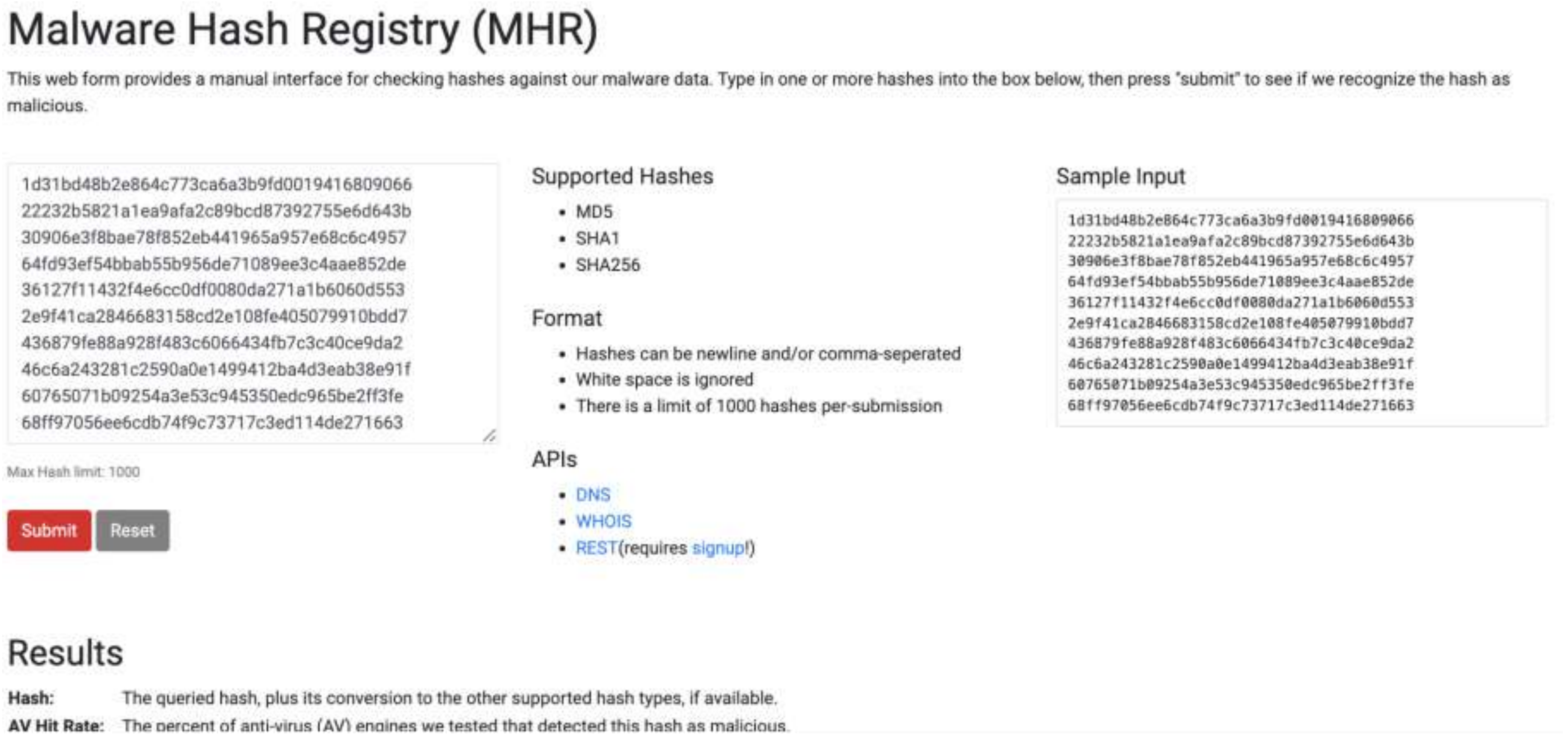
Company

Country *

Job Title

How to implement MHR in your org.

- You can use the MHR service via a number of different interfaces:
    - Web Interface – This is a very low volume method. You paste your hash into our web interface and we then check our databases and report back to you on the web. https://hash.cymru.com/



Malware Hash Registry (MHR)

This web form provides a manual interface for checking hashes against our malware data. Type in one or more hashes into the box below, then press "submit" to see if we recognize the hash as malicious.

```
1d31bd48b2e864c773ca6a3b9fd0019416809066
22232b5821a1ea9afa2c89bcd87392755e6d643b
30906e3f8bae78f852eb441965a957e68c6c4957
64fd93ef54bbab55b956de71089ee3c4aae852de
36127f11432f4e6cc0df0080da271a1b6060d553
2e9f41ca2846683158cd2e108fe405079910bdd7
436879fe88a928f483c6066434fb7c3c40ce9da2
46c6a243281c2590a0e1499412ba4d3eab38e91f
60765071b09254a3e53c945350edc965be2ff3fe
68ff97056ee6cdb74f9c73717c3ed114de271663
```

Max Hash limit: 1000

Supported Hashes

- MD5
- SHA1
- SHA256

Format

- Hashes can be newline and/or comma-seperated
- White space is ignored
- There is a limit of 1000 hashes per-submission

APIs

- DNS
- WHOIS
- REST(requires signup!)

Sample Input

```
1d31bd48b2e864c773ca6a3b9fd0019416809066
22232b5821a1ea9afa2c89bcd87392755e6d643b
30906e3f8bae78f852eb441965a957e68c6c4957
64fd93ef54bbab55b956de71089ee3c4aae852de
36127f11432f4e6cc0df0080da271a1b6060d553
2e9f41ca2846683158cd2e108fe405079910bdd7
436879fe88a928f483c6066434fb7c3c40ce9da2
46c6a243281c2590a0e1499412ba4d3eab38e91f
60765071b09254a3e53c945350edc965be2ff3fe
68ff97056ee6cdb74f9c73717c3ed114de271663
```

Results

Hash: The queried hash, plus its conversion to the other supported hash types, if available.

AV Hit Rate: The percent of anti-virus (AV) engines we tested that detected this hash as malicious.

How to implement MHR in your org.

- We support queries via DNS
  - https://hash.cymru.com/docs_dns
  - You can formulate a query by using either an A or TXT RR_Type
    - For example:

```
dig +short 8a62d103168974fba9c61edab336038c.hash.cymru.com TXT
dig +short 8a62d103168974fba9c61edab336038c.hash.cymru.com A
```

    - The first will return a string Time in EPOCH and a Hit percentage in AV's
    - The second will return a traditional 127.0.0.x depending on if it is found or not
    - When doing an A search if you get NXDOMAIN then the hash was NOT FOUND
    - When doing a SHA256, you have to break the hash up into two records

```
dig +short \
9b573bc2555d8d35e4a2e927cc14217e.b112f0725cb4ebff4878976a229fde45.hash.cymru.com A
```

How to implement MHR in your org.

- We support queries via WHOIS protocol
  - https://hash.cymru.com/docs_whois

  - For low volume queries you can use a command line whois
    - whois -h hash.cymru.com 84af04b8e69682782607a0c5796ca56999eda6b3

  - For higher volume we recommend using GNU NetCat
    - With netcat you can create a file that has upto 1000 hashes and submit that via netcat.
    - You will get a response back for each hash
    - It is important to use the older gnu netcat 0.7.x code

How to implement MHR in your org.

- We support a REST API interface as well.
  - This interface is great way to integrate into your existing work flows
  - Requires specific signup approval
  - Permits higher volume / automated queries
  - Please let us know what your anticipated query rates so we can plan the infra-structure accordingly.

QUESTIONS ??

CAP – CSIRT Assistance Program

CAP Module Overview

- What is the CAP (CSIRT Assistance Program) Service?
- What problem(s) are we helping to solve ?
- Requirements to signup for the CAP Service.
- How to signup for the CAP Service.
- How to implement CAP Service on your network.
- Questions ?

What is the CAP Service?

- CAP = CSIRT Assistance Program
  - CSIRT = Computer Security Incident Response Team

- A dedicated support program for non-commercial regional and national CSIRT organizations
- Free Threat Intel for your region / area of influence
- More information:

  https://www.team-cymru.com/csirt-ap

What problem are we helping to solve?

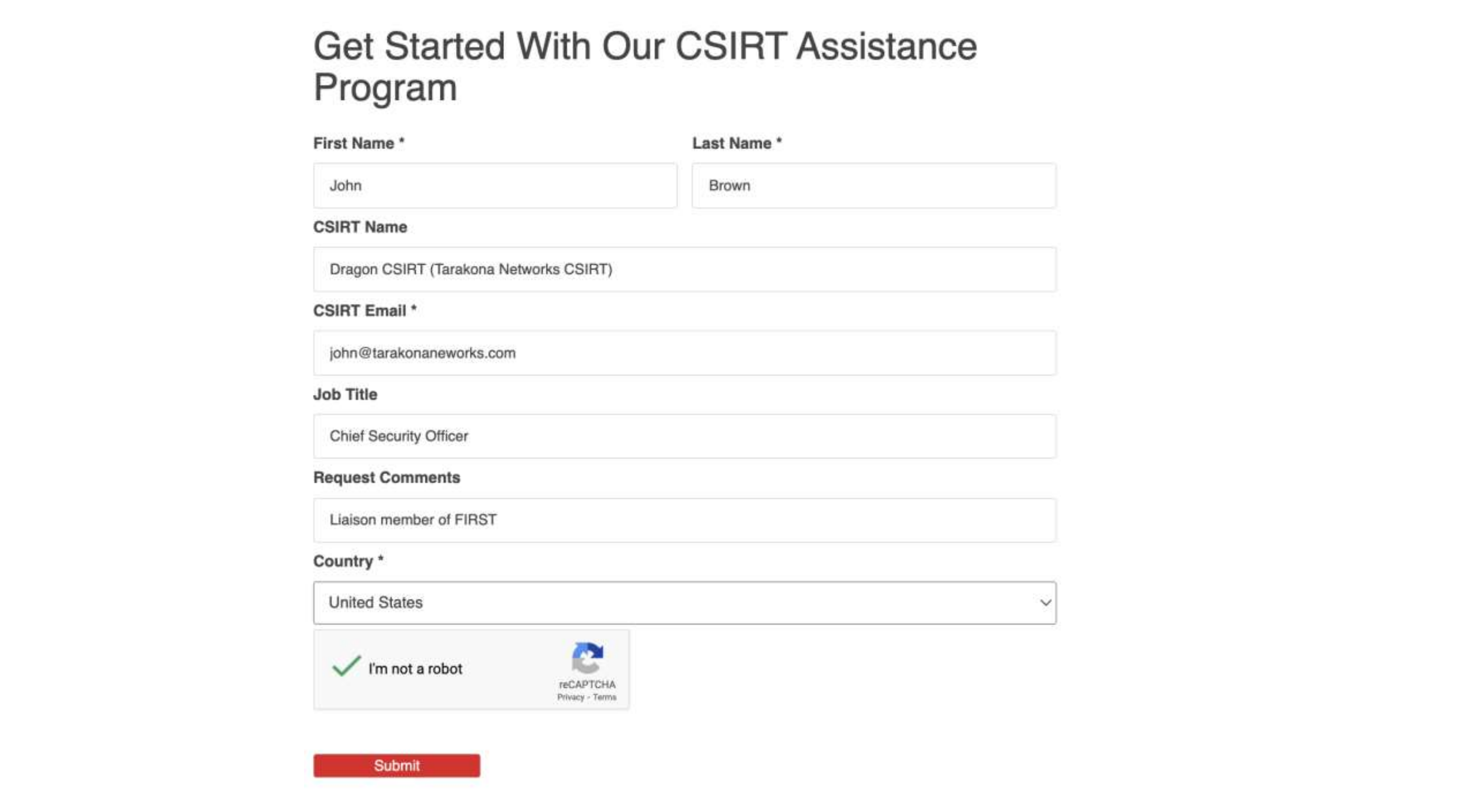
- **Better visibility into global threat data that impacts your local region.**
- **Leveraging the Team Cymru world-class global threat visibility by sharing detailed information about threats to your community and region.**
- **CSIRT's don't always have the visibility to see what is happening elsewhere on the globe and how it impacts their local region.**

Requirements to signup for CAP

- Must be a recognized non-commercial CSIRT
- Must be a regional or national level entity
- Must be vetted by our internal team
- Must sign a short MOU (Memorandum of Understanding)
- Strongly recommend that you have reviewed and follow RFC2350. https://www.rfc-editor.org/rfc/rfc2350

How to signup for CAP

- **Signing up for CAP is a straightforward and easy process**
- **Goto https://www.team-cymru.com/csirt-ap**
- **Complete the form on the web page.**
- **Be prepared to answer some additional questions from our team as we process your request. Please make sure emails don’t land in your spam folder!**



Get Started With Our CSIRT Assistance Program

First Name *

John

Last Name *

Brown

CSIRT Name

Dragon CSIRT (Tarakona Networks CSIRT)

CSIRT Email *

john@tarakonaneworks.com

Job Title

Chief Security Officer

Request Comments

Liaison member of FIRST

Country *

United States

✓ I'm not a robot

How to implement CAP services

- Once you are approved, we recommend that you attend and receive training on our tools.
- Develop a process and workflow that integrates the threat data we supply into your existing workflows
- Take needed steps to help notify / protect those that are being impacted based on the threat intel provided via the program.
- Share data back with Team Cymru so we can leverage it to help other CSIRT’s around the globe.

QUESTIONS ?

- Tarek Sendi, Security Evangelist, Team Cymru
- Mobile: +216 99 263 218
- US office: +1 847 378 3338
- Skype: sendi_tarek
- Email: tsendi@cymru.com / outreach@cymru.com
- @teamcymru
- www.team-cymru.com