OSINT - Open-Source Intelligence

OSINT means collecting and gathering information from publicly available sources, like google, Social medias like, Facebook, WhatsApp, telegram, Instagram etc….

Who Uses OSINT?

- **National Security & Law Enforcement:** For global awareness, threat assessment, and investigations.
- **Cybersecurity:** To identify vulnerabilities, track malicious actors, and understand emerging threats.
- **Businesses:** For due diligence, market research, competitive analysis, and risk management.
- **Journalists & Researchers:** To uncover stories, verify facts, and document events.

Examples of OSINT in Action:

- **Cybersecurity:** Finding an organization's unpatched software or leaked credentials by searching public forums and code repositories.
- **Threat Intelligence:** Monitoring ransomware leak sites and hacker forums to understand new tactics.
- **Background Checks:** Gathering public social media and professional information about individuals.

Tools used in OSINT

There are multiple tools available for OSINT, which helps investigators to gather information across the digital and physical society.

1. Maltego

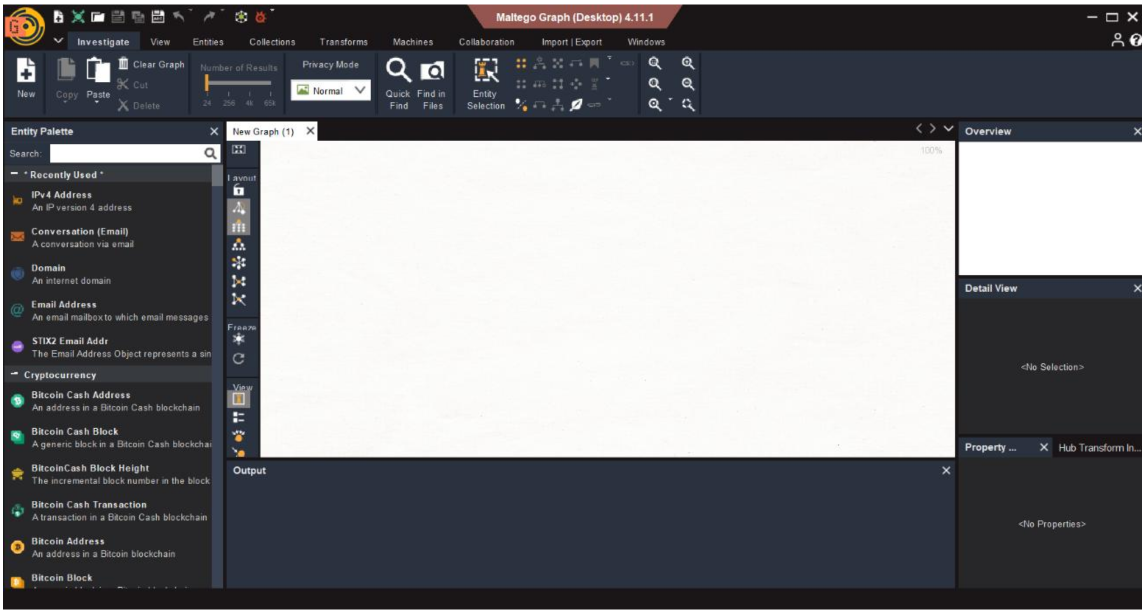
This is a tool for data mining and relationship mapping. It's a Graphical link analysis tool. This transforms data into interactive graphs for investigations.

In this hands-on tutorial, I'll demonstrate how to use **Maltego** – a powerful OSINT (Open Source Intelligence) tool – to map a target's digital footprint using **TryHackMe.com** as our case study.

Step by step Guide to Map TryHackMe's Infrastructure

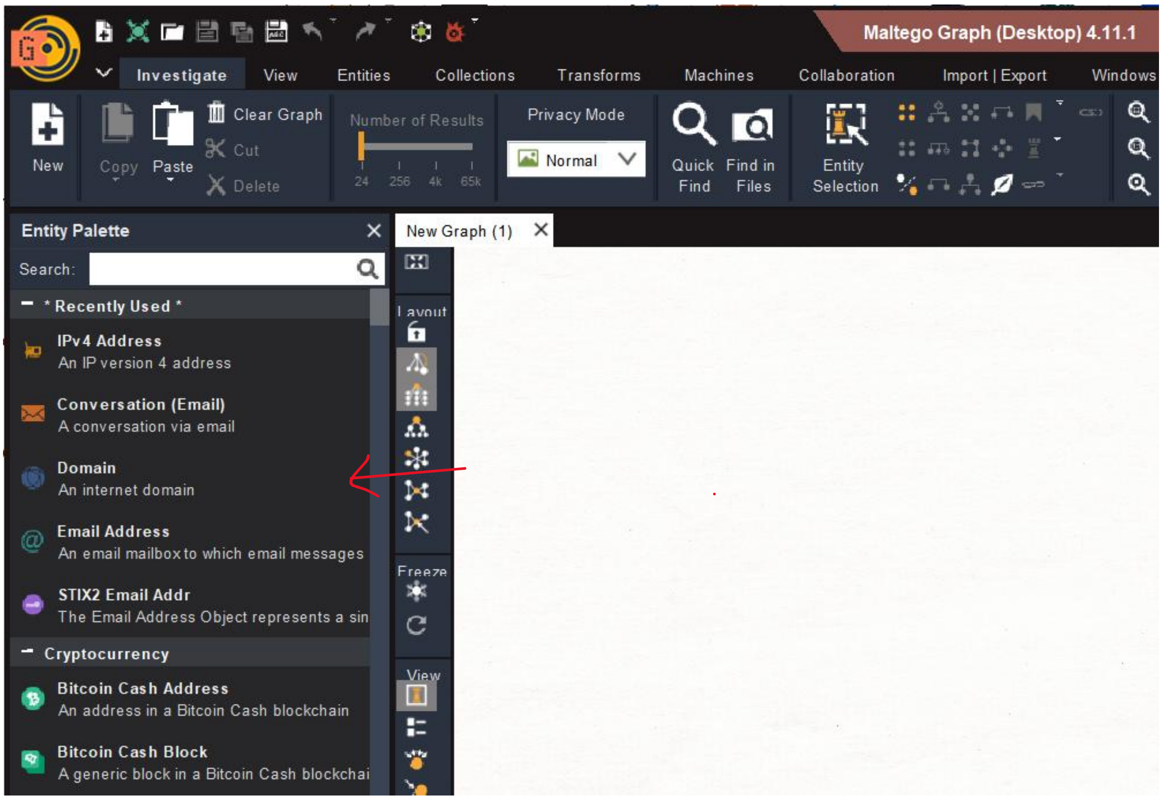
Step 1: Installation & Setup

- Download the Community Edition of Maltego by visiting it's official website **Maltego.com**
- Create an Account during the installation for free
- Open Maltego and create a new graph for our investigation

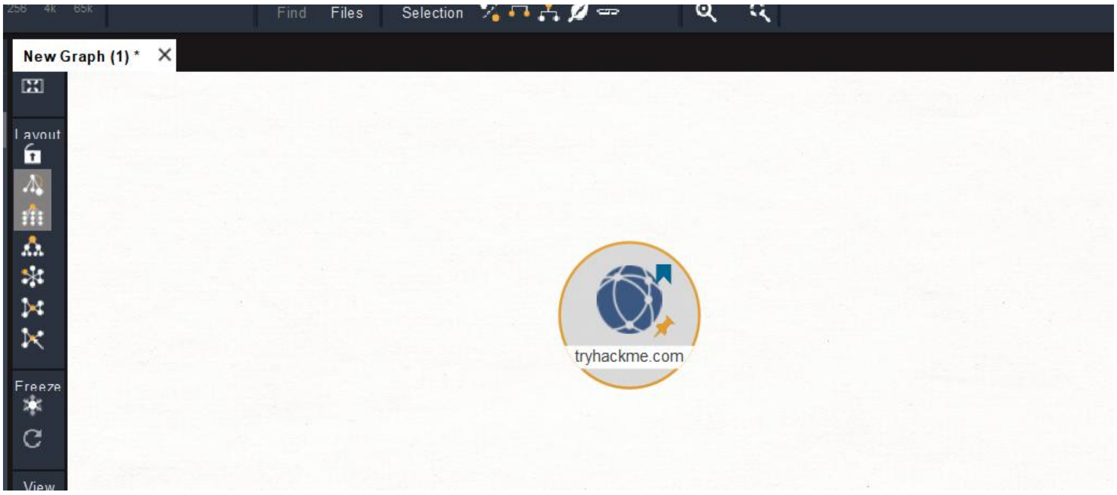


Step 2: Initial Domain Analysis

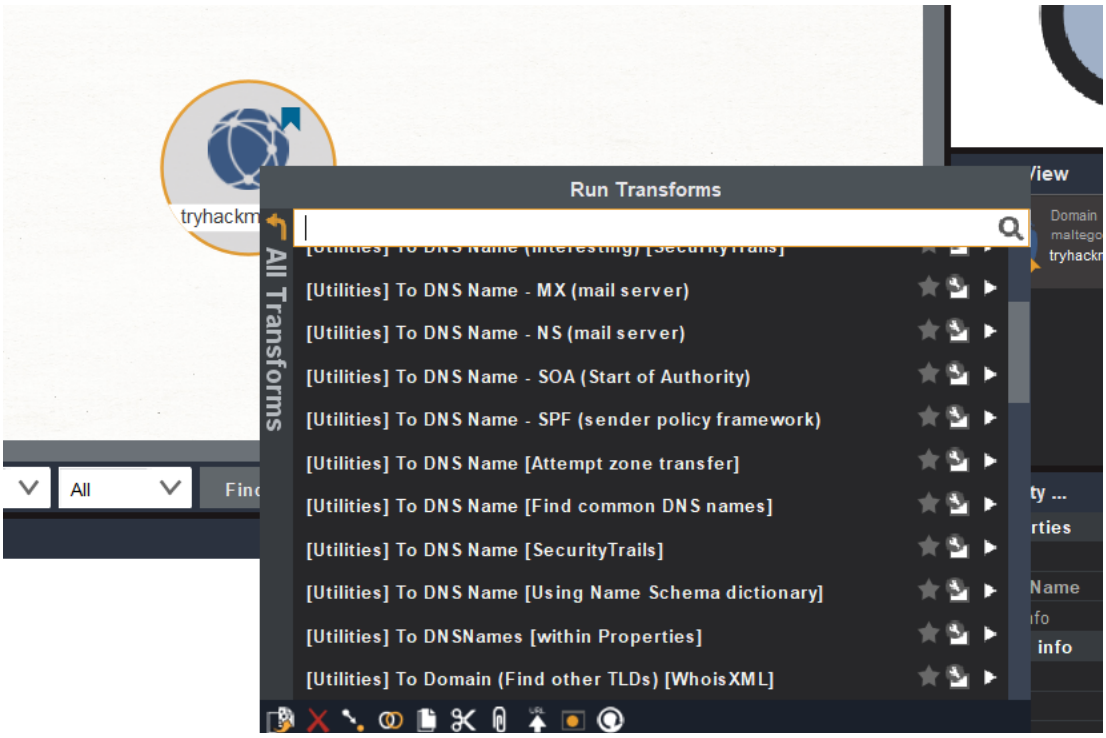
- Drag a “Domain” entity onto the Canvas



- Double-Click and enter tryhackme.com



- Right Click → Run Transform → Select **"To DNS Name"**


tryhackm
Run Transforms
All Transforms
[Utilities] To DNS Name (Interesting) [SecurityTrails]
[Utilities] To DNS Name - MX (mail server)
[Utilities] To DNS Name - NS (mail server)
[Utilities] To DNS Name - SOA (Start of Authority)
[Utilities] To DNS Name - SPF (sender policy framework)
[Utilities] To DNS Name [Attempt zone transfer]
[Utilities] To DNS Name [Find common DNS names]
[Utilities] To DNS Name [SecurityTrails]
[Utilities] To DNS Name [Using Name Schema dictionary]
[Utilities] To DNSNames [within Properties]
[Utilities] To Domain (Find other TLDs) [WhoisXML]
All
Fin
View
Domain
maltego
tryhackn
ty ...
rties
Name
nfo
info

Step 3: Explore DNS and Infrastructure

After running the **"To DNS Name"** transform, Maltego will resolve the domain to associated DNS records. In our investigation of tryhackme.com, we discovered multiple subdomains and related infrastructure. Some of the notable DNS names found include:

- **blog.tryhackme.com**
- **help.tryhackme.com**
- **remote.tryhackme.com**
- **tryhackme.com.cdn.cloudflare.net**
- **worker-test.tryhackme.com**

This reveals TryHackMe's use of Cloudflare for CDN and DDoS protection, as well as separate subdomains for blogs, help centres, and remote access services.

Step 4: Identify IP Addresses and Geolocation

By transforming DNS names to IP addresses, we uncovered the following IPv4 addresses linked to TryHackMe's

- 104.20.29.66
- 172.66.164.239

These IPs correspond to Cloudflare proxy servers, confirming the use of reverse proxy services to protect origin servers.

Step 5: Extract Email Addresses and Contact Information

Maltego can also uncover email addresses associated with the domain. For TryHackMe, we identified several organizational emails:

- sales@tryhackme.com
- support@tryhackme.com
- hello@tryhackme.com
- qa@tryhackme.com
- stuxnet@tryhackme.com

These emails appear in help articles, legal pages, and community discussions, indicating points of contact for sales, support, quality assurance, and possibly internal development.

Step 6: Map Related URLs and Help Resources

The tool also extracted numerous URLs from the help centre and legal documentation, such as:

- https://help.tryhackme.com/en/articles/6498338-user-tokens
- https://tryhackme.com/pricing
- https://help.tryhackme.com/en/articles/8469856-legal-compliance-requirements

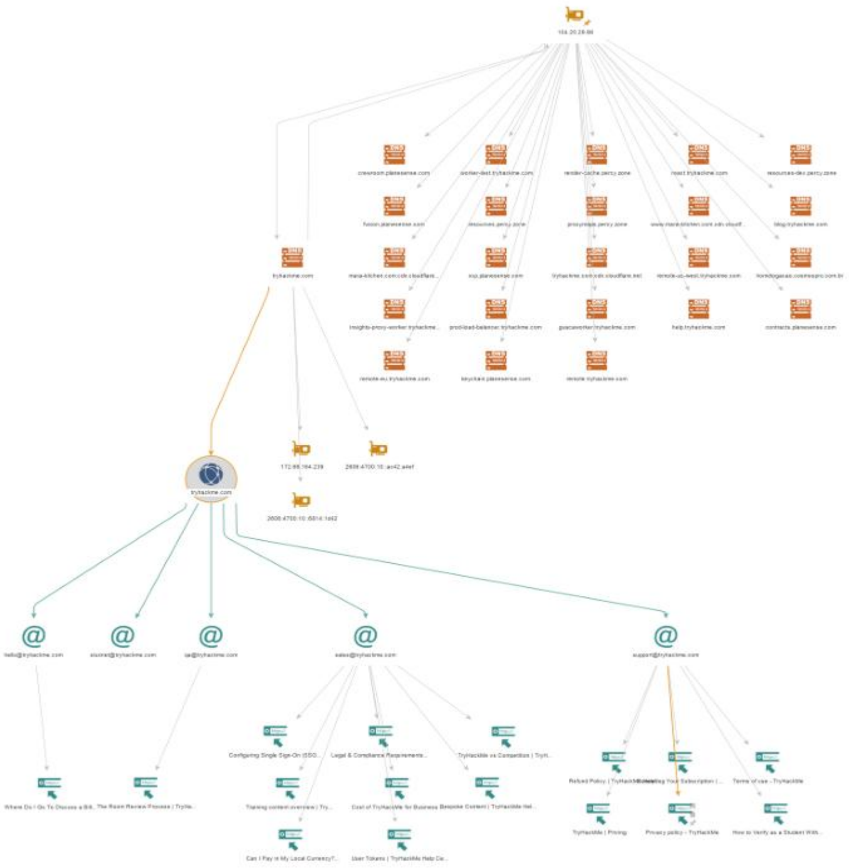
These resources reveal how TryHackMe structures its support and legal documentation, and where users are directed for billing, compliance, and token management.

Step 7: Visualize Relationships with Entity Graphs

Maltego allows us to visualize the connections between entities. Below is a summary of the top linked entities from our scan:

Rank	Entity Type	Value	Total Links
1	IPv4 Address	104.20.29.66	25
2	Email Address	sales@tryhackme.com	9
3	Email Address	support@tryhackme.com	7
4	Domain	tryhackme.com	6
5	DNS Name	tryhackme.com	6

Maltego Mapping Graphically



104.20.29.66
crewroom.planesense.com
worker-test.tryhackme.com
render-cache.percy.zone
react.tryhackme.com
resources-dev.percy.zone
fusion.planesense.com
resources.percy.zone
proxyimage.percy.zone
www.maria-kitchen.com.cdn.cloudf...
blog.tryhackme.com
tryhackme.com
maria-kitchen.com.cdn.cloudflare...
sop.planesense.com
tryhackme.com.cdn.cloudflare.net
remote-us-west.tryhackme.com
insights-proxy-worker.tryhackme...
prod-load-balancer.tryhackme.com
guacaworker.tryhackme.com
help.tryhackme.com
contracts.planesense.com
remote-eu.tryhackme.com
keychain.planesense.com
remote.tryhackme.com
172.66.164.239
2606:4700:10::ac42:a4ef
tryhackme.com
2606:4700:10::6814:1d42
hello@tryhackme.com
alumni@tryhackme.com
sa@tryhackme.com
sales@tryhackme.com
support@tryhackme.com
Configuring Single Sign-On (SSO...
Legal & Compliance Requirements...
TryHackMe vs Competitors | TryH...
Where Do I Go To Discuss a Bill...
The Room Review Process | TryHa...
Training content overview | Try...
Cost of TryHackMe for Business
Bespoke Content | TryHackMe Hel...
Can I Pay in My Local Currency?...
User Tokens | TryHackMe Help Ce...
Refund Policy | TryHackMe
Cancelling Your Subscription | ...
Terms of use - TryHackMe
TryHackMe | Pricing
Privacy policy - TryHackMe
How to Verify as a Student With...

1. Top 10 Entities

Total number of entities	50
Total number of links	50

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	DNS Name	www.mara-kitchen.com.cdn.cloudflare.net	1
2	DNS Name	homologacao.cosmospro.com.br	1
3	DNS Name	tryhackme.com.cdn.cloudflare.net	1
4	DNS Name	remote-us-west.tryhackme.com	1
5	URL	User Tokens | TryHackMe Help Center	1
6	URL	TryHackMe | Pricing	1
7	URL	Where Do I Go To Discuss a Billing Issue with THM Support? : r ...	1
8	IPv4 Address	104.20.29.66	1
9	DNS Name	keychain.planesense.com	1
10	URL	Training content overview | TryHackMe Help Center	1

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	IPv4 Address	104.20.29.66	24
2	Email Address	sales@tryhackme.com	8
3	Email Address	support@tryhackme.com	6
4	Domain	tryhackme.com	5
5	DNS Name	tryhackme.com	5
6	Email Address	qa@tryhackme.com	1
7	Email Address	hello@tryhackme.com	1
8	DNS Name	www.mara-kitchen.com.cdn.cloudflare.net	0
9	DNS Name	homologacao.cosmospro.com.br	0
10	DNS Name	tryhackme.com.cdn.cloudflare.net	0

Ranked by Total Links

Rank	Type	Value	Total links
1	IPv4 Address	104.20.29.66	25
2	Email Address	sales@tryhackme.com	9
3	Email Address	support@tryhackme.com	7
4	Domain	tryhackme.com	6
5	DNS Name	tryhackme.com	6
6	Email Address	qa@tryhackme.com	2
7	Email Address	hello@tryhackme.com	2
8	DNS Name	www.mara-kitchen.com.cdn.cloudflare.net	1
9	DNS Name	homologacao.cosmospro.com.br	1
10	DNS Name	tryhackme.com.cdn.cloudflare.net	1

2. Entities by Type

DNS Names (24)

- blog.tryhackme.com
- contracts.planesense.com
- crewroom.planesense.com
- fusion.planesense.com
- guacaworker.tryhackme.com
- help.tryhackme.com
- homologacao.cosmospro.com.br
- insights-proxy-worker.tryhackme.com
- keychain.planesense.com
- mara-kitchen.com.cdn.cloudflare.net
- prod-load-balancer.tryhackme.com
- proxymaps.percy.zone
- react.tryhackme.com
- remote-eu.tryhackme.com
- remote-us-west.tryhackme.com
- remote.tryhackme.com
- render-cache.percy.zone
- resources-dev.percy.zone
- resources.percy.zone
- tryhackme.com
- tryhackme.com.cdn.cloudflare.net
- worker-test.tryhackme.com
- www.mara-kitchen.com.cdn.cloudflare.net
- xcp.planesense.com

Domains (1)

- tryhackme.com

Email Addresses (5)

- hello@tryhackme.com
- qa@tryhackme.com
- sales@tryhackme.com
- stuxnet@tryhackme.com
- support@tryhackme.com

IPv4 Addresses (2)

- 104.20.29.66
- 172.66.164.239

IPv6 Addresses (2)

- 2606:4700:10::6814:1d42
- 2606:4700:10::ac42:a4ef

URLs (16)

- Bespoke Content | TryHackMe Help Center
- Can I Pay in My Local Currency? | TryHackMe Help Center
- Cancelling Your Subscription | TryHackMe Help Center
- Configuring Single Sign-On (SSO) for your Organisation ...
- Cost of TryHackMe for Business / Education | TryHackMe Help Center
- How to Verify as a Student Without a Student Email | TryHackMe ...
- Legal & Compliance Requirements | TryHackMe Help Center
- Privacy policy - TryHackMe
- Refund Policy | TryHackMe Help Center
- Terms of use - TryHackMe
- The Room Review Process | TryHackMe Help Center
- Training content overview | TryHackMe Help Center
- TryHackMe vs Competition | TryHackMe Help Center
- TryHackMe | Pricing
- User Tokens | TryHackMe Help Center
- Where Do I Go To Discuss a Billing Issue with THM Support? : r ...

3. Entity Details

IPv4 Address
IPv4Address
104.20.29.66

Weight	50
IP Address	104.20.29.66
Internal	false

Incoming (1)

DNS Name	tryhackme.com

Outgoing (24)

DNS Name	blog.tryhackme.com
DNS Name	contracts.planesense.com
DNS Name	crewroom.planesense.com
DNS Name	fusion.planesense.com
DNS Name	guacaworker.tryhackme.com
DNS Name	help.tryhackme.com
DNS Name	homologacao.cosmospro.com.br
DNS Name	insights-proxy-worker.tryhackme.com
DNS Name	keychain.planesense.com
DNS Name	mara-kitchen.com.cdn.cloudflare.net
DNS Name	prod-load-balancer.tryhackme.com
DNS Name	proxymaps.percy.zone
DNS Name	react.tryhackme.com
DNS Name	remote-eu.tryhackme.com
DNS Name	remote-us-west.tryhackme.com
DNS Name	remote.tryhackme.com
DNS Name	render-cache.percy.zone
DNS Name	resources-dev.percy.zone
DNS Name	resources.percy.zone
DNS Name	tryhackme.com
DNS Name	tryhackme.com.cdn.cloudflare.net
DNS Name	worker-test.tryhackme.com
DNS Name	www.mara-kitchen.com.cdn.cloudflare.net
DNS Name	xcp.planesense.com

Email Address
EmailAddress
sales@tryhackme.com

Search Engine Results

TryHackMe vs Competition | TryHackMe Help Center

[https://help.tryhackme.com/en/articles/8469838-tryhackme-vs-competition]

Please **contact** your Customer Success Manager or Technical Support. Please **contact** sales@**tryhackme.com** if you'd like to explore whether TryHackMe could be a good ...

User Tokens | TryHackMe Help Center

[https://help.tryhackme.com/en/articles/6498338-user-tokens]

Please **contact** your Customer Success Manager or Technical Support. Please **contact** sales@**tryhackme.com** if you'd like to explore whether TryHackMe could be a ...

Can I Pay in My Local Currency? | TryHackMe Help Center

[https://help.tryhackme.com/en/articles/8484112-can-i-pay-in-my-local-currency]

Existing B2B or EDU customer and have questions? Please **contact** your Customer Success Manager or Technical Support. Please **contact** sales@**tryhackme.com** if you'd ...

Training content overview | TryHackMe Help Center

[https://help.tryhackme.com/en/articles/8484133-training-content-overview]

Existing B2B or EDU customer and have questions? Please **contact** your Customer Success Manager or Technical Support. Please **contact** sales@**tryhackme.com** if you'd ...

Search Engine Results

Cost of TryHackMe for Business / Education | TryHackMe Help Center

[https://help.tryhackme.com/en/articles/8484063-cost-of-tryhackme-for-business-education]

Business License. Please **contact** TryHackMe's Sales team (sales@**tryhackme.com**) for up-to-date pricing, demos, or a free trial. · EDU Licenses. An EDU license ...